网络之路
ROUTE TO NETWORK

监控专题

2010年第3季度总第14期

H3C
ITolP Solutions Expert

目录

01 联网监控促进安防软件进行3.0时代 朱 兵

09 监控实况业务传输 王连朝

15 IP监控中的存储备份和回放 李玉天

24 视频编解码基础概述 郭 琪

33 IP视频监控中的音视频质量提升 吴参毅

45 监控产品的跨域业务控制 李 旻

49 监控产品的告警联动 周后取

56 IVS视频监控系统双机热备 周绪龙

63 实时流量分析及网络部署 杜超华、袁飞

69 无线监控简介 任俊峰

77 传统VPN在监控中的应用分析 任俊峰

86 图像质量主观评价方法介绍 郭 琪

92 视频质量客观评价方法介绍 袁 飞

主办单位：H3C测试中心

策　　划：刘　宇 陈旭盛 杜祥宇

主　　编：陆宇翔

本期编委：朱　兵 王连朝 李玉天 郭　琪
吴参毅 李　旻 周后取 周绪龙
杜超华 袁　飞 任俊峰

测试中心 TESTCENTER

联网监控促进安防软件进行3.0时代

■ 文/朱 兵

本文通过总结安防软件过去20多年的发展历程，指出了安防软件从1.0、2.0到3.0的三个典型发展阶段，对驱动安防软件发展的原因进行分析说明，并结合H3C公司IMOS IP多媒体应用平台对安防软件的发展趋势作了分析和展望。

安防软件的发展历程

从上世纪90年代起，随着计算机、通信、控制和多媒体技术的高速发展，安防软件作为安防系统的关键组成部分，在安防系统数字化、网络化、智能化发展的大趋势下，其重要性越来越被客户所重视，其本身也得到了极大的发展。

安防软件的管理范围包括视频监控、入侵防范、门禁出入、环境监控等，在上世纪90年代初，安防软件主要还是采用配套安防系统硬件的方式进行销售，比如配合视频监控矩阵的矩阵控制软件、配合门禁系统的门禁管理软件和配合专业入侵防范系统的接警管理软件，更多属于配套和选配的角色，主要提供厂商都是安防系统硬件厂商，其中国内主流硬件厂商在提供硬件时一般会提供免费的选配管理软件，这个时期的安防软件功能简单单一，参与厂商少，其价值和重要性都没有得到充分的重视。

90年代中后期，随着智能建筑市场的快速发展，结合IBMS智能建筑管理系统的要求，市场上出现一些专业的厂商，可以提供将矩阵控制、报警接警和门禁管理等主要安防系统整合在一起管理的第一代安防集成管理软件，同时通过OPC服务器等通用接口，还可以实现和BA楼控系统的联动协同，共同构建智能建筑管理平台，此时作为安防系统最主要的组成部分，视频监控系统还主要是采用模拟矩阵加模拟录像机的全模拟架构。能够提供这种软件的公司主要是几大国际安防厂商及其配套厂商，在一些高档的智能建筑中，第一代安防集成软件得到了初步的应用，但在国内其整体价值和重要性依然没有得到普遍性的认可，直到今天，大多数智能建筑还是使用各安防子系统提供的独立软件。

需要关注的是，90年代中后期，在中国的运营商领域（当时叫邮电部），提出了建设电信机房动力与环境联网监控系统，基于电信DDN专网，网络建设联网监控的用户单位，将各地的电信机房中的动力、环境、报警、门禁系统基于一套软件进行统一管理。到了90年代末期，电信部门首次提出对机房图像进行数字化编码并实现联网监控的需求，并首次大规模在机房监控中使用基于硬件级视频压缩采集卡的PC式DVR产品。参与机房监控的单位并不多，严格意义上来说，机房监控系统还不属于安防监控软件的范畴，在当时也没有引起全行业的重视，但其中的技术是相通的，这其中许多厂商及其从业人员都成为今天国内联网安防监控软件开发的中坚企业和骨干力量。

上世纪末的最后几年，安防软件真正大规模在行业中应用并得到普遍重视，其契机是硬件视频压缩卡的推出，以及基于硬件视频压缩卡的通用DVR数字硬盘录像机软件的开发成功，安装了视频压缩卡和DVR硬盘录像机软件的PC式DVR开始在银行柜员制录像改造领域中进行应用，逐步取代传统模拟录像机，推动了视频监控从模拟监控过渡到数字监控时代。由于DVR软件开发门槛低，使得大量的本土企业第一次有能力进入安防监控核心产品的开发之列，打破了日韩系企业多年来对视频监控产品的垄断地位，时至今日，中国的硬盘录像机产品已经在国际市场占据了较大份额，是第一个被国外市场整体承认的核心安防产品。在这期间也涌现出许多后来市场占有率较高的专业PC DVR软件开发单位，如天视、黄金眼、飞龙（朗视）、捷诺等，这些企业也成为今天联网视频软件开发的参与者。

进入21世纪，在数字视频监控快速发展的大趋势下，安防软件的发展呈现百花齐放的态势，可以看到存在四个主要发展方向：

1) 传统的智能建筑安防集成软件开始将数字图像监控融合入其软件中，如美国LENEL将DVR软件和门禁报警软件整合，国内丛文软件将专业入侵报警和DVR、门禁软件的整合；

2) 原来的安防硬件配套软件开始支持简单的

安防系统联动集成，如以色列DSS门禁软件实现和DVR数字监控软件的融合联动，一些DVR数字监控软件可以实现对专业入侵报警主机管理；

3) 原来的机房联网监控软件开发厂商和PC-DVR软件厂商开始推出以视频监控为主的通用安防联网管理软件，如中兴力维、共济等，在机房联网、银行联网、公安联网监控中得到初步的应用；

4) 一些开发PC-DVR、机房监控软件甚至工业控制SCDA软件的开发厂商结合部分行业用户的特殊要求，通过定制开发，将通用的视频联网监控软件应用与平安工程、金融异地守库、审讯指挥、企业生产监控、景区监控宣传、远程保险定损甚至幼儿园宝宝看护等多种领域，有些甚至不属于安防领域，但本质上都属于安防软件的衍生产品。

上世纪90年代末期前的安防软件可以称之为安防软件1.0，其主要特征是多为配套安防硬件选配的单系统软件，功能单一，集成能力低，不支持数字图像监控技术，不支持大规模联网。

随着数字图像编码技术在安防领域的应用，PC式DVR软件的出现，从上世纪末开始，安防软件进入2.0时代，其主要特征是图像存储和联网采用数字编码技术，安防其它应用和图像监控技术开始集成和融合，从管理软件本身的角度出发，从产品架构和功能设计上可以基本满足安防系统集成联网的需求。进入这个时代后，安防软件开始得到大规模的应用并为客户所重视，尤其是在金融、公安、电信机房等联网监控项目中已经成为整个系统的核心组件，涌现出大量的安防软件企业，其中大多数基于PC-DVR软件开发衍生而来，也有部分来自传统安防集成软件、机房监控软件甚至工业控制SCADA软件企业。

在安防2.0软件的开发单位中有部分企业，在安防软件的开发技术上已经处于领先地位，其设计不仅仅只是以满足客户对功能的需求，而是站在上层应用软件整体设计的角度来开发集成软件，采用IT软件开发中的成熟技术，包括SOA、J2EE/.NET中间件技术、WEB2.0技术、面向对象开发、LDAP、单点登录等标准的IT软件开发技术，在软件本身的灵活性、可扩展性和开发技术相对一般的安防软件都有了大幅度的提升，推出了通用视频联网监控平台软件，并基于此面向行业推出行业联网监控软件。

安防软件中间件的提出

数字视频监控软件是安防软件发展中最具活力和应用范围最广的软件，随着银行联网监控、平安工程联网监控和电力、能源、环保等各个行业对视频监控联网需求的不断增加，安防软件所面临的环境、需求也越来越复杂，原有的单机版PC-DVR软件已经无法满足这类客户的需求。

联网监控已经成为推动安防软件不断发展的最大动力，在联网视频监控市场中，网络从局域网扩展到VPN专网、INTERNET等广域联网范围，用户数量从单机访问发展为大并发量访问，同时对视频存储要求越来越高，存储的天数、容量不断增加，同时前端接入的设备种类也从单一品牌PC-DVR延伸到各种品牌PC-DVR、嵌入式DVR、DVS视频服务器和视频编解码设备，部分客户还要求同时实现对入侵报警和门禁系统的管理。

面对市场需求，新的软件形态诸如流媒体服务器、网络存储服务器、设备接入服务器、代理服务器、WEB服务器、GIS服务器、报警处理服务器层出不穷，市场繁荣的同时也出现了各种问题，没有统一可行的行业标准，产品质量良莠不齐，各厂商之间甚至厂商自己的产品之间不能互连，无法稳定可靠的组成能容纳不同厂商产品的监控系统；

由于大型联网监控系统软件开发的技术门槛很高，有能力开发高质量的系统级监控软件的公司为数不多，面对这个市场许多缺乏实力的小厂商被淘汰，在此背景下，个别有实力的数字监控设备厂商为了降低安防软件商开发对其设备进行联网管理的软件技术门槛，推动联网视频监控市场的开拓和发

展，提出了一种新的、规范的、开放式的联网监控软件开发模式——基于“安防软件中间件”的开发模式；

借鉴了IT软件领域成熟的中间件开放模式，安防软件中间件定位在安防应用软件和操作系统硬件之间，可以运行于多种硬件和OS平台 ，支持分布计算，提供跨网络、硬件和OS平台的透明性的应用或服务的交互 ，支持标准的协议和接口，满足大量视频监控应用的需求，符合安防行业软件开发的发展方向，符合整个IT业的软件发展方向，具体产品组成包括：1）DVR/DVS 设备代理；2）流媒体转发； 3）权限验证； 4）播放及电视墙； 5）数据库； 6）防火墙穿越；7）网络存储 ；8）电子地图 ；9）消息传递等。

该中间件的提出，理论上确实可以大大降低软件开发商开发出一整套联网视频监控软件的难度，但是在实际应用中，由于该类中间件主要针对的只是中间件厂商自己的前端DVR/DVS设备，而且要求软件开发商具备一定的软件架构设计能力，而实际项目中前端管理设备往往不止一种品牌，真正有一定实力的软件厂商还是选择基于不同厂商前端DVR/DVS来开发联网监控软件，而缺乏实力的软件厂商由于市场竞争和后入劣势，也很难通过基于该中间件的开发获得足够的竞争优势，加上该中间件平台缺少对安防报警、门禁等其他系统的支持，因此，最终并没有获得市场的普遍认可，没有成为主流的产品开发形态。

还有一些软件厂商，在其安防集成联网软件的基础上，对集成商提供了功能裁剪、界面布局自定义、界面皮肤更换和电子地图设计等个性化定制功能，也将其软件定义为安防软件中间件平台，从严格意义上，由于第三方无法利用该平台开发更高级的应用，因此，只能将这类软件定义为具备一定灵活定制能力的安防组态软件，还不能称之为真正的中间件。

当前安防软件集成平台和安防软件中间件存在的主要问题

目前，整个安防监控系统已经进入了网络监控的时代，无论是视频监控的编解码、报警接入、门禁控制还是共用的存储与网络，都开始呈现以IP为主要特征的网络化发展趋势，各行业联网监控需求的快速增长，更是对安防软件提出了全新的要求，如何用尽可能简洁的架构、最高的效率实现跨区域联网监控系统全局范围内的看、控、存、管、用基本业务成为每一个安防软件厂商必须考虑的问题。

在这个时期，无论是安防软件1.0、2.0还是安防软件中间件，由于开发单位能力的限制，很难涉足开发联网监控系统的各个方面，其设计思路着眼点还是在各个安防系统之上去考虑安防软件的设计，重点在安防软件本身，而不是基于联网监控需求对对整个安防系统进行融合优化。

而事实上，当联网监控范围不断扩大，海量的视频访问和视频存储依靠传统软件设计已经存在一些不可逾越的瓶颈，从传统软件厂商的视角来看，解决问题只能从软件本身出发，无法从网络监控的整体架构角度去考虑优化。最终的结果就是异构非标的硬件、不同厂商存储、网络加上安防软件平台，靠软件去捏合这些的硬件，可以说是集成也可以说是拼凑。传统的安防软件生态环境中，软件只能被动的去适应硬件，试图去构建网络监控环境下硬件和软件的桥梁，而无法从整个网络监控监控的角度去对网络监控的各个相关组件进行整体优化，这些组件包括前端、存储和网络设备内嵌的软件。也因此才会出现流媒体服务器、网络转存服务器、设备代理服务器等组件来实现实时、存储视频流的处理和信令处理，面对海量多媒体信息管理存储的需求，这些设备的集群、负载均衡、故障倒换等可靠性设计以及其整体架构的性能瓶颈已经成为阻碍网络监控发展的重要因素。

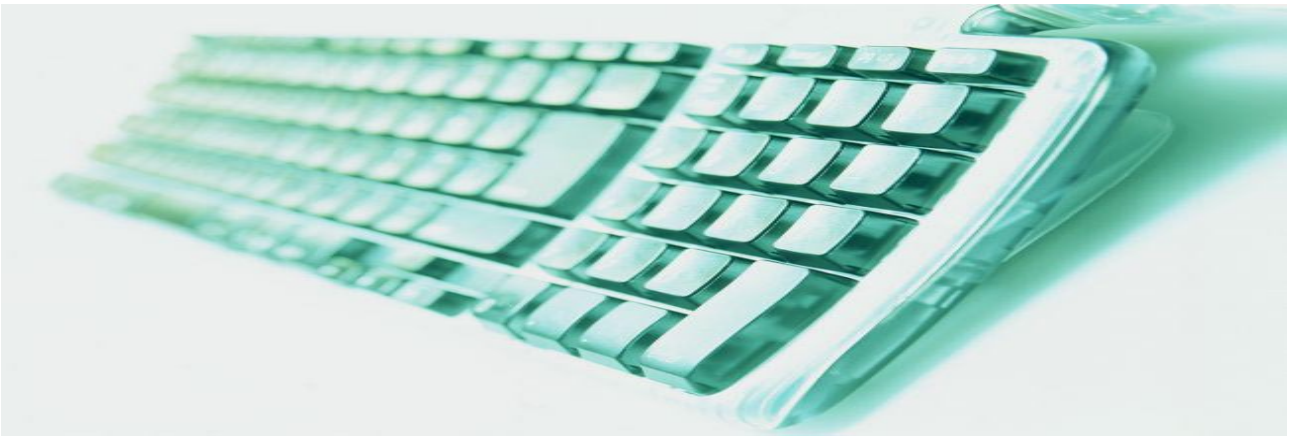
另外一个趋势是，网络监控的一大特征是网络带宽和海量存储数据容量的指数增加，当前无论是安防监控还是其他领域的监控管理都开始呈现出多媒体化的特征，通过视音频编解码技术的应用，利用融合视频监控、视频会议、语音通信、即时通信、视频信息发布等多种多媒体手段实现管理控制效率的提升，同时需要对大量的多媒体数据进行保存和按需检索，这些多媒体数据融合和海量存储数据综合管理技术也不是一般安防软件厂商所能充分掌握的，面对整个行业多媒体管理监控需求的迅速增加，传统安防软件厂商和集成商正面临前所未有的挑战，一方面需要保持在局部市场的盈利能力，另一方面还要投入大量的研发资源满足联网监控市场对海量监控管理可靠性、稳定性、多媒体管理不断增长的需求，由于在网络、多媒体、存储等网络监控新增组件技术积累方面的匮乏，在当前的经济环境下，如何实现盈利已经成为这些企业当前急需考虑的问题。

联网监控推动安防软件进入3.0时代

安防监控市场的快速发展，以及其在联网监控发展过程中出现的问题，让许多大型网络IT企业看到了机会，利用其在网络、存储、多媒体领域丰厚的经验积累，从整体架构角度上对安防监控系统进行了重新的审视和规划设计，包括国际上的CISCO、IBM、诺基亚西门子和国内的H3C、华为、中兴都开始介入这个市场。这其中H3C在2006年，凭借其在行业市场多年的IP网络、IP存储、IP多媒体和业务软件平台产品开发经验率先对安防监控系统进行了重新的设计和规划，提出从联网监控的整体架构角度对网络、存储、视频编解码和管理软件四大组成部分进行融合设计。

H3C的联网监控方案的最大特点是可以针对联网监控的需求进对其交换机、IPSAN盘阵和编解码内嵌软件和管理软件进行优化设计，而不仅仅是依靠管理软件去适配硬件，正因为此也实现了许多传统安防软件无法实现的功能，这其中包括通过管理平台的配合编解码器内嵌软件可以实现编码的视频存储数据直接写入IPSAN存储盘阵，无需传统网络监控的流媒体转存软件；利用网络交换机内嵌的组播软件优化，实现基于交换机组播协议海量视频数据的访问，无需传统的网络监控的流媒体服务器；利用编码器和交换机的流控帧软件优化，实现接入交换机的码流接入效率接近100%，超过传统网络监控交换机利用率50%以上，同时网络存储能力和实况流延时得到优化改善。

针对联网需求，系统的对包括所有网络监控组成组件（交换机、存储、编解码器）内嵌软件在内的网络安防软件进行优化融合设计，是安防软件3.0的重要标志，这同时也是IC网络通信、IT信息技术和SA安防自动化技术的第一次融合。安防软件3.0实现了从整体架构的角度对网络监控系统进行了重新的设计优化，使得联网监控应用变得更加简单、高效和可靠，可以方便的实现全局看、控、存、管、用业务，而不仅仅依靠管理软件本身来管理一堆堆砌的设备。



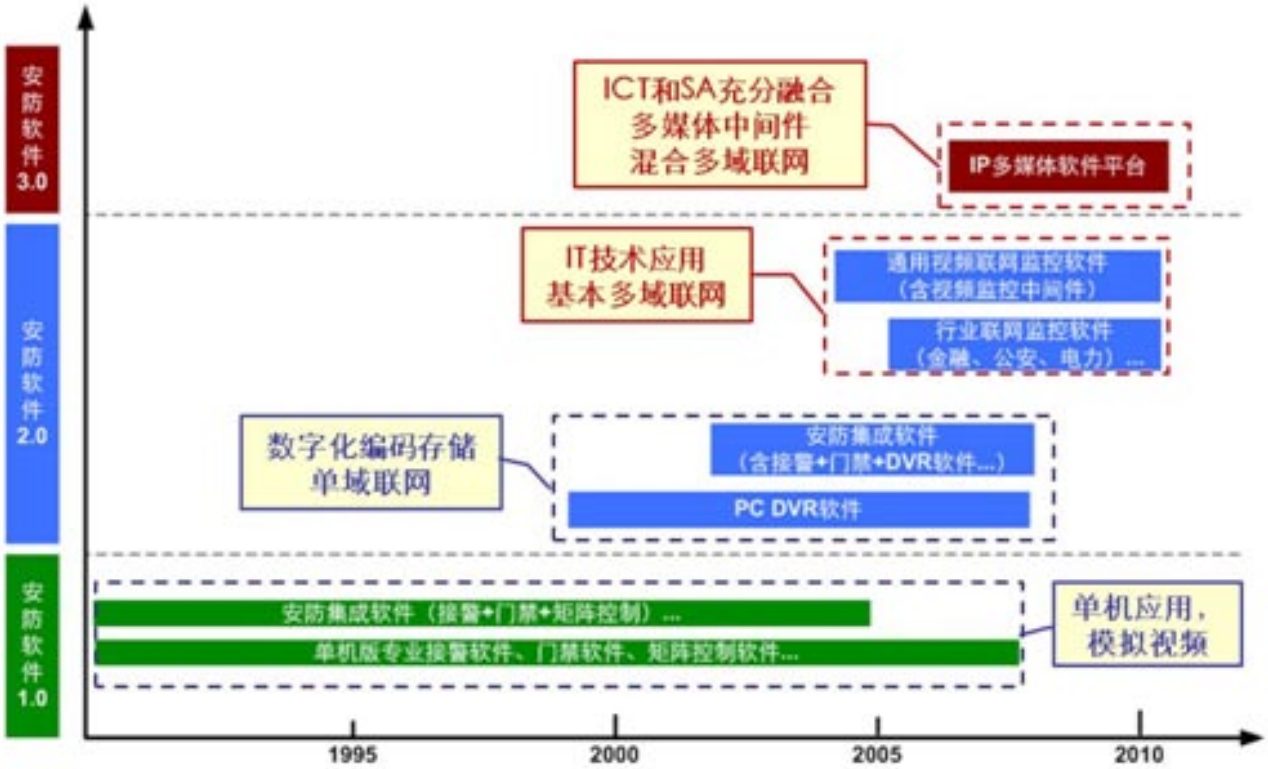


图1 安防软件的发展历程

IMOS与安防软件3.0

针对全行业管理控制多媒体化发展的趋势，2009年，H3C针对联网监控和多媒体融合管理的需求，推出了定位于IP多媒体基础软件平台的IMOS（IP多媒体操作系统），IMOS是H3C IP监控、视讯会议等多媒体产品共有的软件平台，其本质上是一个通用的含括多媒体综合监控、会议通信、语音通信、信息发布的中间件平台，即可以支撑管理平台组件也可以支撑所有的多媒体编解码终端设备，所有组件都针对联网监控业务进行了融合优化设计，可以方便的支持各种跨区域联网监控系统的全局看、控、存、管、用业务需求。同时，针对多媒体综合管理应用进行优化融合设计是安防软件3.0的另一个重要特征，也是全行业多媒体化管理控制应用发展的必然要求。

不仅是H3C的所有产品，所有多媒体监控、通信领域的软件厂商都可以借助该平台快速开发各种多媒体综合应用平台，该平台的推出将有助于降低原有应用软件厂商的开发成本，对监控产业价值链的优化梳理起到很好的推动作用。

图2 IMOS应用框架图

IMOS平台定位与中间件平台，和传统的安防软件中间件不同的是：

1）作为安防软件3.0的核心支撑平台，不仅针对上层管理平台，对网络监控中编解码器、网络存储、网络传输交换都进行了优化支撑，可以方便的支持各种跨区域联网监控系统的全局看、控、存、管、用业务需求。

2）作为开放平台其管理设备也不仅仅局限H3C自己的前端设备，除了可以管理其他数字图像前端外，通过通用I/O引擎还可以管理安防报警、门禁、SCADA等各种设备；

3）其开放程度也不仅仅局限于最上层的应用，由于其模块化、平台化设计，在软件的各个层面都遵循SOA的开放架构，提供比传统安防软件中间件丰富的多的二次开发手段；

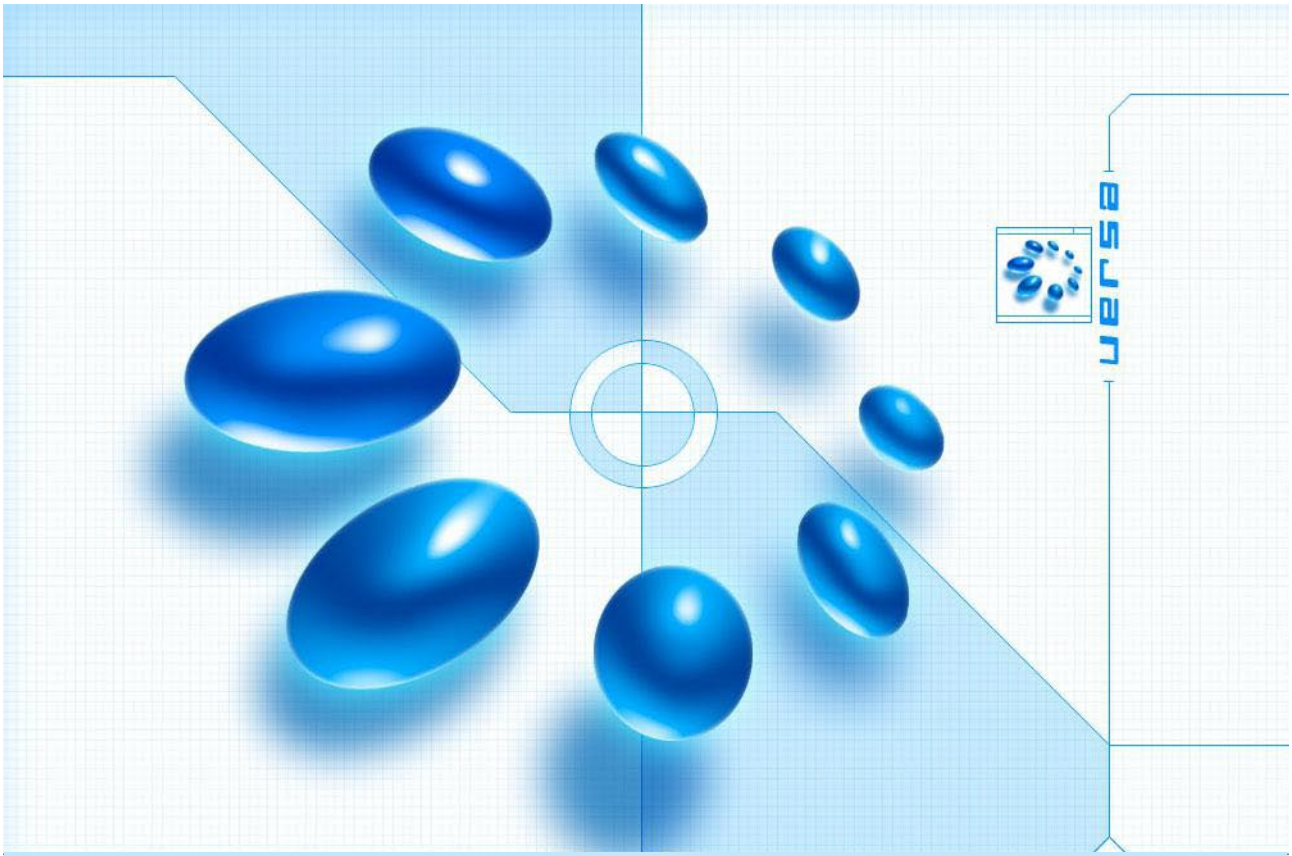
4）由于是多媒体综合应用平台，支持多媒体领域几乎所有的国际标准和SIP信令标准，可以方便的实现监控系统和视讯会议、视频点播、视频直播、语音通信、即时通信、多媒体信息发布等多媒体应用系统的融合，使得未来的监控体验和协同报警处理手段得到极大的丰富，面对行业多媒体管理应用变得更加得心应手；

5）面对多媒体监控管理对海量存储数据应用的需求，IMOS创新的整合了MAS（Media Access Service）的多媒体存储架构，详细分析了多媒体数据以及在不同的应用场景下的多媒体系统特征，将多

媒体存储数据管理分成流媒体应用层、媒体数据直接访问接口层、数据组织层、存储资源屏蔽层和物理资源层，提出了更适合于多媒体数据特征和视频监控和会议多媒体系统中的访问特征的“虚拟多媒体文件系统”，建立了多媒体存储数据和和智能特征数据之间的数据关系矩阵，适合各种存储媒介，同时可以方便的实现存储数据的生命周期管理，使得多媒体数据的应用和管理的效率得到了极大的提升。

结束语

可以预见的是，不断增长的联网监控需求，推动着安防软件3.0的出现和发展，同时，整个安防行业的生态环境将可能产生重大的变化，即使是3.0时代的平台厂商也不可能快速满足所有行业应用定制需求，原有2.0时代的安防软件的另外一条出路就是转向行业应用软件开发或者软件集成市场。基于市场的博弈，包括H3C在内的IT企业从原先相对封闭的市场策略开始走向全面合作的市场策略，H3C将自己定位在提供高质量、高可靠和标准化的多媒体基础应用平台，希望借助行业应用合作伙伴在行业定制软件方面的灵活、快速的开发能力，共同为客户提供完整的解决方案。■



监控实况业务 → 传输

■ 文/王连朝

实况业务介绍

监控。顾名思义，监：古人以水为镜,“监”就是一个人弯着腰，睁大眼睛，从器皿的水中照看自己的面影。本义：监督,察看督促；控：操纵、制约控制。

因此，监控就要达到既可见又可控的效果。而“可见”和“可控”在使用者面前的实际呈现就是实况和轮切。

监控业务由传统的模拟监控（CCTV）已经发展到了网络监控的阶段。对于监控数据的实时浏览和摄像机控制的要求也越来越高。

监控系统的主要工作流程依次为：a 摄像机采集图像信号；b 采音设备采集声音信号；c 音视频编解码设备对信号进行模数转换和数据压缩编码等处理，并通过网络进行传输；d 中央管理控制设备接入网络后对系统进行管理控制认证等工作、通过中心集中存储等方式进行录像数据的处理；e 各接收端通过接入网络的电脑终端可方便的查看视频图像，同时通过解码器发送到监视器墙显示。

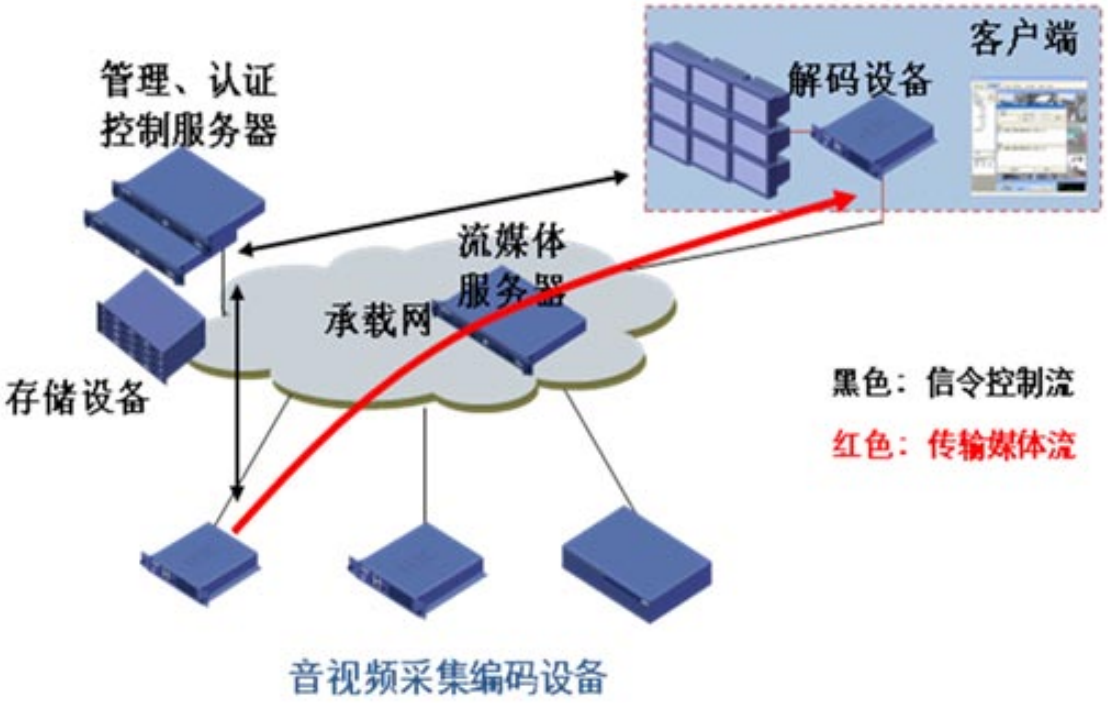


图1 监控系统概图

实况是指将前端摄像头获取的图像实时地显示在监视器或者用户PC的软解客户端上。

轮切是伴随实况产生的一个必然结果。在实际监控环境中，前端的摄像头（编码器）数量是远大于监控中心的解码设备的，往往是摄像头的数量成百上千，而监视器的数量在十几到几十个。这必然不能够保证每一个摄像头的图像都显示在监视器上，而且也没有必要。只要隔一段时间对所有的摄像头图像做一遍巡视即可，当发现某地出现问题时，再进行一对一实况。轮切就是适应这种需求而产生的。

传统监控实况业务采用同轴电缆或模拟光端机和数字光端机通过把视频及控制信号转换为光信号进行一对一的传输。通过视频切换矩阵在同一个监视器上对若干个监控摄像机的图像进行轮循显示。

网络监控在实时数据的传输和显示，通过对模拟音视频信号进行转换和压缩，利用越来越广的IP网络进行传输，基于IP网络单组播协议实现了一对多的实时业务。

实况业务的要求

不同于传统监控方式的模拟信号的传输，网络监控的优势就在于将模拟视频信号转换为数字信号，编码压缩并封装在IP包中进行传输，通过IP传输的特点使其不受线缆的铺设影响而可以在任何网络接入的地点可以方便的进行实况的浏览和视频数据的查询。

对于实况业务，行业、商业以及各个地方都出台了不少相关的标准。具体的细节本文不加以详述，概括起来无外乎以下部分：1 图像的采集与处理，2 接收数据解码与现实，3中心控制与认证服务，4音视频数据的分发和存储。

网络监控系统中，要求实现通过网络的实时音视频浏览。可以在远程计算机上实时监控，亦可实现在远程通过硬件解码器在监视器、电视墙上观看实时视频。浏览客户端可采用B/S或C/S架构。可实现对电视墙投放视频的灵活控制。

承载网络本身必须对视频监控业务端到端的视频传送服务质量(QoS)提供保障。网络视频监控系统的QoS实现要求IP承载网络在承载端到端的视音频IP包码流时，做到延迟小、抖动低、丢包率低。其中对网

络视频监控系统QoS影响最重要的指标是丢包率。

IP承载网络指标要求：

	网络延迟	延时抖动	丢包率
网络指标	≤ 500ms（图像有时延，但可以接受） ≤ 50ms(图像无明显时延)	≤150ms（视频较流畅，轻微卡顿，可以接受） ≤ 80ms （视频流畅，无卡顿现象）	≤ 5%（图像偶尔花屏，但可以接受） ≤ 3%（视频流畅，无马赛克）

业务传输要求：

	音视频传输码流可控（分档）	音视频流控制传输延时
业务传输指标	128kbps、384kbps、512kbps、768kbps、1Mbps、1.5Mbps	< 2S

实况音视频数据在IP网络上的传输应用

实现音视频数据在IP网络上进行传输，可以采用多种方式。TCP不能支持像交互视频，会议等的实时服务，原因是由于TCP是一个“慢”协议，需要三次握手。因此在IP层上UDP是比TCP更好的选择。但是UDP是本质上是一个不可靠协议，不支持在丢包情况下的重传机制。为了消除UDP的缺点，RTP是作为应用层而被提出来的。

RTP提供各种服务包括有效负载识别，序列编号，时间戳和投递监听。当包在收端不是按顺序到达的时，RTP能够重新对包进行序列化。序列号用来识别是否存在丢包。时间戳用于媒体有效的播放。到达的数据一直被RTCP监听，以通知RTP层来校正其编码和传输的参数。例如，如果RTCP层检测到包丢失，它会通知RTP层减缓发送速率。

RTP报文的封装

RTP（real-time transport protocol）是用于Internet上针对多媒体数据流的一种传输协议。RTP被定义为在一对一或一对多的传输情况下工作，其目的是提供时间信息和实现流同步。RTP通常使用UDP来传送数据，但RTP也可以在TCP或ATM等其他协议之上工作。当应用程序开始一个RTP会话时将使用两个端口：一个给RTP，一个给RTCP。RTP本身并不能为按顺序传送数据包提供可靠的传送机制，也不提供流量控制或拥塞控制，它依靠RTCP提供这些服务。通常RTP算法并不作为一个独立的网络层来实现，而是作为应用程序代码的一部分。实时传输控制协议RTCP。RTCP(real-time transport control protocol)和RTP一起提供流量控制和拥塞控制服务。在RTP会话期间，各参与者周期性地传送RTCP包。RTCP包中含有已发送的数据包的数量、丢失的数据包的数量等统计资料，因此，服务器可以利用这些信息动态地改变传输速率，甚至改变有效载荷类型。RTP和RTCP配合使用，它们能以有效的反馈和最小的开销使传输效率最佳化，因而特别适合传送网上的实时数据。

RTP提供端对端网络传输功能，适合通过组播和点播传送实时数据，如视频、音频和仿真数据。为了实现音视频数据的传输，必须对压缩编码后的数据进行封装。RTP报文封装的格式如下：

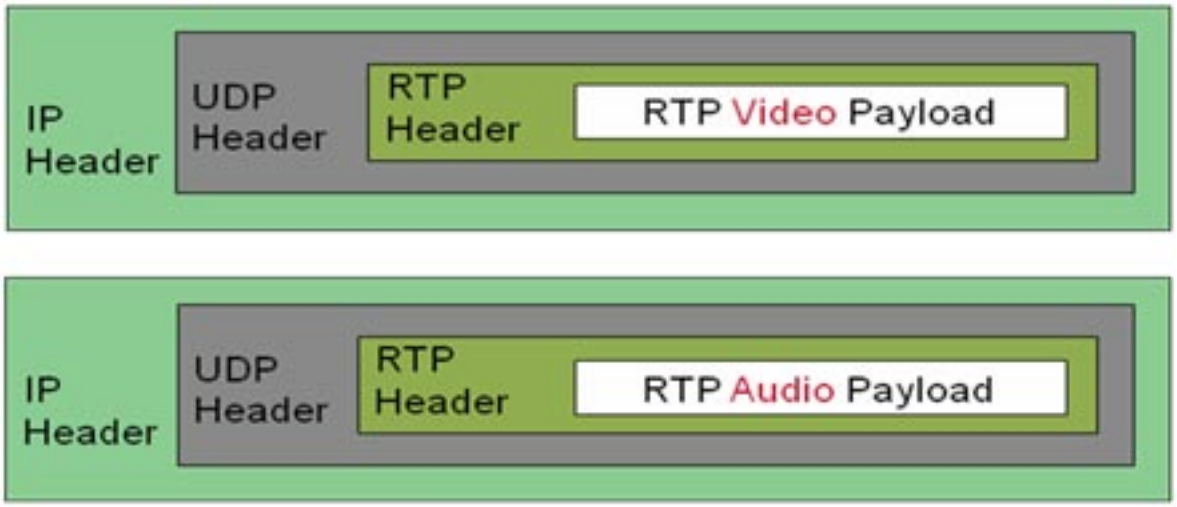


图2 音视频数据在IP报文中的封装

可以看出RTP是承载在UDP协议报文之上的。而RTP报文又将音视频数据进行封装进行传输。

RTP 头格式如下：

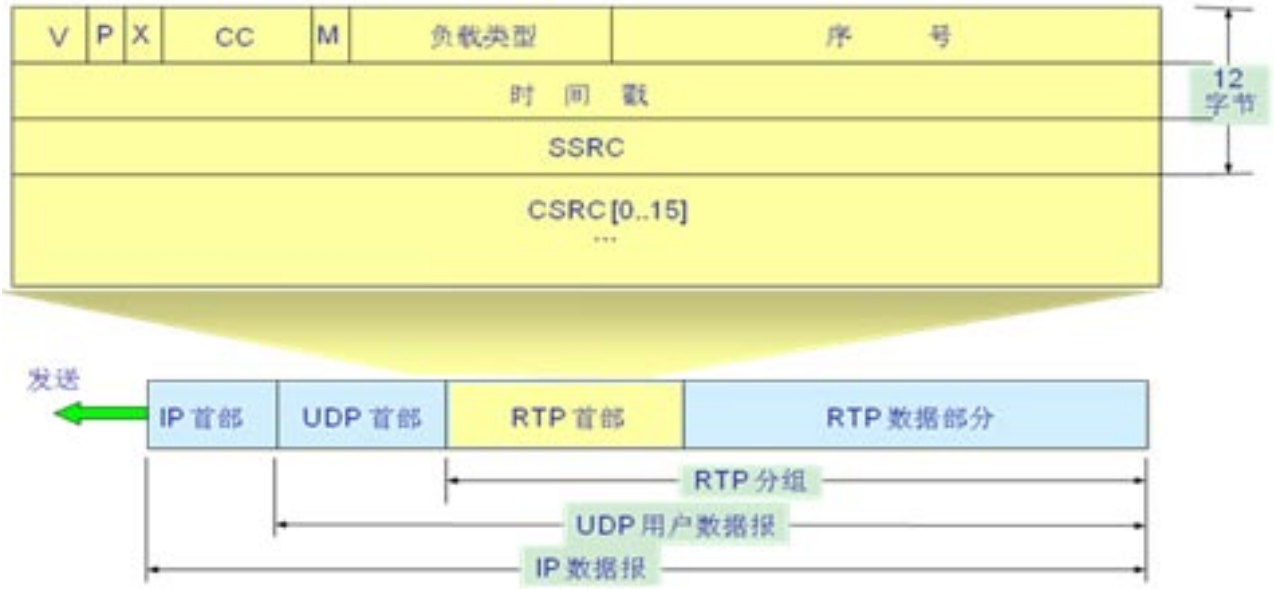


图3 RTP报文头格式

前12个字节出现在每个RTP包中，仅仅在被混合器插入时，才出现CSRC识别符列表。其中：

版本(V)：2比特，定义RTP的版本。

填充(P)：1比特;

扩展(X)：1比特，若该位置1，固定头后面跟随一个扩展头;

CSRC计数(CC)：4比特，CSRC计数包含了跟在固定头后面CSRC识别符的数目;

标志(M)：1比特，它用来允许在比特流中标记重要的事件，如帧边界;

负载类型(PT)：7比特，此域定义了负载的格式，由具体应用决定其解释。可以规定负载类型码和负载格式之间一个默认的匹配。其他的负载类型码可以通过非RTP方法动态定义。

序列号（sequence number）：16比特

每发送一个RTP数据包，序列号加1，接收端可以据此检测丢包和重建包序列。序列号的初始值是随机的。

时间戳（timestamp） 32比特

时间戳反映了RTP数据包中第一个字节的采样时间。采样时间必须来自于一个线性单调递增的时钟以保证同步及抖动计算。时钟精度必须足以保证时间同步的精确度和测量包到达的抖动（每视频帧一秒是绝对不够的）。

SSRC：32比特

用以识别同步源。标识符被随机生成，以使在同一个RTP会话期中没有任何两个同步源有相同的SSRC识别符。

CSRC列表：0到15项，每项32比特

CSRC列表识别在此包中负载的所有贡献源。

根据上述的封装方式，音视频数据被封装在RTP报文中进行传输。

音视频数据的封装与识别

在对音视频进行封装时，必须对所封装的音视频数据加以标识，以便接收者在接收到音视频数据包之后，可以直接获知封装的数据为那种编码格式。为此，RTP协议规定了一个默认的音视频映射表。RTP发送端在任意给定时间切换RTP负载类型；接收者必须忽略它不能识别的负载类型包。如图4所示：

PT	encoding name	media type	clock rate(Hz)
24	unassigned	V	
25	CelB	V	90,000
26	JPEG	V	90,000
27	unassigned	V	
28	nv	V	90,000
29	unassigned	V	
30	unassigned	V	
31	H261	V	90,000
32	MPV	V	90,000
33	MP2T	AV	90,000
34	H263	V	90,000
35–71	unassigned	?	
72–76	reserved	N/A	N/A
77–95	unassigned	?	
96–127	dynamic	?	
dyn	H263–1998	V	90,000

图4 RTP类型与视频编码格式对应

而采用静态对应的方式已经不能满足编解码格式的增多，为此，RTP协议提供动态对应方式，允许动态分配适合复杂负载格式的使用，同时节约PT域的空间。当今使用的大部分负载格式需要关于负载类型分配的配置，并通过信令来交互。

信令交互协商编解码格式的方式有多种，可以采用SIP协议内的能力协商，也可以直接进行指定，具体的方式在本文中不再加以详述。如有兴趣可以参见附录的参考资料。

音视频数据的传输与控制

实时音视频数据的传输方式则有可能是单播，也有可能是组播。当采用单播时，音视频数据被以点对点的方式进行传输；当采用组播方式传输时，音视频数据被发送到一个组播组内进行传输，而接收者加入该组来接收并进行显示，这种方式是一对多的形式。

为了实现对实时传输音视频数据传输状态的检测和控制，对应的RTP控制协议（RTCP）提出并实施。RTCP协议通过周期性的发送不同类型（主要有5类，发送者报告、接收者报告、源描述项、BYE和APP报文）来通过发送者和接收者的状态，以便发送源和接收端根据信息进行发送和接收数据的调整。

RTP依赖于底层协议来提供RTP数据的多路化。RTP使用偶数目的端口而对应的RTCP流使用紧接下来大的那个奇数端口。RTP和RTCP的端口绝对不能相同，因为RTP依靠端口号来多路传输RTP数据和RTCP控制流。

当音视频数据被正确封装在IP报文中以后，实际的传输则直接采用IP数据传输来实现。对于IP数据的传输和转发，这里就不再赘述。■

与监控中的存储备份和回放

■ 文/李玉天

iVS8000视频监控系统实现为每一路摄像机制定存储计划，使摄像机采集的视频数据在存储计划规定的时段进行存储；通过检索数据库，支持VC（Video Client 视频客户端）对视频数据的快速精确检索，并实现对视频录像信息进行点播回放和备份。

DM服务器和VM服务器是存储、回放、备份流程中非常重要的组件，DM服务器与VM服务器之间保持通信，对存储设备、存储资源以及视频数据进行集中管理。从大量复杂的存储设备管理信息中提取与监控业务相关的信息，实现了对视频监控系统所有存储资源的集中管理和视频数据的高可靠可控存储，支持音视频数据存储、查询和回放等业务功能。

在多域组网环境中，有且仅有一个中心域，集中管理备份资源、备份数据。本地DM管理IP SAN中的SAN数据和ECR中的NAS数据，中心域DM管理除具备本地DM管理功能外，还管理IP SAN中的NAS数据。

系统结构介绍

系统构成主要包括：音视频编解码器、视频管理服务器、视频管理客户端、数据管理服务器、媒体交换服务器、IP SAN、IP NAS存储设备等。可实现实况、存储、备份、回放等业务。

编码器EC

编码器是将模拟的视频、音频信号（如摄像机、麦克风等视音频源信号）转换成数字信号并进行编码压缩的设备，它采用TCP/IP技术，支持单播、组播传送方式。编码器包括EC1101-HF、EC1501-HF、EC1001-HF、EC1004-HC、EC2004-HF、EC2016-HC、EC3016-HC和EC1001八款，其中前七款都支持真双流格式编码、iSCSI和NAS方式存储，并能够外接在带存储功能的ECR系列编码器上统一组网；EC1001支持MPEG2/MPEG4格式编码、iSCSI方式存储，EC1101-HF、EC1501-HF、EC1001集成EPON子卡，支持EPON组网。

视频管理服务器VM

视频管理服务器是整个IP网络监控系统的管理中心，负责管理和协调系统各组件正常工作，包括AS（应用服务视频管理服务器）和CC（呼叫控制视频管理服务器）两个组件。

AS主要提供业务开发支持，以及SIP协议适配层、数据库访问中间层、业务管理模型、框架、基本的SIP协议等业务功能的处理。

CC主要提供终端设备注册、认证、注册状态保活，终端设备状态查询、呼叫的接续、保持、断开，呼叫信息的保活，状态处理。

视频管理客户端VC

视频管理客户端是视频监控系统的主要业务操作和配置终端，分为VC用户版、VC管理员版、VC告警台版三个模块，将业务操作、配置管理与告警分开，每个模块需要单独登录。通过这三个模块的使用，可对编/解码器、摄像机和媒体播放器等进行管理和配置，并进行实时监控、视频回放等监控业务操作，并可查询告警消息。

数据管理服务器DM

数据管理服务器是视频监控系统中的一个重要组件，主要功能是管理存储在IP SAN/IP NAS或ECR设备中的音视频数据，包括定时巡检存储设备并记录数据存储状态、协助EC建立与存储资源的连接、协助VC检索回放音视频数据、备份音视频数据、存储资源状态监控等功能。

IP SAN存储设备

专业的网络存储设备，基于高速以太网的SAN（Storage Area Network，存储区域网络）架构，同时可以提供NAS服务，通过iSCSI（Internet SCSI，Internet小型计算机系统接口）协议来实现存储数据在服务器和存储设备之间高速传输。监控方案主要使用IX1000/VX1500存储海量的音视频数据，为用户提供历史音视频数据点播回放服务。

IP NAS存储设备

NAS（Network Attached Storage—网络附加存储），是一种文件共享服务。拥有自己的文件系统，通过NFS或CIFS对外提供文件访问服务。

NAS包括存储器件（例如硬盘驱动器阵列、CD或DVD驱动器、磁带驱动器或可移动的存储介质）

和专用服务器。专用服务器上装有专门的操作系统，通常是简化的unix/linux操作系统，或者是一个特殊的win2000内核。它为文件系统管理和访问做了专门的优化。专用服务器利用NFS或CIFS，充当远程文件服务器，对外提供文件级的访问。iVS8000方案中目前仅支持EX1000（已停产）、IX1540两款作为IP NAS存储设备。

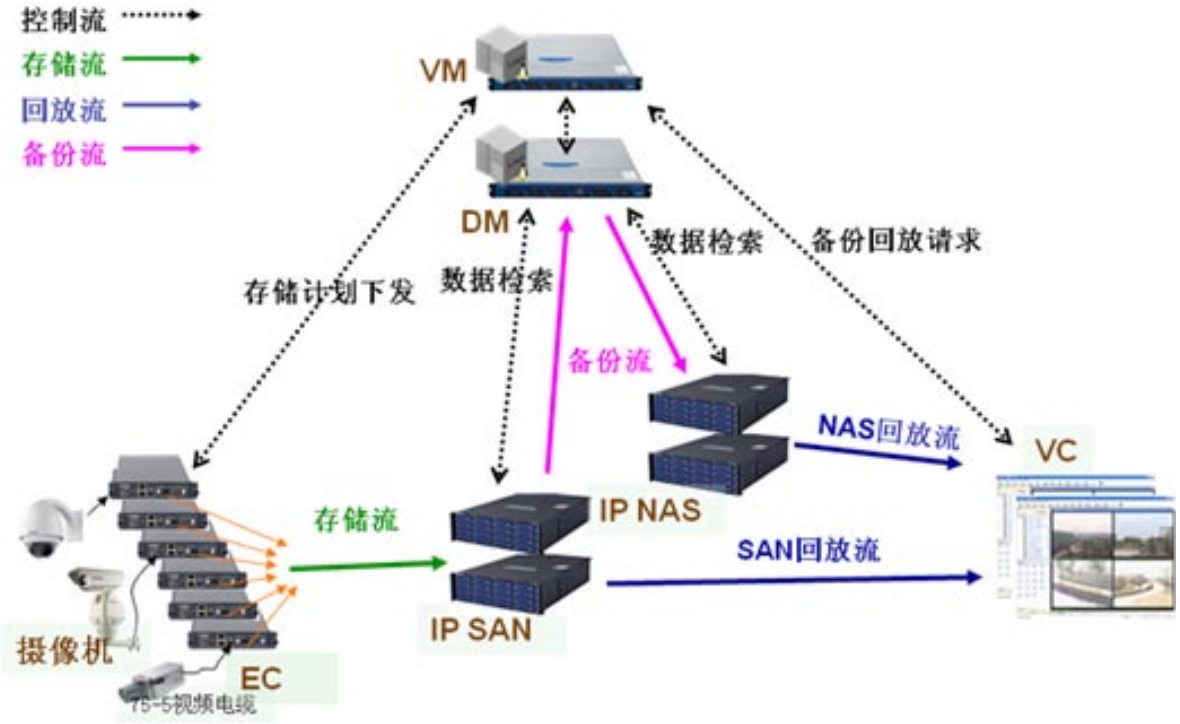


图1 iVS8000监控方案组网图

存储业务

存储功能实现将摄像机采集的视频数据在规定时间内存储到存储设备中。按存储方式不同，可以分为SAN存储和NAS存储。这里仅介绍SAN存储。

在iVS8000系统里，为实现SAN存储，主要分为以下几个步骤：

- IP SAN上创建DMClient、VCClient；
- IP SAN上创建ECClient、SAN资源，并绑定SAN资源；
- 下发存储计划给EC；
- EC挂载SAN资源，启动存储；

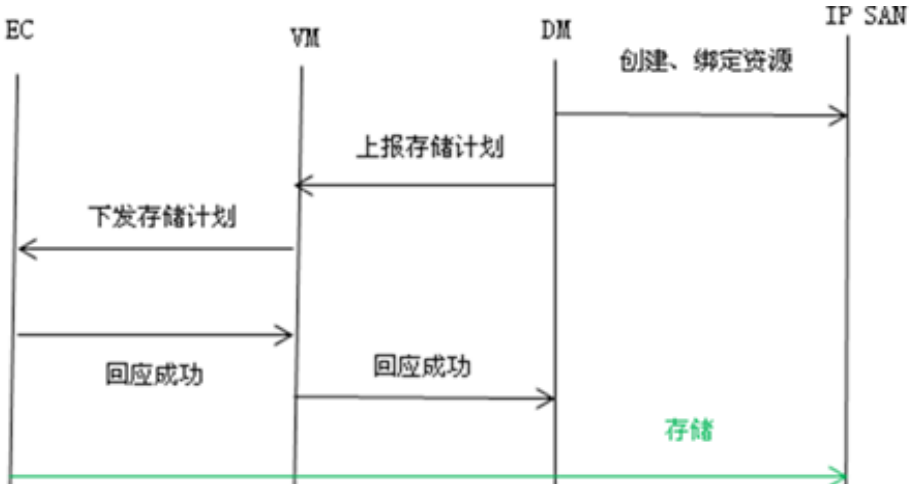


图2 存储计划下发的消息流程图

IP SAN上创建DMClient、VCClient

每添加一台IP SAN设备，DM都会去创建1个DMClient和20个VCClient，分别用于DM和VC客户端对IP SAN上的SAN资源访问。每个DMClient，对应着一个Initiator和一个Target；每个VCClient，对应着一个Initiator和四个Target。一个DMTarget下面可绑定多个SAN资源； 一个VCTarget下面最多只会绑定一个SAN资源。如下图所示：

图3 DM/VC SAN客户端结构示意图

每个摄像机对应着一个存储资源，即上面说到的SAN资源，客户端需要通过Initiator和Target来访问SAN资源。从上面所述的资源绑定关系，我们可以看到，在一台IP SAN上，一台DM可以同时访问多个摄像机的存储资源；而一个VC用户，只能同时访问四个不同的摄像机的存储资源。

IP SAN上创建ECClient、SAN资源，并绑定SAN资源

添加IP SAN设备后，就可以开始给EC摄像机制定存储计划。

首先DM会在指定的IP SAN上创建ECClient和SAN资源；其中SAN资源的大小，需要根据配置的存储码流、存储计划以及留存期计算出来；每个ECClient对应着一个Initiator和多个Target，一个ECTarget最多绑定一个SAN资源。这样，EC可以通过不同的Target，找到相应的SAN资源，写入存储数据。

然后将创建的SAN资源分别与ECTarget、DMTarget进行绑定，这样根据ECTarget和DMTarget就可以访问刚创建好的SAN资源了。

登录IP SAN的控制台，可以看到DMTarget和ECTarget下都已经绑定了SAN资源；如下图所示：

图4 DM/EC SAN客户端结构示意图

下发存储计划给EC

完成SAN资源绑定后，DM会通知VM，同时携带EC存储计划以及IP SAN地址、ECInitiator、ECTarget、端口号等用于访问存储资源的相关信息；由VM将该消息转发给EC。

EC挂载磁盘，启动存储

EC收到VM下发的消息后，根据IP SAN地址、ECInitiator、ECTarget等信息，通过SCSI方式挂载SAN资源，开始写入数据。

在iVS8000方案里，每块SAN资源都会被EC分为超级块、一级块、二级块和数据区四个部分，其中：

超级块有16KB，主要记录EC通道号、录像写入的起止时间等；

一级块，也称主索引，有64KB，主要记录是否已经复写，以及每256MB存储空间，EC写入的开始时间等；

二级块，也称二级索引，有256KB，主要记录每个I帧组（blocks的最小单位是16KB）；

如下图所示：

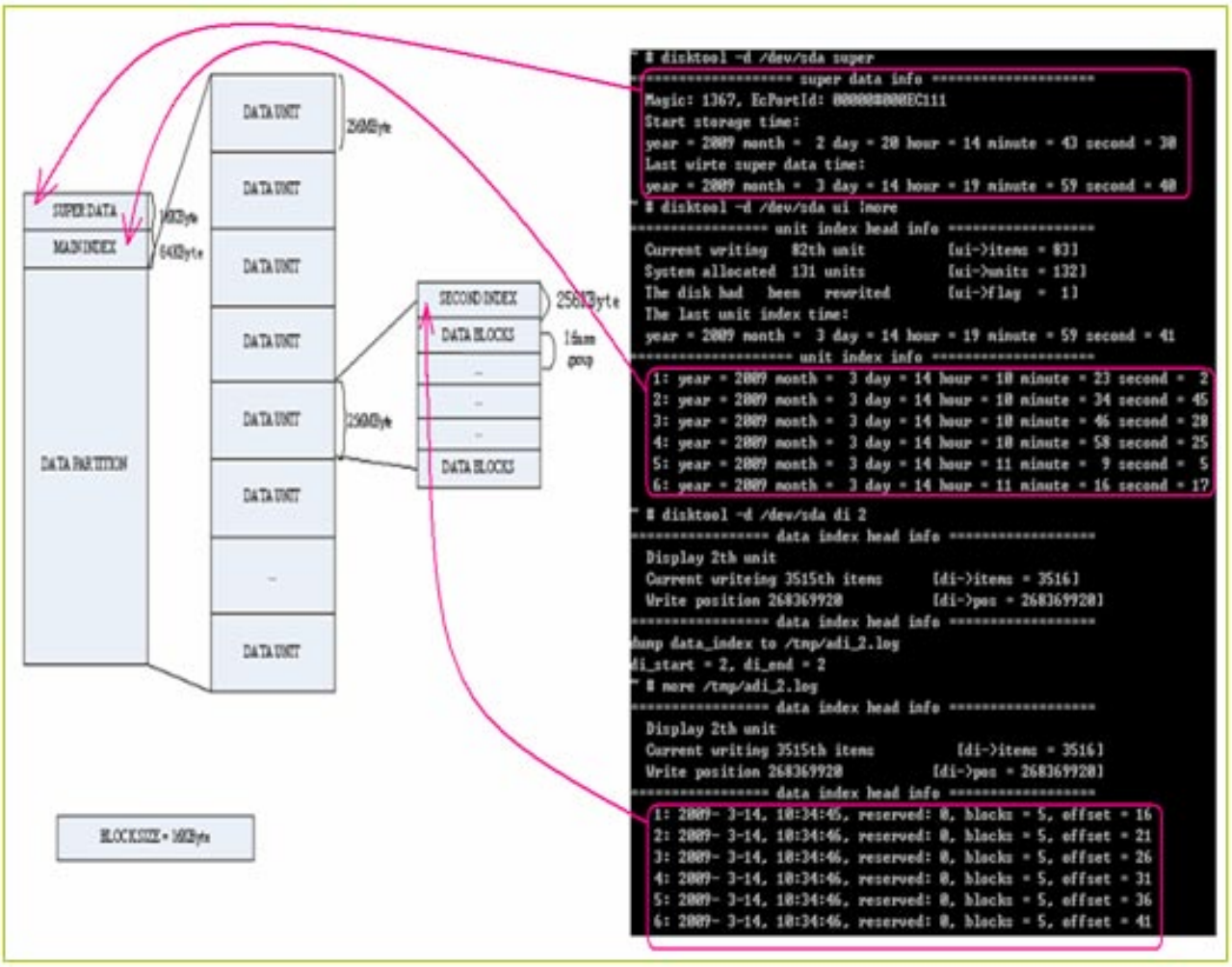


图5 EC SAN存储索引结构图

回放业务

回放功能实现对存储录像按时间检索和回放。

录像检索

1. VC向VM发起数据检索请求，该请求中携带有EC通道号、查询的开始时间以及持续时间等信息；

2. VM收到VC的回放请求后，向DM转发回放请求；

3. DM收到后，按照EC通道号、起始和终止时间检索，查询本地数据库（如果查询的时间段，DM还没来得及巡检，会直接查询IP SAN，即快速检索），然后将该EC通道的存储计划及实际存储的时间段信息返回给VM；

4. VM通知VC在界面上显示出来。

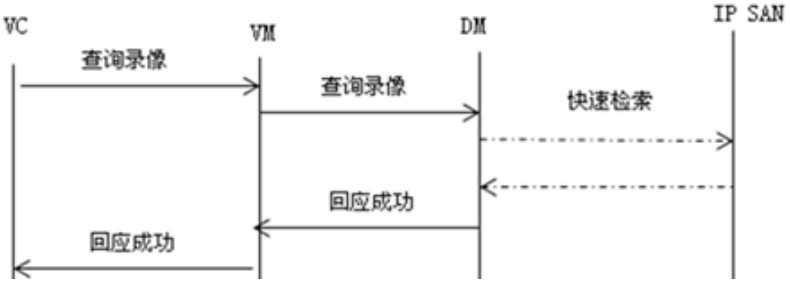


图6 录像查询的消息流程图

点播回放

1. 用户查询检索得到回放录像后，选择所需回放的视频录像，向VM发送回放请求，该请求中携带有EC通道号、查询的开始时间以及持续时间等信息；

2. VM收到VC的回放请求后，向DM转发回放请求；

3. DM收到后，为VC分配资源访问权限，将请求回放的SAN资源挂载到某一个空闲的VCTarget下面，并返回VCInitiator和VCTarget信息；

4. VM收到DM的回应后，向MP转发回放挂载的信息；

5. MP收到后，开始挂载磁盘，成功后给VM回应OK；

6. VM收到后，给VC回应回放请求成功的消息。

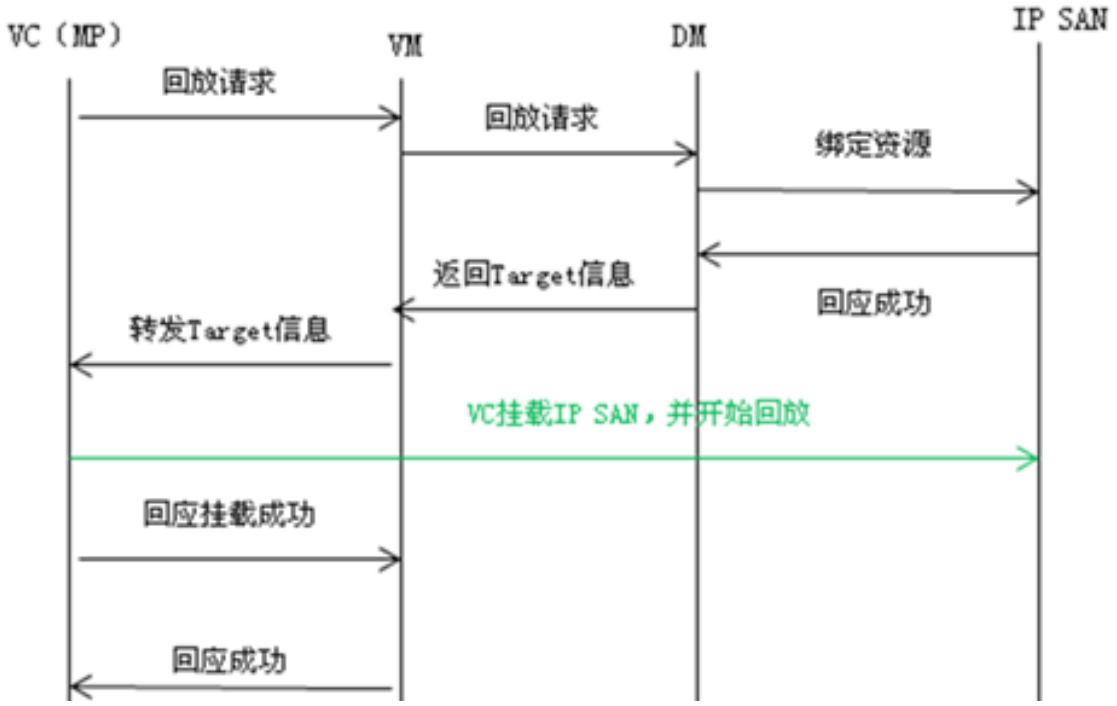


图7 点播回放的消息流程图

备份业务

随着时间的推移，存储资源中的视频数据会不断地被循环覆写，早期的数据将会丢失。视频数据的备份功能，可以将重要的视频数据备份到IP NAS设备中进行长久保存。目前DM支持的IP NAS设备只有EX1000（已停产）和IX1540。

数据备份功能支持多域或单域的组网环境。在多域组网环境中，备份资源和权限管理只由中心域的DM服务器负责，各级各域（包括中心域）的重要数据都集中备份到中心域的IP NAS设备，保证备份数据的安全性和可靠性。在单域组网环境中，备份资源和权限管理由本域的中心DM服务器负责。 简单来说，普通DM仅支持录像的查询回放，而中心DM除支持录像查询外，还支持备份功能。备份分手动备份和自动备份，下面以手动备份为例，进行介绍。

在iVS8000系统里，为实现备份业务，主要分为以下几个步骤：

- 添加IP NAS或IP SAN+NAS设备；
- 添加域资源；

◆ 请求、发起备份；

◆ 备份录像的查询、回放；

添加IP NAS设备

在中心DM上添加一台IP NAS设备后，DM会给自己创建一个NFS客户端；

图8 DM NAS客户端结构示意图（1）

添加域资源

在中心DM上添加域资源，DM分别对IP SAN执行下面几个操作：

1. 创建NAS资源；
2. 设置windows共享；
3. 将NAS资源与DM 客户端绑定；

说明：由于中心DM可支持多个域的备份，各个域资源以域名进行区分，因此创建域资源时，域名需填写正确，否则会导致备份失败。

图9 DM NAS客户端结构示意图（2）

请求、发起备份

1. 首先，在VC上查询一段录像，与回放业务中的录像检索操作一样，这里不再重复说明；
2. 输入案例名称后，发起备份请求；

3. VM收到请求后，发消息给中心DM，携带备份案例名称、备份EC通道号以及备份时间段等信息；

4. 中心DM收到后，将备份路径、登录的帐号等信息返回给VM；

5. VM发消息给备份DM，携带备份路径和备份录像等信息；

6. 备份DM收到消息后，回应OK，然后开始备份（由备份DM将录像数据备份到相应的备份资源中）；

7. 备份完成后，备份DM通知VM，备份完成；

8. VM回应OK，然后通知中心DM，备份完成；

9. 中心DM回应OK，生成备份案例；

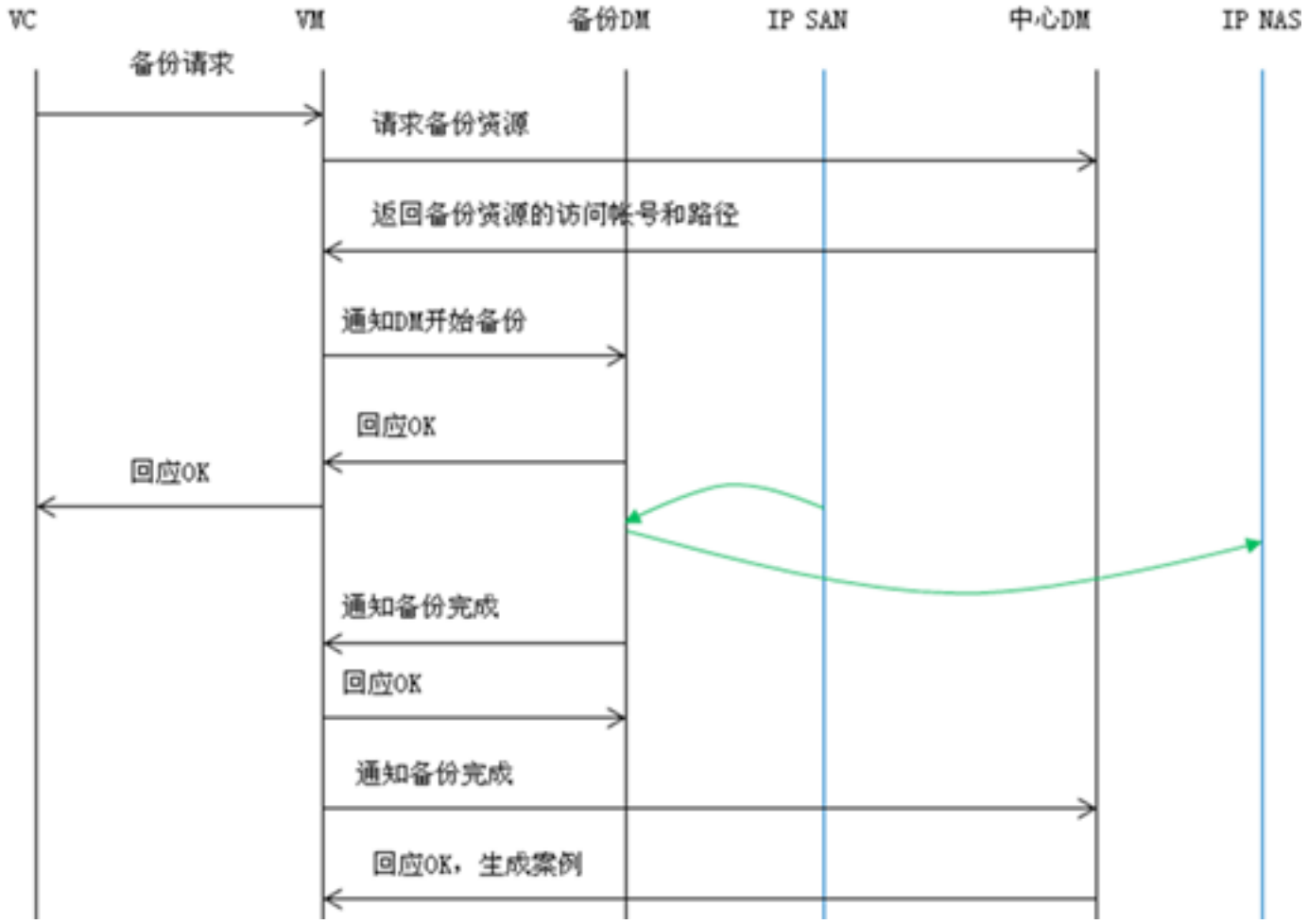


图10 手动备份的消息流程图

说明：备份DM对应的是管理待备份录像的DM；在iVS8000单域系统中，备份DM与中心DM是同一台设备；而在多域系统中，可能会涉及两个VM之间的报文转发，在这里不细说，直接以VM代替。

备份录像的查询、回放

备份录像的查询回放流程与普通的回放业务类似，这里不再重复。■

视频编解码基础概述

■ 文/郭 琪

前言

随着互联网的飞速发展，消费类电子、通信、影视及广播、计算机技术日益紧密地结合起来，使得基于互联网的多媒体产业成为本世纪初发展最快、规模最大的产业之一。

众所周知，人类通过视觉获取的信息量约占总信息量的70%，而且视频信息具有直观性、可信性等一系列优点。但是，多媒体数据在没有经过压缩前，数据量非常大。对于分辨率为720*576的静态图片，如果没有压缩，在RGB空间下需要的存储空间为：

720 * 576 * 3 (byte)=9.49Mb

以每秒25帧的帧率发送该分辨率对应的运动图像需要的传输带宽为：

9.49(Mbits/frame) * 25= 237.3(Mbps)

可见，在不进行数据压缩的情况下，传输的数据量非常大，单纯用扩大存储器容量、增加通信干线的传输速率的办法是不现实的。因此，必须对多媒体数据进行压缩编码，以压缩形式存储、传输，既节约了存储空间，又提高了通信干线的传输效率。所以，视频编码压缩技术是多媒体技术中的关键。

基本概念介绍

像素和分辨率

数字图像是由按一定间隔排列的亮度不同的像点构成的，形成像点的单位称“像素”，也就是说，组成图像的最小单位是像素。一幅图像有很多行组成，而每一行又有很多个像素点组成，很多幅图像连续起来就组成活动的图像。

图像的分辨率是指组成图像的每一个方向上的像素数量。分辨率1024*768，其中“1024”表示水平方向显示的像素点数，“768”表示垂直方向的像素点数。因此，所谓分辨率就是指画面的清晰度，像素点数值越大，图像就越清晰。

目前数字电视标准,按照显示格式的不同，共分为以下5种规格：

D1：480i格式，分辨率为640×480，隔行扫描/60Hz，行频为15.25KHz。

D2：480P格式，分辨率为640×480，逐行扫描/60Hz，行频为31.5KHz。

D3：1080i格式，分辨率为1920×1080，隔行扫描/60Hz，行频为33.75KHz。

D4：720P格式，分辨率为1280×720，逐行扫描/60Hz，行频为45KHz。

D5：1080P格式，分辨率为1920×1080，逐行扫描，专业格式。

其中D1和D2标准是我们一般模拟电视的最高标准，并不能称得上高清晰，D3的1080i标准是高清晰电视的基本标准，它可以兼容720P格式，而D5的1080P只是专业上的标准，不是民用级别的。

色度空间

绝大部分数字视频程序都依赖于彩色视频的显示，这样的话，就需要方法来捕捉并表示颜色信息。一副单色的图像，只需要对空间内的每个像素点的亮度或透明度用一个值表示即可。但对于彩色图像来说，任一像素点至少需要三个数值才能准确表达颜色信息。用来表示亮度和颜色的方法叫做色度空间。

RGB

在RGB色度空间中，一个带颜色的图像采样是用三个值来表示一个像素点的红、绿和蓝色比。任何

颜色都可以通过红、绿、蓝的不同配比得到。

YCbCr

人类视觉系统(HVS)相比亮度而言对颜色不是那么敏感。在RGB色度空间中，三种颜色的重要度相当，并使用相同的分辨率进行存储，数据量很大。通过把图像的亮度信息和颜色信息分离，并使用不同的分辨率进行存储，对亮度值取更高的分辨率，Cb和Cr使用更低的分辨率。这样可以占用极少的带宽，并且不影响图像质量的主观感受。

YCbCr色度空间及其变换(通常写为YUV)是一种流行而高效的表示一个颜色图像的方法。YCbCr是将图像亮度和色度分离的表示彩色图像的方法，Y表示明亮度，Cr和Cb表示色差。其中，Cr反映了RGB输入信号红色部分与RGB信号亮度值之间的差异，而Cb反映的是RGB输入信号蓝色部分与RGB信号亮度值之同的差异。

一帧视频图像：

图 1 原始视频图像

RGB色度空间的视频图像：

Red　　Green　　Blue

图 2 RGB色度空间的视频图像

YUV空间的视频图像：

Y　　Cb　　Cr

图 3 YUV色度空间的视频图像

帧和场

一个视频信号可以逐行扫描或隔行扫描来进行采样。

每一帧画面都自上而下，逐一完成每一条水平扫描线，称作逐行扫描。每一帧画面自上而下，先扫描所有奇数扫描线，再完成偶数扫描线，就是隔行扫描。一幅只含奇数行或偶数行的画面称为一“场(Field)”，其中只含奇数行的场称为奇数场或前场 (Top Field)，只含偶数行的场称为偶数场或后场(Bottom Field)。也就是说一个奇数场加上一个偶数场等于一帧(一幅图像)。

一帧图像在经过编码压缩后，根据编码方式的不同，分不同类型的帧：I帧、P帧和B帧。

I帧（帧内编码帧）是一种自带全部信息的独立帧，无需参考其它图像便可独立进行解码。I帧的缺点在于它们会占用更多的数据位。

P帧（帧间预测编码帧）需要参考前面的I帧和/或P帧的不同部分才能进行编码。与I帧相比，P帧通常占用更少的数据位。

B帧（双向预测编码帧）需要同时以前面的帧和后面的帧作为参考帧。

当视频解码器逐个帧地对比特流进行解码以便重构视频时，必须始终从I帧开始解码。如果使用了P帧和B帧，则必须与参考帧一起解码。

视频编解码流程

典型的视频编解码流程的第一步是将从摄像机输入的视频从RGB色度空间转换到YCbCr色度空间。输入的视频图像通常被分割为互不重叠的宏块分别编码，宏块的大小通常是16x16的亮度块信息和对应的色度块信息，然后使用分块的运动补偿从已编码的帧对当前帧的数据进行预测，接着使用块变换或者子带分解来减少空域的统计相关性。最常见的变换是8x8的离散余弦变换(DCT Discrete cosine transform)，对这些小方块的数据从空间域转换到频域。变换的输出系数接下来被量化，量化后的系数进行熵编码并成为输出码流的一部分。

源编码器的一般形式如下图4所示：

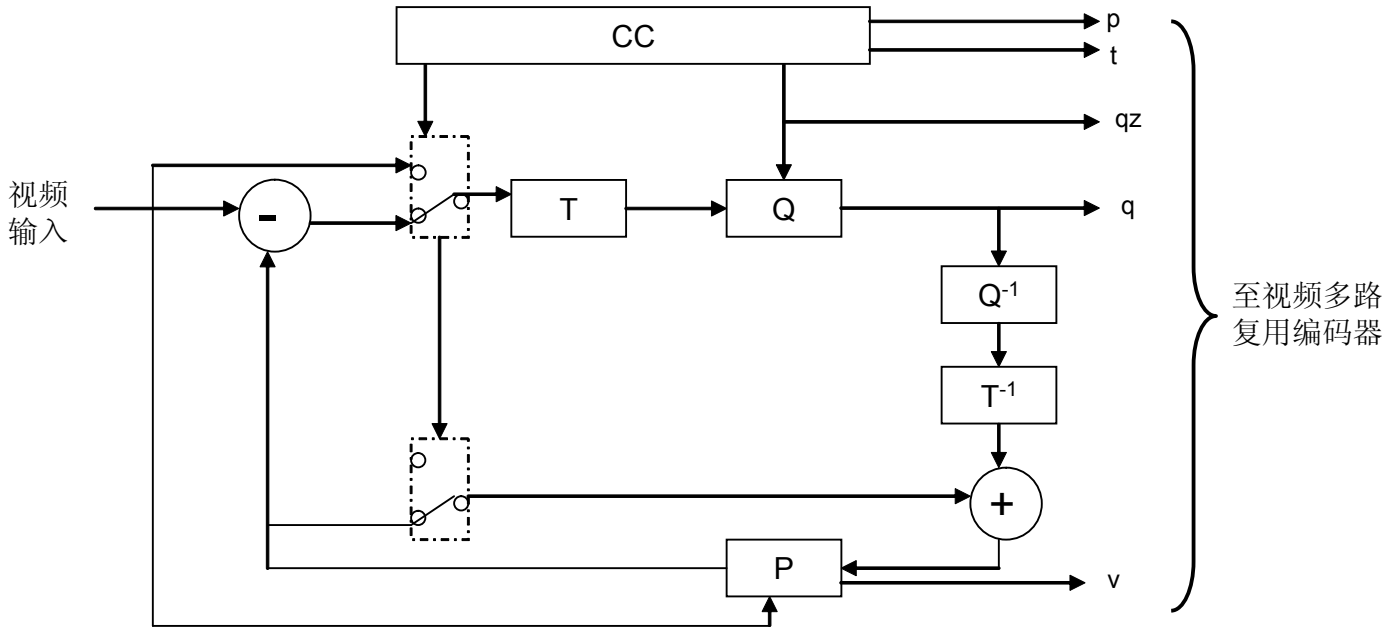


图 4 编码器的一般形式

T ——变换

Q ——量化器

P ——具有运动补偿可变延迟的图像存储器

CC——编码控制

p —— INTAR/INTER方式标记

t ——传输与否标记

qz ——量化器指示

q ——变换系数的量化索引号

v ——运动矢量

下面对编码过程中的几个主要环节作深入的阐述。

采样

采样是指用每隔一定时间的信号样值序列来代替原来在时间上连续的信号，也就是在时间上将模拟信号离散化。

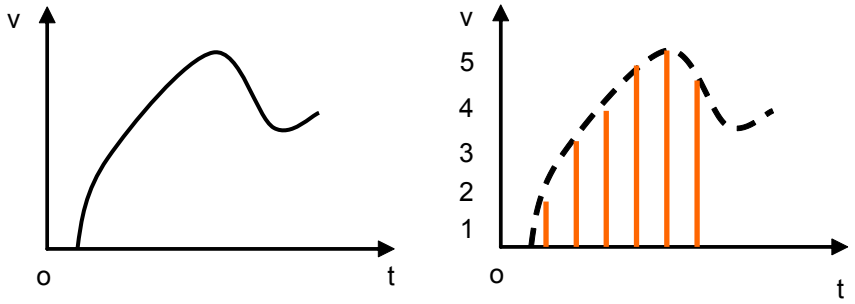


图 5 采样

一个自然视频场景在空间和时间上是连续的。数字视频就是在数字形式下的一个视频场景的空间采样和时间采样的表示方式。每一个时–空采样（像素）用一个数或一组数来表示，用来描述采样点的亮度和色度。

空间采样通常是通过在视频图形面上用长方形格处理，对于每个格交点处的点进行采样。选择粗糙的采样格会得到低分辨率的采样图像，而增加采样点的数量就会增加采样图像的分辨率。

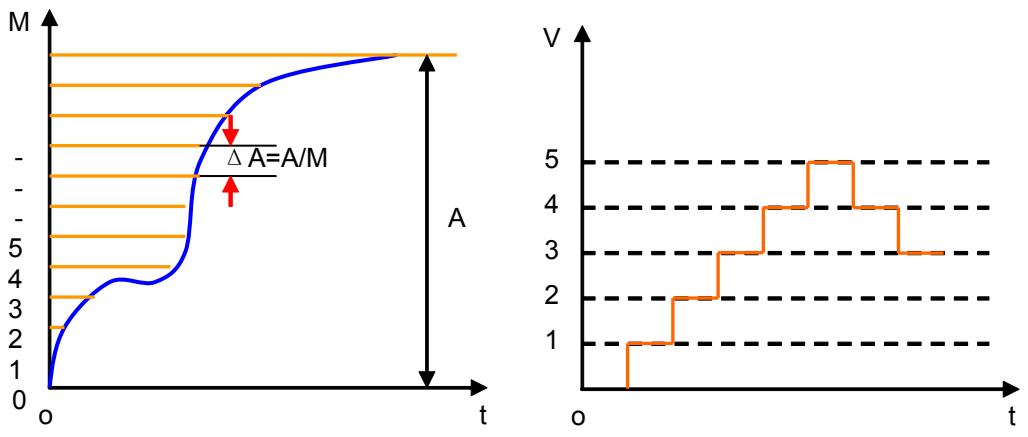
一个可动的视频图像是通过对信号在周期性的时间间隔上进行快照得到的。重放这一系列的帧会得到运动的效果。一个高的时间采样率(帧率)会产生更加平滑的运动，相对应就有更多的采样需要被捕捉和保存。

量化

量化是在幅度轴上，把模拟信号的连续幅度变为有限数量的、有一定间隔的离散值。

在时间轴上已变为离散的样值脉冲，在幅度轴上仍会在动态范围内有连续值，可能出现任意幅度，故还必须用有限电平等级来代替实际量值。量化的过程是把取样后信号的电平归并到有限个电平等级上，

并以一个相应的数据来表示。



量化等级的划分

图 6 量化

编码

编码则是按照一定的规律，把量化后的值用二进制数字表示，然后转换成二值或多值的数字信号流。

具体说来，就是用n比特二进制码来表示已被量化的样值，每个二进制数对应一个量化值，然后把它们排列，得到由二值脉冲组成的数字信息流。

表 1 量化编码对应表

量化电平	自然 二进制码
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

视频信号有两种编码方式，即复合编码和分量编码。复合编码是将复合彩色信号直接编码成PCM形式。复合彩色信号是指彩色全电视信号，它包含有亮度信号和以不同方式编码的色度信号。分量编码将三基色信号R、G、B分量或亮度和色差信号Y、(B－Y)、(R－Y)分别编码成PCM形式。

压缩

视频图像数据有极强的相关性，也就是说有大量的冗余信息。其中冗余信息可分为空域冗余信息和时域冗余信息。空域冗余是指同一时间的视频图像，在空间上存在的冗余信息。时域冗余是指前后时间的视频图像间具有相似性，而存在的冗余信息。压缩技术就是将数据中的冗余信息去掉，压缩技术包含帧内图像数据压缩技术、帧间图像数据压缩技术和熵编码压缩技术。

预测法是最简单和实用的视频压缩编码方法，经过压缩编码后传输的并不是像素本身的取样值，二是该取样的预测值和实际值之差。

为什么取像素预测值与实际值之差作为传输的信号？因为大量统计表明，同一幅图像的邻近像素之间有着相关性，或者说这些像素值相似。邻近像素之间发生突发或“很不相似”的概率很小，而且同帧

图像中邻近行之间对应位置的像素之间也有较强的相关性。人们可以利用这些性质进行视频压缩编码。

通过帧内预测消除同一副图像内的冗余信息，帧间预测使用基于块的运动矢量消除不同图像间的冗余，再通过对预测残差进行变换和量化消除图像内的视觉冗余，最后，运动矢量、预测模式、量化参数和变换系数用熵编码进行压缩，以消除编码码字冗余。

下面对上述压缩技术作详细的介绍。

帧内/帧间预测编码

帧内预测编码和帧间预测编码是两种不同的编码压缩方式，均用于消除视频图像中存在的冗余信息。 由于帧内压缩和帧间压缩分别用于消除不同的冗余，因此，这两种压缩方式常同时使用，以获得最大的压缩效果。

帧内压缩又可分为空域和频域预测压缩。空域预测是对一幅图像，通过周边的像素点的值估计当前块的像素点的值，仅考虑本帧的数据而不考虑相邻帧之间的冗余信息；频域预测则是通过周边块的AC/DC系数，预测当前块的AC/DC系数。

帧间压缩是基于许多视频或动画的连续前后两帧具有很大的相关性，或者说前后两帧信息变化很小的特点。根据这一特性，帧间压缩用于压缩相邻帧之间的冗余量，进一步提高压缩量，减小压缩比。一般而言，帧间预测编码的编码效率比帧内更高。

运动估计和运动补偿

在帧间预测编码中，由于活动图像邻近帧中的景物存在着一定的相关性，即当前画面上的图像可以看成是前面某时刻画面上图像的位移，位移的幅度值和方向在画面各处可以不同。因此，可将活动图像分成若干块或宏块，并设法搜索出每个块或宏块在邻近帧图像中的位置，并得出两者之间的空间位置的相对偏移量。得到的相对偏移量就是通常所指的运动矢量，得到运动矢量的过程称为运动估计。

利用运动位移信息与前面某时刻的图像对当前画面图像进行预测的方法，称为前向预测。反之，根据某时刻的图像与位移信息预测该时刻之前的图像，称为后向预测。

基于块的运动估计和运动补偿考虑到视频序列中构成新帧的大量信息都可以在前面的帧中找到，但可能会在不同的位置上。所以将一个帧分为一系列的宏块。然后，通过在参考帧中查找匹配块的方式，逐块地构建或者“预测”一个新帧（例如P帧）。如果发现匹配的块，编码器只需要对参考帧中发现匹配块的位置进行编码。与对块的实际内容进行编码相比，只对运动矢量进行编码可以减少所占用的数据位。

运动矢量和经过运动匹配后得到的预测误差共同发送到解码端，在解码端按照运动矢量指明的位置，从已经解码的邻近参考帧图像中找到相应的块或宏块，和预测误差相加后就得到了块或宏块在当前帧中的位置。

通过运动估计可以去除帧间冗余度，使得视频传输的比特数大为减少，因此，运动估计是视频压缩

处理系统中一个重要的组成部分。

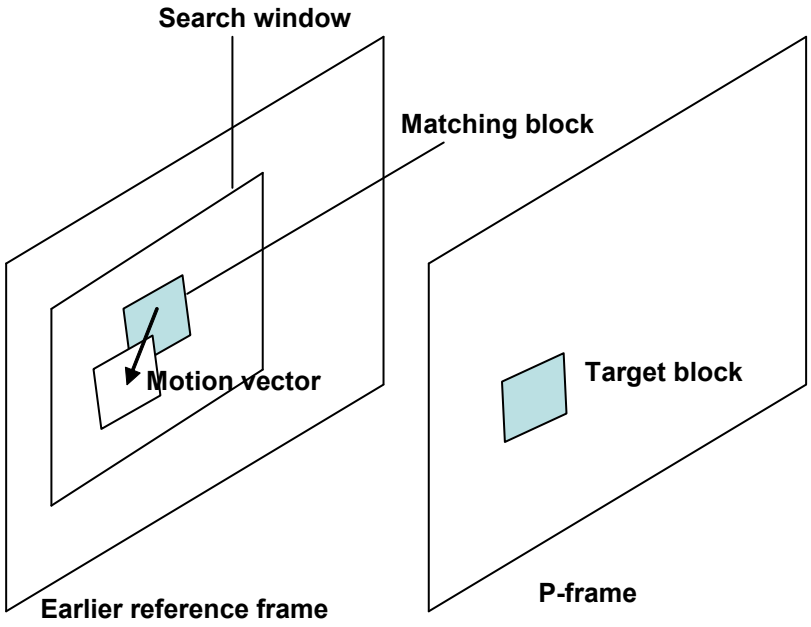


图 7 基于块的运动估计和运动补偿

图7文字：

Search window	搜索窗口
Matching block	匹配块
Motion vector	运动矢量
Target block	目标块
Earlier reference frame	前面的参考帧
P–frame	P帧

变换编码

绝大多数图像都有一个共同的特征：平坦区域和内容缓慢变化区域占据一幅图像的大部分，而细节区域和内容突变区域则占小部分。也可以说，图像中直流和低频区占大部分，高频区占小部分。这样，如果将空间域的图像变换到频域或所谓的变换域，就会产生相关性很小的一些变换系数，并可对器进行压缩编码，即所谓的变换编码。

常见的变换编码有K–L变换、离散余弦变换（DCT）等。编码性能以K–L变换最理想，但缺乏快速算法，且变换矩阵随图像而异，不同图像需计算不同的变换矩阵，因而只用来参考比较。DCT编码性能最接近与K–L变换，略次而已，但它具有快速算法，广泛应用于图像编码。

熵编码

利用信源的统计特性进行码率压缩的编码方式称为熵编码，也叫统计编码。视频编码常用的有两种：变长编码（也称哈夫曼编码）及算术编码。

解码

解码基本上执行和编码的过程完全相反的过程。其中不能被完全恢复原来信息的步骤是量化。这时候，要尽可能接近的恢复原来的信息。这个过程被称为反量化，尽管量化本身已经注定是个不可逆过程。

视频编解码标准

目前视频流传输中最为重要的编解码标准有国际电联的H.261、H.263，运动静止图像专家组的M-JPEG和国际标准化组织运动图像专家组的MPEG系列标准，此外在互联网上被广泛应用的还有Real-Networks的RealVideo、微软公司的WMT以及Apple公司的QuickTime等。

表2说明目前流行的视频编解码标准的特点，以及各自的优缺点：

表 2 各视频编解码标准说明

标准	主要特点	优点	缺点
MJPEG	基于静态视频压缩发展起来的技术，它的主要特点是基本不考虑视频流中不同帧之间的变化，只单独对某一帧进行压缩。	可以获取清晰度很高的视频图像，可以动态调整帧率、分辨率。	没有考虑到帧间变化，造成大量冗余信息被重复存储，因此单帧视频的占用空间较大，目前流行的MJPEG技术最好的也只能做到3K字节/帧，通常要8~20K。
MPEG-1	主要针对CIF标准分辨率(NTSC制为352X240；PAL制为352X288)的图像进行压缩.压缩位率主要目标为1.5Mb/s。	较MJPEG技术，MPEG1在实时压缩、每帧数据量、处理速度上有显著的提高。	存在存储容量还是过大、清晰度不够高和网络传输困难的缺点。
MPEG-2	在MPEG-1基础上进行了扩充和提升，和MPEG-1向下兼容，主要针对存储媒体、数字电视、高清晰等应用领域，分辨率为：低(352x288)，中(720x480)，次高(1440x1080)，高(1920x1080)。	MPEG-2视频相对MPEG-1提升了分辨率，满足了用户高清晰的要求。	由于压缩性能没有多少提高，使得存储容量还是太大，也不适合网络传输。
MPEG-4	相对于MPEG-1/2在低比特率压缩上有着显著提高。	1）从清晰度和存储量上都比MPEG1具有更大的优势，更适合网络传输。 2）可以方便地动态调整帧率、比特率，以降低存储量。	
H.264	集中了以往标准的优点，在许多领域都得到突破性进展，使得它获得比以往标准好得多整体性能	1)和H.263+和MPEG-4 SP相比最多可节省50%的码率，使存储容量大大降低； 2)H.264在不同分辨率、不同码率下都能提供较高的视频质量； 3)采用“网络友善”的结构和语法，使其更有利于网络传输。	

IP监控中的音视频质量提升

■ 文/吴参毅

音视频质量是视频监控的核心，它体现了多媒体产品的品质与主观体验。针对监控业务的实际应用，应用以下几种方案能够有力的提升监控产品的核心价值。

低带宽下的场景切换图像质量优化方案

目前视频监控系统中，在低带宽下，由于压缩率较大，在快速运动或复杂场景下，图像质量下降较大，而在静态场景或者运动量较小、低复杂度场景下，图像质量相对较清晰。这样，在复杂或者快速运动场景切换至静态或低复杂场景的过程中，存在一个从模糊、质量较差到清晰、质量较好的过程。为了使这个过渡过程快速完成，视频监控中的视频编码器大多采用INTRA宏块(MB)刷新模式。即编码器的带宽降低时，或者场景复杂度上升时，通过使用INTRA宏块刷新，避免误差持续扩散造成图像质量恶化，以保证图像质量恒定。

INTRA宏块刷新技术，只对每帧的若干宏块进行随机刷新，造成每帧的图像质量不均匀。方块效应更加明显，并且方块在动态的变化，给人造成较差的主观感觉。另外，方块效应的动态变化，从主观上，也加重了色偏的感觉——整体图像色彩不均匀或者色偏现象。并且，利用INTRA宏块刷新技术，图

像从较差质量到较好质量的恢复速度较慢。

针对低带宽下，视频场景变换，尤其是帧和帧之间变换较大，图像方块效应动态变化、色彩不均匀以及图像从较差质量到较好质量的恢复速度等问题，可采用如下解决方案。该方案分为两个部分：

场景切换检测

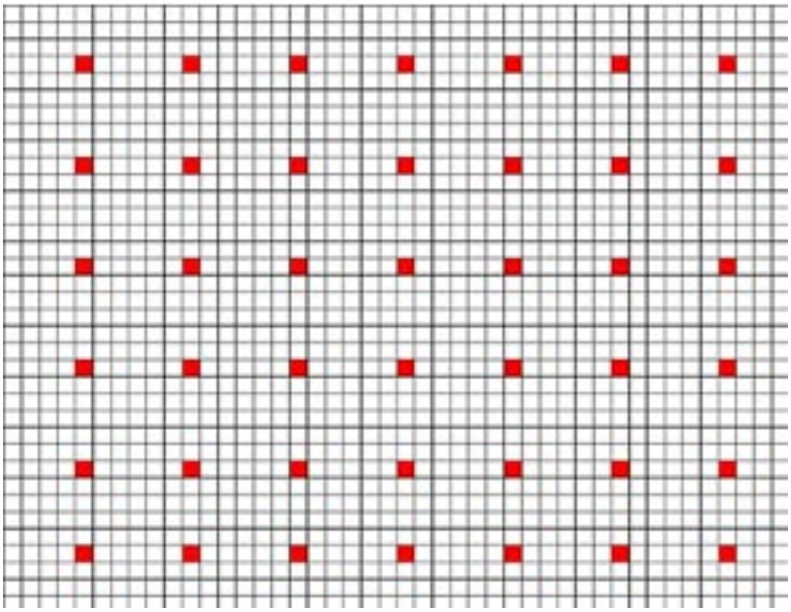


图1场景检测基准点

在一帧图像中，以中心位置的K个宏块为检测基准点。图1为场景检测基准点示意图（K=42为例）。第 个MB的运动矢量MV表示为

(x_n, y_n)， n为第n个MB。 (1)

首先，分别计算每帧基准检测MB运动矢量在 和 轴方向上的偏移量的绝对值之和：

$$X_{offset} = \sum_{K}^{n=1} | x_n | \quad (2)$$

$$Y_{offset} = \sum_{K}^{n=1} | y_n | \quad (3)$$

然后，分别计算当前帧的前 帧中的前 帧 的和 的和，以及后 帧 的和 的和（包括当前帧）：

$$FrontX_m = \sum_{m}^{n=1} X_{offset,n} \quad (4)$$

$$FrontY_m = \sum_{m}^{n=1} Y_{offset,n} \quad (5)$$

$$BackX_m = \sum_{m}^{n=1} X_{offset,n} \quad (6)$$

$$BackY_m = \sum_{m}^{n=1} Y_{offset,n} \quad (7)$$

最后，计算前m帧和后m帧在 和 轴方向上的偏移量和的比值：

$$a = \frac{FrontX_m}{BackX_m} \quad (8)$$

$$b = \frac{FrontY_m}{BackY_m} \quad (9)$$

I帧消除累积误差

在低带宽下，当从相对静态的场景切换到动态场景，或者从相对动态的场景切换到静态场景时，图像质量都会存在一个从清晰到模糊，然后再从模糊到清晰的过程。显然，从模糊到清晰的转变过程，所耗费的时间越短越好，并且在带宽一定的情况下，无论时间长短，总会存在模糊的瞬间感受。

由此，使用上述场景切换检测方法，在检测到场景切换达到一定要求的情况下，通过编码一个I帧，缩短模糊到清晰的转换时间。以m = 3为例，蓝色表示P帧，红色表示I帧，编码一个I帧进行消除累积误差，加速图像从模糊到清晰的恢复速度，取决于：

$$j = ga + hb \quad (10)$$

式(10)中，γ ，η 表示x和y轴方向上的系数因子，且 $\gamma \in [0,1], \eta \in [0,1]$ 。例如：当满足 $\varphi > 150$ ，任务发生场景切换，插入I帧。如图2所示，以3帧为一组进行检测，比如当前帧为第6帧时，计算得知满足条件，下一帧（第7帧）编码为I帧，如图3所示。

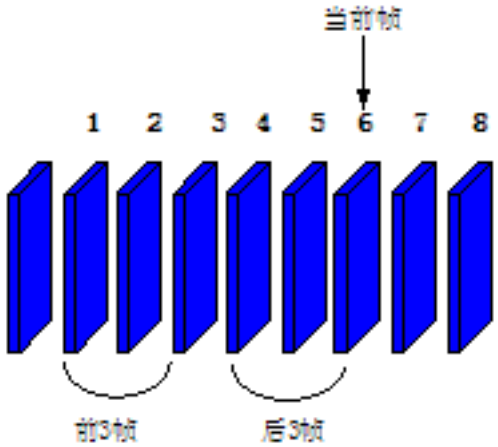


图2 第六帧时检测到条件满足

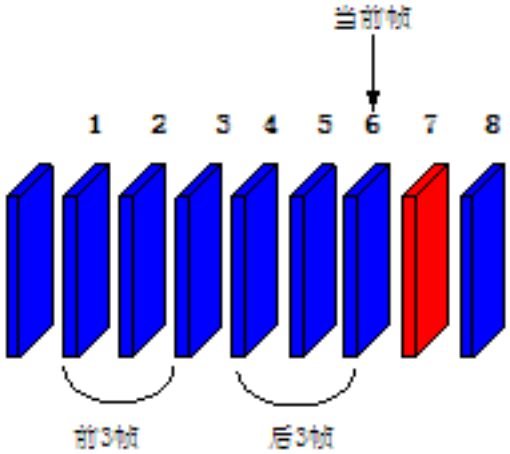


图3 第七帧编码为I帧消除累积误差

使用该种方案，在低带宽下的视频通信应用领域中，提高了视频图像场景切换从模糊到清晰的速度，保证了整体视频图像质量。

解交织处理方案

视频监控中对隔行扫描的视频源，直接通过视频编码压缩得到的效果并不好，目前的H.264等视频压缩标准都支持对场模式的编码。业界通用的解决办法是在编码端做场模式编码，在解码端进行解交织处理。这样的处理方法在低带宽下压缩效率较低，解码恢复图像效果不好。传统的解码端进行解交织的方法，会导致编码性能不高，损伤图像质量，同时增加了解码端的计算开销。

下面将要介绍的一种方案，解决常规方案增加的计算负荷和编码质量较低的问题。结合视频编码信

息在编码端进行解交织处理，通过编码过程得到的运动矢量信息，控制解交织滤波器的强度，降低计算复杂度，在带宽受限的情况下，提高编码质量。

该方案的具体实施如图4。包含视频采集器（CA）、解交织处理器、视频编码器，编码码流通过网络传输到目的端。视频采集器（CA）将采集的数字图像信号输入到解交织处理器中，解交织处理器根据编码器送来的运动矢量信息进行自适应解交织处理，处理后的图像数据传给编码器，得到的视频码流发送到网络中。

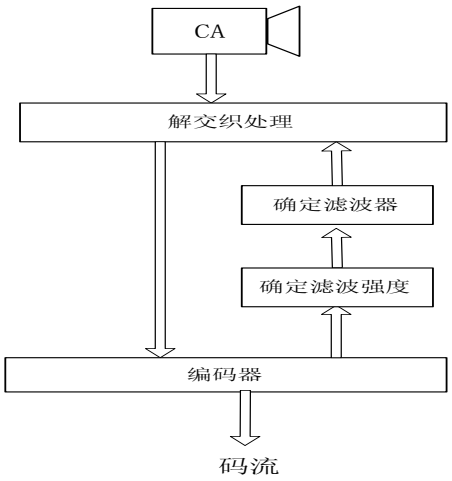


图4 系统解交织方案框架图

图5是实时解交织处理系统的功能模块图。解交织处理模块有两个输入：CA模块的视频数据和视频编码器传送的运动矢量信息。自适应处理模块根据运动矢量信息计算出进行解交织处理的滤波强度，利用得到的滤波强度，滤波模块不需要根据视频图像内容进行非常复杂数据分析，就可选择出合适的滤波器和滤波模式，根据滤波模式选择对CA模块输入的数据进行相应处理，得到解交织处理后的图像。最后，把处理后的图像送入编码器进行编码和网络传输，解码端直接把恢复的视频图像送到显示单元，不需要额外的计算开销。

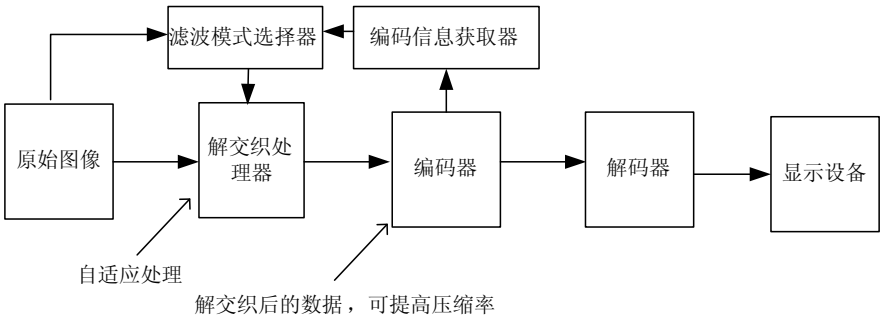


图5 实时解交织处理系统的功能模块图

该方案解决了带宽受限的情况下，在编码侧使用很少的计算负荷，完成了解交织的处理，并提升了压缩率，不增加解码端的性能开销。

背景噪声抑制方案

实际监控系统中应用环境的复杂性在音频采集音方面表现为拾音范围广、背景嘈杂，导致各种干扰源会被拾音设备采样，严重影响音频效果。同时随着监控系统的IP化发展，不同厂商设备的互联互通不可避免，各厂商设备质量有差别，如何保证基于不同设备厂商部署的系统保持一致音频效果也迫在眉睫。

通常需要从前端考虑提高音频信号质量，常见的做法是选用性能较好的拾音设备，达到抑制部分噪声的目的。虽然有些拾音设备带有一定的噪声抑制功能，但它们都是在硬件上通过滤波手段过滤带外噪声，但在音频频带内的噪声无能为力。同时有些内部集成了DSP，由于DSP本身的性能不高，处理能力一般，只能完成一些简单的处理算法，对噪声环境的适应性很低，而且价格高的惊人，性价比很低。

针对第二个问题，如果采用第一个问题的解决思路，可以在前端考虑尽量配备相当规格的拾音设备，提高前端的信号质量，从而保证后端的呈现效果尽量一致。假设不考虑各设备接口类型的差异，上述策略可行。但如果要在一个涉及不同地域的广域型IP监控系统内完成一次成千上万监控点的全网部署和升级是一件成本多么高昂、多么困难的事件。

现在的芯片处理能力越来越强、数字信号处理技术越来越灵活、实用。在监控系统后端处理中心利用高性能的通用CPU处理器或高性能数字信号处理器，实现一套复杂的信号处理算法已经没有任何的瓶颈。我们针对监控系统对音频要求的特点，提出一种基于软件来解决上述问题的方法及装置。该方法和装置的部署可以自适应的学习和抑制环境背景噪声，基于现场环境特点，动态自适应的调整抑制程度，提高监控系统中的音频呈现效果，解决系统中异构设备组网下音频效果一致性问题。

该方案提供一种针对非稳态环境下的自适应背景噪声抑制(ANS)算法，并将其部署在音视频业务层的客户端和解码器侧。对监控接入层传来的音频采集编码码流在解码回放前进行一次统一的噪声抑制处理，处理基于背景噪声估计，动态的调整噪声抑制程度，到达屏蔽前端音频采集差异，增强音频呈现效果目的。

图6中，监控接入层编码器负责音频信号的采集和编码，不限定前端采集必须利用昂贵的拾音器材来保证采集音频的纯净，即允许编码发送的音频码流是含背景噪声的。在音频应用层的解码器侧接收前端码流，完成解码后将含噪音频原始数据输入到ANS处理模块，基于算法的自适应学习能力，完成背景噪声的估计及滤除，然后送后级播放呈现。基于ANS的自适应学习特性，在解码侧切换前端码流后能够重新学习、估计，保证后端对前端的适应跟踪。

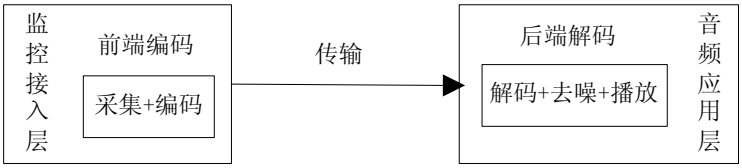


图6 系统结构图

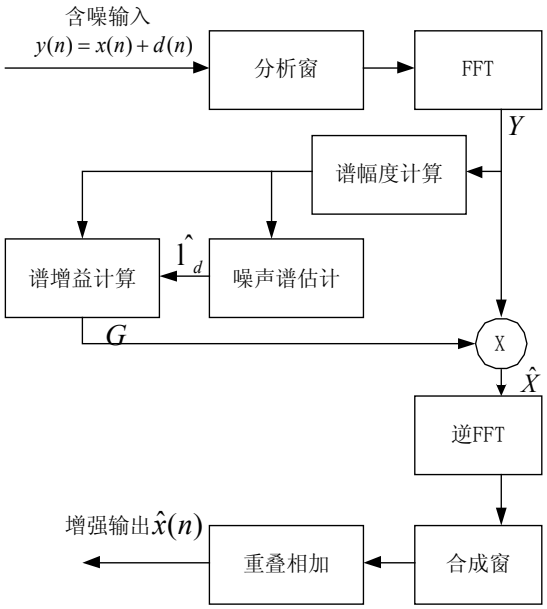


图7 ANS流程框图

图7是自动噪声抑制算法的流程图，设原始语音信号为X(n) ,受到与X(n) 不相关的加性宽带噪声d(n)干扰的带噪语音为y(n) 。设第l帧加窗语音、噪声和带噪语音信号的第k个短时谱幅度分量分别为X(k,l)、D(k,l)、Y(k,l) 。带噪语音短时谱的相位为$\varphi_y(k,l)$,噪声方差为$\lambda_d(k,l)$ 。数学公式表示如下：

$$y(n)=x(n)+d(n) \qquad <1>$$

$$Y(k,l)=\sum^{N-1} y(n+lM)h(n)e^{-j(2p/N)nk} \qquad <2>$$

语音信号的短时谱幅度估计就是基于带噪语音信号的短时谱幅度，用某种最优准则求出X(k,l)的估计$\hat{X}(k,l)$。我们基于最小均方误差准则的短时对数谱估计(MMSE–STSA)目标函数如下

$$E\{(\log\ A(k,l)-\log\ \hat{A}(k,l))^2\} \qquad <3>$$

其中：

$$A(k,l)=|X(k,l)|$$

$$\hat{A}(k,l)=\exp\{E[\log A(k,l)\,|\,Y(k,l)]\}$$

基于该准则的目标函数最小化为目标，我们将语音增强理解成一个滤波过程，即增强语音谱的估计可以表示为带噪语音短时谱与一个增益函数G(k,l)乘积，即

$$\hat{X}(k,l)=G(k,l)Y(k,l) \qquad <4>$$

最后利用人耳听觉对语音相位变化不敏感的特性，我们用带噪语音的相位信息通过逆傅立叶变换重构出纯净的语音信号$\hat{x}(n)$

$$\hat{x}(n)=\sum\sum^{N-1}\hat{X}(k,l)\tilde{h}(n-lM)e^{j(2p/N)k(n-lM)} \qquad <5>$$

从流程图看语音的增强处理重点在增益函数G(k,l)的计算，具体过程见下文。

图8是本文改进的增益函数的计算模型图。传统的MMSE算法计算增益函数时总是基于处理的信号全部是语音的假设，没有考虑实际环境中信号还存在无语音的噪声段，语音信号是概率出现的，导致在噪声段的估计偏差大。基于传统MMSE算法的改进引入了语音概率，变形的增益公式如公式<7>所示，表示的是语音段增益估计和噪声段增益估计的加权，算法中的G_{MIN}是基于现场噪声的经验估计值，通常是一个静态常量。由于监控系统中的现场环境千差万别，导致背景噪声差异很大，所以应用中无法用一个固定经验值来表征环境噪声，为此我们提出一种基于现场环境来自适应的计算更新G_{MIN}的方法，通过当前信号的幅度谱及噪声估计值，计算信号的信噪比，基于信噪比和G_{MIN}的线性关系更新 值。

经典MMSE–STSA的增益函数如下：

$$G_{MMSE}(k,l)=\frac{\mathrm{x}(k,l)}{1+\mathrm{x}(k,l)}\exp\left(\frac{1}{2}\int_{v(k,l)}^{\infty}\frac{e^{-t}}{t}dt\right) \qquad <6>$$

其中：$\mathrm{x}(k,l)=\frac{1_x(k,l)}{1_d(k,l)}$，$\mathrm{g}(k,l)=\frac{|Y(k,l)|^2}{1_d(k,l)}$，$v(k,l)=\frac{\mathrm{g}(k,l)\mathrm{x}(k,l)}{1+\mathrm{x}(k,l)}$

$\xi(k,l)$表示先验信噪比， $\gamma(k,l)$表示后验信噪比

本方案改进的自适应增益函数计算公式如下：

$$G(k,l)=\{G_{MMSE}(k,l)\}^{p(k,l)}G_{MIN}^{\;1-p(k,l)} \qquad <7>$$

其中：$p(k,l)=\{1+\frac{q(k,l)}{1-q(k,l)}(1+\mathrm{x}(k,l)\exp(-\mathrm{n}(k,l))\}^{-1}$

表示条件语音出现概率

$q(k,l)$表示先验语音缺失概率 。

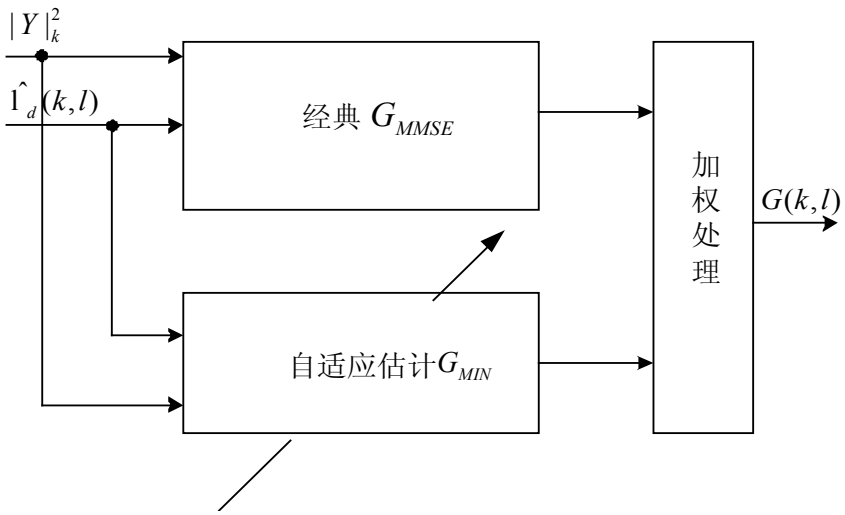


图8 增益计算框图

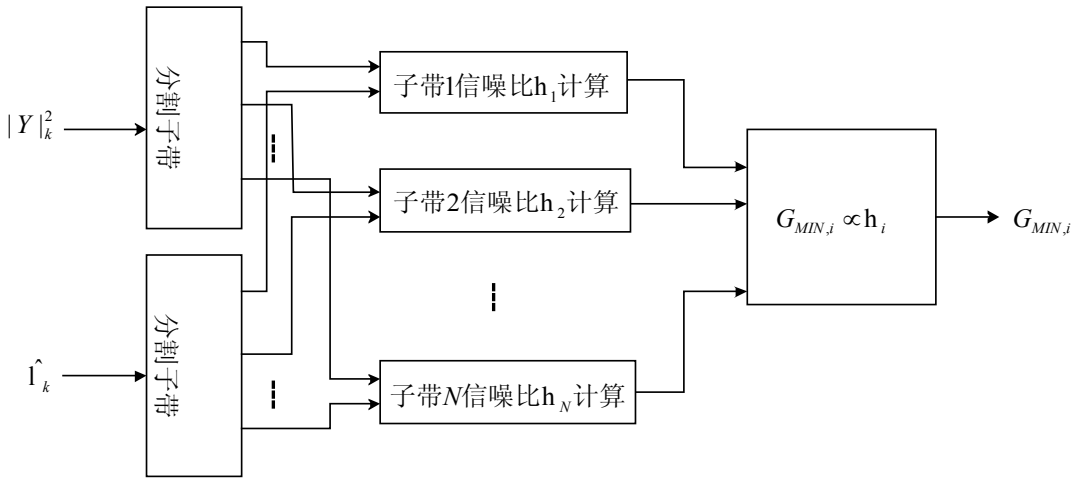


图9 增益常量计算框图

图9是增益常量G_{MIN}的自适应计算、调整过程。G_{MIN}的计算更新基于如下基本原理：在信噪比高时，语音成分重，通过设置较大的噪声抑制阈值，能够达到保证语音的前提下尽可能的抑制噪声；在信噪比低时，语音成分轻，通过设置较小的噪声抑制阈值，能够抑制噪声的同时保证尽量少的损伤语音。从而使得算法具有良好适应性，保证不同场景下都有较高的语音清晰度。另外，由于人耳对语音各频段的感知不同，对低频段的信号感知更灵敏。利用该特性，将信号分割成多个子带，在每个子带内分别计算更新G_{MIN}，可以更好的提高语音效果。下面阐述G_{MIN}的具体计算过程。

如图10所示，输入信号为频域的信号幅度谱$|Y|_k^2$及噪声谱估计$\hat{\lambda}_k$，其中k表征的是频域索引值，我们基于k值将输入信号均分成N个子带，然后计算出各子带的信噪比，公式如下。

$$h_i = 10\log\left(\frac{|Y|_i^2}{\hat{\lambda}_i}\right)(dB), \quad i = 1, \cdots, N \qquad <8>$$

各子带内$G_{MIN,i}$与信噪比η_i成线性关系，映射公式如下：

$$G_{MIN,i} = \begin{cases} -10 & , \quad h_i \le 10 \\ a\,h_i + b & , \quad 10 < h_i < 50 \\ -25 & , \quad h_i \ge 50 \end{cases} \qquad <9>$$

基于实验我们取N=8，η_i限定在[10, 50] dB，$G_{MIN,i}$限定在[−25, −10] dB, 公式9中α、β参数分别取值为−0.375和−6.25。

图10 是ANS模块在系统集成的局部展示图，模块在后端的解码后、音量控制前，完成噪声的自适应抑制功能，增强音频播放的呈现效果。

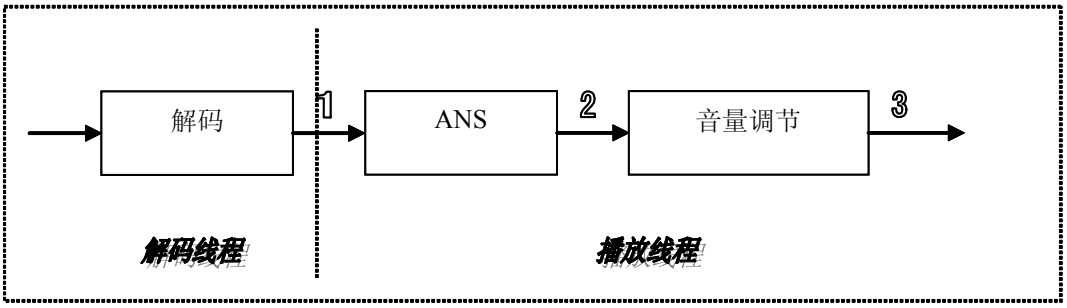


图10 ANS模块集成局部图

使用该方案可以增强监控系统的音频呈现效果；同时屏蔽系统前端设备音效差异化，保证全网系统的音频呈现表现一致性，并且由于该装置部署在系统后端的监控管理中心，便于部署和维护，节省系统管理开销。

网络视频监控中编码器平滑发送存储流

网络化存储是IP视频监控的一个重要应用，业界通常采用NAS或iSCSI技术来实现。但是，无论NAS还是iSCSI都无法保证存储流的平滑发送，即存储流在网络上传输的流量突发现象明显。当多路存储流在同一网络上传输时，突发现象将变得更严重，进而造成网络资源利用率低下。存储流传输不做平滑处理会产生如下问题：

1. 流量突发导致网络带宽利用率低下。为了保证存储流的正常传输，不得不分配比实际需要大得多的网络带宽，造成网络带宽资源浪费严重。

2. 当实况流和存储流一起传输时，存储流的流量突发会影响实况流，带宽有限的情况下，容易导致实况流丢包，从而影响网络视频监控用户的视频质量体验。

针对以上问题，可应用如下方案，该方案解决了IP视频监控中存储流传输时带宽利用率低的问题。

IP视频监控中摄像机与编码器相连接，编码器先将摄像机的模拟信号经过模数转换，然后送给数字信号处理器进行视频压缩编码，最后将码流送入采用本发明的CPU进行处理。CPU先是对媒体流进行标记，然后在流量控制模块根据标记将存储流识别出来对其进行平滑发送处理。平滑发送后，消除了存储流流量突发对网络的冲击效应，进而提高了存储流传输时网络带宽的利用率。

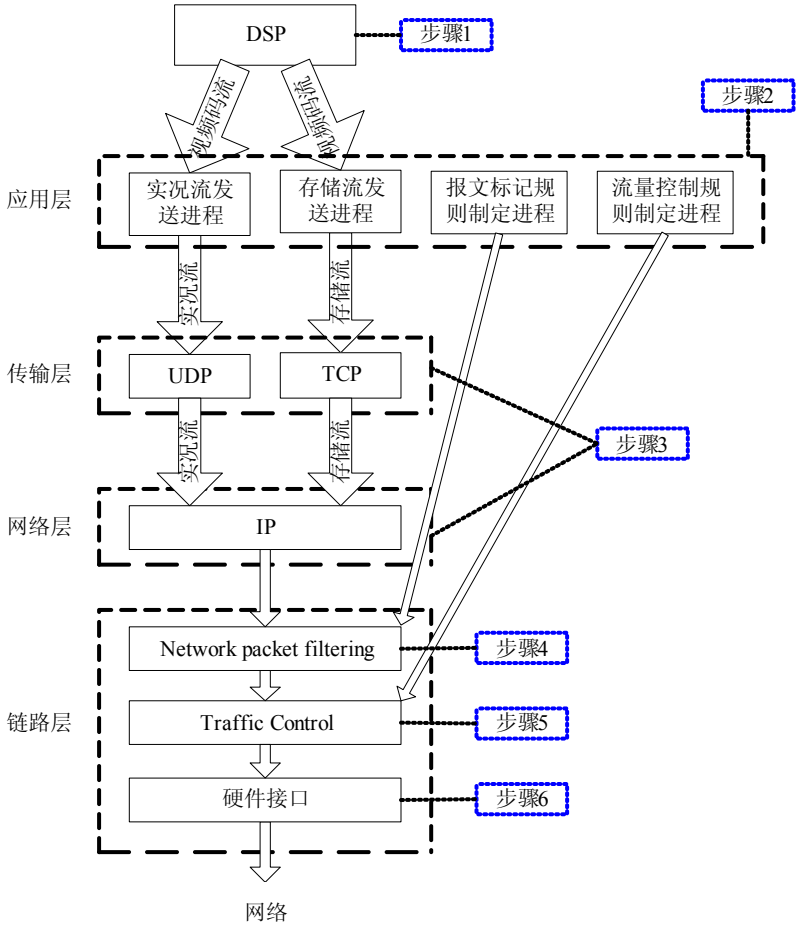


图 11　CPU平滑发送存储流的流程图

图11是本方案的CPU平滑发送存储流的流程图，其工作步骤如下：

步骤1：DSP对数字视频信号进行压缩编码，产生出视频码流。

步骤2：该步骤包含了以下四个进程的相互分工及协作。

1) 实况流发送进程：通常用RTP协议将视频码流打包发送，为网络实时监控应用服务。

2) 存储流发送进程：通常用iSCSI或NAS协议将视频码流打包发送，为网络存储服务。

3) 报文标记规则制定进程：要想在链路层实现存储流平滑发送，首先就要对媒体流做以特殊标记，使后续的流量控制能将存储流与实况流区别对待。此进程就是根据存储流的目的IP地址、端口号，制定实况流、存储流报文标记规则，实际的标记操作是在链路层的“Network packet filtering”模块实现的（图中箭头所指的模块）。

4) 流量控制规则制定进程：根据存储流的视频码率，制定能使存储流平滑发送的流量控制规则，实际的流量控制操作是在链路层的“Traffic Control”模块实现（图中箭头所指的模块）。

步骤3：实况流、存储流经过传输层、网络层，送至链路层。

步骤4：Network packet filtering（网络包过滤）模块包含在Linux 2.4以后的内核中，它在内核中实现了报文过滤功能。该步骤根据事先制定的报文标记规则（步骤2–3），对各路媒体流分别做以不同的标记。

步骤5：Linux内核中提供了Traffic Control（流量控制）功能，流量控制通过输出流量整形（Shaping）、调度（Scheduling）、分类（Classifying）、输入流量监管（Policing）四种方式来实现。该步骤根据事先制定的流量控制规则（步骤S402–4），对存储流进行输出流量整形，使其平滑地发送到网络上。

步骤6：被平滑后的存储流，通过硬件接口发送到网络上。这种被平滑后的存储流，能有效地提高网络带宽的利用率。

图12是图11中流量控制规则制定模块的实现模型，在详细阐述该实现模型之前，先简单介绍流量控制的基本原理。

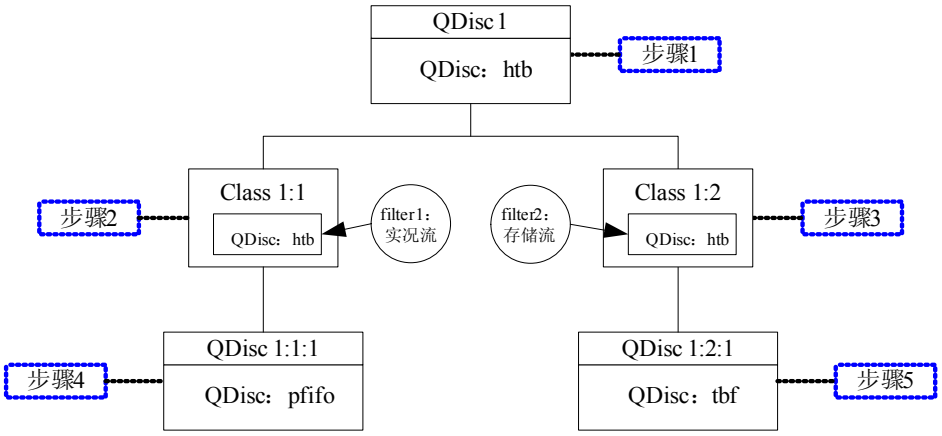


图12 流量控制规则制定模块的实现模型

流量的处理由三种对象控制，它们是：

QDisc（排队规则）：是Queueing Discipline的简写，它是理解流量控制的基础。无论何时，内核如果需要通过某个网络接口发送数据包，它都需要按照为这个接口配置的QDisc把数据包加入队列。然后，内核会尽可能多地从QDisc里面取出数据包，把它们交给网络适配器驱动模块。

CLASS（类）：某些QDisc可以包含一些类别，不同的类别中可以包含更深入的QDisc，通过这些细分的QDisc还可以为进入的队列的数据包排队。通过设置各种类别数据包的离队次序，QDisc可以设置网络数据流量的优先级。

FILTER（过滤器）：用于为数据包分类，决定它们按照何种QDisc进入队列。无论何时数据包进入一个划分子类的类别中，都需要进行分类。分类的方法可以有多种，使用FILTER就是其中之一。使用FILTER分类时，内核会调用附属于这个CLASS的所有过滤器，直到返回一个判决。如果没有判决返回，就作进一步的处理，而处理方式和QDISC有关。 需要注意的是，FILTER是在QDisc内部，它们不能作为主体。

QDisc按其属性划分，可以分为CLASSLESS QDisc（不可包含类的QDisc）和CLASSFUL QDdisc（可包含类的QDisc）。其中，CLASSLESS QDisc包括[plb]fifo、pfifo_fast、red（Random Early Detection）、sfq（Stochastic Fairness Queueing）、tbf（Token Bucket Filter）等；CLASSFUL QDdisc包括cbq（Class Based Queueing）、htb（Hierarchy Token Bucket）、prio（n-band strict priority scheduler）等。

下面只对图12中将用到的QDisc进行详细介绍。

pfifo：它是最简单的QDisc，它不对进入的数据包做任何的处理，数据包采用先入先出的方式通过队列。不过，它会保存网络接口一时无法处理的数据包。

tbf：令牌桶过滤器，它只允许以不超过事先设定的速率到来的数据包通过，但可能允许短暂突发流量超过设定值。

htb：分层的令牌桶，它实现了一个丰富的连接共享类别体系，可以很容易地保证每个类别的带宽，虽然它也允许特定的类可以突破带宽上限，占用别的类的带宽。htb可以通过tbf实现带宽限制，也能够划分类别的优先级。

下面对图12的各步骤做说明。

步骤1：建立一个根htb类型的QDisc“1”，htb是可包含类的QDisc。

步骤2：在QDisc“1”下建立第一个Class“1:1”，它内含了一个htb类型的Qdisc，同时该Qdisc含有一个Filter——filter1，它的作用是利用之前所做的报文标记把实况流过滤出来。

步骤3：在QDisc“1”下建立第二个Class“1:2”，它内含了一个htb类型的Qdisc，同时该Qdisc含有一个Filter——filter2，它的作用是利用之前所做的报文标记把存储流过滤出来。

步骤4：在Class“1:1”下建立一个pfifo型的QDisc“1:1:1”。将pfifo配置成最简单的先入先出方式，使实况流能快速地发送到网络上。

步骤5：在Class“1:2”下建立一个tbf型的QDisc“1:2:1”。根据存储流码率，配置tbf的rate、burst、limit、peakrate、minburst等参数，就能实现存储流平滑发送了。以下是tbf部分参数的说明。

rate：是该队列保证得到的带宽值。

burst：桶的大小，以字节计。这个参数指定了最多可以有多少个令牌能够即刻被使用。通常，管理的带宽越大，需要的缓冲器就越大。如果缓冲区太小，就会导致到达的令牌没有地方放（桶满了），这会导致潜在的丢包。

limit：确定最多有多少数据（字节数）在队列中等待可用令牌。也可以通过设置latency参数来指定这个参数，latency参数确定了一个包在tbf中等待传输的最长等待时间，后者计算决定桶的大小，速率和

峰值速率。

peakrate：如果有可用的令牌，数据包一旦到来就会立刻被发送出去，就象光速一样。那可能并不是所希望的，特别是有一个比较大的桶的时候。峰值速率可以用来指定令牌以多快的速度被删除。也就是说释放一个数据包，然后等待足够的时间后再释放下一个。通过计算等待时间来控制峰值速率。

minburst：是指峰值桶（peakrate bucket）的大小。

该方案解决了网络视频监控中存储流发送时流量突发导致的网络带宽利用率低的问题，能够节省网络带宽资源。同时解决了网络视频监控中实况流和存储流一起传输情况下，存储流发送时的流量突发会影响实况流发送的问题。■

监控产品的跨域业务控制

■ 文/李　旻

随着监控业务的发展，越来越多的用户要求把各个孤立的自治监控域进行互通，达到资源共享的目的。但由于监控系统的标准众多，物理资源分散在各个自治域中，给域和域之间的互通带来了很多障碍和困难。怎么样把众多的物理资源整合起来，屏蔽掉由于不同厂商、不同标准带来的差异？如何进行跨域业务控制，实现跨域业务互通？我们从跨域联网、资源管理、业务实现等几个方面来阐述。

跨域联网

跨域联网需要把不同厂商、不同实现方法的各个孤立的域联系起来，使其能互联、互通、互控。为此我们需要定义一套标准、通用的域间通信协议，以便各个域之间可以互通。原先不支持该联网协议的监控域可以通过添加一个联网单元的设备来进行域内和跨域信令的转换，以便和其他域进行互通。

网络结构

若干个相对独立的视频监控系统以联网单元为核心，通过IP传输网络，实现跨域视频监控资源的共享。网络结构如图1所示：

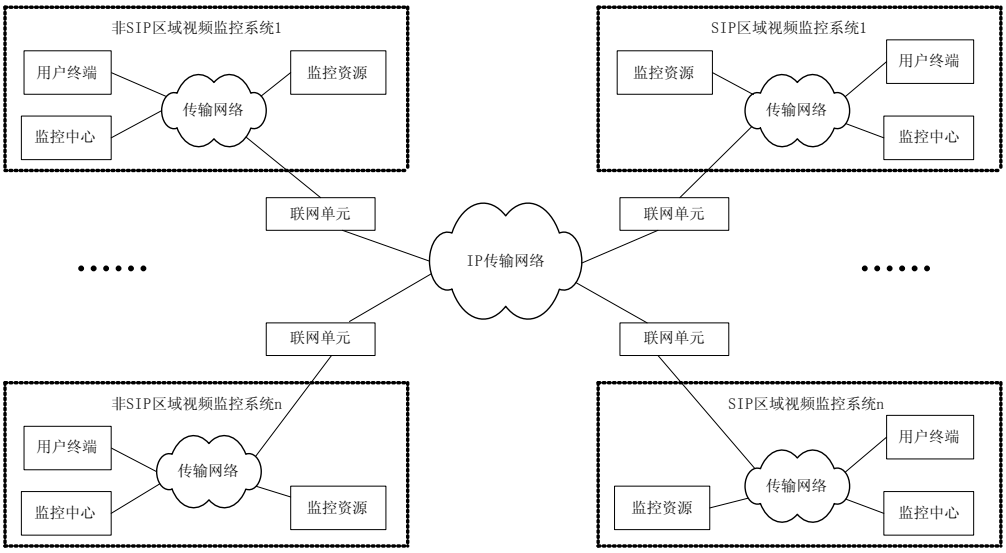


图1 网络结构图

视频监控系统跨区域联网共享主要有以下两种方式：

● 基于非SIP区域视频监控系统的联网共享

非SIP区域监控网络系统是指其中的监控资源、用户终端、监控中心等不符合RFC3261规定的SIP协议的监控网络，该类系统通过联网单元进行SIP协议转换，实现监控网络系统之间的互联互通、资源共享；

● 基于SIP区域视频监控系统的联网共享

SIP区域监控网络系统是指其中的监控资源、用户终端、监控中心等符合RFC3261规定的SIP协议的监控网络，该类系统直接采用SIP协议，通过联网单元实现区域监控网络系统之间的互联互通、资源共享。

联网单元

联网单元是组成视频监控系统跨区域联网共享接口的逻辑实体，可以独立的设备形式存在或内置在视频监控系统内的监控服务器中。

联网单元负责实现联网过程中的控制命令和视频数据的传输和转换，联网接口采用RFC 3261和RFC 3265协议。

传输与控制协议

实现高效的互联互通，传输与控制协议的选择至关重要。基于SIP会话协议的开放性和可扩展性，跨域联网的信令控制协议采用遵循RFC 3261和RFC 3265的SIP会话协议。在媒体传输协议上，我们选择业界普遍使用的TS/RTSP协议。

监控资源管理

跨域联网后，使整个网络系统一下庞大起来。原先单域的组织架构加入了其他域的内容，其他域的划分标准还不尽相同；原先有限的监控设备一下子扩展了几倍或几十倍，这些资源还隐藏在不熟悉的各个外域下……，种种的一切会给最终用户带来迷茫和不便。

虚拟域

为了解决这个问题，我们在物理域的基础上提出虚拟域的概念。

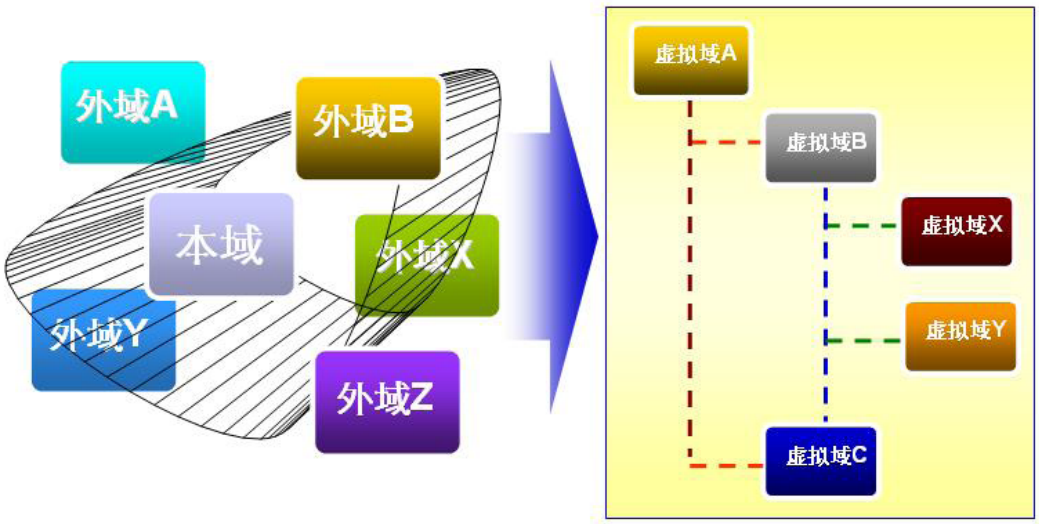


图2 构建虚拟域

虚拟域是相对物理域而言，用户可以根据实际需求或偏好来划分自己的虚拟域，比如按照实际的组织结构来构建等等。虚拟域可以跨多个物理域，也可以在一个物理域中搭建多个不同的虚拟域。它还可以是多层次的，虚拟域下也可以挂虚拟域。

用户、角色和权限控制

每个虚拟域都可以添加属于本虚拟域的角色，角色类似于普通企业中的岗位。我们可以给角色添加域的权限，也可以单独添加该虚拟域下某个资源的权限，方便的把虚拟域下个体资源权限和域的权限统一起来。

通过把角色赋给用户的方式使用户具有不同的权限。一个用户可以同时拥有多个角色，以便获取不同的权限。

通过角色设置，我们把用户和权限分离开来。可以通过角色方便的给类似的用户（用户组）拥有一样的权限，也可以通过角色的设置给用户拥有多个不同的权限。

设备共享

每个域都可以给其他域设置共享设备，可以给每个设备单独设置权限。通过设备推送的方式把共享设备传递给其他域。这样可以把域A的资源给域B的用户使用，达到域间设备的共享。

设备划归

把物理域中的设备通过划归的方式添加到虚拟域中，这样用户可以根据实际的需求把各个域的设备划归到一个虚拟域中。一个物理设备可以划归到多个不同的虚拟域；本域的设备和外域共享过来的设备都可以进行划归。

我们把划归后的监控设备称为资源。最终用户看到的是划定后的虚拟域和虚拟域所属的各种资源。

存储设备虚拟化

目前的存储存在两方面的问题。对于一个多域的系统，存储资源散落在各个域中，并且由各个域管理。导致可能在配置不当的情况下存储资源产生很大的浪费。比如域A的存储资源已经用完，想存的存不了，但是在域B中，还有很多空余的存储资源。另一方面，各种存储资源的访问接口不尽相同，也给二次开发增加了难度，兼容性不能保证。

因此我们提出了“域间存储资源共享”和“虚拟化存储”的概念。

存储资源的共享就是打破域和域之间的界限，把多域的物理存储资源统一管理，并且划分虚拟的存储资源簇。用户在给摄像机分配存储资源的时候就不需要指定物理的存储设备，只要选择一个虚拟的存储资源簇并指定大小就可以了，使用简单方便。由于存储资源都得到统一管理，摄像机和具体的存储资源没有紧密的关系，这样就可以无缝的添加和删除存储资源，使存储资源的扩容更易实现。

实现了存储资源的共享后，管理员可以把存储资源可以放在各个域中，也可以集中管理；整个多域系统的存储资源可以统一调配，充分利用。当系统的存储资源不足时，管理员可以在任何一个域添加新的存储资源。当存储资源有变化（删除或替换）的时候，摄像机不需要重新申请存储资源。

虚拟化存储是指提供一套共用的接口，屏蔽不同的存储资源挂载，不同的读写操作，也可以屏蔽不同的存储格式。用户在获取存储资源的时候，只需要调用固定的接口，不需为兼容不同的厂商开发多套适配接口。

跨域监控业务

域间注册和保活

通过上级、下级、平级域的设置把各个域构建成一个树状或网状的拓扑图。

通过下级域注册到上级域或平级域之间的相互注册来获知各个域的在线状态。

通过域间的保活来维护或更新各个域的状态。

注册和保活消息采用通用的SIP协议，提高互联协议的通用性和兼容性。

监控设备的域间推送

给外域设置了共享设备后，当该外域上线后，主动把共享给该外域的设备信息推送给外域。在共享设备的状态发生变化（比如摄像机的上下线、视频丢失和恢复等）的时候，也需要把该信息实时告知该外域。

同样，我们也接收各个外域推送给我们的共享设备，可以看作是我们本域的设备一样，供本域的用户使用。

域间监控业务的实现

通过虚拟域的设置和设备划归，最终用户看到的是自己熟悉的组织结构（虚拟域）和各个虚拟域所属的监控设备（资源），屏蔽了设备的物理差异。用户对一个监控设备发起了一个业务，业务控制服务器自动会区分该设备是本域设备还是外域设备，如果是外域设备，业务控制服务器把业务请求发送给联网单元，联网单元把业务请求转换成跨域联网统一的互通信令。

目前跨域的监控业务包括跨域实况请求、跨域轮切、跨域云台控制、跨域录像检查和回放、跨域告警订阅等。

总结

跨域联网通过统一的域间通信标准来保证域间的互通互联。对于原先已经存在的域，可以通过联网单元来接入。通过跨域联网的虚拟化技术，屏蔽各个域之间的信令交互差异、媒体存储格式差异、监控设备的地域差异，使用户可以按照实际的组织结构构造各异的虚拟域，方便的操作本域和外域的监控设备。■

监控产品的告警联动

■ 文/周后取

在监控领域，告警联动几乎涉及到了监控的每一个角落。不管是在各种设备如编码器、解码器、摄像头等组成部件发生故障时，需要通过告警来通知管理员进行及时处理；还是通过各种智能的分析工具对视屏图像进行智能检测和分析后，发现异常，需要通过告警来通知监守人员采取相应措施。把林林总总的告警联动在一套监控系统中整合起来已经成为业界的一种共识。

最新的多媒体平台IMOS基于平台化设计，在功能的可扩展性上更加注重，IMOS提供的告警联动框架为上层业务提供了良好的支持，使基于其上的监控业务只需进行少量产品化工作即可具备完善的告警联动功能。IMOS的告警联动框架可分解为两个模块：告警模块和联动模块。

告警模块

告警模块负责告警采集、告警分析入库、告警呈现，其系统结构如图1：

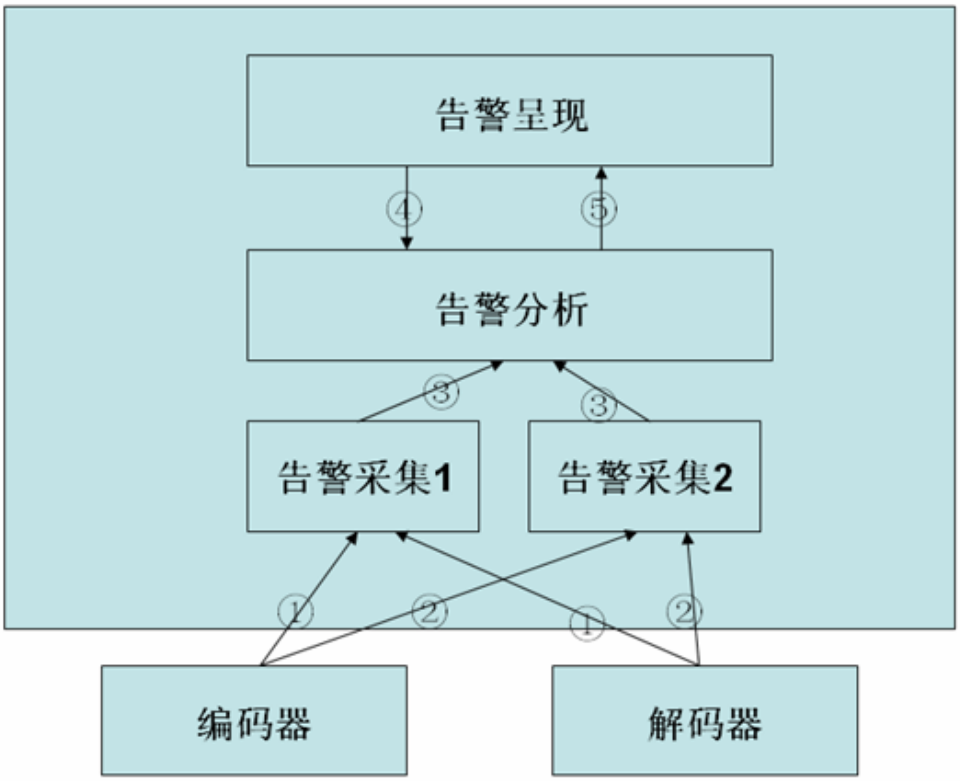


图1 告警模块系统结构图

① 设备向中心发送的SNMP格式Trap告警

② 设备向中心发送的SIP格式业务告警

③ 经过告警采集并进行预处理后以统一格式发往告警分析程序

④ 告警呈现模块事先向告警分析模块注册需要呈现的告警类型

⑤ 告警分析程序负责对告警入库并转发给事先注册好的模块

（1）告警采集层：告警采集层可以有多种采集器，用于对不同协议的告警数据进行采集。收到告警数据并进行预处理后以统一格式发往告警分析层。

（2）告警分析层：告警分析层是告警模块的关键部分，完成告警策略的实现、告警入库、注册/转发、确认等操作。告警策略支持给告警进行重命名、修改告警的默认级别、是否自动确认等，同时告警策略本身可以使能或不使能。在告警分析层可以进行告警策略的扩展，比如告警过滤、告警升级、告警恢复等策略。

（3）告警呈现层：包括实时告警和历史告警查看。实时告警查看通过事先注册到告警分析层，然后由分析层转发实时告警来进行即时呈现；历史告警通过直接查询告警数据库中的告警数据进行呈现，告警数据在告警分析层进行数据写入；告警查询支持多种过滤方式。

通过告警模块的层次划分，为后续接收其他协议或格式的告警提供了良好的框架支撑，基本上只需要在告警采集层开发针对性的告警采集插件即可。

联动模块

联动模块包括联动动作注册管理、联动策略管理、联动策略实施与跟踪，其系统结构如图2所示：

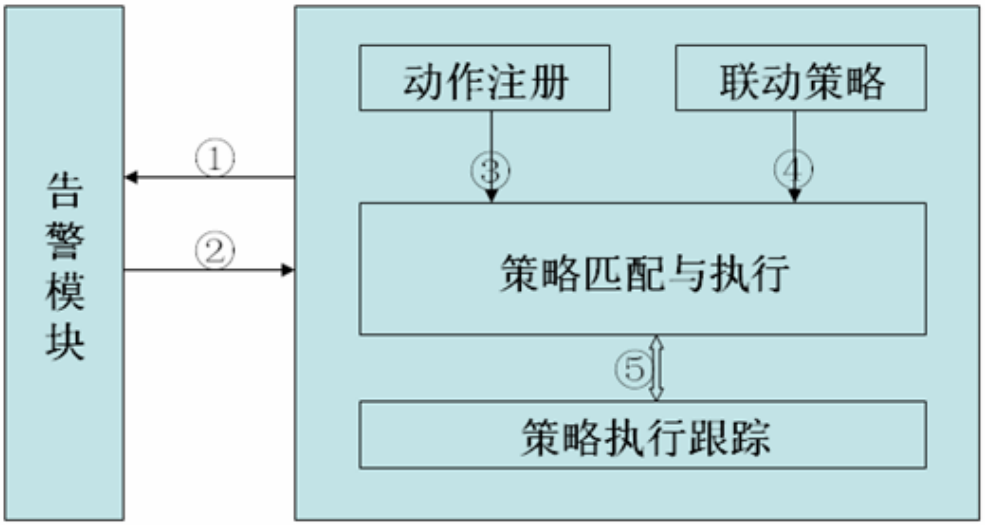


图2 联动模块系统结构图

① 联动模块向告警模块注册需要的告警，其时机为系统初始化以及用户配置联动策略。

② 告警模块向联动模块转发注册过的告警

③ 系统初始化时通过XML以及动态库的方式提供动作注册

④ 用户通过界面增删改联动策略

⑤ 负责跟踪策略的执行

动作注册

联动模块支持以XML形式的配置文件进行动作的注册，只有注册了的动作才能配置到联动策略中。动作的主要信息包含：动作名、动作对应的动态库文件名、动作对应的函数名（函数需要满足统一的要求）、动作的参数等信息。具体可参考如下示例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!--动作集合-->
<actions>
    <!--一个具体的动作描述(中心联动动作)。name:动作名，用于区别与其他动作-->
    <action name="sendMail">
            <!--动作描述-->
            <disName>发送E-mail</disName>
            <!--动作类别：0：中心联动动作；1及以上:与MIB对应的前端联动动作类型-->
            <type>0</type>
            <!--动作所在的动态库名-->
            <dllLib>lib1</dllLib>
            <!--动作其实所调用的函数名-->
            <dllFuntion>sendMail</dllFuntion>
            <!--动作所需要的参数描述-->
            <params>
              <!--具体参数描述-->
                  <param>
                        <!--参数的名字-->
                        <name>toAddress</name>
                        <!--参数描述-->
                        <disName>发送地址</disName>
                        <!--是否可配置：1，可配置，即用户可以给参数赋值；0，不可配置，即
直接从告警属性中得到参数值-->
                        <configurable>1</configurable>
                        <!—参数顺序-->
                        <squence>1</squence>
                  </param>
                  <param>
                        <name>subject</name>
                        <disName>主题</disName>
                        <configurable>1</configurable>
                        <squence>1</squence>
```

```
                    </param>
                    <param>
                        <name>content</name>
                        <disName>内容</disName>
                        <configurable>0</configurable>
                        <squence>1</squence>
                    </param>
            </params>
        </action>
        <!--前端联动动作举例-->
        <action name="ptz">
            <desc>云台到预置位</desc>
            <type>2</type>
            <params>
                    <param>
                        <name>location</name>
                        <disName>预置位</disName>
                        <configurable>1</configurable>
                        <squence>1</squence>
                    </param>
            </params>
        </action>
    </actions>
```

联动策略

联动策略可在系统运行过程中通过用户界面来进行配置，一个联动策略包括触发源、动作、其他属性三个部分。触发源包括告警源（如摄像头）、告警类型；动作可以为多个，多个动作可以并行或串行执行；其他属性有：是否立即启用，策略类型，时间计划。

策略类型：前端联动策略和中心联动策略。前端联动策略是指一旦启用将被下发到设备，由设备直接控制联动；中心联动策略则由中心，即联动模块来控制执行动作。前端联动和中心联动必须配置触发源，即都是由告警触发的。

是否立即启用是指只有当策略启用后，该策略才能去匹配告警，触发动作，不然是不可用的。故一个策略如果不启用，即使有匹配的告警发生，它也不会关心。

时间计划：默认策略没有时间计划，即任何时间点的告警过来，匹配后都可以触发执行。可以为策略添加时间计划。

策略匹配

联动框架接收到告警模块转发的告警后，把告警与启用的联动策略进行匹配，得到匹配的联动策

略。策略匹配只针对中心联动策略。

策略的匹配分为两个过程：告警类型及告警源信息匹配、动作参数获取。

告警及告警源信息匹配的属性有：告警源设备、告警类型和告警参数。匹配的原则：策略中的字段值为空或与告警属性相匹配，则策略匹配。

动作参数的获取：当动作中有不可配置参数时，尝试从告警中获取该参数值。如果获取成功，则正确匹配，不然则匹配失败。

策略执行与跟踪

当接收到的告警匹配到中心联动策略，将产生一个策略流，该策略立即被调度执行。

策略流：记录策略的执行状态，每次策略执行时产生策略流记录，即一个策略可以对应多个策略流

策略触发限制

实现对联动策略的触发做了一定的限制，防止由于告警风暴造成的短时间内不断触发联动策略，影响系统性能。

触发限制允许启用两种触发条件限制中的一种：

1) 固定时间内的最大触发次数：在固定时间间隔内，某个策略的匹配次数必须大于阈值时才能真正触发执行。

2) 最小触发间隔：某个策略匹配后，与上次触发时间间隔必须大于最小触发间隔。

同一时间只能使用一种限制条件，启用任何一种都会使另一种无效。

监控系统支持的告警

当前监控系统支持三类告警：设备通过SNMP Trap上报的告警、设备通过SIP上报的告警以及中心产生的告警。

设备SNMP Trap告警包括：

1) 设备CPU利用率高告警、内存利用率高告警

2) 设备风扇故障告警

3) 设备高温告警、设备低温告警

设备SIP告警包括：

1) 视频丢失告警

2) 运动检测告警

3) 遮挡检测告警

4) 输入开关量告警

5) 存储满告警、存储读写失败告警

中心告警包括：

1) 设备上线告警

2) 设备下线告警

监控系统支持的联动

当前监控系统支持的联动可分为前端联动和中心联动，前端联动表示前端设备检测到告警时直接在前端执行动作，联动策略也是配置在前端设备；中心联动则由中心进行联动，一般跨设备或客户端时采用中心联动。

前端联动

1) 联动预置位

2) 联动开关量输出

3) 联动存储

中心联动

1) 联动预置位

2) 联动开关量输出

3) 联动存储

4) 联动实况到用户窗格

5) 联动实况到监视器■

IVS视频监控系统双机热备

■ 文/周绪龙

HA是双机热备High Ability的英文简称。对于一些重要的应用服务，用户一般采用两台服务器互作备份，共同执行同一服务，当一台服务器出现故障，可以由另一台服务器继续提供服务，在不需要人工干预的情况下，自动保证系统服务的正常运行。

HA相关原理和使用场景

障，另一台备份服务器通过心跳保活，诊断出Active节点出现故障，会将备用服务器（Standby节点）激活继续提供服务。但双机热备不具有修复故障服务器的功能，而只是将故障隔离。

工作方式

按切换方式HA热备技术分为：主-备方式（Active-Standby方式）和双主机方式（Active-Active方式）。

主-备方式即指的是一台服务器处于某种业务的激活状态（即Active状态），另一台服务器处于该业务的备用状态（即Standby状态)。

双主机方式即指两种不同业务分别在两台服务器上互为主备状态（即Active-Standby和Standby-Active状态）。

注：Active-Standby的状态指的是某种应用或业务的状态，并非指的是服务器状态。

数据处理方式

1）基于共享存储（磁盘阵列）的方式：

共享存储方式主要通过主备机共用磁盘阵列（MD），保障服务切换后，数据的完整性和连续性。用户数据一般会放在磁盘阵列上，当主机故障后，备机继续从磁盘阵列上取得原有数据。如图1所示。

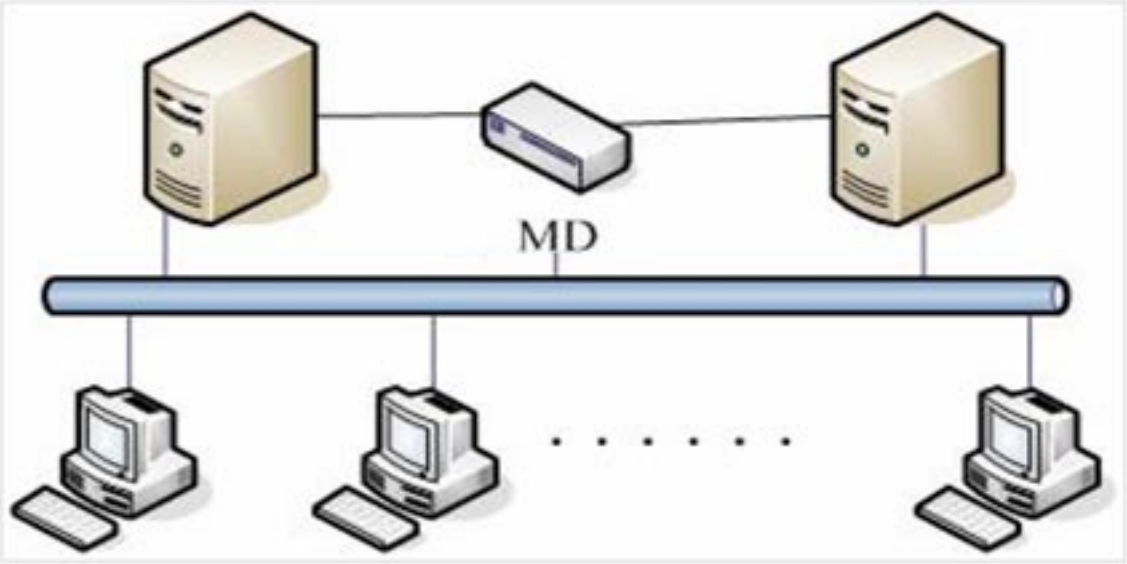


图 1 共享存储方式

这种方式因为使用一台存储设备，往往被业内人士称为磁盘单点故障。共享存储设备会成为安全瓶颈，但一般来讲安全性较低，而且需用额外增加存储设备，开销较大。

2）基于数据复制的方式：

这种方式主要利用数据的同步方式，保证主备服务器的数据一致性，如图2所示.

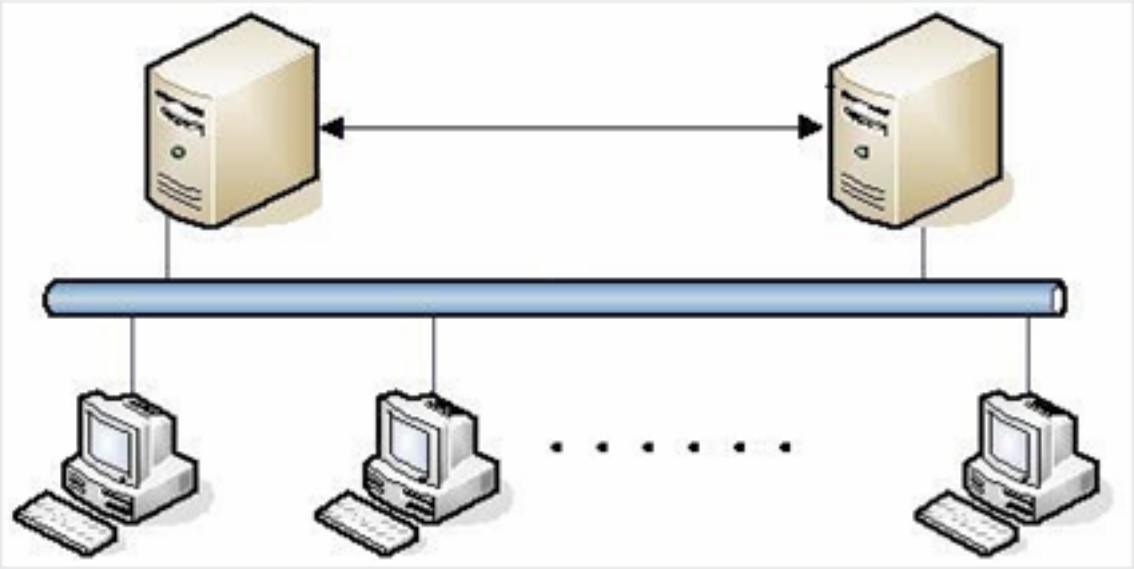


图 2 数据同步方式

基于数据复制的方式有多种方法，其性能和安全也不尽相同，其主要方法有以下几种：

a.单纯的文件拷贝方式：以文件方式的拷贝主要适用于WEB页的更新，FTP上传应用，对主备机数据完整性，连续性要求不高的情况下使用。不适用于数据库等应用，因为打开的文件是不能被复制的，如果要复制必须将数据库关闭，这显然是不可以的。

b.利用数据库所带有复制功能：比如SQLServer 2005所带的定阅复制，但主要还是应用于数据快照服务，不适合用作双机热备中的数据同步。

c.硬盘数据拦截：目前国际国内的双机热备软件通常会使用硬盘数据拦截的技术，也称为镜像软件即Mirror软件，这种技术当前已非常成熟，拦截的方式也不尽相同，分为以下两种：

◆ 分区拦截技术：基于硬盘分区，通过驱动级的拦截方式，提取写往硬盘的数据，并先写到备用服务器，以保证备用服务器的数据最新，然后再将数据回写到主机硬盘。这种方式将绝对保证，主备机数据库的数据完全一致，无论发生哪种切换，都能保证数据库的完整性与连续性。用户可以根据需要划分适合大小的分区来完成数据同步工作。

◆ 硬盘拦截技术：主要是基于一整块硬盘的数据同步工作，往往在硬盘初始化时需要消耗大量的时间。

这两种拦截技术的配置易用性和可维护性比较接近，主要的差异是备份对象是基于分区，还是整块硬盘。

热备故障检测

故障检测是双机热备技术的任务，故障检测的覆盖范围决定了双机热备软件在功能和性能上的优劣性，因为并不是所有的软件都具有相同的检测功能。检测范围分为系统级、应用级、网络级三个方面。

◆ 系统级检测主要通过双机热备技术软件之间的心跳提供系统的检测功能。

◆ 应用级检测提供用户应用程序、数据库等的检测功能。

◆ 网络级检测提供对网卡的检测及可选的对网络路径的检测功能。

H3C的IVS视频监控系统双机热备技术具有全系统全故障的检测能力。

双机热备技术的切换

双机热备都会有一个切换过程，这个切换过程可能是一分钟左右，也可以通过减少故障的检测周期和最终确认的次数，缩短切换时长，在3-10秒内完成切换。在切换过程中，服务是有可能短时间中断的。 但是，当切换完成后，服务将正常恢复。因此，双机热备不是无缝、不中断的，但它能够保证在出现系统故障时，能够很快恢复正常的服务，业务不致受到影响。而如果没有双机热备，则一旦出现服务器故障，可能会出现几个小时的服务中断，对业务的影响就可能会很严重。

IVS-HA的使用场景及优点

IVS-HA组网应用

为了满足高可用性的需求，IVS监控系统的VM8000/VM5000/DM8000服务器与HA组合应用，实现IVS主从方式的双机热备功能。如图3所示。

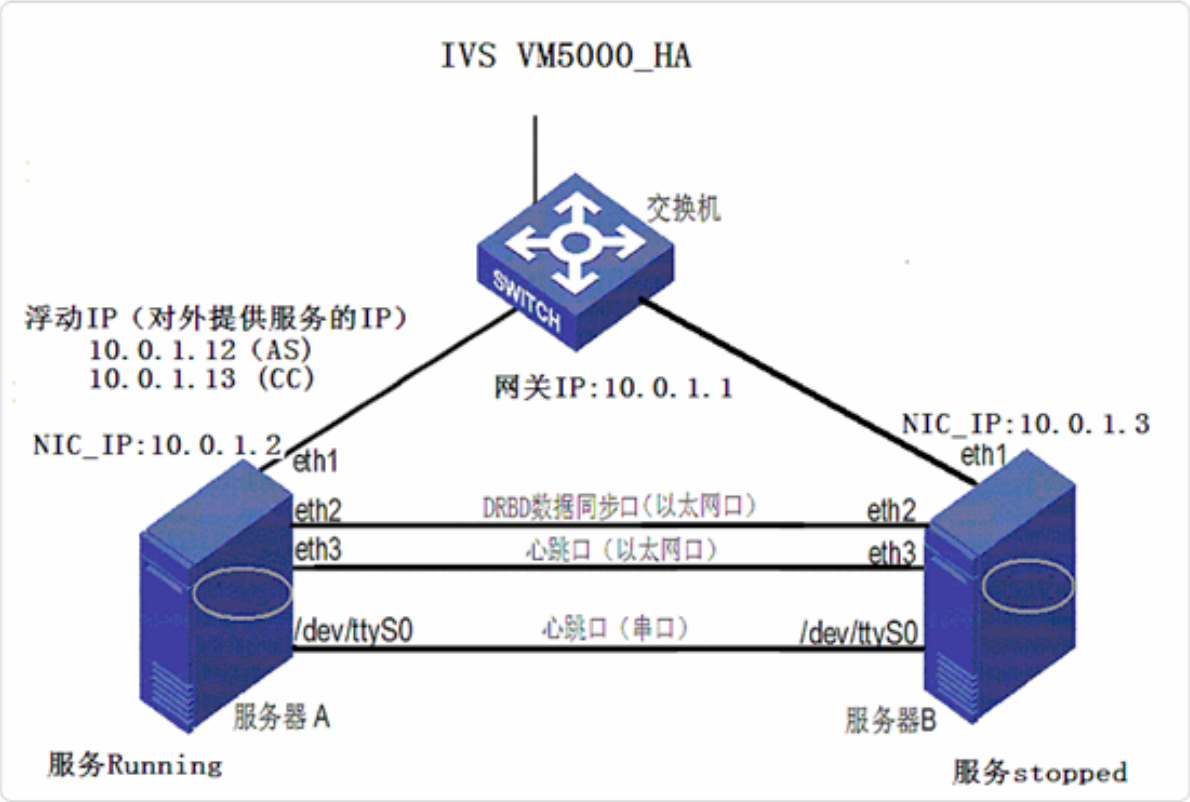


图3 IVS–HA典型配置示例图

表1 服务器A和服务器B上的网络信息

项目	用途	服务器A	服务器B
eth1的IP地址	NIC的实IP，即业务口实IP	10.0.1.2/24	10.0.1.3/24
eth2的IP地址	DRBD数据同步链路（以太网口）	192.168.2.2/24	192.168.2.3/24
eth2的同步线名称	标示数据同步链路（以太网口）	hb311	hb321
eth3的IP地址	心跳检测链路（以太网口）	192.168.3.2/24	192.168.3.3/24
eth3的心跳线名称	标示心跳检测链路（以太网口）	hb411	hb421
ttyS0的心跳线名称	标示心跳检测链路（串口）	/dev/ttyS0	/dev/ttyS0
AS服务的IP地址	浮动IP，对外提供IVS服务	10.0.1.12/24	运行服务时生成
CC服务的IP地址	浮动IP，对外提供IVS服务	10.0.1.13/24	运行服务时生成
网关IP地址	心跳检测链路的冗余备份	10.0.1.1/24	10.0.1.1/24

表2 双机软件的基本术语

术语	描述
节点	安装运行双机软件的计算机
服务	指用户应用相关的一组资源的集合，包括用户应用的进程资源、磁盘资源、网卡资源、浮动IP资源以及DRBD镜像资源等。服务可以是其中几种资源或者全部资源的组合。服务也可以为空，即不包括任何资源
主节点/主服务器	指服务运行所在的节点或服务器
从节点/从服务器	指完全没有服务运行的节点或服务器 如果主节点发生任何故障，服务就会从主节点迁移到从节点。此时的从节点也就转变成主节点，此前的主节点也就转变成从节点
DRBD（磁盘镜像设备）	是指对两个节点各自大小相同的本地磁盘分区进行实时镜像操作，使得这两个本地磁盘对双方节点而言，可以当作一个虚拟的共享磁盘阵列来使用，这个虚拟的共享磁盘阵列就叫做DRBD 设备，可以把DRBD当作普通的磁盘设备来使用

IVS服务切换流程

当触发双机切换的条件产生后，IVS服务切换流程，如图4所示:

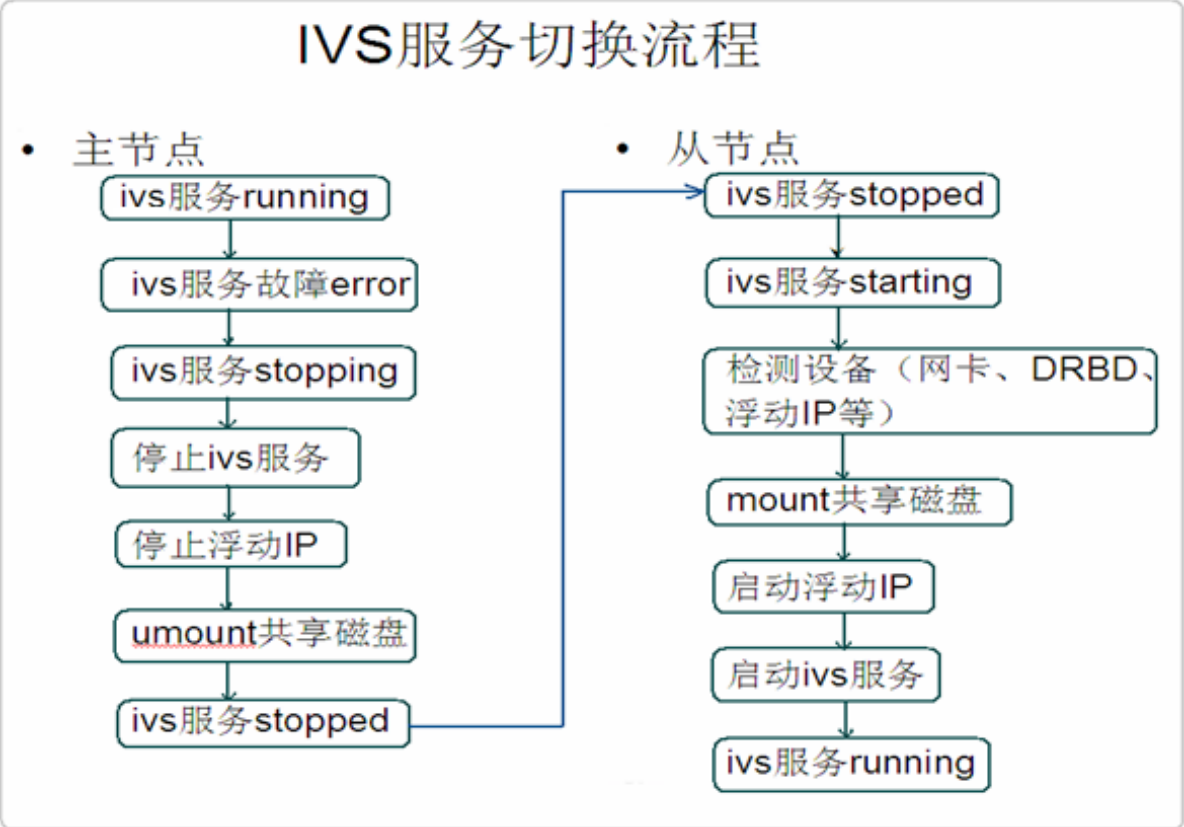


图4 IVS服务切换流程图

IVS-HA的技术要点

◆ 服务的完整性: 同一时刻，IVS服务只会运行在一个服务器节点上，避免了服务跨设备运行，带来的异常风险。

IVS的VM5000、VM8000、DM8000软件包含AS、CC、DM、PGSQL等多项服务，经长期的测试验证，发现“服务跨设备运行”所蕴含的种种异常，要远超于“服务单设备运行”。考虑到当前市场上成

熟的服务器硬件性能技术，除非是在极少的“服务的负载均衡”需求下，还是极力推崇“服务的整体切换”方案。

◆ 服务信息恒定不变性: IVS服务切换后，对外提供的IVS平台服务信息（VM服务IP、AS/CC服务ID等信息），不存在变更的问题，用户可以按照先前的IVS平台信息继续访问IVS服务。

IVS双机热备利用服务与虚拟IP(浮动IP)绑定的技术，对外提供各项服务的IP，是指定的虚拟IP地址。IVS服务启动时，会在运行服务的设备网卡上自动生成虚拟IP。当主服务器节点发生服务切换后，会先释放当前的虚拟IP，并在备服务器节点上生成虚拟IP，从而保证IVS平台服务信息的恒定性。

◆ 服务切换的触发因素: 检测当运行服务的服务器节点出现“系统故障、服务故障、硬件故障、存储故障、网络故障”，IVS-HA都将触发双机切换。

a.IVS-HA利用IVS服务的检测脚本，周期性检测IVS各项服务(AS、CC、DM、PGSQL等)的运行状态，在连续数次都检测到某项服务异常error后，将触发双机切换。

b. 运行IVS服务的节点，出现“设备业务口的网络链接异常”，比如“网卡故障、网络线脱落、网络设备故障”等现象，将触发双机切换。

c. 运行IVS服务的节点，出现“设备断电”现象，备节点通过心跳检测链路，接受不到对方节点的心跳响应，将触发双机切换。

◆ 服务的快速恢复: 触发双机切换的故障发生后，能在“20s-60s”内完成服务的切换，迅速恢复IVS业务，其中包含故障的检测时间，检测时间在HA安装配置时指定（“5s-40s”）。

通过IVS服务的启停和检测脚本，可以定期检测IVS各项服务的运行状态，控制服务的启停、切换。发现当前某服务、服务器设备发生故障（如服务异常、设备宕机、断电、网络故障），双机软件将IVS服务换到另外一台备份服务器上，对外迅速恢复IVS服务。

◆ 心跳检测冗余备份。主备服务器之间可以配置了多条心跳检测链路。

图3配置了2条心跳链路（以太网口、串口）并互作备份，加强了IVS双机热备系统的可靠性。

◆ 故障检测: IVS双机热备软件涵括所有的HA软件都能具备的所有检测功能，检测范围包含系统级、应用级、网络级三个方面。

a.系统级检测。主要通过IVS双机热备之间的心跳提供主备服务器系统状态的检测功能。

b.应用级检测。提供IVS的VM、DM应用服务、数据库状态等的检测功能。

c.网络级的检测。提供对主备服务器网卡的检测及可选的对网络路径的检测功能，因此称为全故障检测能力。

◆ 数据镜像实时同步。在IVS两台服务器的硬盘上，分别划出15G大小的空间，用作磁盘镜像设备（DBRD），使用RAID1分区拦截技术(DRBD服务)，通过以太网口实现IVS主备服务器之间数据的实时同步。RAID1分区拦截技术已经是一项比较成熟的数据同步技术，能快速可靠的解决数据实时同步过程中出现的故障问题。具体的数据实时同步流程及故障异常的处理技术，在此就不再赘述。

◆ 安装配置操作简单易用。IVS-HA双机热备的安装配置操作，可参考《H3C IVS双机高可用方案配置指导（V1.05）.doc》，在此就不再赘述。

IVS-HA其简便的安装和设置、详细的日志信息，减轻了用户日常的维护工作，使得系统管理员的操作和管理更加方便。

IVS-HA的关键技术原理

心跳工作过程

iVS主备两台服务器之间存在基于TCP/IP Socket联结方式、串口联结方式等的心跳检测链路，iVS主备服务器通过心跳路径，周期性的发出检测测试包，检测对方节点的系统是否正常。

◆ 心跳检测链路并不是主服务器一旦宕机，备服务器就会启动相关服务，而是主服务器宕机后，备服务器要经过反复验证后才可以确定主机确实已经停止工作或宕机了。而这个检测时间周期和故障验证次数是在HA软件的安装时配置。

◆ 当运行IVS服务的服务器节点上出现以下多种情况时，会触发IVS服务切换：掉电、停止应用程序、拔业务线。

数据同步过程

◆ 数据库镜像使用RAID1分区拦截技术(即:DRBD服务)，通过以太网口实现IVS主备服务器之间数据的实时同步。

◆ IVS的主备节点都有一个状态，可能是‘主’状态或‘辅助’状态。只有在“主”状态的节点上，IVS服务才能访问读写DRBD分区（/dev/sda1）。每次写入都会发往本地低层设备和带有‘辅助’状态的节点中，状态为“辅助”的备节点只能简单地把数据写入它的低层块设备上。“主”状态节点只有在收到‘辅助’状态节点完成写数据的返回信息后，才认为完成此次的写入操作完成。这种方式将绝对保证，主备节点数据库的数据完全一致，无论发生哪种切换，都能保证数据库的完整性与连续性。

◆ 相对于“共享存储（磁盘阵列）的方式”，该技术充分利用IVS主备服务器现有的硬盘资源，不但节省了额外的存储设备的开销，同时又避免共享存储设备会成为安全瓶颈的问题。相对于“硬盘拦截技术”，又较大程度上缩短了消耗时间。

虚拟IP技术（浮动IP）

◆ IVS服务在安装时，会与虚拟IP作相应的绑定。例如VM5000有2个服务（AS服务、CC服务）分别绑定2个虚拟IP，分别为：10.0.1.12—AS服务、10.0.1.13—CC服务。其目的是为了保证双机切换时，IVS平台服务信息对于前端设备、对用户而言是恒定不变的。

◆ VM5000服务启动时，在运行服务的设备网卡上，自动生成这2个虚拟IP。虚拟IP地址是在主服务器节点的业务口实IP网卡上生成，用户通过虚拟IP地址访问IVS服务。当IVS服务切换时，虚拟IP地址会自动从主服务器节点上释放，并在备服务器节点的业务口实IP网卡上生成，但对用户来说，用户访问的仍然是虚拟IP地址。所以用户只会在切换的过程中发现有短暂的通信中断，经过一个短暂的时间，用户就可以按照先前的登录访问信息继续访问IVS服务。

总结

上述的双机热备技术建立在基于H3C的IVS监控系统平台之上，分别在2台IVS服务器硬盘上划出一个分区（推荐15G-20G），作为数据同步镜像分区，并安装一套双机软件，即可完成IVS监控系统的双机热备。

H3C的IVS服务双机热备技术方案在长期的市场应用中总结了很多宝贵的经验。针对行业特点及对数据安全性的需求，这套技术方案具备卓越的性能和可靠的安全特性。未来，H3C还将不断完善IVS双机热备技术，保证客户系统的长期稳定性、为客户提供更加可靠、安全的服务。■

实时流量分析及网络部署

■ 文/杜超华、袁飞

概述

实时流量提供了实时的交互式应用，如视频会议系统、网真视频系统、视频监控系统及VoIP系统等，其中视频会议系统、网真系统及VoIP系统对交互性的要求较高，这些系统都要求连接两端的视频或声音能够及时且持续不断地同步传递到连接的另一端；而视频监控系统相对来说交互性要低一点，但同样要求音视频信号能够及时及持续不断地从远端传递给监控人员；上述应用的固有要求决定了在部署这些实时应用时，必须保证具有足够的网络资源。下面我们将简单的分析这些实时应用与传统数据应用的区别及其本身所具有的流量特征，并根据分析结果给出实时网络的部署方案，最后，介绍了业界权威的IP多媒体网络传输质量的评估方法。

实时应用流量特征分析

实时应用与传统数据应用的区别

我们知道IP网络仅提供不可靠的网络传输，传统的数据应用为了保证数据传输的可靠性，通常使用

TCP协议。TCP 通过流量控制机制，加快发包速率直到出现网络丢包再减小网络发包速率，这种机制决定了普通数据业务流量占用的带宽是突发的。

同时TCP也带来较大的传输时延，而实时应用则要求时延越低越好。相对于传统的数据应用，实时流量则具有如下的几个特征：

◆ 通过对真实环境的实时图像及声音进行持续不断的采样编码，实时应用的终端持续发出实时流（包括语音、图像等），这就在理论上决定了实时应用占用的网络带宽资源在运行过程中是恒定不变的。

◆ 实时应用对时延非常敏感。实时流是对连续时间的图像或声音的采样和再生，产生的实时流必须在正确的时间到达目的地。如果一个报文迟到或者丢失，就会引起显著的实时应用的服务质量的下降。

因为以上的特征，实时应用通常会采用UDP协议来传输报文。然而，UDP是一种尽力而为的传输协议，没法保证数据传输的可靠性，这就为网络部署提出了更高要求。

实时应用对承载网络的要求

那么，如何来进行网络部署？首先我们来看一下影响实时应用的一些网络参数，下图是ITU G.114给出一张端到端时延和会话质量的关联图，它给出了实时应用的服务质量指标：

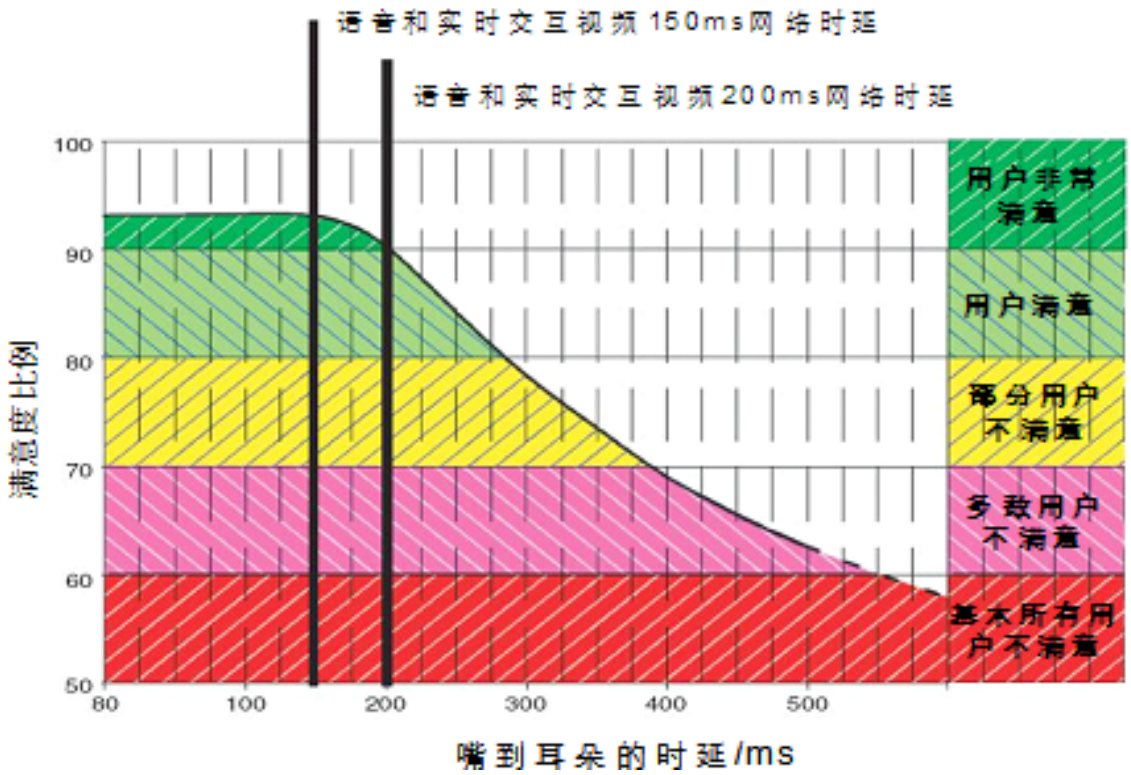


图 1 端到端时延与会话质量的关系

如图1显示，随着时延的增加，用户的满意度也在持续的下降，当时延超过250ms时，就会有20%以上的用户不满意服务质量。

丢包对视频播放质量有直接的影响。试验表明，无论视频丢包的类型（I, B, P帧），在没有适当的视频解码补偿或者丢包重传机制下，视频播放质量都会出现不同程度的下降。当丢包率为千分之一时，大部分人便可以感觉到图像有花块。同时，根据图像压缩编码技术理论，不同的数据包对于重构图像的重要性不同，即使少量的丢包也可能导致图像质量严重下降。

时延抖动即时延的变化是影响视频质量的重要原因之一，会造成图像语音不连贯、图像的横条等现

象。抖动基本上是由于排队延时导致的。如果报文通过一个空队列，延时非常小，但如果从一个满队列通过，需要被延迟很久才会被转发。

根据YD-T 1171-2001《IP网络技术要求--网络性能参数与指标》中规定：进行实时交互式应用时，网络性能要求达到1级或1级以上；具体的网络性能等级参数如表1：

表 1 网络性能参数与指标

			QoS等级			
	网络性能指标	默认值	0级	1级（交互式）	2级（非交互式）	3级（U级）
IP传输时延	平均IPTD的上限值	需要规定	150ms	400ms	1s	U
IP时延抖动	IPTD的1-10-3百分位值减去IPTD的最小值	需要规定	50ms	50ms	1s	U
IP丢包率	包丢失率的上限值	需要规定	1×10-3	1×10-3	1×10-3	U
IP包误差率	包误差率的上限值	1×10-4	默认	默认	默认	默认
虚假包率	虚假包率的上限值	默认（待定）	默认	默认	默认	默认

对于监控实时业务而言，图到眼（模仿嘴到耳）的时延要求没有实时语音视频会议那么高，我们推荐的一般端到端时延要求是单向300ms，反馈延时500ms以内。按国家标准，进行多媒体传输(视讯业务)，网络性能要求达到1级或1级以上。

实时多媒体应用的网络部署

从上面的分析，我们知道为了获得良好的实时多媒体应用效果，在网络部署时，就必须考虑到网络的传输时延，丢包率以及时延抖动等要求。足够的带宽可以提供较低的网络传输时延及时延抖动、极少的丢包率。由于数据流量的突发性，在实际部署中是无法保证提供的带宽是足够的，因此在实际部署中，我们只能通过端到端的QoS机制来优先保证实时多媒体应用的带宽资源。在部署QoS之前，我们要考虑如下方面：流分类、带宽需求评估、可用带宽评估以及采用的广域网技术。

流分类

流分类是区分流并以不同的优先级标记它们，使得交换机和路由器可以识别，它是QOS实施的基础。下面介绍了在何处进行流分类及实时多媒体应用流分类的基本原则：

终端设备进行流分类

目前多数终端设备自身具有标识语音和视频流的QoS标签能力。终端设备是网络中最智能的组件，因为它包含并理解应用程序。对终端设备而言，标记哪些流是语音视频流的内容，哪些流是普通数据流，哪些是控制流是很容易的事情。绝大部分语音视频终端都有一个配置选项来指定高优先级流的QOS标记。但是为了防止伪造的QoS标签，网络设备通常会不信任终端所打的QoS标签。

网络设备进行流分类

网络设备自己进行流分类。这表明边缘交换机或路由器必须查看包的内容来决定哪些报文需要优先服务，然后重新标记它们。核心设备或者core路由器信任边缘路由器进行的标记。通常可以根据IP地址、端口号、物理端口并结合终端设备自生的优先级标记来进行分类。

企业分类原则

每个企业应该对如何进行流分类制定相关规则，此规则随着终端数量的增加仍然工作的很好。通过

规则可以可靠地标记实时流而不破坏网络的完整性。默认情况下，路由器是不信任终端优先级的，所有的入报文被标记为尽力服务类型。使能QOS而且只在终端进行标记通常是不够的。要确保边缘路由器信任终端的分类或者它自己来进行分类。通过在接收端抓包，观察报文QOS标记是否在整个传输过程中保持不变是常用的办法。

对于多媒体业务流，假设已经根据具体的特征（IP地址，端口，协议号等）进行了区分，如何具体设置相应流的优先级，IETF对此有一个指导表格：

表 2 应用QoS分类标签

Service Class	DSCP	PHB Used	Queuing	AQM
Network Control	CS6	RFC2474	Rate	Yes
Telephony	EF	RFC3246	Priority	No
Signaling	CS5	RFC2474	Rate	No
Multimedia Conferencing	AF41 AF42 AF43	RFC2597	Rate	Yes per DSCP
Multimedia Streaming	AF31 AF32 AF33	RFC2597	Rate	Yes Per DSCP
OAM	CS2	RFC2474	Rate	Yes
High Throughput Data	AF11 AF12 AF13	RFC2597	Rate	Yes Per DSCP
Low Priority Data	CS1	RFC3662	Rate	Yes
Standard	DF (CS0) + other	RFC2474	Rate	Yes

1、CS6和CS7默认用于协议报文，比如说OSPF报文，BGP报文等应该优先保障，因为如果这些报文无法接收的话会引起协议中断。而且是大多数厂商硬件队列里最高优先级的报文。

2、EF用于承载语音的流量，因为语音要求低延迟，低抖动，低丢包率，是仅次于协议报文的最重要的报文。

3、CS5用来承载语音的信令流量。这里大家可能会有疑问为什么这里语音要优先于信令呢？其实是这样的，这里的信令是电话的呼叫控制，你是可以忍受在接通的时候等待几秒钟的，但是绝对不能允许在通话的时候的中断。所以语音要优先于信令。监控环境中的控制流也可以打上此类标记。

4、AF4可以用来承载IPTV的直播流量，直播的实时性很强需要连续性和大吞吐量的保证。监控环境中实时流/存储流可以考虑。

5、AF3可以用来承载VOD的流量，相对于直播，VOD要求实时性不是很强，允许有延迟或者缓冲。比如监控的回放流。

6、AF2可以承载不是很重要的专线业务，如监控中的备份流。

7、最不重要的业务是INTERNET业务，可以放在BE模型来传输。

带宽需求评估

在对网络中的流量类型进行分类分析后，我们需要评估各类流量所需要占用的带宽，尤其是多媒体应用中的一些服务器等特殊设备。承载预期实时流的每条链路必须配置足够的带宽。带宽需求分析有多种办法。如果公司本身已经对不同的链路上不同时间的带宽使用情况有一定的统计信息，可以直接使用这个统计信息。需要注意的是：

1. 在估计带宽的时候要注意对IP和ATM头的消耗

头消耗带宽的比例近似如表3所示：

表 3 各种网络封装的头消耗比率

Type	Ethernet/MPLS	PPP	ATM
Voice G.711	36%	25%	40%
Video	20%	18%	25%

G.729下的会议头消耗带宽的比例比表格中稍高。IP网下一个384Kbps的视频会议消耗384Kbps x 1.2 = 460Kbps网络带宽。

2. 在带宽评估的时候对关键部件要进行特殊考虑

在监控网络中，规划网络前要考虑好MS、VM、DM、IPSAN等服务器的带宽需求。

MS、VM、DM、IPSAN一般部署在网络的核心层，这样能够支持大量终端的并发接入。

对视讯会议网络，首先要考虑MCU。如果网关被集成在MCU上，这部分带宽应该与视频会议的带宽需求加在一起。

评估可用带宽

考虑到带宽需求后，我们需要一种评价现有的网络带宽和利用率的方法，以确定是否有足够的资源来支持新的实时流量业务。每一个环节的网络需要有足够的带宽，以支持实时多媒体流量和现有的数据应用程序。

要评价WAN链路的可用带宽有两点是需要考虑的。首先，预计语音和视频（实时）负载应不会超过35%的链接能力。超过这个水平，基于优先级的QoS机制开始失去其有效性。第二是总带宽利用率，包括实时流和普通数据流。对实时流而言，这个比较好确定，而数据应用占用的带宽是突发的，确定其带宽比较困难。

如果带宽不足，在网络繁忙的时间评估通过关键链路的流量是非常有价值的。通过这个办法可以确定这些流中哪些是不合理的业务应用。发现和消除这些不必要的流往往可以释放带宽。

给出可接受的具体的使用率是非常困难的，因为每个企业都有不同的组合流和不同的需求。35%的总利用率是意味着所有应用程序可以获得好的性能。百分之七十（ 70 % ）以上的带宽利用率可能会使应用程序性能降低。

广域网部署

最后，我们通过WAN将企业的各个地点联系起来。运营商链路成为企业网的一部分，也是承载多媒体实时流的一部分。这就是我们必须关注运营商在接入链路和核心网上部署的QOS策略以及这个部署对多媒体实时流的影响。

QOS in the WAN core

运营商有一个高速的核心网，因为队列被清空的很快，网上的抖动非常小。有些运营商支持为不同的流提供不同的服务等级。我们应该选择在这样的运营商网络中部署我们的实时网络，因为他们能为实时流提供更好的承诺。

WAN访问链路上的QOS

在多媒体实时应用的两个终端间，WAN访问链路是可用带宽最窄的地方，这意味着这里是最有可能发生丢包和抖动的。高速链路向低速链路发送数据的地方就会发生排队，在这个地方实施QOS是非常关键的。

如果WAN提供商的核心网没有实施QOS,至少要保证在流离开WAN核心网进入访问链路的时候对流实施了QOS。同时要确保运营商带的QOS标记被正确的传递到出口路由器，我们可以通过在流离开WAN进入企业网的时候抓包，验证QOS标记是否完整不变。

企业网到广域网QOS的切换

绝大部分WAN支持IETF的diffsev标记，并使用它把流映射到不同的类别中。将企业QOS等级与WAN的等级保持一致是非常重要的，当企业垮多个运营商的时候保持运营商之间的QOS等级一致性也是非常重要的。当然可以在运营商的边界路由器上进行重标记，但是在不需要的情况下重标记添加了不必要的复杂性。选择当前或最可能的运营商并学习他们的QOS标记策略，依据它来进行企业的QOS策略。

实时传输网络的评估

网络部署以后，我们需要对网络的实际情况进行实时监控和测量，以保证部署的网络能够满足实时多媒体业务的要求。目前比较权威的测量指标是有Cisco公司和IneoQuest公司共同提出的MDI(Media Delivery Index)媒体传输指标，是对媒体流在IP网络传输质量进行评估的测量指标。

在MDI标准中定义了两个视频流传输的指标：延迟因素DF(Delay Factor)和媒体丢包率MLR(Media Loss Rate)，并根据DF及MLR对视频流传输性能进行评测。

DF值表明被测试视频流的延迟和抖动状况。DF的单位是毫秒(ms)。DF将视频流抖动的变化换算为对视频传输和解码设备缓冲的需求。被测视频流抖动越大，DF值越大。当网络设备和解码器的缓冲区容纳的视频内容时间不小于被测视频流DF时，将不会出现视频播放质量的下降。

MLR（Media Loss Rate：媒体丢包率），媒体丢失率统计的是在选定的时间间隔内的丢失或乱序的数据包，这些数据包承载了流媒体应用的信息。该数值表明被测试视频流的传输丢包率。对乱序数据包的检测非常重要，因为许多设备往往不对接收到的数据包重新排序，而直接将其发送到解码器。任何数据包丢失（即出现非零MLR时）都会对视频质量带来不利影响，并造成视觉失真或异常以及不均匀的视频回放。

理想情况下的IP视频流传输要求MLR的数值为零。因为具体的视频播放设备对丢包可以通过视频解码中进行补偿或者丢包重传，在实际测试中MLR的阈值可以相应调整。

MDI主要反应了视频流传输的抖动和丢包特性。但是，MDI：MLR不能反应丢包的持续性。 实验数据表明，连续小量的丢包比一次大量的丢包对视频观看质量有更明显的影响。因此，MLT－15（过去15分钟媒体丢失总数），MLT－24（过去24小时媒体丢失总数）可以帮助使用者看到测试时间内的累积丢包数目。

小结

部署VOIP、视频会议、网络视频监控等应用的网络给IP网带来新的挑战，对网络中的流量和各类流量的带宽需求分析是成功部署该类网络的基础。本文在分析实时应用与传统数据应用的区别及其本身所具有的流量特征的基础上，根据分析结果给出实时网络的部署方案，最后，介绍了业界权威的IP多媒体网络传输质量的评估方法。■

无线监控简介

■ 文/任俊峰

无线监控的概念及功能

监控和无线传输技术的结合产生了无线监控，无线监控系统就是基于WLAN通信的监控系统。从某种意义上讲，无线监控是对现有有线监控的扩展和补充，将监控系统无线化，使用户能更方便的得到突发事件地点图像。

无线监控可以通过无线通讯手段，将不同地点的现场信息实时传送到监控中心，并且自动形成视频数据库便于日后的检索回放。在无线监控系统中，无线监控中心需要实时得到被监控点的视频信息，并且该视频信息必须是连续、清晰的。

在无线监控点，通常使用摄像头对现场情况进行实时采集，该监控点可以是固定点，也可以是移动接入点。接入点将采集到的视频信号进行编码后，再将视频数据交给无线传输网络，数据传到应急指挥中心，通过解码之后，可以放映到电视墙、VC客户端，或者接入到视讯系统，视讯会议参与方可以同时进行观看，达到对远程现场的一个即时监控。通过移动接入点，我们可以做到随时随地无线监控。

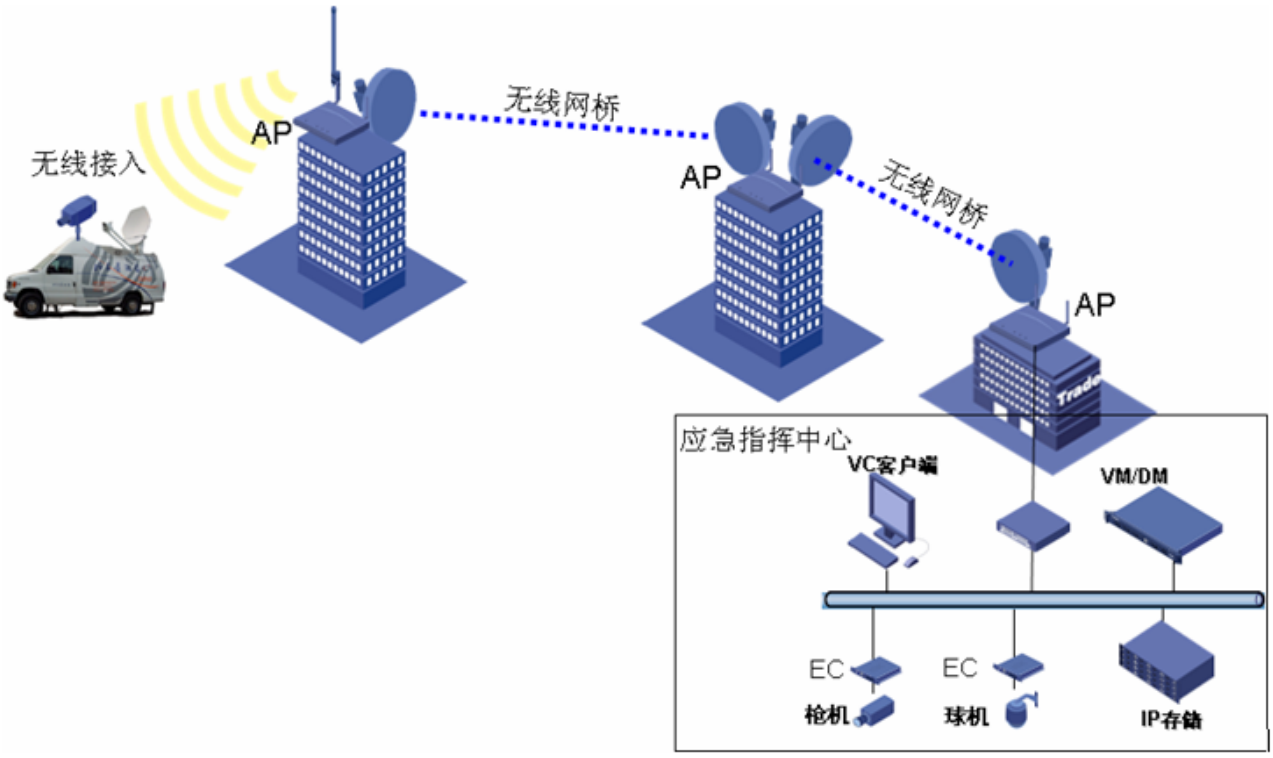


图1 无线监控应用组网图

无线监控的应用场景

无线监控可以广泛应用于范围广、分布散的安全监控、交通监控、工业监控、家庭监控等众多领域。如：

- 取款机、银行柜员、超市、工厂等无线监控服务
- 看护所、幼儿园、学校提供远程无线监控服务
- 电力电站、电信基站的无人值守系统
- 石油、钻井、勘探等无线监控系统
- 智能化大厦、智能小区无线监控系统
- 流水线无线监控系统，仓库无线监控系统
- 森林、水源、河流资源的远程无线监控
- 户外设备无线监理
- 桥梁、隧道、路口交通状况无线监控系统

无线监控的优点

无线监控和传统的监控方案相比，具有以下三大优点：

● 综合成本低，只需一次性投资，无须挖沟埋管，特别适合室外距离较远及已装修好的场合；在许多情况下，用户往往由于受到地理环境和工作内容的限制，例如山地、港口和开阔地等特殊地理环境，对有线网络、有线传输的布线工程带来极大的不便，采用有线的施工周期将很长，甚至根本无法实现。这时，采用无线网可以摆脱线缆的束缚，有安装周期短、维护方便、扩容能力强，迅速收回成本的优

点。

● 组网灵活，可扩展性好，即插即用，网络管理人员可以迅速将新的监控点加入到现有网络中，不需要为新建传输铺设网络、增加设备，轻而易举地实现远程视频监控。

● 维护费用低，无线网络维护由网络提供商维护，前端设备是即插即用、免维护系统。

无线传输系统的选择

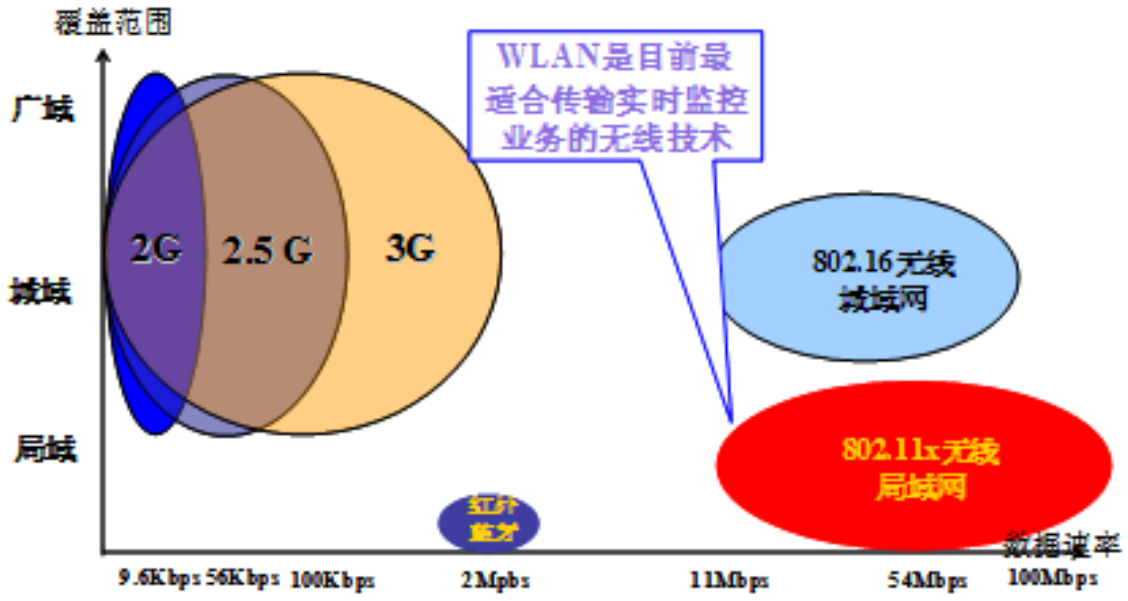


图2 各无线技术传输速率及覆盖范围

当前无线传输技术主要有2G技术（GSM）、2.5G（GPRS/CDMA）、3G（WCDMA/TD－SCDMA）、无线城域网技术和无线局域网技术，如上图所示

上图可以看出GPRS、CDMA1x 等无线方式无法满足对带宽需求较高的用户需求(GPRS拨号速率仅为144Kbps，CDMA1x速率为307Kbps)，WiMAX 主要是针对城域网范围的接入覆盖，将会与WLAN融合发展。但是目前WiMax由于频段的问题仍然受到国家管制，难以大规模得到应用；无线局域网技术的优势是具备可移动性、建网快，不受线缆资源以及工程安装环境的限制，可随时随地的给最终用户提供服务。目前无线局域网技术已成熟完善，802.11技术标准制定了网络接入、空口安全、用户隔离、多AP间慢速切换等特性规范。随着WLAN的802.11n技术和产品的成熟已使得无线能够达到300Mbps的带宽，因而WLAN是目前最适合传输实时视频监控业务的无线技术。

另外随着3G技术的发展与延伸，3G移动通信无线系统从概念的运作，到小范围的试点，再到目前的正式商用，经历了漫长的过程，三大运营商纷纷提前规划基于3G高速无线接入特性的业务，在将来基于3G无线网络的视频监控应用将是核心支柱。

无线监控的部署

相对于有线监控，无线监控的承载网为无线信号，我们在进行无线网络部署的时候，需要充分考虑到无线传输网络的特性，以下图为例，这是一个小型的园区网无线监控系统，使用WLAN作为传输网络。中心1号点作为落地点，以有线的方式接入到监控中心服务器，其他的监控节点都使用无线的方式接入到1号点。

接入方式选择，接入方式共有3种：

● 点对点接入：7号点使用点到点的方式接入到中心1号点；

● 点对多点接入：2号点和3号点使用点对两点的方式接入到中心1号点，这两个节点共享该频段的带宽；

● 多点级联：4号点、5号点、6号点级联接入到中心1号点

各监控点的平均可用带宽：

● 7号点独享一个频段的网络带宽，一个频段的带宽20Mbps，按50%的余量计算还有10M带宽

● 2、3号点共享一个频段的网络带宽，平均每点可得5M带宽

● 4、5、6号点共享6号点到1号点的一个频段带宽，平均每点可得3.3M带宽

图3 某园区网无线监控部署组网图

在实际部署时，可以根据上面三种方式的带宽分享情况来选择接入方式。11a、11g共有8个互不干扰的信道，因此每个落地点的设计频段不能超过8个。

无线天线的选择：

无线天线按方向性分类可分为：全向天线和定向天线，全向天线发出去的射频能量在各个方向上平均分布，适用于大面积的接入；而定向天线的射频能量主要集中在某一个方向上，适用于远距离传输或者扇形覆盖。

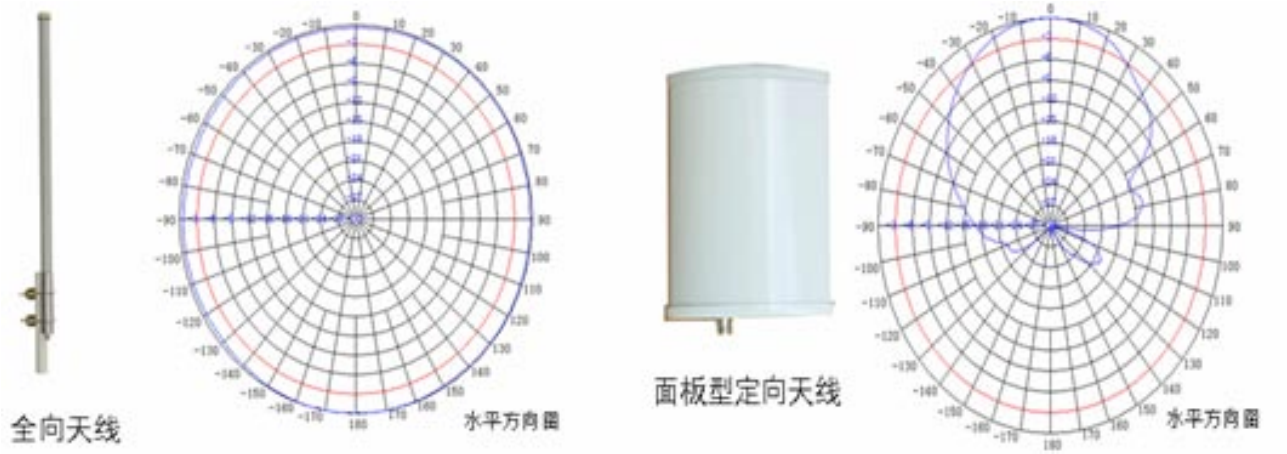


图4 无线天线外型及覆盖范围

在点到点或者多点级联方式时，建议使用定向天线；点到多点接入方式时，需要考虑多点的角度大小，可使用增益较小的定向天线或者全向天线。如果无线接入点是移动接入点，则前端需要使用全向天线进行覆盖。

无线视频业务对于误码率、切换效率、时延、带宽稳定性、安全等方面的有较高的依赖性。实际应用中，如下几点必须达到用户要求。

● 系统安全

对于无线网络，其传输介质是开放的，任何人都可以监听到你发出去的无线信号，也可以主动向你发送无线信号。因此，既需要对无线接入点进行身份认证，也需要对无线传输信号进行加密。

● 切换效率

当前端是移动接入点时，会从一个服务区漫游到另一个服务区，在跨服务区的时候，需要进行无缝切换，图像不能有明显的丢帧现象。

● 带宽及带宽稳定性

无线网络带宽需求要参照系统规划说明书，一条无线网桥最多同时传输几路视频信号，而每路视频信号的码流带宽又有多大，总和加起来之后，就是这条无线网桥必须要达到的带宽。无线网络的真实带宽受到空间距离、信号强度以及环境干扰等因素的影响。另外带宽稳定性也是一个很重要的因素。

● 网络丢包兼容性

无线网络是一个不可靠的网络，误码和丢包是经常会发生的。监控系统需要对网络有一个比较强的兼容性，即使发生了一定的错包、丢包，也能保证音视频的质量。

● 延时及抖动

在无线网络受到干扰，发生丢帧重传时，会导致报文出现较大的延时及抖动，这样在编码器端需要进行缓存解码，防止图像出现时快时慢的现象。另外客户在进行前端云台操作时，也不应出现明显的滞后感。

H3C无线监控方案

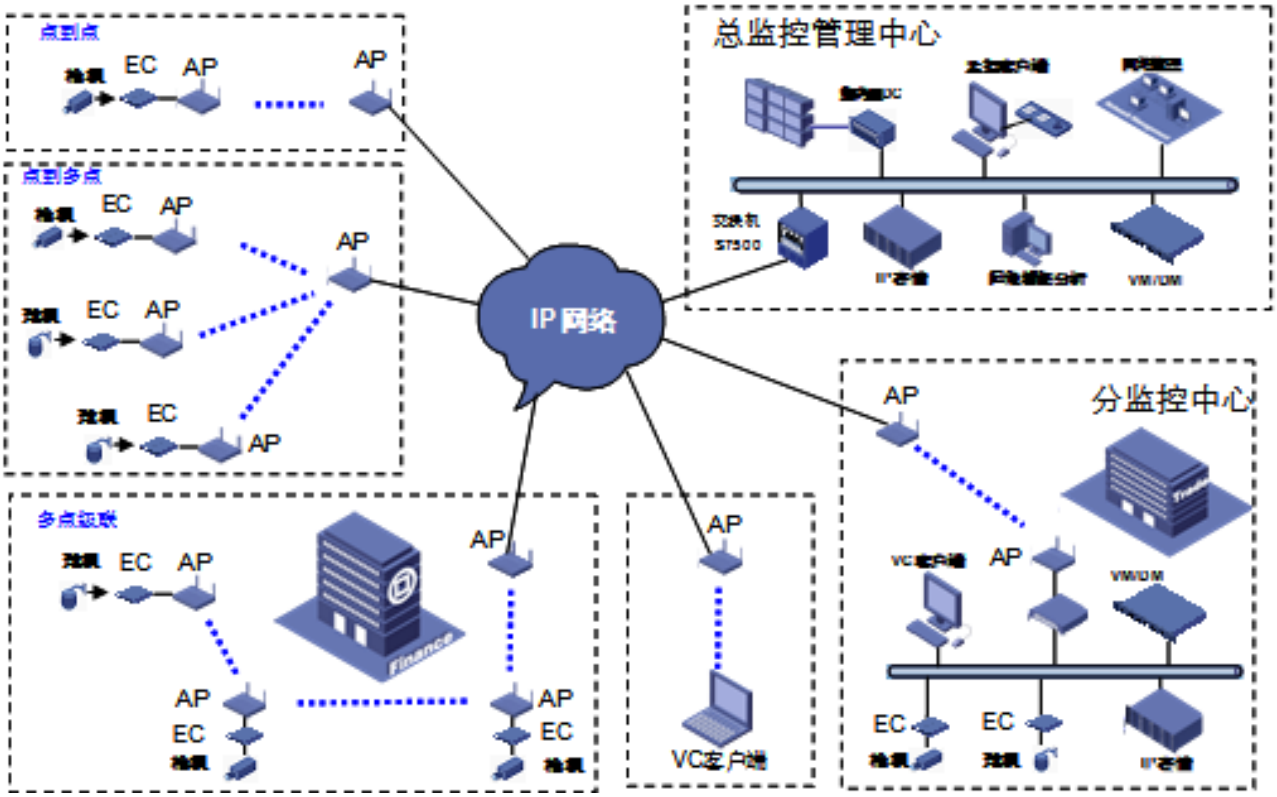


图5 H3C无线监控解决方案

H3C无线监控解决方案整合了公司无线网络和视频监控解决方案的优势，将IP智能监控从通常的有线网络接入延伸到无线网络接入，根据用户的应用场景提供丰富多样的无线组网接入模式，通过统一网管对无线资源和监控资源进行统一管理和控制，形成整体的无线监控解决方案。

无线监控解决方案整体由总控中心、分控中心、前端接入和客户端接入几部分组成，通常总控中心利用局域网互连，分控中心、前端接入和客户端接入都可以通过多种无线方式接入到总控中心的网络，总控中心主要由视频数据管理服务器（VM /DM）、IP存储、智能分析系统、管理客户端、显示系统和统一智能网管等核心部件组成；分控中心较为简单，通常部署IP存储和管理服务器等，通过多级多域方式接入到总控中心，在无线监控解决方案中分控中心可通过高带宽的点到点的无线方式接入，保障控制中心间的监控业务的相互查阅和调用；客户端接入通过无线网卡接入到固定AP上，对视频图像进行实时查看和历史查询；前端接入通常包括摄像头、编码器和AP等，通常会存在多个前端接入场景，可采用点到多点和多点级联方式接入。

对应于无线网络特性，下面谈一下H3C监控产品的部分特性。

TCP码流

无线传输环境，容易导致网络丢包，引起图像质量下降。而原有的实时播放流程使用的是UDP协议，在网络环境差的情况下，比如低带宽或无线传输情况，可能会丢失报文，导致图像无法正常播放。故针对实况播放的流畅性，在实时播放流程增加TCP协议连接，用于低带宽或无线传输等会导致大量丢失报文的环境，支持前后端设备在NAT后的组网环境，并且在通过媒体服务器（MS）转发的传输模式下，还支持UDP/TCP分段传输。

TCP/UDP分段传输是通过MS转发来实现。

● 编码器EC与MS之间传输方式取决于EC选择的传输方式，若EC的前端属性选择UDP，则EC对应的实时监控采用UDP的传输方式，若EC的前端属性选择TCP，则EC对应的实时监控采用TCP传输方式。

● MS与MS之间传输方式取决于上级域MS入口媒体流选择，可以在管理员版媒体服务器选项中进行修改若上级域MS选择UDP传输方式，则MS之间采用UDP传输方式；若上级域MS选择TCP传输方式，则MS之间采用TCP的传输方式。

● MS与DC/VC之间传输方式取决DC/VC选择的传输方式，若DC/VC选择UDP传输方式，则DC/VC对应的实时监控采用UDP的传输方式，若DC/VC选择TCP传输方式，则DC/VC采用TCP的传输方式。

缓存解码

Jitterbuffer缓存是将接收到的网络中的语音包缓存一定的时间，然后顺序平滑的发送到解码器，使得接收端从Jitterbuffer缓冲区流向语音解码器的语音包流和发送方是一致的或相近的，从而减轻网络抖动对语音质量造成的影响。缓冲是以牺牲一定的网络时延为代价的，时延越大，对抖动的过滤越好。但是延时也不能过大，以免带来不必要的延时。对于算法优秀的动态JitterBuffer，可以实现在延时及抖动中找平衡，同时应用优秀的排队及及时丢包处理以得到更加完美的互联网语音质量。

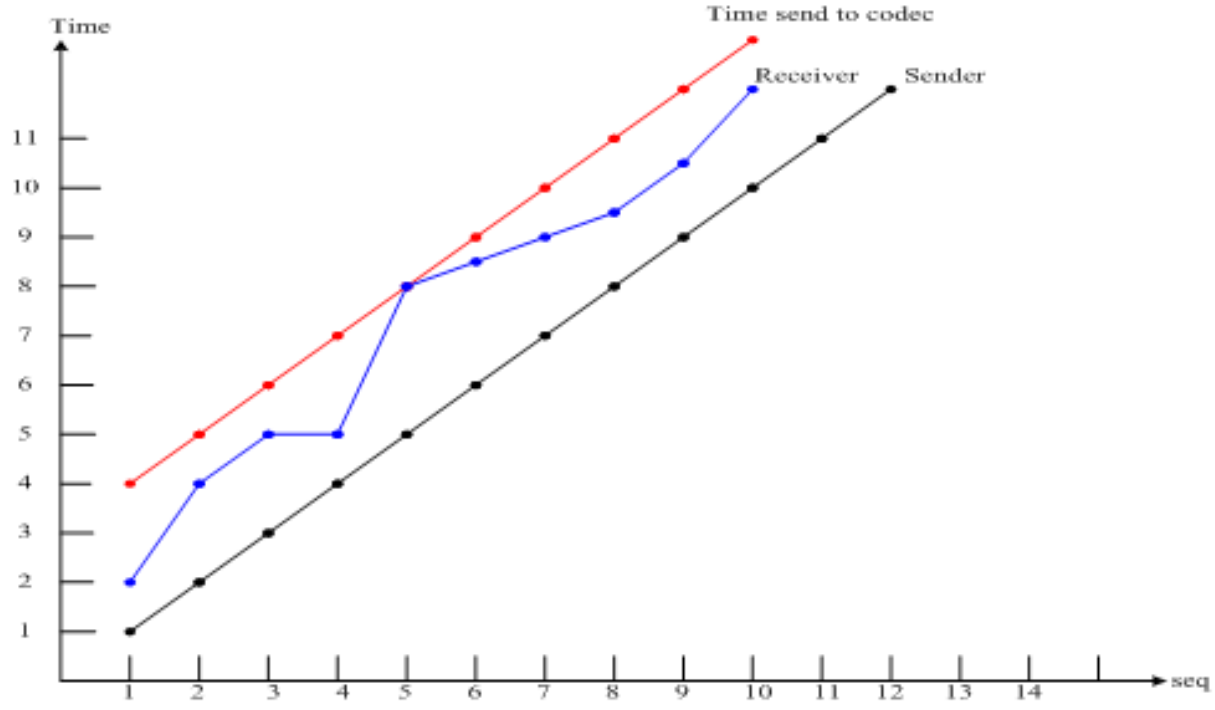


图6 Jitterbuffer缓存原理

通过JitterBuffer，我们可以将从网络上接收的语音包延迟一段时间后才开始播放。如上图所示，我们在接收方设置JitterBuffer，并将从网络上接收到的语音包缓存在其中，然后在t4时刻开始按照发送方的固定时间间隔将缓存在其中语音包传给编解码器处理并放音。由于所有的语音包在它们被播放的时刻之前已经到达，并且没有发生丢包的情况，因此语音包是按照固定间隔被播放的，因此语音质量得以改善。

而对于监控来说，不仅仅包含音频包，而且还有视频包，并且视频包的数量远比音频包多。在H3C监控产品中，Jitterbuffer可以实现的功能有：

● 利用IPcloud模拟网络延时，延时100~500ms，在开启jitterbuffer缓存情况下，图像能正常播放，

而在不启用缓存情况下，图像很卡，不连贯。

● 利用IPcloud模拟网络乱序，开启缓存，图像能正常播放，而不开启缓存则图像不连贯，甚至会花屏。

● 对于重复到达的包，也会进行处理。

前端存储

如果受到较强的外界干扰，无线网络带宽会下降，甚至无线网络邻居都有可能会断掉，这时候视频流就不能完整地传到监控中心进行实况或者存储，存在监控盲点。为了降低不法分子对开放的无线网络进行恶意的扫描攻击所带来的影响，也为了进行24小时的安全保障，H3C公司推出了前端EC本地存储功能，前端EC在正常业务的基础上，同时进行本地U盘或者移动硬盘的存储备份。在无线网络恢复后，客户可以将前端上的存储文件下载到本地进行存储，做到有据可查。■

传统VPN在监控中的应用分析

■ 文/任俊峰

概述

VPN（Virtual Private Network，虚拟专用网）是一种基于公共数据网的服务，它依靠ISP（Internet Service Provider）和NSP（Network Service Provider），在公共网络中建立虚拟专用通信网络。VPN可以极大地降低用户的费用，并且提供比传统专线方式更强的安全性。

在VPN中广泛使用了各种各样的隧道技术，有二层隧道技术，也有三层隧道技术。常用隧道协议包括：L2TP、GRE、IPsec、SSL VPN等。那么，什么是隧道呢？

隧道是一种封装技术，它利用一种网络协议来传输另一种网络协议，即利用一种网络传输协议，将其他协议产生的数据报文封装在它自己的报文中，然后在网络中传输。实际上隧道可以看作一个虚拟的点到点连接。

隧道技术简单地说就是：原始报文在A地进行封装，到达B地后把封装去掉，还原成原始报文，这样就形成了一条由A到B的通信隧道。隧道技术就是指包括数据封装、传输和解封装在内的全过程。

在监控应用组网中，经常会出现EC（编码器）设备或者VC（视频管理客户端）用户在远端私网，需要接入到总部监控中心的情形。在这种情形下，监控协议本身支持NAT穿越是一种解决方案，这种方案适用于私网----->公网模式，即EC和VC为私网地址，监控中心为公网的IP地址。但是如果双方都在私网内部，即：私网--->私网模式，由于彼此私网间通讯不能直接穿透公网，协议本身已经无法解决这个

问题，通过VPN隧道技术是最好的办法。我们将结合实际组网应用，介绍适合的VPN组网方式。

本文讨论的方案均基于如下前提：单域，VM、DM、MS、IPSAN等均配置在私网中，通过Internet（公网）与VC、EC/ECR等终端相连。

在VPN互连业务中，我们根据监控业务的实际应用，重点研究各类VPN在下面几个方面的适用性。

单播/组播

所有的VPN都天然支持单播，因此我们重点考虑组播对VPN的影响。监控业务中包括实况与存储两条数据流，其中在多点实况点播的情况下，实况流需要通过组播方式发送，因此所采用的VPN是否支持组播，对于监控业务来说是至关重要的。

NAT穿越

在现实组网中，我们经常遇到这样的情况：企业专网（包括总部、分支机构、接入终端）采用私网地址10.1.1.0/24，监控系统也利用这套网络进行媒体流、数据流传输。同时，分支机构坐落在某写字楼内，使用私网192.168.1.0/24。分支机构要通过VPN接入总部，隧道封装报文要先经过写字楼的私网，经过出口NAT再进入到运营商公网。此时， 所选择的VPN技术必须要支持NAT穿越。

动态地址获取与动态路由

分支机构的出口路由器可能使用的是拨号上网方式，动态获取公网IP地址，这就需要VPN隧道支持隧道端点采用动态IP地址。如果总部网络很大，分支机构较多，路由比较复杂的情况下，配置手工静态路由会相对比较麻烦，可维护性也很差。因此，是否支持动态路由也是选择VPN的一个重要因素。

加密

监控数据在网上进行传输，安全是一个非常重要的指标，需要防止各种不法分子窃取视频数据。

支持加密的VPN包括：IPsec VPN、SSL VPN

不支持加密的VPN有：L2TP、GRE

VPN载荷效率

如前所述，VPN是一种封装技术，会在初始报文上增加传输开销，增加的字节数量越多，有效载荷效率就越低。

以下部分我们将分别展开讨论VC和EC的VPN接入组网模型。

VC接入

对于监控图像的查看需求是随时随地的，因此要求视频管理客户端VC能够安装在任意一台电脑上，使用者利用合法的用户名和密码登录后，即可查看实时、历史监控图像。VC可能出现在各种场合，按照其接入位置，可分为分支机构、移动办公两种。

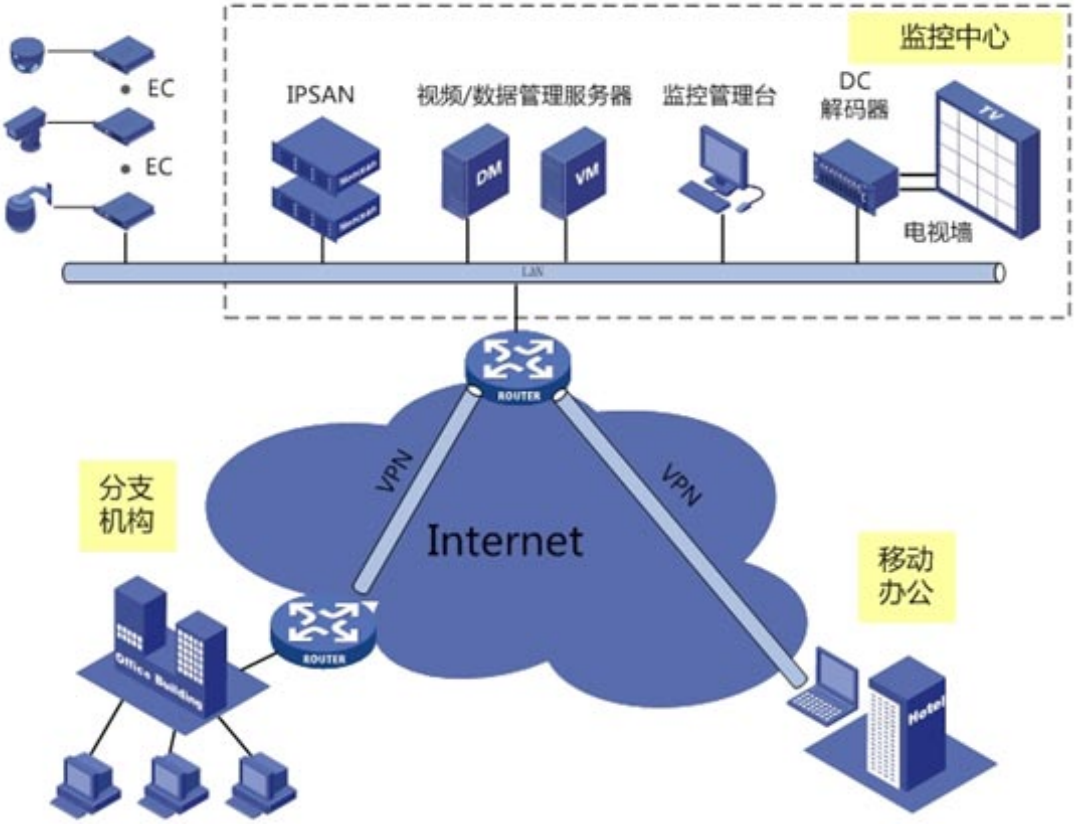


图1 VC分支机构与移动办公接入

分支机构

分支机构一般指该专网在某地设有常驻的分支机构，分支机构网络与总部一样，也采用私网地址，通过路由器与总部路由器/防火墙建立VPN隧道，穿越Internet公网与总部相连。对于分支机构VC接入，我们推荐以下几种隧道接入方式：

GRE

GRE是对某些网络层协议（如：IP，IPX，AppleTalk等）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议（如IP）中传输，这是GRE最初的定义。最新的GRE封装规范，已经可以封装二层数据帧了，如PPP帧、MPLS等。在RFC2784中，GRE的定义是“X over Y”，X和Y可以是任意的协议。

GRE隧道不能配置二层信息，但可以配置IP地址。GRE利用为隧道指定的实际物理接口完成转发，转发过程如下：

（1）所有发往远端VPN的原始报文，首先被发送到隧道源端。

（2）原始报文在隧道源端进行GRE封装，填写隧道建立时确定的隧道源地址和目的地址，然后再通过公共IP网络转发到远端VPN网络。

GRE隧道源端与目的端的关系依赖于手工维护，因此适用于有固定关系的网络设备之间建立隧道，符合分支机构与总部的组网方式，但不适合直接由PC机发起链接的移动办公方式。

1. 单播与组播

GRE隧道具有虚接口的概念，隧道一旦建立成功后，该隧道对于监控的单播或者组播都是天然支持的。下面以网关（GW）建立VPN隧道，描述组播业务开展。

1）GW1支持动态组播协议时，在VC侧启用IGMP，在Tunnel口上启用PIM SM。在监控中心网关GW2的Tunnel上也启用PIM SM，这样GW1和GW2能建立PIM邻居，GRE隧道两端就在同一个动态组播域中，对于所有的组播业务都能支持。

2）GW1不支持动态组播协议或者不起用动态组播协议时，可以在私网侧启用IGMP，将Tunnel接口作为IGMP Proxy的上行口，而在GW2的Tunnel口上启用IGMP。这样对于GW2来说，GW1不再是一个PIM邻居，而只是一台主机。

2. NAT穿越

GRE隧道两端需要静态指定对端的公网IP，且GRE封装头中没有传输层端口，所以GRE不支持采用端口复用的NAT网关(应用最广泛的一种方式)。

3. 动态地址分配

GRE隧道双方需要静态指定对端的公网IP，因此不支持动态地址方式。

4. VPN载荷

GRE头一般长4个字节，而新IP头为20个字节，所以新的报文增加了24个字节开销。

GRE Over IPsec

IPsec VPN基于一组开放的网络安全协议，能够提供服务器及客户端的双向身份认证，为IP及其上层业务数据提供安全加密保护。IPsec能够支持数据加密（包括常见的DES,3DES,AES加密算法），数据完整性验证，数据身份验证，以及防重放等功能，充分保证业务数据的安全性。

IPsec的加密确保了通讯的机密性，在端到端的VPN中，IPsec VPN是应用的最多的一种。但是IPsec VPN设计没有独立接口，不支持组播，也不支持动态路由协议。所以很多情景下会与GRE或者L2TP隧道嵌套使用，即先使用GRE或者L2TP进行报文封装，然后再使用IPsec进行加密。

1. 单播与组播

IPsec协议本身天然支持单播，但因为IPsec隧道没有接口的概念，无法支持动态的组播协议。

采用GRE Over IPsec模式，可以利用GRE天然的单播、组播支持能力，满足监控网络的各种组播需

求。

2. NAT穿越

IPsec支持NAT穿越。IPsec 隧道在使能了NAT穿越特性后，在封装的时候会增加一个UDP的封装头来支持NAT穿越。如果认证使用Pre-share-key方式，则需要使用野蛮模式的Name方式；如果使用了PKI方式，使用第三方证书进行身份认证，支持NAT穿越。关于IPsec的NAT穿越问题，有兴趣的读者可参阅《网络之路》第四期相关章节。

采用GRE Over IPsec模式，由于IPsec封装在外， GRE作为乘客协议不受NAT影响。

3. 动态地址分配

IPsec使用野蛮模式的Name方式时，IPsec 隧道支持动态地址分配。可使用loopback口作为GRE隧道的源和目的，这样虽然设备的出口地址是动态获取的，但GRE的隧道地址依然使用静态地址。

4. VPN载荷

如果使用常用的隧道模式，使用ESP加密/认证算法，不使用AH，IPsec共增加了68个字节（包含了穿越NAT所需要添加的字段）。其它方式这里不作赘述。

GRE Over IPsec模式的VPN载荷相当于IPsec载荷与GRE载荷之和，即68＋24＝92字节。

L2TP

L2TP中定义了3个角色：CLIENT、LAC、LNS。LAC与LNS间是一个IP网络，LAC与CLIENT之间一般是一个PPP链路（常用的是PPPoE、DDR方式的PPP等）。L2TP的目的是建立一条跨LAC的CLIENT与LNS之间的PPP链路，LAC将CLIENT过来的PPP报文封装到IP报文(先是一层L2TP的封装，然后是UDP的封装，再封装到新的IP头），最后发送到LNS端。

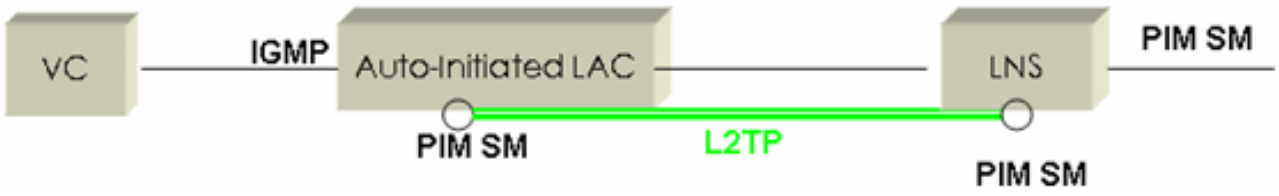
在实际应用中，L2TP隧道的建立方式有两种情况：触发建立、永久建立。

在分支机构组网方式下，VC接入总部监控中心，建议使用隧道永久建立方式，该方式下，LAC和CLIENT两个角色在同一个设备上，我们称之为Auto-Initiated LAC设备。

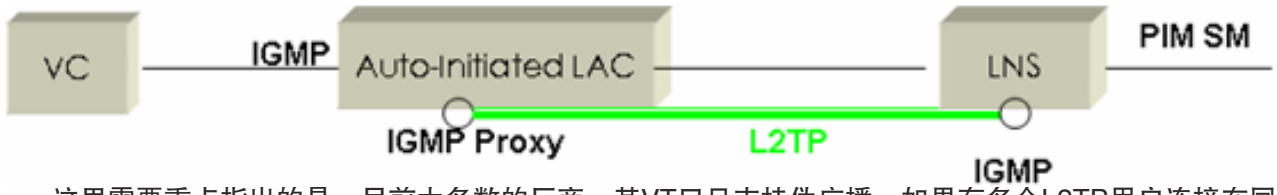
1. 单播与组播

大多数厂商的L2TP都有虚接口VT的存在，在隧道建立后，隧道链路就相当于一条实际的链路连接了两个VT口，天然支持单播报文转发，同时VT口也可以启用组播协议。

1）Auto-Initiated LAC设备支持组播协议时，可以在Auto-Initiated LAC的接VC端起用IGMP，VT口上启用动态路由协议PIM SM；在LNS的VT口和内网口上启用PIM SM，则Auto-Initiated LAC和LNS能建立PIM邻居，隧道两边就处于同一个组播域中，对于组播的相关特性都能支持。



2） Auto-Initiated LAC设备不支持或者不起用动态路由协议时，可以作为IGMP Proxy设备，将VT口作为IGMP Proxy的上行口，而LNS的VT口上启用IGMP，这样Auto-Initiated LAC设备对于LNS设备来说就是一台主机。



这里需要重点指出的是：目前大多数的厂商，其VT口只支持伪广播，如果有多个L2TP用户连接在同一个VT口上，则设备在出方向会把组播和广播报文为每个连接复制一份。也就是说如果存在多个Auto-Initiated LAC连接到一个VT口，同一个组播报文会向每一个Auto-Initiated LAC都发送，即使很多Auto-Initiated LAC下的VC用户根本不需要这条组播流。这样浪费了大量的带宽资源。在这里，我们就需要对组网方式进行一定的规划和限定。如果是分支机构，我们知道这种机构是有限的，并且可控的，我们可以为这些分支分别建立不同的VT口，这样，分支间的组播流就不会互相干扰了。如果是移动用户，这些用户是临时的，且非常多，虽然选择使用组播方式也能正常地工作，但是付出的带宽代价太大，同时我们也不可能为这些用户分别分配VT口，因此这些用户只能单独共用一个VT口，且用户在进行实况业务的时候，请在VC客户端上选择不支持组播。

2. NAT穿越

通常L2TP数据以UDP报文的形式发送，那么协议本身就支持公网NAT的穿越。当然分支肯定是要作为隧道的发起者。

3. 动态地址分配

LNS对LAC和client使用的是隧道和用户名的认证方法，对接入IP没有要求，因此天然支持动态地址分配。

4. VPN载荷

L2TP封装会增加的字段包括PPP头 4个字节、L2TP头6个字节、UDP8个字节、新IP头20个字节，共38个字节。

移动办公

移动办公是指安装VC的PC独立移动，在任何位置接入Internet，由PC机自身与总部路由器/防火墙建立VPN隧道。

在移动办公情况下，单个VC接入到总部监控中心，建议使用隧道触发建立方式，PC自身作为LAC，由PC直接发起L2TP，与总部路由器或防火墙建立VPN隧道。如果需要提高网络安全性，可以使用IPsec做一次加密，即采用L2TP Over IPsec模式。

SSL VPN

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，为基于TCP的应用层协议提供安全连接，如SSL可以为HTTP协议提供安全连接。SSL协议广泛应用于电子商务、网上银行等领域，为网络上数据的传输提供安全性保证。

SSL VPN系统是一款采用SSL连接建立的安全VPN系统，为企业移动办公人员提供了便捷的远程接入服务。

首先我们需要对SSL VPN进行一定的了解，以便于我们选择合适的、可用的接入方式。SSL VPN有三种接入方式：Web接入、端口转发(TCP接入)、网络扩展(IP接入)。这三种方式有着不同的特点。

● Web接入使用的是proxy代理原理，通过修改URL来达到对内网Web服务器的访问。

● TCP接入通过在接入端自动安装SSL VPN客户端代理，用户只需要与SSL VPN客户端不同的监听端口建立TCP的连接，SSL VPN就可以将用户的数据报文转发到目的主机，本方式主要用于基于TCP的内网业务访问。

● IP接入方式则会自动在接入端安装一个虚拟网卡，虚拟网卡先与SSL VPN服务器建立一条SSL VPN隧道， 用户访问内网的数据都是通过这条隧道来加密、封装和转发，本方式适用于基于IP的内网业务访问。

由于监控业务中有部分协议不是基于TCP的，而且部分TCP应用的端口是临时协商的，譬如FTP，所以web方式和TCP端口方式在这里并不适用。因此我们推荐第三种方式：IP接入方式，SSL VPN仅在VC和企业总部间建立一条隧道，对所有的IP报文都进行加密，对具体的业务不作区分。在SSL VPN服务器端，将监控设备的网段加入到IP网络资源中，允许监控用户访问所有的监控设备。在SSL VPN客户端，将IE打开，登录到SSL VPN服务器端地址上，使用分配好的用户名、密码登录，完成后，即可采用VC客户端对监控中心进行访问。

1. 单播与组播

天然支持单播。

对于SSL VPN Server设备的虚拟SSL VPN接口，用户只能配置IP地址，不能进行其他的配置，也不能启用IGMP功能，因此不支持组播业务。

2. NAT穿越

SSL封装是在TCP之上的，因此其天然支持NAT穿越功能；

3. 动态地址分配

SSL VPN Server并不关心Client的IP地址，所以支持动态地址方式。

4. VPN载荷

IP接入方式封装多了SSL加密部分20个字节， SSL头5个字节，TCP头20个字节，IP头20个字节，共65个字节。

3 EC/ECR接入

EC/ECR接入与VC接入方式类似，分为两种，一种是区域EC/ECR接入（即一个区域多台EC/ECR接入），另一种是远端单一EC/ECR接入。与VC接入不同的是，EC/ECR是物理设备，而非软件，不能安装在PC机上，不能由PC机直接发起VPN链接。因此在两种方式下，EC/ECR均需要借助路由器或其他网络设备建立VPN隧道，与VC分支机构接入方式类似，因此后文中不再区分EC/ECR的接入方式，归并为一类进行讨论，同时仅描述与VC分支机构接入方式有差别的部分，相同部分参照VC接入中相关部分。

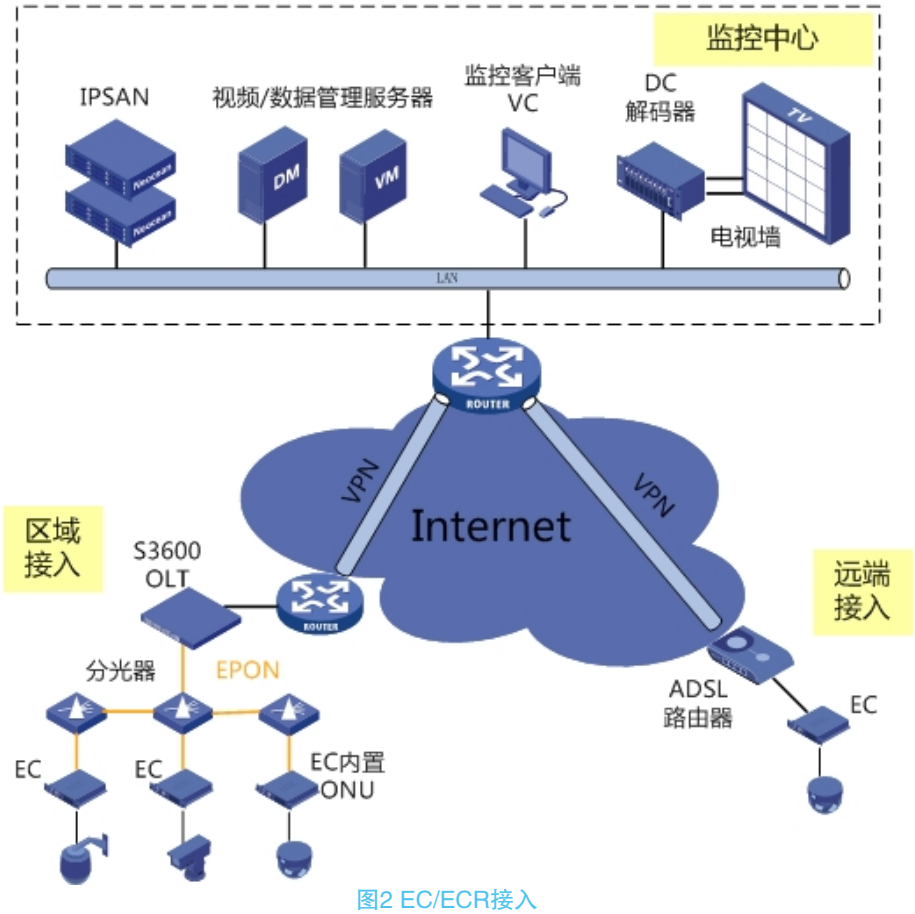
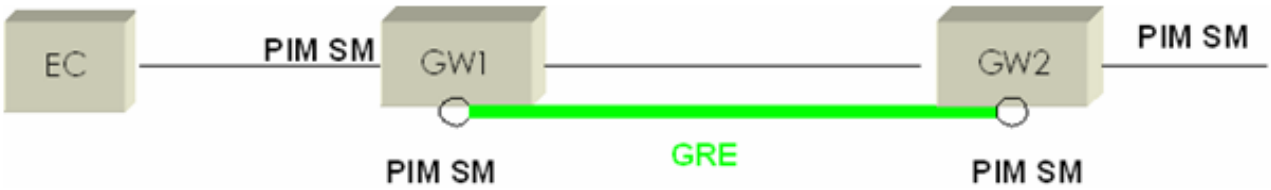


图2 EC/ECR接入

GRE

天然支持单播。为了支持组播在GW1的内网接口和GW1 GRE隧道接口上都启用动态组播协议，在监控中心网关GW2的Tunnel上也启用PIM SM，这样GRE隧道两端就在同一个动态组播域中，对于所有的组播业务都能支持。

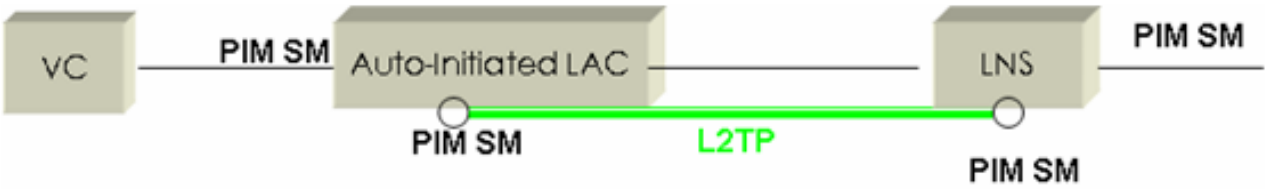


NAT穿越、动态地址分配等与VC接入方式中的GRE章节描述一致。

GRE over IPsec 方式与前文VC接入方式中的GRE over IPsec 章节描述相同

L2TP

使用隧道永久建立方式即将LAC与CLIENT合并。在Auto-Initiated LAC和LNS的私网端和VT口上都启用动态路由协议PIM SM，则Auto-Initiated LAC和LNS能建立PIM邻居，隧道两边就处于同一个组播域中，对于组播的相关特性都能支持。



使用隧道触发建立方式：

LAC对报文进行二层透传，因此对LAC没有要求，EC相当于一个组播源与LNS直连，仅需要在LNS的VT口和私网端起用动态路由协议即可。当然这种方式需要EC支持PPPoE。

需要注意的是：因为L2TP隧道是可以一对多的，如果点播用户VC也在私网侧，且和该EC都登录到了同一个VT接口，这样LNS上的PIM表项就无法建立了，因为上行口和下行口都是同一个VT接口，流量就无法通过组播转发到VC上。

NAT穿越、动态地址分配等与分支机构使用L2TP接入部分的描述一致。

总结

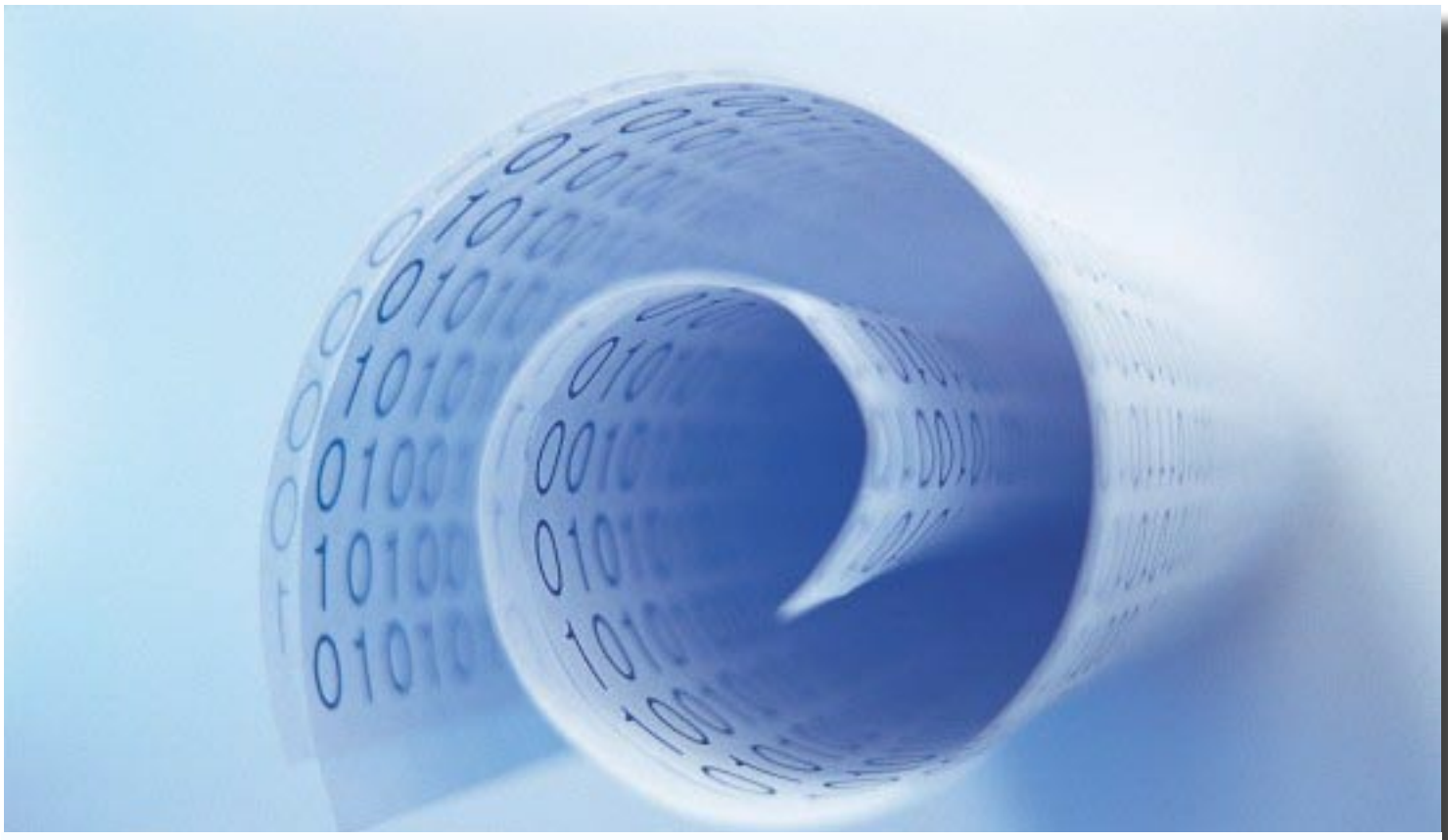
VPN支持能力一览

隧道	是否支持NAT穿越	是否支持动态获取IP地址	是否支持动态路由	是否支持组播		封装增加的字节数	是否支持加密
				VC在私网侧	EC在私网侧		
GRE	N	N	Y	Y	Y	24	N
L2TP	Y	Y	Y	Y	Y	38	N
IPsec	Y	Y	N	N	N	68	Y
SSL VPN	Y	Y	N	N	N	65	Y
GRE over IPsec	Y	Y	Y	Y	Y	92	Y
L2TP over IPsec	Y	Y	Y	Y	Y	106	Y

各类组网情况下，推荐使用的VPN方案

		主推VPN方案	
		加密	不加密
VC接入	分支机构	GRE over IPsec	GRE
	移动办公	SSL VPN	L2TP
EC接入	区域接入	GRE over IPsec	GRE
	远端接入	GRE over IPsec	GRE

■



图像质量主观评价方法介绍

■ 文/郭 琪

当今社会中，多媒体通信应用越来越广泛，主流的多媒体通信系统包括会议电视系统、视频监控系统、IPTV系统、移动流媒体系统和手机电视系统等。在这些多媒体通信领域中，视频图像信息的处理一直是研究的热点。

数字视频图像在采集、压缩、处理、传输和重现的过程中会引入各种各样的失真，影响图像的质量，从而直接影响用户的主观感受。在实际应用中，视频图像质量的好坏是评价多媒体通信系统重要的、必不可少的指标。因此，图像质量的评价方法研究有着重要的理论意义和广泛的应用需求。

当前对图像质量的评估方法主要分成两类：主观评价和客观测量。本文就数字视频图像质量评价中的主观评价方法做详细论述。

主观评价模型

目前，图像质量主观评价的方法与标准已相对完善，主观评价国际标准ITU-R BT.500-11《Methodology for the subjective assessment of the quality of television pictures（电视图像质量主观评价方法）》、ITU-R BT.710-4《Subjective Assessment of image quality in High-Define television（高清晰度电视图像质量的主观评价）》和国家标准GY/T 134-1998《数字电视图像主观评价方法》中均公布了可借鉴的主观图像评价方法。上述标准对数字视频处理系统的图像处理能力进行图像质量主观评价时需要的相关方面进行了介绍。

图像质量主观评价就是按照主观评价标准中规定的要求，如观看条件、信号源、评价系统、测试素材、观看员、评价测试过程等方面的约束下，将待评价的图像序列播放给观看者观看，并记录他们的打分，然后对所有观看者的打分进行统计，得出平均分作为评价结果。

下图1形象地展示了图像质量主观评价的测量方式。

图1 观看员正在进行主观评价

主观评价系统采用如下图2所示模型。信号源直接提供基准数字图像信号，并作为被测系统的输入，经被测系统则成为被测图像。由定时开关切换输出图像到评价用监视器上，输出图像或直接来自信号源，或经过被测系统，或来自灰场信号发生器。

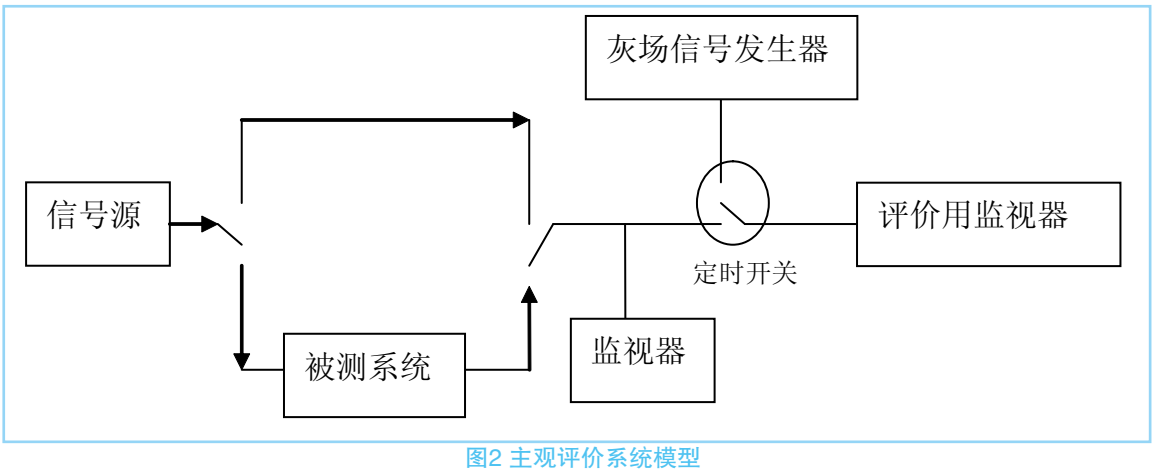


图2 主观评价系统模型

受邀参加评价打分的观看员观看评价用监视器显示的图像，并负责对图像序列进行打分。常用的主观评分标准主要有五级评分等级、七级评分等级（高清晰度采用）和比较评分标度。表1、表2、表3分别列示了三种评分标准的内容。

ITU–R 五级评分等级

表1 五级主观质量评分等级

五级评分等级	五级质量标度	五级损伤标度
5	优	5 无觉察损伤
4	良	4 稍可觉察，但不讨厌
3	中	3 略为讨厌
2	差	2 讨厌
1	劣	1 非常讨厌

ITU–R七级评分等级（高清晰度采用）

表2 高清七级主观质量评分等级

评分等级	高清晰度采用七级评分等级	评价
7	不能觉察任何图像损伤	特别好
6	刚能觉察有图像损伤	相当好
5	不同程度的觉察，轻度损伤	很好
4	有损伤，但不令人讨厌	好
3	有令人讨厌的损伤	稍差
2	损伤令人讨厌，但尚可忍受	很差
1	非常令人讨厌损伤，无法观看	劣

ITU–R比较评分标度

表3 比较评价标度

评分等级	比较评分标度
–3	差得多
–2	较差
–1	稍差
0	相同
+1	稍好
+2	较好
+3	好得多

在每个评价测试阶段开始时，应该向观看员详细、正确地介绍评价方法、测试中可能出现的主要损伤类型和质量要素、使用的评分标度以及图像显示、评分的时间和顺序，并进行评价示范显示。

一个评价测试阶段包括示范说明在内一般不超过半个小时。在正式测试开始前，需要引入3至5个测试周期来稳定观看员的判别力，其结果的数据不纳入测试结果的统计中。不同测试图像的显示顺序采用伪随机方式。评价测试阶段流程图如图3所示。

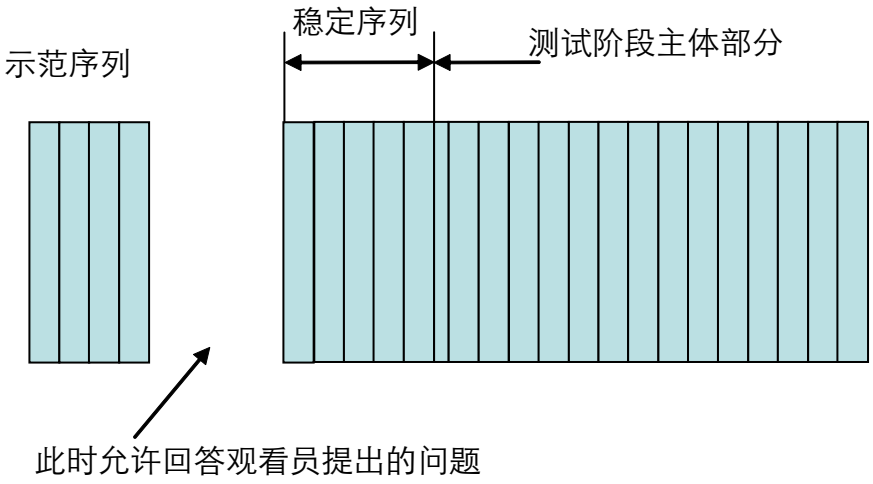


图3　评价测试阶段流程图

对评分结果，就每项测试参数，给出评分值统计分布的平均值、标准偏差和95%的置信区间。若评价中采用改变参数值来改变损伤程度的话，则采用曲线拟和技术得到一条曲线。

主观评价方法

国际标准ITU-R BT.500-11《Methodology for the subjective assessment of the quality of television pictures（电视图像质量主观评价方法）》、ITU-R BT.710-2《Subjective Assessment of image quality in High-Define television（高清晰度电视图像质量的主观评价）》和国家标准GY/T 134-1998《数字电视图像主观评价方法》中列举了许多主观评价方法。目前已有的主观评价方法包括双刺激连续质量标度方法（double-stimulus continuous quality-scale，DSCQS）、双刺激损伤标度方法（double-stimulus impairment scale，DSIS）、单刺激方法（Single-stimulus，SS）、刺激比较方法（Stimulus-comparison）、单刺激连续质量评价方法（Single stimulus continuous quality evaluation，SSCQE）、同时双刺激连续评价方法（Simultaneous double stimulus for continuous evaluation，SDSCE）和新近提出的视频质量主观评价方法（Subjective Assessment Method for Video Quality Evaluation，SAMVIQ）。

常用的两种主观评价方法为双刺激连续质量标度方法（DSCQS）和单刺激连续质量评价方法（SSCQE）。

在双刺激连续质量标度法中，要求观看员对每个测试图像的两种状态，即基准状态（直接来自信号源）和被测状态（经被测系统）的图像总体质量进行评价，基准图像和被测图像应以伪随机次序排列，交替显示一次和两次后进行评分，并在评分表上作出标记。

单刺激连续质量评价方法，只把被评价的序列播放给观看者看。该方法适用于仅只一次地主观观看图像材料而没有源图像参考时的评价。

评价方法的选择

图像评价中使用着广泛多样的基本测试方法。但实际上，具体的方法应用来解决具体的评价问题。对于典型评价问题所采样的主观评价方法在下表4中列示。

表4 测试方法的选择

评价问题	所用方法	描述
测量相对于参考系统的系统质量	双刺激连续质量评估（DSCQS）法（1）	ITU–R BT.500建议书，5节
测量系统的坚实性（即失效特性）	双刺激连续质量评估（DSCQS）法（1）	ITU–R BT.500建议书，5节
定量系统的质量（无参考系统可应用时）	比例标度法（2）或分类标度法，正在研究中	ITU–R BT.500建议书，5节
比较两种系统的质量（无参考系统可用时）	比例标度法（2）或分类标度法，正在研究中	ITU–R BT.1082报告书
认识在哪些系统中感知到差别的因素，测量其知觉影响	方法正在研究中	ITU–R BT.1082报告书
确定损伤变的可见的点	强制选择法做阈值评估或是调整法，正在研究中	ITU–R BT.1082报告书
确定各系统间是否被感知到有区别	强制选择法，正在研究中	ITU–R BT.1082报告书
测量立体图像编码的质量	双刺激连续质量评估法（3）	ITU–R BT.500建议书，5节

备注：
（1）对双刺激连续质量评估法和双刺激损伤评估法进行了某些相关影响的研究。已发现，双刺激损伤评估法的结果在一定程度上受到相关影响的偏差。
（2）一些研究指出，当有完全范围的图像质量可供应用时，此方法更为稳定
（3）当评价立体图像时，由于可能感觉高度疲劳，一个测试时段的总时间不应超过30分钟

图像质量评价要素

一般的图像质量主观评价只针对总体评价进行打分评价。也可以对每种具体图像质量要素进行单独评价，每种质量要素单独评价后，再加权获得总体主观评价分数。

各种图像质量评价要素主要包括以下几个方面：

颜色平滑度

颜色平滑度指的是图像经过系统处理再还原后，颜色过渡处理的好坏程度。

当色度分辨率过度下采样，采样位置不是很准确，采集芯片对色度信号分离不是很理想，或编码器对色度分量过度压缩时，都会出现还原画面色度偏移，造成颜色不够平滑。

一般采用制作成色带形式的标准视频源，或采用色彩变化比较丰富的标准视频源，作主观对比。

画面还原清晰度

画面还原清晰度指的是图像经过编码处理再还原后，画面纹理细节还原质量的好坏。

图像压缩或处理都会出现信息丢失，尤其是高频纹理细节信息，都会被压缩掉。导致解码还原时，纹理细节不清晰。

一般画面还原清晰度检测序列选择对清晰度要求较高的高纹理场合，如银行点钞。多数电视机或监视器的清晰度本身是不够的，所以应尽量排除显示器材引入的图像清晰度问题。

快速运动图像处理

当视频编码过程中遇到图像画面中较为剧烈运动的场景时，受时间预测和码率的限制，解码端重建图像质量可能会急剧下降，快速运动图像处理就是针对这一情况的检测方法。快速运动图像处理指的是系统针对快速运动图像编码时，帧间物体偏移距离过大时，为提高每帧图像的时间预测的准确性，保证解码端图像质量的处理方法。

通常对快速运动图像，以重建图像不出现马赛克及图像细节清晰度作为衡量标准。

复杂运动图像处理

复制运动图像处理指的是对复杂运动环境中物体形状进行有效提取的处理方法。

复杂运动不仅是指图像画面纹理细节的复杂，同时也有运动方向的复杂。一般的复杂运动图像处理是以能识别、区分物体特征及动作来衡量。一般采用具有高纹理运动场景的图像序列作为该质量要素的测试序列。

低照度环境图像处理

低照度环境图像处理指的是对低照度环境下产生的噪声而进行最低抑制处理。

低照度情况下，视频信号噪声主要表现为雪花亮点随机出现，因而主要通过观看重构视频序列中雪花亮点的多少和是否带来图像模糊，由此导致无法看清关键物体，来衡量低照度处理效果。

边缘处理

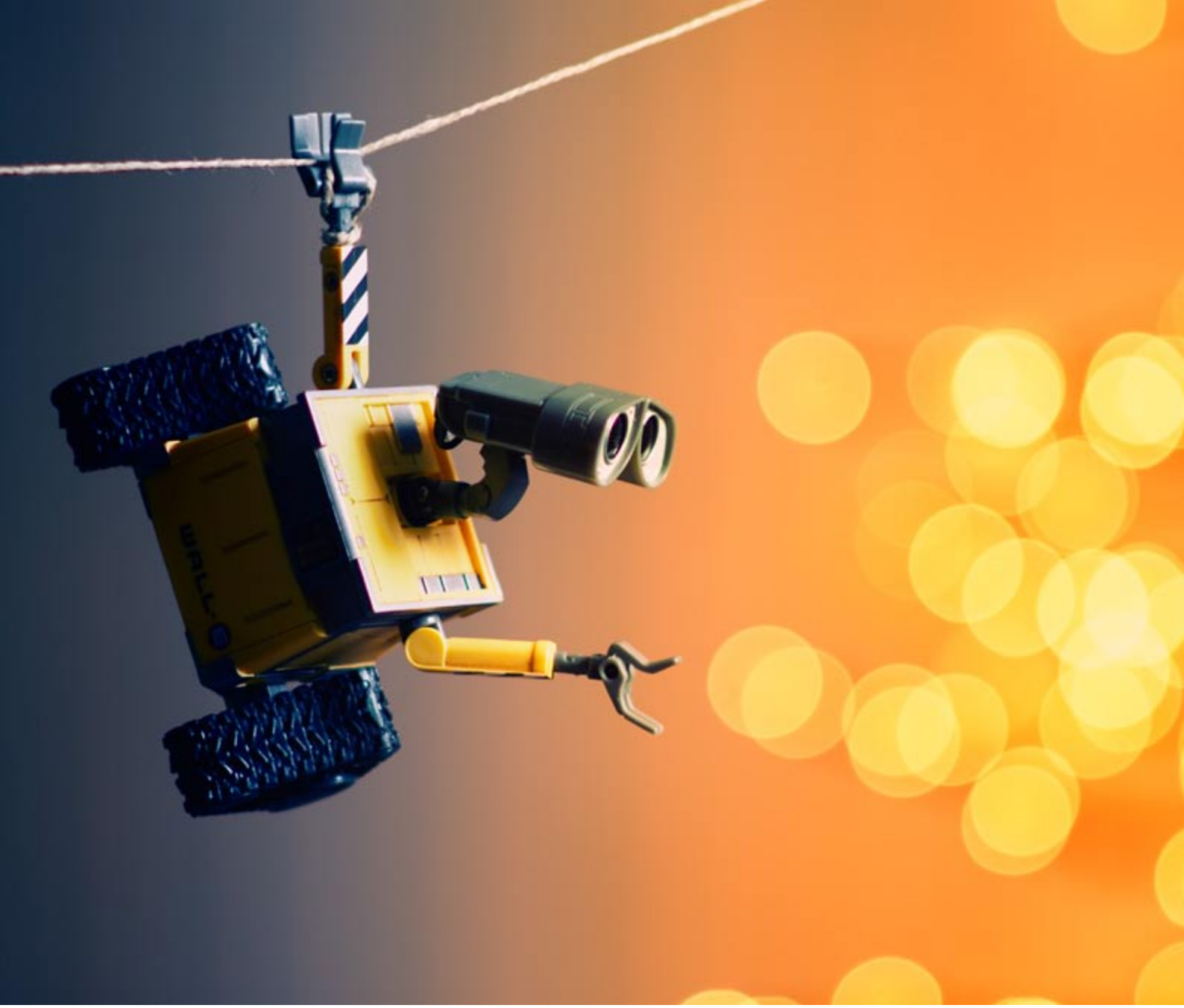
边缘处理指的是为图像经过系统处理后物体边缘出现抖动、云雾、模糊等情况，造成图像轮廓不清晰而进行的编码处理方法。

边缘处理的好坏主要体现在物体轮廓的清晰和逼真。

图像流畅性

图像流畅性指的是视频序列经过系统处理还原后，视觉上是否会出现跳动的现象。

图像质量主观评价虽然从人眼主观感受出发，能真实地评价图像的质量，但存在人力和物力投入大，为时较长，容易发生主观上的差错，且不能进行实时监测的缺点。目前，各国组织正着力于研究图像质量的客观测量方法和仪器，减少了对人力、物力的需求，测量时间大大缩短，达到与主观评价较吻合的评价结果。■



视频质量客观评价方法介绍

■ 文/袁　飞

视频质量评价方法可用来评价视频质量的好坏以及视频压缩传输处理方法的优劣，在视频处理和视频质量监控领域至关重要。视频质量评价方法分为两大类：主观评价方法和客观评价方法。主观质量评价方法是最可靠的评价方法，但在实际应用中将花费大量时间和费用，代价很高。因此，基于PSNR（峰值信噪比）和MSE（均方误差）等客观评价方法仍然因其低复杂度和简单清楚的物理意义而广泛地应用在视频评价领域。但是由于它们没有充分考虑人眼视觉特性，因此会造成客观评价结果和实际视觉效果的不一致。

为了得到与主观评价结果一致的评价结果，目前多个研究组织已经提出了基于人眼视觉特性（HVS）仿生模型的视频质量客观算法；这些算法依据人眼的视觉特性从采集的视频文件中提取一些人眼可感知的特征，

在对这些特征进行相应地计算，得出客观评价值。这些客观评价算法相对于PSNR及MSE来说，其评价结果与主观评价结果已经有了很大的接近。下面将简单的介绍视频质量客观评价常用的客观测试模型及几种与主观评价结果关联较大的客观测试算法。

视频质量客观测试模型

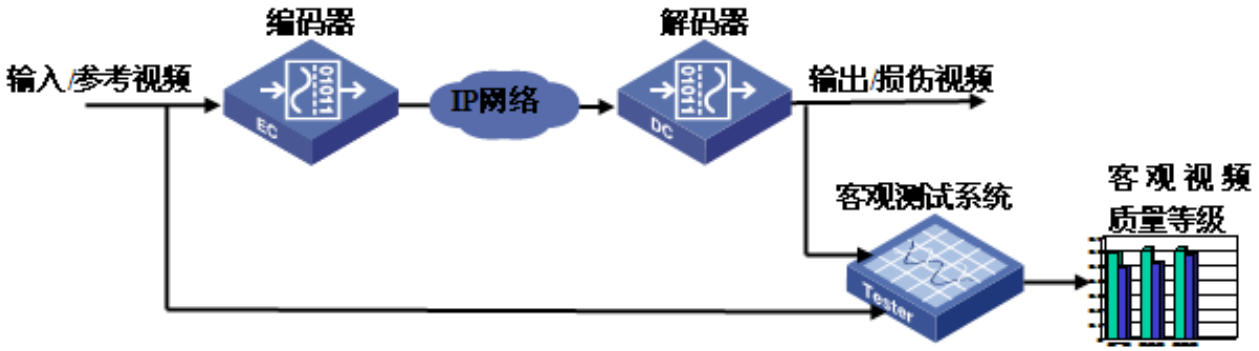


图 1 全参考视频质量客观测试模型

在上述视频质量客观测试模型中，客观测试系统会对输入视频及输出视频按照一定的客观算法进行相应的比较，最后给出客观的视频质量等级评价。客观测试系统在对输入/输出视频进行比较之前，需要参考输入视频对损伤视频进行时间和空间上的偏移纠正以及增益调整，每种客观测试算法都会有自己的纠正算法，通过这些纠正算法可以排除时间的前后偏移、空间的上下左右偏移、以及增益的变化对最终的计算结果的影响，以给出较可靠的客观的视频质量评价。下面我们来介绍一些目前相对来说与主观评价近似度较高的客观测试算法。

视频质量客观测试算法介绍

目前最常用的客观评价方法就是基于统计理论的PSNR，该评价算法在数学上处理容易，物理意义比较明确，因此使用范围也最广，但是该评价方法得出的结果与主观评价的结果存在较大的偏差，因此通常视频系统的开发人员只将其作为参考信息，而不能完全替代主观评价。

相对于容易实现但与主观结果偏差较大的PSNR，目前有多个机构提出了与主观评价结果关联较好的客观评价算法，如美国国家电信和信息管理局（NTIA）提供的视频质量度量（VQM）算法及其模型、英国电信BT提供的全参考视频质量模型及其算法（BTFR）、巴西电信研究中心（CPqD）提供的基于分段的图像评价算法(IES)，以及泰克公司和Sarnoff公司提供的PQR算法等，下面简单对其中的VQM、BTFR及PQR算法进行简单介绍及说明

VQM

VQM是由美国国家电信和信息管理局提供的视频质量客观评价方法，其具体模型及计算过程如图2所示：

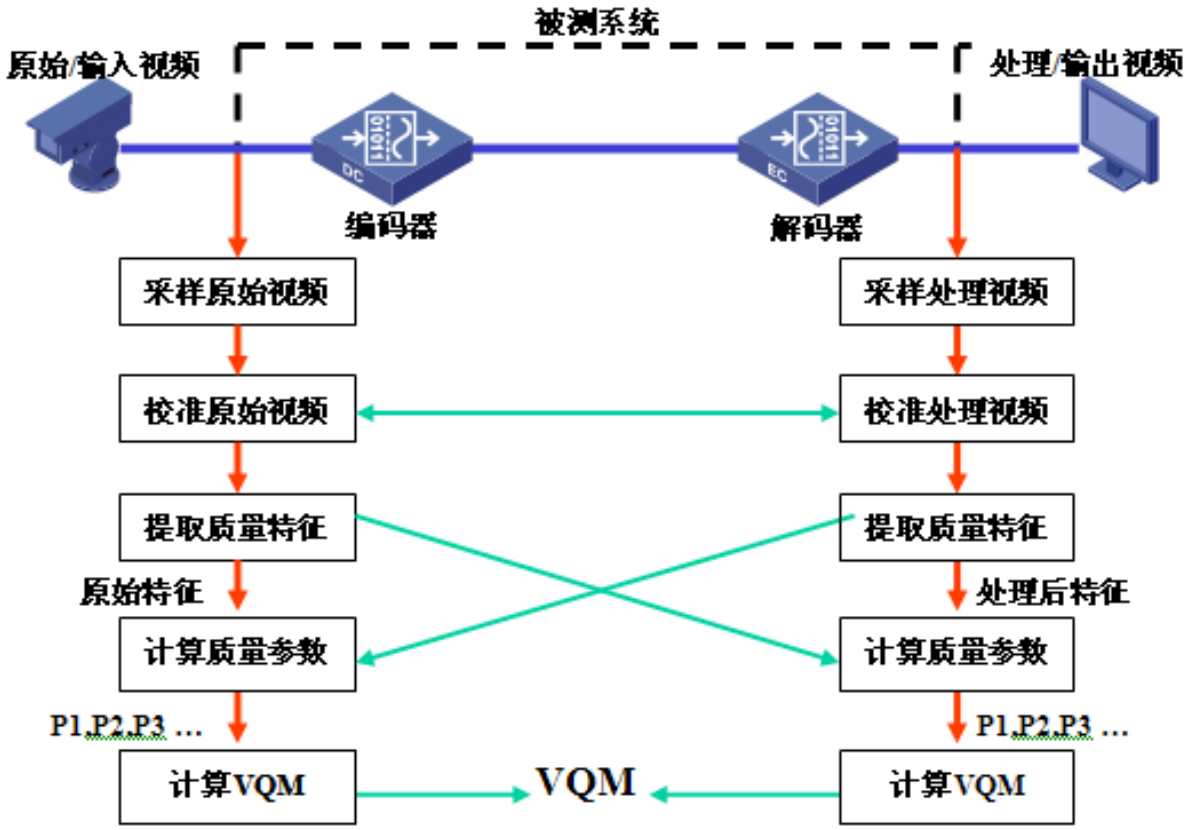


图 2 VQM算法模型及处理过程

说明：

VQM客观评价测试方法在给出视频质量客观评价结果之前需要经过如下几个过程：

1. 原始及处理后视频流的采样

此过程负责将原始或处理后的视频由模拟/数字信号转换成含有Y、CB、CR 三种分量信号的视频格式文件，为后续进一步处理提供基础文件。

2. 原始及处理后视频流的校准

此过程比较输入/原始及输出/处理视频文件，并且依据原始/输入视频文件的图像内容移除掉输出/处理视频内容中的时间、空间偏移及增益调整，为后续处理排除掉编解码之外的干扰因素。

3. 原始及处理后视频图像感知特征的提取

负责提取原始/输入及处理/输出视频文件中的人眼可感知视频特征，这些特征主要为：空间梯度的特征信息、色度特征信息、对比度特征信息、运动量特征信息、对比度与运动量特征之间的正交信息。这些特征为后续的质量参数计算提供了翔实的数据信息。

4. 视频质量参数的计算

此步骤负责测量视频质量由于特征值的增加和损耗所导致失真的质量参数，对步骤3提取的原始/输入和处理/输出视频特征使用比较函数进行比较计算，接着对比较计算得出的结果使用整个空间和时间的错误合并函数来模拟人们如何推导主观质量评级；最后考虑到参数值和感知质量间的非线性关系，将使用最终的时间平滑参数值进行缩放和修剪，来进一步减少参数敏感度。

5. VQM值计算

此步骤负责将步骤4计算的各种质量参数按照一定的加权关系进行合并运算，得出视频质量客观评价值（VQM）；最终计算获得的VQM值位于0到1之间，数值越小代表视频处理损伤越小

BTFR

BTFR为英国电信提供的全参考视频质量评估模型，具体模型如图3：

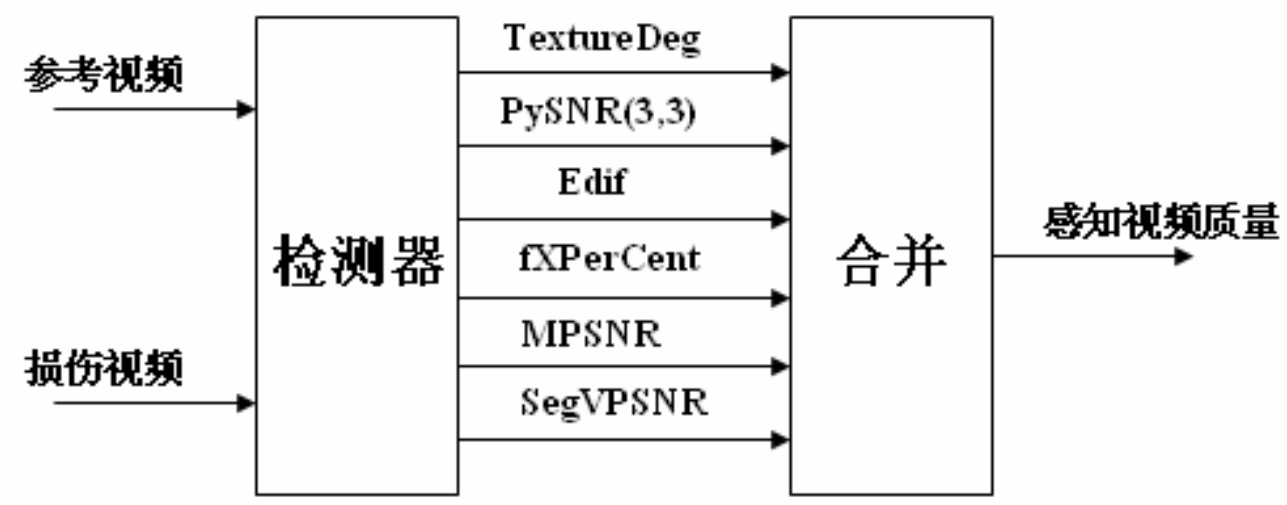


图3 全参考视频质量评估模型图

从上述示意图可看出：BTFR算法主要包括两个阶段即检测阶段及随后的合并阶段；检测阶段负责计算参考视频与损伤视频序列中的可感知特征参数，这些参数将交给合并阶段，合并阶段再进行适当的加权得到可察觉的视频质量。检测阶段检测内容及合并阶段加权参数的选择依据目前对人眼视觉系统的时间、空间遮掩性质研究及校准实验来决定。

PQR

PQR算法为泰克公司和Sarnoff公司提供的基于JND（最小可觉差异）的客观视频质量评价方法，具体处理过程如图4：

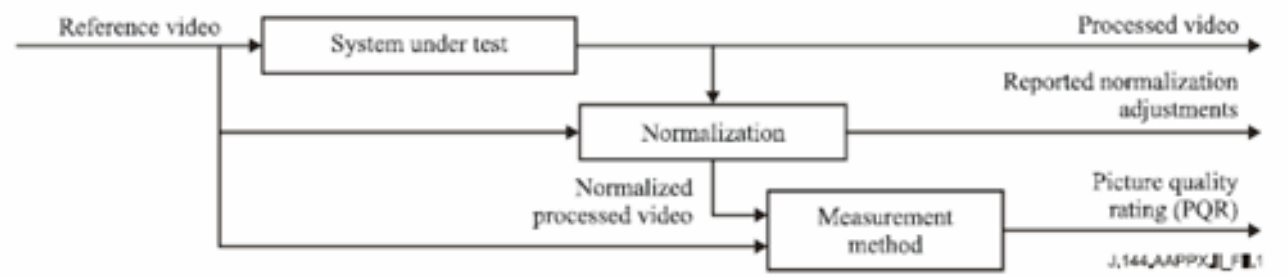


图4 基于JND的客观视频质量评价方法

PQR算法在给出视频质量评价等级之前需要经过两个过程：首先需要依据参考视频片段对经过被测系统的处理后的视频片段进行标准化处理，具体包括为时间、空间偏移调整、亮度和色度等增益的调整；之后再对参考视频及标准化后的处理视频进行JND算法，给出PQR值。

客观测试算法验证

之前我们说过PSNR客观测试方法与主观评价的结果偏差较大，那么VQM、BTFR及JND算法与主观评价的结果关联性又如何呢？对此，视频质量专家组VQEG与2003年8月对各研究组织提供的客观测试算法进行了一次集中测试并给出了各种客观测试方法与主观评价结果的关联性统计，具体信息如表1和下表2所示

表格 1 PAL制式下客观评价与主观评价结果关联性

Metric	BT	Yonsei/SKT/RRL	CPqD	NTIA	PSNR (Note)
Annex	A	B	C	D	
Pearson correlation	0.937	0.857	0.835	0.938	0.804
RMS error	0.075	0.110	0.117	0.074	0.127
NOTE – The PSNR values reported here are taken from the VQEG Phase II final report. These values were calculated by Yonsei.					

表格 2 NTSC制式下客观评价与主观评价结果关联性

Metric	BT	Yonsei / SKT / RRL	CPqD	NTIA	PSNR
Annex	A	B	C	D	
Pearson correlation	0.779	0.870	0.898	0.886	0.733
RMS error	0.113	0.089	0.079	0.083	0.122

上述表格中Pearson correlation 表示客观评价结果与主观评价结果的关联性，值越大关联性越好；RMS error 为像素值的均方根错误，值越小越好。据此根据表中的数据我们可看出对于两种制式（PAL制和NTSC制）来说，NTIA提供的VQM模型及其算法表现较好，两种测试情况下的关联性都位于前列。■

网络之路-监控专题
ROUTE TO NETWORK

主办单位：H3C测试中心
策　　划：刘　宇 陈旭盛 杜祥宇
主　　编：陆宇翔
本期编委：朱　兵 王连朝 李玉天 郭　琪
吴参毅 李　旻 周后取 周绪龙
杜超华 袁　飞 任俊峰

2010年第3季度
总第十四期