

视频监控网络的建设解决方案

摘要:

随着电信运营商宽带网络建设的不断完善,随着图像压缩编码与流媒体技术的逐步演进,基于宽带技术的网络图像应用在网络视频监控中逐步得到推广使用,使得电子监控已不仅仅局限于安全防范,而是已成为一种对各行各业都较为行之有效的监督手段和管理资源。由于市场潜力巨大,目前国内各大运营商已经开始建设网络视频监控平台,如中国联通的宽视界项目,中国电信的全球眼项目等,该平台的建设将使行业用户及公众用户实现远程视频监控成为可能。既然视频监控系统将作为一种业务,那么如何保障业务的可靠性及安全性,什么样的网络适合承载视频监控业务流将是运营商面临的技术问题。本文以****公司的视频监控系统承载网建设项目为例证,从技术分析、方案实施、接入选择等多方面来阐述系统的组网方式及如何保障媒体流的安全性。

正文:

2007年3月****的**分公司(简称****公司)提出了建设****公司骨干网视频监控系统项目,该项目历经6个月的调研、实施终于上线。该网络视频监控系统基于宽带网络为用户提供视音频及各种报警信号远程采集、传输、储存及处理。这是一个由前端、中心平台、后端三部分组成的系统。前端由镜头、摄像机、云台、报警开关、视频编解码设备、主机控制设备和监控软件组成;中心管理平台具有业务平台的管理功能,对传送过来的图像进行转发、分发或存储,对报警进行联动处理;在后端用户可在网络的任何一个接入点,无论是监控现场,监控中心,或者是远端,只要通过IE浏览器或客户端软件,在通过用户认证后可任意观看视频,可控制摄像机的角度、拉近拉远镜头、控制远端设备,并可接收报警信息。通过这一业务,用户只需轻点鼠标,通过宽带网络,可以该公司客户从显示器得到清晰、逼真、实时的监控图像。

本人所在深圳****技术有限公司,承接了该项目的分析、设计和实施的工作,本人为该公司的技术总监,确保该工程的顺利完工。

1. 关键技术分析

MPLS VPN是一种基于 MPLS 技术的 IP-VPN,是在网络路由和交换设备上应用 MPLS 技术,简化核心路由器的路由选择方式,利用结合传统路由技术的标记交换实现的 IP 虚拟专用网络 (IP VPN),可用来构造宽带的 Intranet、Extranet,满足多种灵活的业务需求。

采用 MPLS VPN 技术可以把现有的 IP 网络分解成逻辑上隔离的网络。MPLS VPN 由于在灵活性、扩展性、QoS 方面的优势,逐渐成为最主要的 IP-VPN 技术,在****公司的电信运营网上得到了广泛应用。

****公司的电信运营网采用 MPLS VPN 为企业提供宽带服务,并保证企业数据流的安全性和服务质量。VPN 业务需要面向多种不同的用户,承载多种不同的业务,采用多种接入方式。运营商可以根据网络的实际情况及用户的需求开通最适合的 VPN 业务,实现统一的资源调度。目前****公司已经能够提供多种 VPN 业务,如 Intranet、Internet、Extranet、Access VPN,而且这些业务可以整合为“VPN 套餐”提供给企业。为实现完整的 VPN 业务,电信运营网络需要融合各种 VPN 技术,包括 MPLS VPN、IPSec、L2TP、GRE、ATM、FR 等。

目前****公司网络设计基本都采用经典的分层结构,如****公司城域网典型结构是骨干—核心—汇聚—接入四层模型,设备性能依次下降,网络规模依次扩大。核心层与骨干层通常采用口字型结构,增加冗余以保证网络的可靠性。

2. 视频监控系统承载网解决方案

视频监控平台通常分两级进行构建:核心视频监控平台至于省中心,放置数据库服务器、AAA 服务器、中心管理服务器、接入服务器、Web 服务器等。为全省的视频监控平台提供核心的控制、认证、管理、北向接口等功能。视频存储服务器、分发服务器通常放置在各地市。建设 MPLS VPN 的网络,需要保证各地必须有足够的 PE 设备作为接入点。同时在合理规划核心网的情况下通过 P 路由互联组成 MPLS VPN 骨干网络。

宽视界平台分为两大部分,一个是省中心的中心管理控制平台及门户,负责业务的控制和管理以及客户的访问;另一个是各地市的存储转发和前端接入平台,负责业务的流媒体转发和存储以及 PU 的接入。建网思路如下:

(1) 省核心平台建设在一个独立的 MPLS VPN 网络中, 平台通过 PE 接入到未来的 MPLS VPN 中, 平台包括中心控制管理平台和分布在各地市的转发存储接入平台。

(2) 目前本地城域网核心网络设备作为 P 设备, PE 设备将直连路由分发到 MPLS VPN 网内, 用户端采用缺省路由进入到 VPN 内。

(3) 核心平台通过防火墙进行严格的保护, 对于来自 Internet 的访问不仅可以通过 MPLS VPN 来阻止网络攻击的入侵还可通过防火墙的拦截, 设置多种安全策略, 可以实现高度的网络安全特性。

(4) 针对行业用户、大客户可以采用 2M 专线、以太网专线或光纤直连, 用户的出口路由器作为 CE 设备, 监控客户端和前端设备可直接进入 MPLS VPN 网, 并使用统一分配的私网 IP 地址。每个大客户使用独立的 MPLS VPN, 并保证各地的 MPLS VPN 与核心网络平台设备的 MPLS VPN 网络实现互通。可以通过互相导入 Router-target 的模式来实现。但各个大客户间的 MPLS VPN 不能直接互通, 因为在 MPLS VPN 层面两个网络的 Router-target 没有实现互相注入和识别所以可以很方便的实现多个大客户之间的互相隔离措施。

(5) 针对公网用户或者零散小企业用户, 可通过 DSLAM, 宽带上网线路通过 PPPoE、VLAN 透传等方式与 PE 设备建立 VRF 映射, 从而获得与视频监控平台的互通。

3. PU 及 CU 的接入方案

在接入层, 用户以及前端的接入主要是利用 DSLAM 的方式, 也有 LAN 的接入方式以及专线接入的方式等。

(1) DSLAM 上联到 BAS

BAS 设备可实现对用户的认证, 该设备承担的用户采用 PPPoE 的方式实现认证。可以通过互联吉比特光纤的方式来进行连接。当 BAS 与 PE 互通后, BAS 汇聚的接入用户, 透传 VLAN 到 PE, 就近实现 PE 节点的接入。CU 和 PU 在 BAS 上利用 VLAN 透传, VLAN 终结在 PE 设备上映射到视频监控的 VPN 中, 实现与 VPN 内业务的平台的互通, CU 以及 PU 设备均配置私网地址。

另外, 还可以新建 SR 设备, 把 DSLAM 采用双上联的方式, 将视频监控的业务分离到 SR, 由 SR 作为 PE 设备, 将业务映射到视频监控 VPN 中。

(2) 以太网透传模式（上联到 3 层交换机）

当 3 层交换机作为接入汇聚设备的节点，下挂有大量的 LAN 小区接入用户以及企业宽带接入用户时。那么其解决方案与采用 DSLAM 上联到 3 层交换机没有什么区别，只是在带宽保障上 LAN 更有优势。

(3) 专线模式

对于采用 DDN、FR 以及数字 2Mbit/s 专线的用户可以为其提供专线到 PE 设备的连接，将业务映射到视频监控的 VPN 网络中。最终由 PE 设备将视频监控的相关信令和媒体流映射到 VPN 网中，实现用户接入视频监控网络。这类用户建议均采用私网地址。

(4) VPDN 方式

对于 ADSL 用户来说，大部分采用 PPPoE 的方式接入。考虑到目前网内可能存在没有下沉 MPLS VPN 业务到 BAS 和附近的 PE 设备上，所以提供 PPPoE 认证和接入的 BAS（LAC）可以通过建立 L2TP 隧道到 PE（LNS）的方式来提供 VPDN 接入业务。这样也可以解决 BAS 不支持 PE 功能的设备入网问题。

具体方法如下：

- CU 或 PU 设备通过 ADSL 线路发起 PPPoE 拨号，发送 PPPoE 请求后收到来自 BAS 设备的认证要求。
- CU 或 PU 设备向 BAS 设备提交一组特殊的用户名和密码，例如：123@gongan。123 是用户名，gongan 是用于区分不同大客户的域名。BAS 根据不同的域名配置，可以建立与远端 LNS 的 L2TP 连接。
- BAS 作为 LAC 与 LNS 建立 L2TP 隧道后，认证将提交为 LNS 进行认证，并由 LNS 提供动态的 IP 地址分配。

由此，CU 或 PU 设备将可以建立从 DSLAM 到 LNS 的全程私网连接。利用广泛的 Internet 资源，将视频监控业务灵活的布放到各级接入设备上。

4. 小结

项目实施很成功，当然也存在着一些问题，主要问题还是在一个分层网络中如何部署 PE 节点，将 PE 部署到核心层汇聚层，还是接入层？我们解决的方法是将 PE 分为多个层次，共同完成全网的 VPN 业务。

这样，与分层分级网络相适应，网络层次越高的 PE 容量和性能要求越高，网络层次越低 PE 的容量和性能要求越低。网络层次越低，PE 数量越大，用户接入能力越强。