中国公共安全杂志社

2005 06 07

中国公共安全 综合版

Mpls Vpn技术在城市视频监控中的应用

文/李骁勇 高学礼 祝玉敏 申永军 郑玉萍

一、城市视频监控的发展

最早的视频监控系统是模拟视频监控系统，其特点是从摄像机到控制主机再到录像机、监视器，全部以模拟视频信号进行传输与存储。而控制信号是以数字信号进行的。稍候的视频监控系统是以多媒体计算机系统或以DVR为控制核心的数字视频监控系统，系统从摄像机到控制主机、控制主机到监视器是以模拟视频信号进行传输；控制信号是以数字信号进行传输;视频信号在控制主机里的处理、控制及存储则是以数字信号进行的，可以看作为“半数字监控”方式。目前的视频监控系统是现场摄像机的模拟视频信号及控制信号在现场即被转换为数字信号通过网络进行传输;监控主机及监视端也是以数字信号接收、控制、存储、显示的。应该讲是“全数字且网络化”方式。
监控的控制和视频图像的存储也由最初的集中控制集中存储因系统的控制范围扩大和视频数量的增多变为分散控制分散存储。网络化和数字化的不断应用和控制功能的进一步划分使控制存储又向分布控制分布存储发展。
城市的视频监控也由最初的各小区、各单位和道路交通的零星分散监控，向分区集中和整个城市监控的方向发展。在城市这样大的范围内，视频信号和控制信号的传输就成了主要的问题。目前的解决方案有：1、自建光纤；2、租用专线；3、组建无线网络（微波通信）；4、利用宽带公网（城域网）。对于经济欠发达的西部省市自建光纤和租用专线的成本过高，而微波无线网络又受高楼大厦和接入数量的影响，因此利用现在Internet无所不在的覆盖范围和城域网的宽带接入是解决这一问题的经济、有效的方法。但Internet或公网的安全性一直影响着这种应用的进一步发展，而构建在公网上的VPN很好的解决了这一障碍。

二、VPN简介

VPN（Virtual Private Network，虚拟专用网）是指一些节点通过一个公用网络，如公共分组交换网、帧中继网、ISDN或Internet等建立的一个临时的、安全的连接，形成逻辑上的专用网络，从而达到在共享或者公共网络（一般是指Internet）上安全地传输私有数据的目的。
VPN提供如下功能
信息机密性，确保通过公网传输的信息以加密的方式传送，即使被他人截获也不会泄露信息完整性，保证信息的完整性。
用户身份认证，能对用户身份进行认证，确定该用户的访问权限。
访问控制机制，用户只能读/写被授予了访问权限的信息。
针对用户的带宽控制机制。
VPN采用的不同的技术

1、基于隧道技术的VPN

隧道技术的基本过程是在源局域网与公网的接口处将数据作为负载封装在一种可以在公网上传输的数据格式中，在目的局域网与公网的接口处将数据解封装，取出负载。被封装的数据包在互联网上传递时所

经过的逻辑路径被称为“隧道”。目前VPN隧道协议有：点到点隧道协议PPTP、第二层隧道协议L2TP、网络层隧道协议IPSec等。

2、SSL VPN

SSL VPN（Security Socket Layer 安全套接层协议）一般的实现方式是在企业网的边缘，即防火墙后面，介于企业服务器与远程用户之间，放置一个SSL VPN网关，通过该网关来控制远程用户和企业服务器二者的通信。当用户在浏览器上输入一个URL（HTTP形式）后，连接将被SSL VPN网关取得，并验证该用户的身份，然后SSL VPN网关将提供一个远程用户与各种不同的应用服务器之间的连接。

3、MPLS VPN

MPLS是由Cisco标记交换演变而来的IETF的标准协议。标记表示路径和服务的属性，在入口的边缘、流入的数据包被处理做上标记，位于核心的设备仅仅读这些标记，赋于适当的服务，然后根据标记转发这些数据包，对这些数据包的分析、分类和过滤只发生一次，在进入边缘设备时，经过出口的边缘设备时，标记被移去，数据包转发到最终目的地。

同传统的VPN不同，MPLS VPN不依靠封装和加密技术，MPLS VPN依靠转发表和数据包的标记来创建一个安全的VPN，MPLS VPN的所有技术产生于Internet Connect网络。

CPE被称为客户边缘路由器（CE）。在Internet Connect网络中，同CE相连的路由器称为供应商边缘路由器(PE)。一个VPN数据包括一组CE路由器，以及同其相连的Internet Connect网中的PE路由器。只有PE路由器理解VPN。CE路由器并不理解潜在的网络。

CE可以感觉到同一个专用网相连。每个VPN对应一个VPN路由/转发实例（VRF）。一个VRF定义了同PE路由器相连的客户站点的VPN成员资格。一个VRF数据包括IP路由表，一个派生的Cisco Express Forwarding (CEF)表，一套使用转发表的接口，一套控制路由表中信息的规则和路由协议参数。一个站点可以且仅能同一个VRF相联系。客户站点的VRF中的数据包含了其所在的VPN中，所有的可能连到该站点的路由。

对于每个VRF，数据包转发信息存储在IP路由表和CEF表中。每个VRF维护一个单独的路由表和CEF表。这些表各可以防止转发信息被传输到VPN之外，同时也能阻止VPN之外的数据包转发到VPN内不的路由器中。这个机制使得VPN具有安全性。

在每个VPN内部，可以建立任何连接：每个站点可以直接发送IP数据包到VPN中另外一个站点，无需穿越中心站点。一个路由识别器(RD)可以识别每一个单独的VPN。一个MPLS网络可以支持成千上万个VPN。每个MPLS VPN网络的内部是由供应商(P)设备组成。这些设备构成了MPLS核，且不直接同CE路由器相连。围绕在P设备周围的供应商边缘路由器(PE)可以让MPLS VPN网络发挥VPN的作用。P和PE路由器称为标记交换路由器(LSR)。LSR设备基于标记来交换数据包。

客户站点可以通过不同的方式连接到PE路由器，例如帧中继，ATM，DSL和T1方式等等。

三、VPN技术在城市视频监控中的应用

模拟摄像机的模拟视频信号要想在VPN中传输必须通过视频服务器或视频编码器转换为数字信号并压缩后才能传输，压缩的标准目前流行的是MPEG4和H.264，压缩比高且压缩后图像效果好。数字摄像机本身内部已集成这些功能所以可直接上网。

1、固定监控点

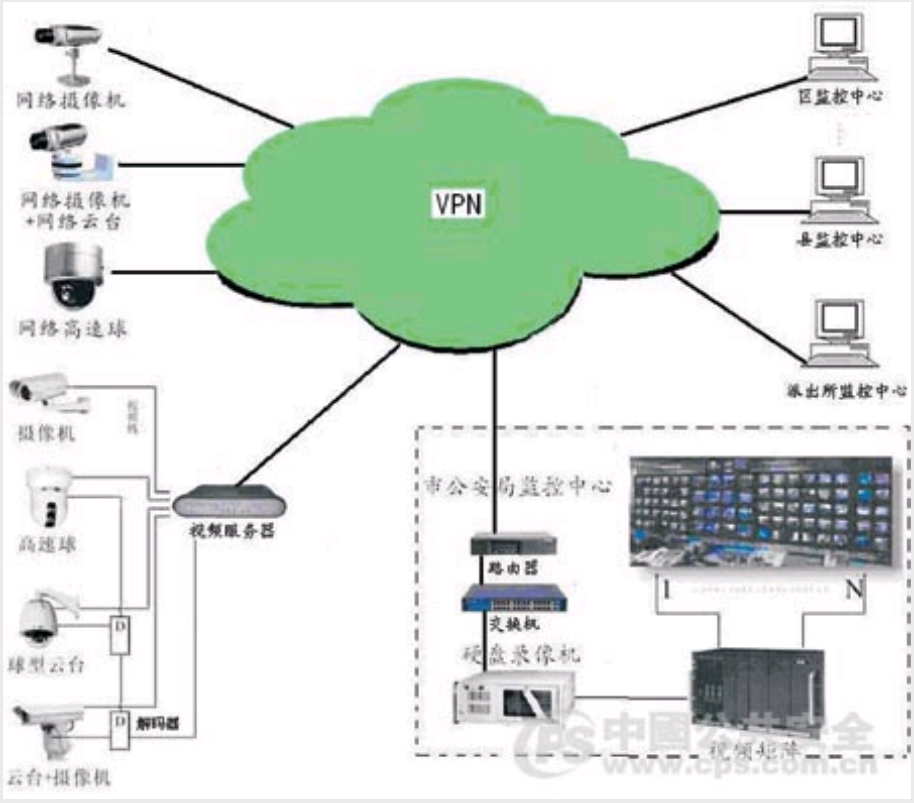
固定在城市各个角落的摄像机可通过以下几种方式接入VPN：

（1）ADSL宽带，对与图像要求较低的位置，可通过ADSL Modem接入VPN。由于ADSL带宽不稳定，当达到标称上行带宽时图像流畅，但当网络拥挤时图像质量就有所降低。

（2）ADSL2+，这是一种新型的ADSL标准，它的上下行带宽都有很大提高，上行带宽能达到3M，足以满足单路图像传输的需要。

（3）光纤，对于摄像机比较集中或监控中心需要大量视频数据上下传输的地点只能依靠租用或自建光缆来传输。

以上接入方式均选择MPLS VPN方式，因为经过各种VPN实现模式比较，只有MPLS VPN符合视频传输的高带宽的要求，并有QoS作带宽保障。因此我们把MPLS VPN作为组网的主要方式，其他方式仅作为必要时的补充。(见图1)

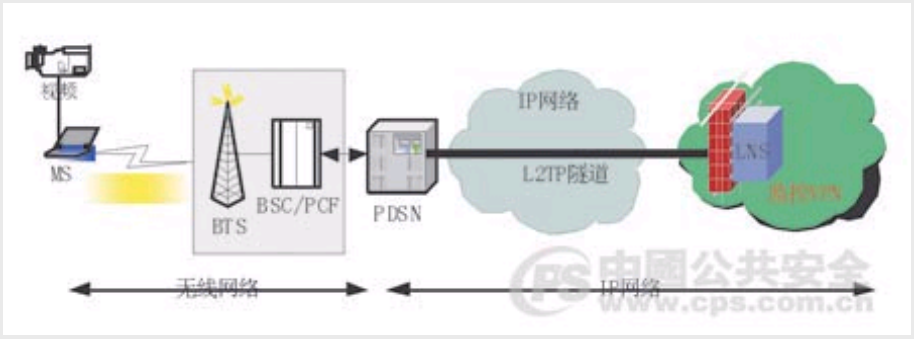


2、移动监控点

移动监控是突发事件、大型活动、警卫任务等临时活动现场中，以及恶性暴力案件的侦破中实现快速反应的有效手段。高效、可靠的移动图像传输系统接入图像数据，将会大大扩展各级公安机关监控中心的监控范围，提高快速反应能力。无线移动图像监控系统可由多种方式接入监控中心，主要有高速宽带的卫通信道，架设方便的微波信道和覆盖范围广的移动运营商提供的信道。由于卫通信道的昂贵，微波的遮挡干扰使我们更愿意选用移动运营商提供的信道。

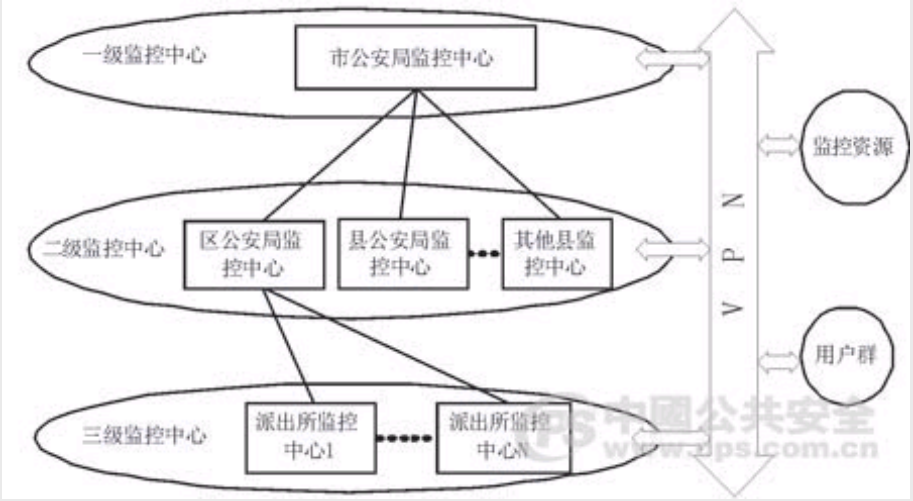
对移动监控设施如单兵图像采集子系统，装有车载摄像机的车载图像传输子系统，以及其他移动图像传输子系统的视频信号如需接入监控网，可先通过电信运营商的GPRS或CDMAlX公共无线数据网络再接入VPN，实现移动远程监控、临时监控。由于无线的带宽不足，要得到高分辨率的图像可以采用存储转发的方式，实时性较弱，但仍可做指挥中心的重要的决策参考和支持。特别是对暂时还没有视频监控的地方，是必要的补充。

在移动运营商网络中，对于需要接入VPN的移动用户，由于MS和PDSN建立的是PPP连接，所以PDSN必须使用隧道技术把PPP连接的终结点延伸到VPN的另一端。L2TP会话是指使用2层隧道技术在PDSN和LNS之间建立数据链路，用来承载PDSN和LNS之间的双向通讯信息。通过建立L2TP会话，可以将MS与PDSN之间的PPP会话拓展到MS与LNS之间，实现了VPN功能。在L2TP会话过程中，PDSN负责管理移动台和安全远程接入服务器（SRAS）之间的L2TP数据报的传输，PDSN作为L2TP 接入集中器（LAC），SRAS作为L2TP的网络服务器（LNS）。(见图2)



3、组网方式

根据城市接警情况的变化，也可选择不同的组网方式。对小城市或集中接警集中出警的城市选择组建统一的VPN网，视频控制、存储由一个中心统一实施。对于大型城市或分散接处警的可以每个区或每个派出所建一个指挥中心并对应一个VPN，所辖区域内的摄像机接入各自的VPN，各指挥中心再与市级指挥中心形成一个VPN，以便有重大活动或警情时全市统一指挥。同时原有的交警指挥中心也可并入。(见图3)



4、安全性保证

MPLS VPN技术采用了严格的路由信息隔离机制，同时采用面向连接的方式在运营商边界（PE）设备之间建立标记交换隧道来传送用户信息，在一定程度上保证了用户信息传送的安全性。但作为基于IP的技术，其安全性是相对于普通的IP数据业务而言的，MPLS VPN仍然有可能遭受来自IP网络的攻击，因此仍需采用必要的安全措施来保障系统的安全性。

控制面的安全性。对用户侧的CE设备进行认证，在经过认证之后才允许进行路由信息的交换。

PE路由器之间MP-BGP路由信息的交换应强制执行认证功能，每个PE路由器都应在认证的基础上接受来自其他实体的连接请求，以防止非法用户对路由信息的窃取和攻击。

PE路由器承担着为用户建立虚拟路由表、转发VPN用户数据包的任务，P路由器为VPN业务提供传送通道，P路由器和PE路由器如果受到过大业务量的冲击而不能正常工作甚至瘫痪，必然会影响VPN业务的正常运作。因此，P路由器和PE路由器上应采取流量控制措施，PE路由器上应对每个接入用户的流量进行限制。

数据面的安全性。主要考虑防止用户数据包被非法截获和篡改，采取的主要安全措施是加密，通常采用在用户的CE路由器侧用IPSec 加密的方式。尤其是用户以无线方式接入或通过IP网络远程接入时更要采用加密措施。

可以对那些需要较高认证和私密性的数据流实行IPSec，而对数据网络的带宽、流量工程和QoS等要求比较高的区域实行MPLS。

5、带宽保证

一是在接入方式上保证有足够的带宽，我们选择了ADSL2+新型宽带接入，对有特殊要求的点可用光纤接入，对传输视频量大的路径（如各指挥中心的接入）也选择了光纤传输；二是利用MPLS VPN从两个方面实现QoS（服务质量）保证：流量工程与直接QoS实现。流量工程实际上是一种间接的QoS实现技术，它致力于对整个网络资源的最优利用，从而改善网络的性能。直接的QoS实现是针对各种对QoS有特殊要求的业务，在网络的各个节点上对各种业务流采取相应的措施，实现其QoS要求的指标。

6、移动用户接入方式

对于授权的移动办公用户，要察看存储的资料可通过SSL VPN和放置在指挥中心的服务器进行登陆认证和资料的传输。

SSL属于高层安全机制，广泛应用于WEB浏览程序和WEB服务器程序。用户通过标准的WEB浏览器就可以访问重要的应用。这使得用户出差时不必再携带自己的笔记本电脑，仅仅通过一台接入了Internet的计算机就能访问资源，提高了效率也带来了方便。

《中国公共安全》杂志社简介 | 编辑委员会 | 各地区联系地址

市 场 版　　综 合 版

主管　中华人民共和国公安部

电话：+86-755-88309125 27035172　传真：+86-755-88309166　QQ：2925872
地址：深圳市深南大道6025号英龙大厦四楼　邮编：518040

ICP证：粤B2-20070271
欢迎行业媒体及展会合作