H3C网络之路 2012年第三期·总第十八期

iMC专题

智能管理中心

H3C

目录 Content

一、网管概论

001 网络管理简介 徐庆伟

006 H3C iMC简介 符 斌

016 iMC云数据中心管理方案 伊莉娜

二、网络基础设施的管理

026 iMC的网络基础设施管理 袁亚屏

035 智能无线业务管理 王白辉

046 EPON和EoC的管理 史计达

052 分支网点的管理 袁 江

058 针对特定类型设备的专用管理软件 袁亚屏

三、业务层面

062 用户身份识别和访问控制 徐泽新

070 网络流量和用户行为分析 袁 江

079 智能IPsec VPN业务管理 其其格

086 MPLS VPN的管理 王守唐

四、应用与管理层面

099 应用与服务健康管理 曾 劼

111 服务运维管理 李 丹

五、测试方法

132 基于LoadRunner实现iMC的高质量压力测试 刘宇征

150 业务软件的自动化测试实践 赵晓丹

网络管理简介

文/徐庆伟

网络管理概述

网络管理发展的历史，就是网络发展的一个缩影。网络管理技术是伴随着计算机、网络和通信技术的发展而发展的，二者相辅相成。从网络管理范畴来分类，可分为对网“路”的管理以及对接入设备的管理；对行为的管理，即针对用户的使用进行管理；对资产的管理，即统计IT软硬件的信息等。

根据网管软件的发展历史，可以将网管软件划分为四代：

第一代网管就是最常用的命令行方式，并结合一些简单的网络监测工具，它不仅要求使用者精通网络的原理及概念，还要求使用者了解不同厂商的不同网络设备的配置命令。

第二代网管有着良好的图形化界面，用户无须过多了解不同设备的配置命令，就能基于相对统一的图形用户界面对多种设备同时进行配置和监控。相对第一代网管大大提高了工作效率，但仍然以网络管理员手工方式配置为主，容易引发误操作，导致网络故障。

第三代网管相对来说比较智能，是真正将网络和管理进行有机结合的软件系统，具有“自动配置”和“自动调整”功能。对网管人员来说，只要把用户情况、设备情况以及用户与网络资源之间的

分配关系输入网管系统，系统就能自动地建立图形化的人员与网络的配置关系，并自动鉴别用户身份，分配用户所需的资源（如电子邮件、Web、文档服务等）。

第四代网管称为云管理，在云计算中，网络管理的作用将首次超过网络本身，网络管理成为网络的大脑，对整个云计算网络进行协调，基于业务流程进行管理。网络管理功能更加精细和专业，超越传统的网络管理功能，整个网络的功能只有在网络管理软件的参与下才能完成。

网络管理标准简介

网络管理标准主要是在管理体系结构、管理信息模型和管理协议方面的规范和建议，提高网络管理的互通与互操作性。国际上有一些组织机构致力于研究、制定、开发网络管理的服务标准、协议和体系结构，其中最重要的有国际标准化组织(ISO)、国际电信联盟电信标准化部(ITU-T)和Internet工程任务组(IETF)。

在这三个组织中，ISO是第一个开发网络管理结构、制定网络管理标准的组织，早在上世纪八十年代初期，ISO就确定了网络管理体系结构作为其工作的组成部分。至今，该组织已制定了大量的有关网络管理的标准，其内容统称为OSI系统管理。

从1985年开始，ITU借鉴OSI管理思想致力于开发和制定电信网的网络管理标准，目前已经形成了较为完善的电信网络管理推荐标准，即TMN网络管理，实际上现在的OSI管理标准与TMN建议可以互为补充。

上世纪八十年代后，Internet发展迅猛，IETF采用了基于OSI的CMIP(Common Management Information Protocol)协议作为Internet的管理协议，并对它作了修改，修改后的协议被称作CMOT(Common Management Over TCP/IP)。但CMOT迟迟未能出台，IETF决定把已有的SGMP(简单网关监控协议)进一步修改后，作为临时的解决方案。这个在SGMP基础上开发的解决方案就是著名的简单网络管理协议（SNMP）。由于SNMP存在一些不足，例如效率低、安全性差等，IETF已经提出了改进的版本SNMPv2和SNMPv3，在多个方面进行改进和强化。目前SNMP已经成为事实上的IP网络管理的标准协议。

从上世纪末开始，网络管理的概念已逐渐超越了网络和网元管理层管理功能，但还没有超出TMN定义的管理层次范围。电信管理论坛（TMF）提出的“下一代电信运营支撑系统”（NGOSS），涵盖了企业生产经营、网络运维、企业管理等各个层面，为企业的运营提供有效且完整的技术支撑。NGOSS中的TOM（电信运营业务框架）将一般的网管扩展到了OSS（电信运营支撑系统）的全部范围，而其后的eTOM则进一步扩展到电信企业的OSS/BSS。从目前规范涉及的主要内容来讲，eTOM现有的内容主要相当于TMN中的商务管理层和业务管理层，而SG4的TMN中现有建议的主体是网络管理层和网元管理层。

网络管理的基本功能

ISO在ISO/IEC 7498-4文档中定义了网络管理的五大功能（简称FCAPS），该五大功能成为当前网络管理中网元和网络层次的基础管理功能。

故障管理 (Fault Management)

故障管理是是对网络中的问题或故障进行定位的过程。包括发现问题、隔离问题和修复问题三个层次。故障管理的最主要作用是给网络管理者提供快速检查问题并启动恢复过程的工具，使得网络的可靠性得到加强。常见故障管理对应的功能有：

故障监测：主动探测或被动接收网络上的各种事件信息，并识别出其中与网络和系统故障相关的内容，对其中的关键部分保持跟踪，生成网络故障事件记录。

故障报警：接收故障监测模块传来的报警信息，根据报警策略驱动不同的报警程序，以报警窗口/振铃或电子邮件、短信等发出网络故障警报。

故障信息管理：依靠对事件记录的分析，定义网络故障并生成故障卡片，记录排除故障的步骤

和与故障相关的值班员日志，构造排错行动记录，将事件–故障–日志构成逻辑上相互关联的整体，以反映故障产生、变化、消除的整个过程的各个方面。

排错支持工具：向管理人员提供一系列的实时检测工具，对被管设备的状况进行测试并记录下测试结果以供技术人员分析和排错；根据已有的排错经验和管理员对故障状态的描述给出对排错行动的提示。

检索/分析故障信息：浏阅并且以关键字检索查询故障管理系统中所有的数据库记录，定期收集故障记录数据，在此基础上给出被管网络系统、被管线路设备的可靠性参数。

计费管理 (Accounting Management)

计费管理记录网络资源的使用，目的是控制和监测网络操作的费用和代价。它对一些公共商业网络尤为重要。它可以估算出用户使用网络资源可能需要的费用和代价，以及已经使用的资源。网络管理员还可规定用户可使用的最大费用，从而控制用户过多占用和使用网络 资源。这也从另一方面提高了网络的效率。

计费管理主要涉及的功能有：

计费数据采集：计费数据采集是整个计费系统的基础，但计费数据采集往往受到采集设备硬件与软件的制约，而且也与进行计费的网络资源有关。

数据管理与数据维护：计费管理人工交互性很强，虽然有很多数据维护系统自动完成，但仍然需要人为管理，包括交纳费用的输入、联网单位信息维护，以及账单样式决定等。

计费策略制定；由于计费政策经常灵活变化，因此实现用户自由制定输入计费政策尤其重要。这样需要一个制定计费政策的友好人机界面和完善的实现计费政策的数据模型。

政策比较与决策支持：计费管理应该提供多套计费政策的数据比较，为政策制订提供决策依据。

数据分析与费用计算：利用采集的网络资源使用数据，联网用户的详细信息以及计费政策计算网络用户资源的使用情况，并计算出应交纳的费用。

数据查询：提供给每个网络用户关于自身使用网络资源情况的详细信息，网络用户根据这些信息可以计算、核对自己的收费情况。

配置管理 Configuration Management

网络配置决定网络的行为，因此配置管理在网络管理中非常重要。配置管理的目的是为了实现某个特定功能或使网络性能达到最优。配置管理的主要功能包括：

自动获取配置信息：在大型网络中，一个先进的网络管理系统应该具有配置信息自动获取功能。即使在管理人员不是很熟悉网络结构和配置状况的情况下，也能通过有关的技术手段来完成对网络的配置和管理。

自动配置、自动备份及相关技术：配置信息自动获取功能相当于从网络设备中“读”信息，相应的，在网络管理应用中还有大量“写”信息的需求。网络的自动配置和自动备份功能，是管理大型网络所必须的手段。

配置一致性检查：在大型网络中网络设备众多，由于管理的原因，这些设备很可能不是由同一个管理人员进行配置的。即使是同一个管理员对设备进行的配置，也会由于各种原因导致配置一致性问题。因此，智能网管系统，应该能对整个网络的配置情况进行一致性检查。

用户操作记录功能：配置系统的安全性是整个网络管理系统安全的核心，因此，必须对用户进行的每一配置操作进行记录以便事后进行审计。

性能管理 (Performance Management)

性能管理用于估价系统资源的使用状况及通信效率等系统性能，运用性能管理信息，管理者可以及时发现网络性能瓶颈，保证网络具有足够的能力满足用户的需求。性能管理的一些典型的功能包括性能监控、阈值控制、性能分析、可视化的性能报

告和实时性能监控以及网络对象性能查询等。

性能监控：由用户定义被管对象及其属性。例如路由器的流量、延迟、丢包率、CPU利用率、温度、内存使用率等。对于每个被管对象，定时采集性能数据，自动生成性能报告。

阈值控制：对于特定被管对象的特定属性，可以针对不同的时间段和性能指标进行阈值设置。可通过设置阈值检查开关控制阈值检查和告警，提供相应的阈值管理和溢出告警机制。

性能分析：对历史数据进行分析，统计和整理，计算性能指标，对性能状况做出判断，为网络规划提供参考。

可视化的性能报表：对数据进行扫描和处理，以直观的图形反映性能分析的结果。

实时性能监控：采用直方图、折线图等形式显示用户指定的性能监视项的统计信息，并根据指定的时间间隔、定时刷新显示界面，实时性能监视功能可以帮助网络管理人员了解设备的当前运行状态，以便于网络管理人员在紧急情况下采取必要措施。

网络对象性能查询：可通过列表或按关键字检索被管网络对象及其属性的性能记录。

安全管理 (Security Management)

随着用户对网络依赖性越来越高，网络安全管理显得非常重要。网络数据的私密性，授权和访问控制是网络安全需要解决的问题。相应的，网络安全管理应包括对授权机制、访问控制 、加密和加密密钥的管理，另外还要维护和检查安全日志，实现对网络事件和用户行为的审计。

网络资源的访问控制，通过管理路由器的访问控制链表，完成防火墙的管理功能，即从网络层(1P）和传输层(TCP）控制对网络资源的访问，保护网络内部的设备和应用服务，防止外来的攻击。

告警事件分析，接收网络对象所发出的告警事件，分析员安全相关的信息（如路由器登录信息、SNMP认证失败信息），实时地向管理员告警，并提供历史安全事件的检索与分析机制，及时地发现正在进行的攻击或可疑的攻击迹象。

主机系统的安全漏洞检测，实时的监测主机系统的重要服务（如WWW，DNS等）的状态，提供安全监测工具，以搜索系统可能存在的安全漏洞或安全隐患，并给出弥补的措施。

网络管理发展的未来趋势

随着网络规模的不断扩大，以及云计算、虚拟化技术的发展，网络管理在整个网络中的地位越来越高，网络管理软件日益成为网络的大脑。同时网络的发展的新趋势，对网络管理提出了更多的要求，未来网络发展不仅需要从网络的角度出发来保障用户和业务，也要从用户和业务的角度出发来优化网络。这意味着需要采用全新的管理模型和灵活的功能架构，并且充分考虑基础设施、技术趋势、业务运行、运维服务等各种管理要素，建立一个开放式、标准化、易扩展、可联动的统一智能管理平台，实现网络的精细化管理

基于业务流程的资源管理

传统以设备管理为核心的FCAPS网管模型，已经不能满足下一代网络和数据中心全新的管理需求。另外面对规模庞大的网络和复杂的功能业务，基于单一设备和功能的管理已经逐步被淘汰。而对于用户来说，任何一个网络活动都可以看作一个业务流程，因此基于业务流程的资源管理成为未来网络管理的核心。

基于业务流程的资源管理思想是把网络业务作为网管对象，通过实时监测与网络业务相关的设备、应用，通过模拟客户实时测量网络业务的服务质量，通过收集网络业务的业务数据，实现全方位、多视角监测网络业务运行情况的目的，从而实现网络业务的故障管理、性能管理和配置管理。

管理的智能化与自动化

在未来网络中，网络规模的爆炸性增长，传统

网络的管理方式已经无法实施无边界网络的管理。随着虚拟化和云计算的发展，基于弹性业务和应用的广泛部署，管理软件也要有灵活的弹性，由此智能化和自动化的网络管理呼之欲出。

网络管理的智能化体现在故障提前预警、准确隔离与有效恢复，基于业务的资源整合与协同、基于统一管理的全面功能融合；自动化体现在根据业务变更以及业务编排，自动实现网络配置与监控管理。

开放的管理架构

未来网络是一个无边界的网络，网络规模也将急剧扩张；未来网络服务和网络应用更加复杂，网络中存在不同厂商，不同结构的网络资源，如何管理这些网络资源是网管面临的巨大挑战。单一的网络管理软件已经无法满足未来网络管理需求，架构开放，走融合之道，才是未来网络管理发展的必经之路。

采用基于面向服务（SOA）的开放管理架构，可以为第三方业务应用提供底层的资源管理调用接口。在实际应用中，用户可以通过调用第三方WEB网管软件对设备进行管理，运营商可通过采集各种设备运行数据汇总提供给BOSS系统进行评估，还可将本地用户认证计费信息与运营商BOSS系统进行共享等。

精细的网络控制功能

从当前网络管理软件来看，网络管理更多的集中在网络监控上，虽然网络管理也有配置功能，但是对网络行为的控制能力有限。网络的转发与QoS等网络行为基本上都是基于单个设备进行单点控制，网管软件很难实施全网的网络控制功能。随着网络新技术的出现和发展，网络行为的控制功能将在网络管理中得到强化。

例如SDN概念的提出，给网络管理赋予了全新的理念。未来网管软件会集成网络转发管理功能，可编程网络控制功能等SDN提出的软件定义网络需求。未来的网络管理更加强调对网络的行为控制功能，特别是基于业务功能需求和全网视图，实现对网络的转发控制与QoS部署。

总结

网络管理伴随着网络出现，从一个微不足道的角色，日益成长为网络至关重要的组成部分，网络管理的功能，也从最基本的“FCAPS”阶段逐步发展为以业务流程为中心的智能管理与自动管理阶段，网络管理的精细化控制以及开放架构越来越受到重视。

H3C iMC简介

——iMC的梦想之路

文/符 斌

引言

随着网络建设的不断深入发展，网络成为承载IT多业务的平台，除了单纯的追求高带宽、高速率外，安全、高效和可运营的网络成为越来越多的用户关注的焦点，网络精细化管理也越来越深入人心，一套好的管理软件无疑对网络的精细化管理起到至关重要的作用。

H3C iMC智能管理中心（Intelligent Management Center）作为H3C IToIP整体解决方案的重要组成部分，从根本上颠覆了传统网管软件的设计思想，提出了智能融合、协同联动、开放架构的管理理念，融合并统一管理用户、资源和业务这三大IT组成要素，采用面向服务架构（SOA）的设计思想，以业务为导向按需装配组件，形成一系列直接面向客户需求的解决方案。使客户真正做到了“精细IT、智能掌控”。

iMC的发展历程

iMC起源于H3C Quidview、CAMS、Xlog等这些传统的、孤立的网络管理产品。基于iMC融合、智能、开放的理念于2006年底推出了iMC V3的第一个版本， 依次推出了iMC 平台、 MVM、UAM、EAD、NTA、UBA、WSM、QoSM、BIMS等组件；2010年升级发布iMC V5版本，使用Web2.0技术，聚焦数据中心管理，依次推出了SHM、APM、CRM、TAM、CAMS等组件；预计2013年将升级发布iMC V7版本， 聚焦于FlexUI，SDN等。

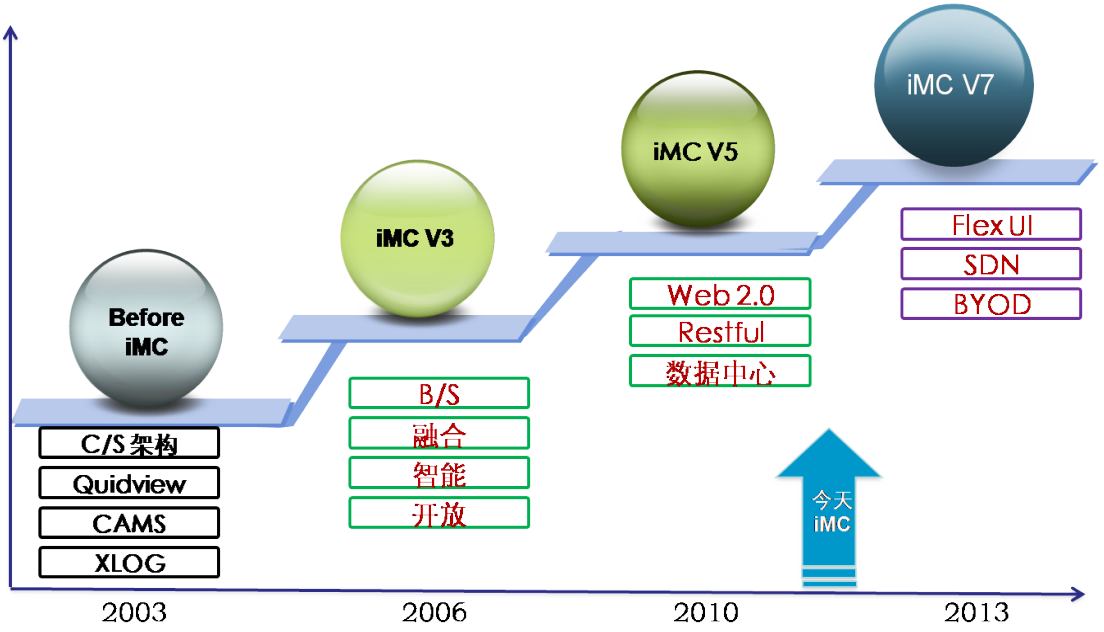


图 1　iMC的发展历程

iMC的全家福

iMC的核心是iMC平台组件，基于平台组件实现了资源、用户、业务的融合管理。从如下iMC全家福可以看出iMC从资源、用户、业务角度提供了丰富的功能组件。

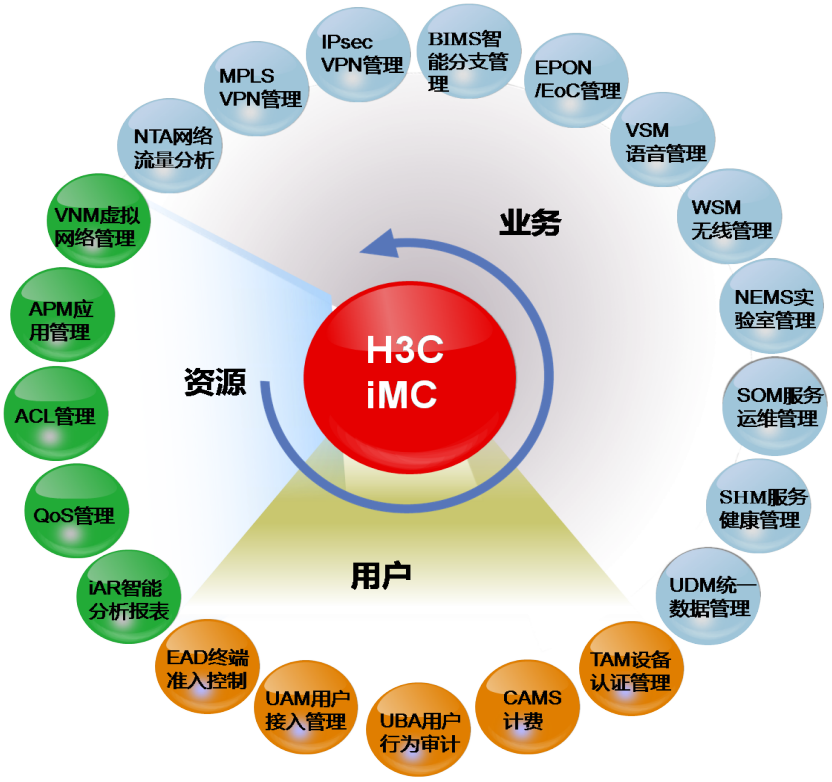


图 2　iMC的全家福

iMC的基本架构和核心价值

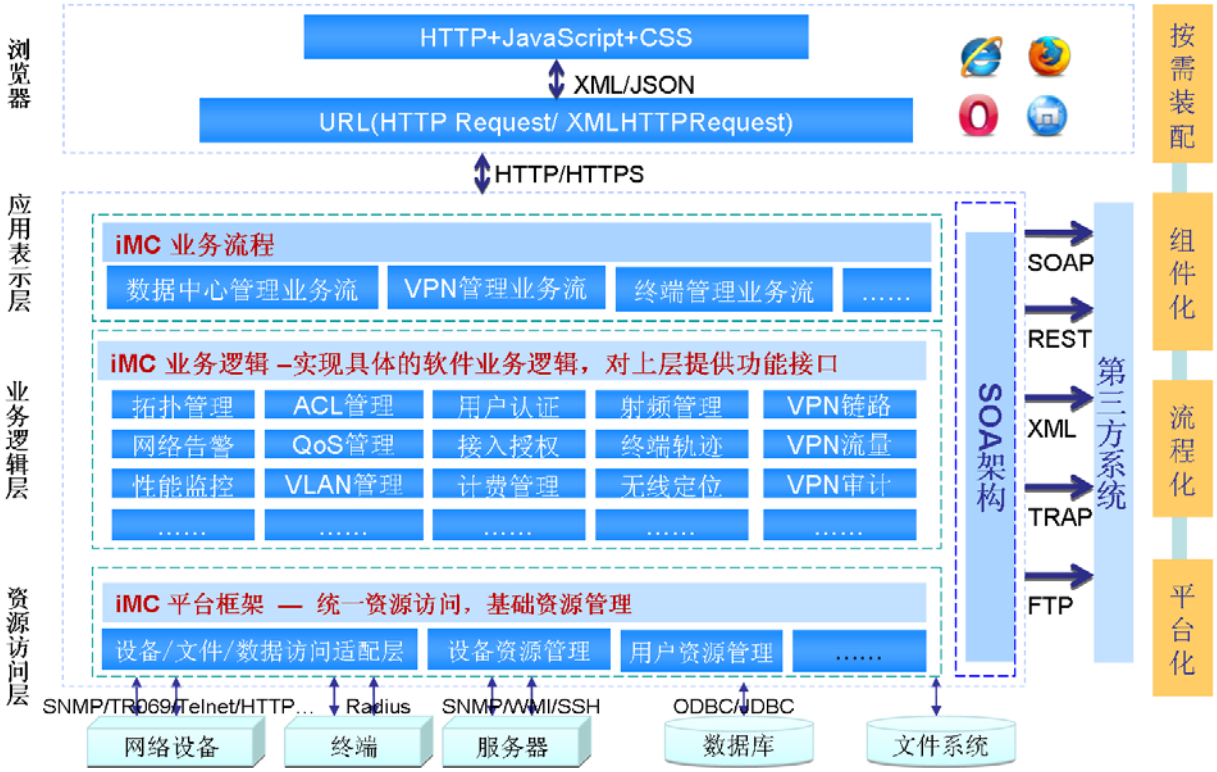


图 3 iMC的基本架构

iMC以资源（设备资源、用户资源、物理资源、虚拟资源）的统一管理为平台，以业务管理和业务流程模型为核心，采用面向服务（SOA）的设计思想，按需装配的组件化结构，为客户提供网络业务、资源和用户的融合管理解决方案，能帮助客户实现网络业务的端到端管理。

同时具备了协同联动、智能融合、开放架构等三大特性。

开放架构：iMC具有SOAP、Restful开放接口，具备构建灵活业务网络的能力。通过向第三方OSS、网管系统以及桌面安全系统开放接口构建增值价值链，提供了标准化、构件化、灵活开放的统一管理平台，可实现第三方业务应用对底层资源的调用管理，为广大合作伙伴与用户提供一个真正的开放智能管理平台，与第三方管理软件乃至应用软件充分实现“互动”。

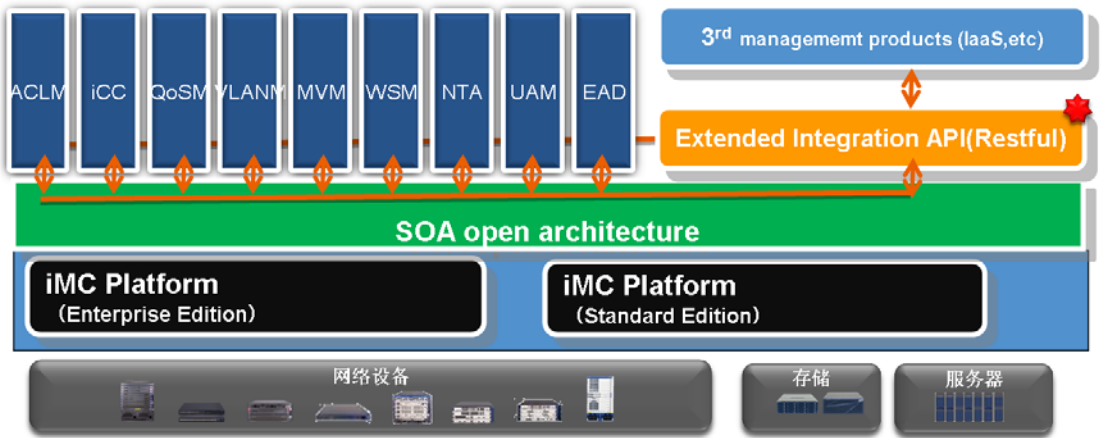


图 4 iMC的SOA开放架构

协同联动：iMC提出的人、资源、业务的联动支撑，为构建自适应的防御、修复、优化的联动网络提供支撑平台；业务功能的整合和发展解决以往各产品因功能割裂而造成的客户体验差、新特性开发难等现实问题，提升业务模块间的协同能力。

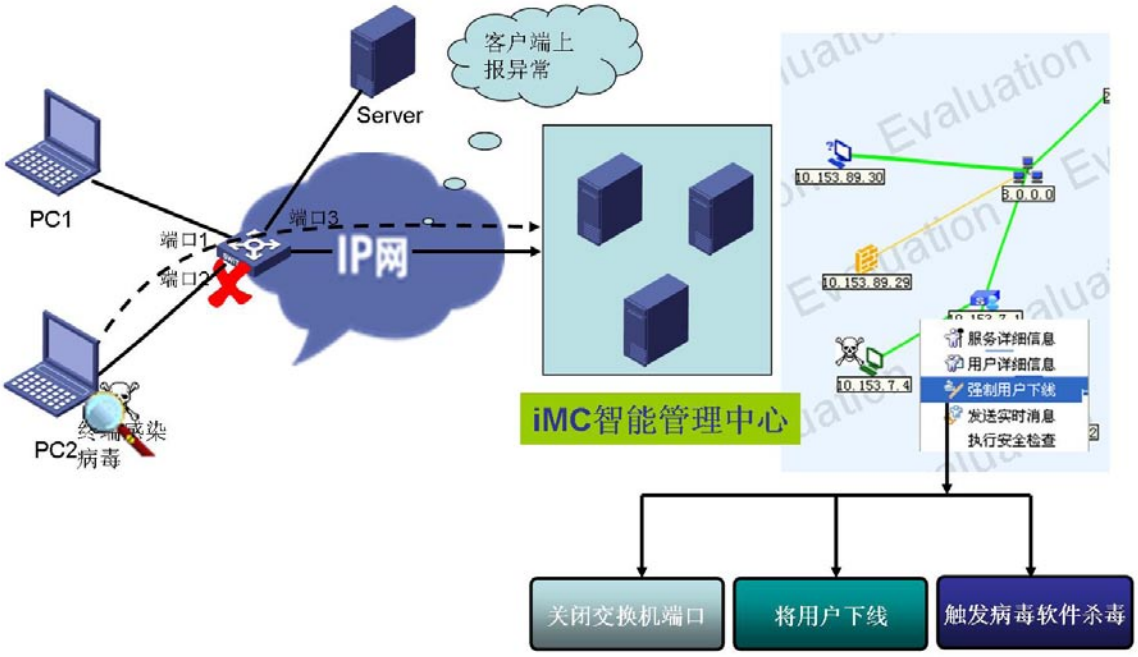


图 5 iMC的网络&用户协同联动

智能融合：iMC构建了IP网络、用户和业务的集成管理平台，提供整合的资源管理，重整业务流程，实现网络业务生命周期(鉴权、部署、监视、调整、审计)的全流程管理。面向解决方案的业务支撑能力基于人、资源、业务集成的平台，支撑丰富的产品构件/业务特性，通过构件间的整合优势，提升解决方案市场竞争力。 如下图，拓扑不仅展示了网络资源的连接关系，更表现出网络资源被使用的情况，与用户接入认证的业务融合。

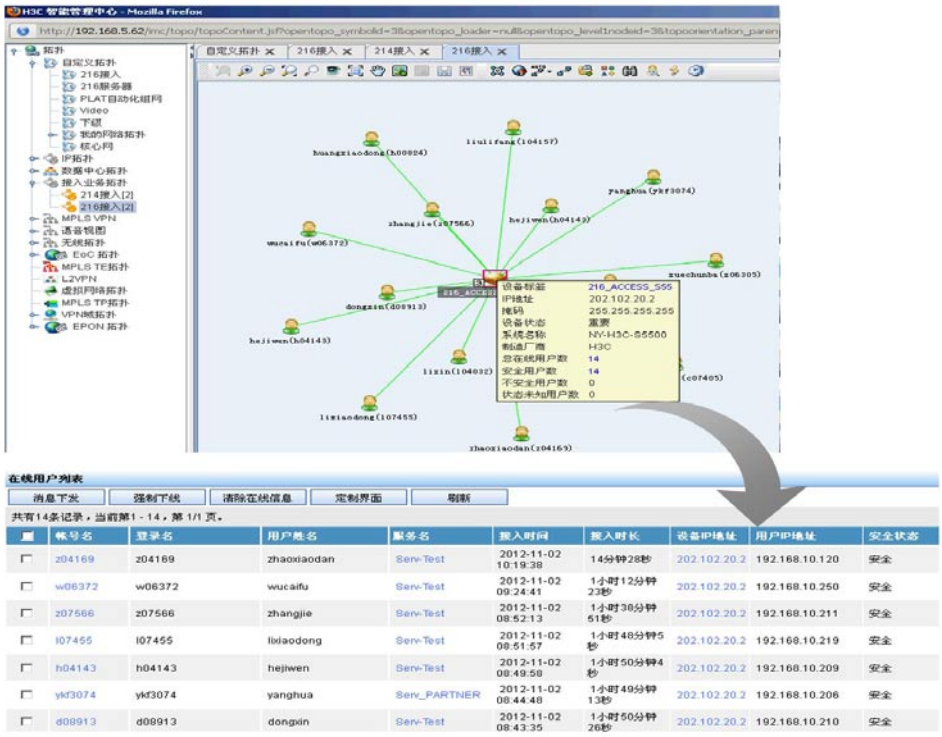


图 6 iMC的网络&用户智能融合

iMC的价值就在于依托开放架构，以业务为导向，实现智能融合和协同联动，将各个业务模块进行端到端整合，实现了端到端的精细化业务流程管理。在为用户IT管理保驾护航的同时，也为用户创造价值。iMC智能管理平台与各个功能模块的无缝整合，将使得H3C成为国内唯一一家可以从资源、业务到用户全方位提供网络管理的专业厂商。

通过用开放的技术架构在基础资源与应用系统之间搭建一座桥梁，加上联动融合的智能管理特性，iMC成功地扮演起“开放智能管理中枢”的角色，帮助用户在网络中更加灵活地开展各种业务应用。用形象的方式来比喻，iMC智能管理中心更像是IT管理的“乐高积木”，用户在用标准的乐高零件组成玩具的同时，可以标准的接口将更多的第三方“零件”拼插到积木上，最终让整个“玩具”变得更宏大、更丰富、更精彩。

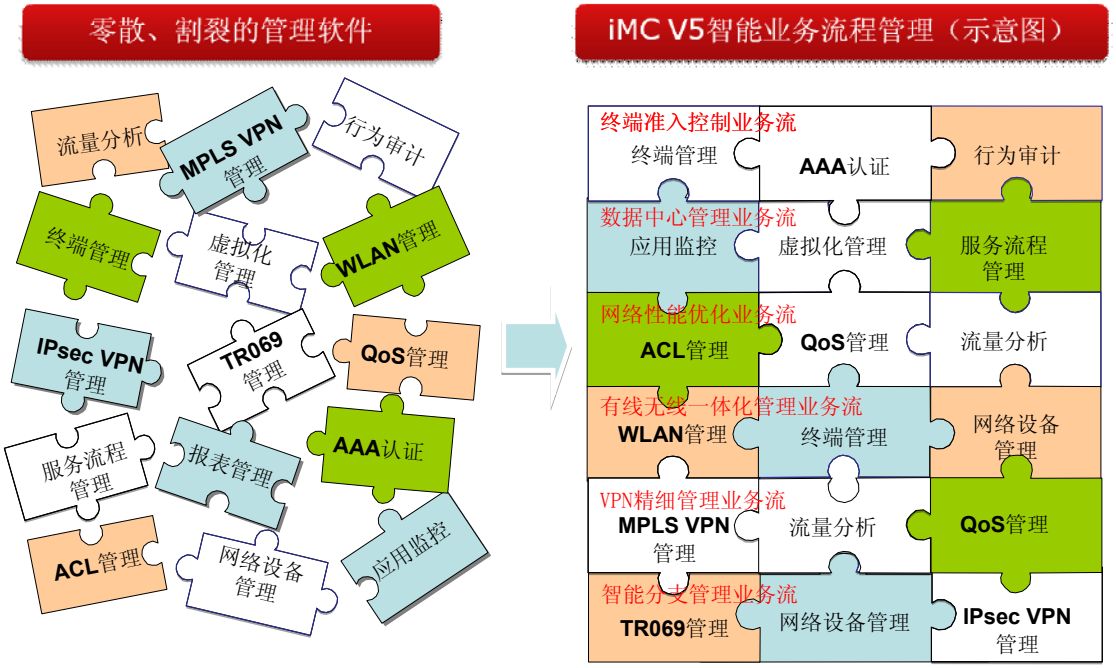


图 7 iMC业务流的搭建

iMC功能的设计思想

网络管理软件的最直接目的应该是：

◆ 减化管理网络的工作量，表现在集中管理、自动化、流程化、智能化。

◆ 使网络体现价值，最主要是连接网络服务的两端：Host/VM/App 到用户/用户网络。

iMC在集中管理方面的设计

单平面

iMC产品族包含20多个组件，覆盖网络、应用、用户、VPN、无线、语音等多个业务领域的管理功能，都能在一个统一的集中管理平面中进行无缝的端到端管理。

图 8 iMC对网络、用户、业务的统一管理平面

多厂家&多类型设备统一管理

除了传统的路由器、交换机外，更能对网络中的无线、安全、存储、语音、监控、视频、服务器、虚拟设备、打印机、UPS等设备进行管理，实现设备资源的集中化管理。

除了H3C的网络设备管理，还实现了对业界其他主流厂家网络设备的管理。缺省提供对来自35+的生产厂商的大约5000+个不同类型设备的管理能力，即便是对新设备的添加，也仅需向导式的配置流程：输入必要的信息、导入MIB、对高级功能增加脚本，从而实现从初步的网络监控到更高级的配置管理的能力扩展。

物理/虚拟资源统一管理

在管理物理网络的同时，对引入计算虚拟化、网络虚拟化后的新型网络架构进行统一管理。比如IRF、VLAN、VPN等技术的网络虚拟化对网络拓扑和管理方式的影响，VMware、Hyper-V、KVM等计算虚拟化使网络的管理边界扩展到计算资源内部，iMC从资源拓扑等各个方面进行统一的管理。

聚焦于拓扑的管理能力

在拓扑中体现IP、二层、VLAN、MSTP等逻辑连接关系，同时体现流量、带宽等监控数据，VPN、无线、用户接入等业务连接关系，数据中心机房/机架方式的物理位置和连接关系。

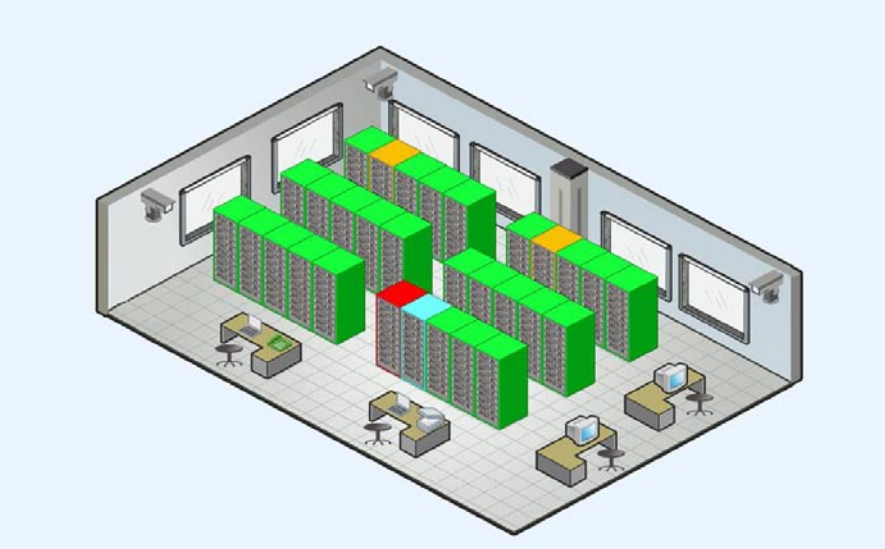


图 9 iMC数据中心机房拓扑

iMC自动化、流程化方面的设计

信息的自动收集和更新

可以从传统网络管理软件的视角（FCAPS）分解iMC，从故障、配置、审计、性能、安全五个方面体现iMC对用户、网络数据的自动化收集和处理能力：

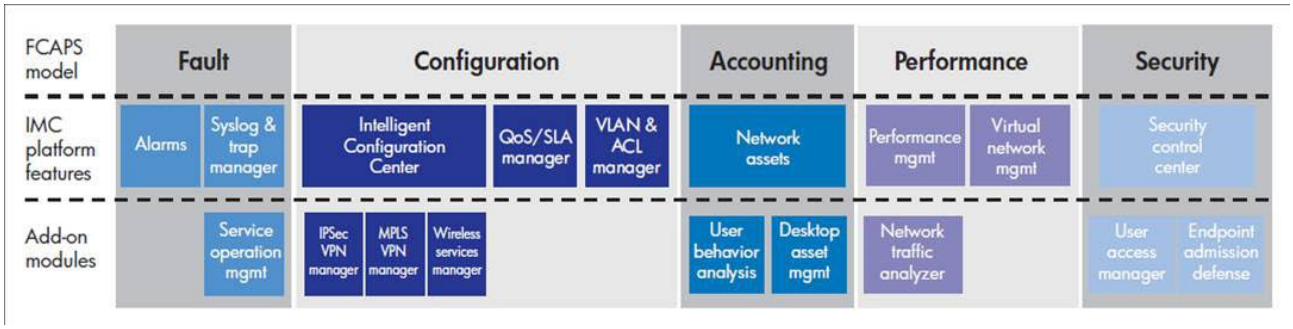


图10 iMC FACPS

监和控的策略化驱动

用户、网络信息的监视收集不是目的，实时动态的对网络进行优化调整才能体现管理的价值。比如前面所提的iMC协同联动能力。

流程化驱动能力

在IT管理领域，随着ISO20000、ITIL v3.0的发布和推广， IT网络运维服务管理已经成为非常迫切的需求。从ITIL对流程驱动、受控变更的思路出发，iMC实现了服务运维流程管理能力，提供了ITIL服务运维领域完整的资产管理、配置管理、变更管理、请求/事件/故障管理、问题管理、知识库管理能力，并提供Service Desk作为IT网络服务的统一管理门户。通过流程化管理能力与iMC告警、配置、软件管理等特性的融合联动，使iMC对IT网络的所有配置和变更、故障定位处理活动都被纳入到可控、可审计、可度量的运维能力要求之中。

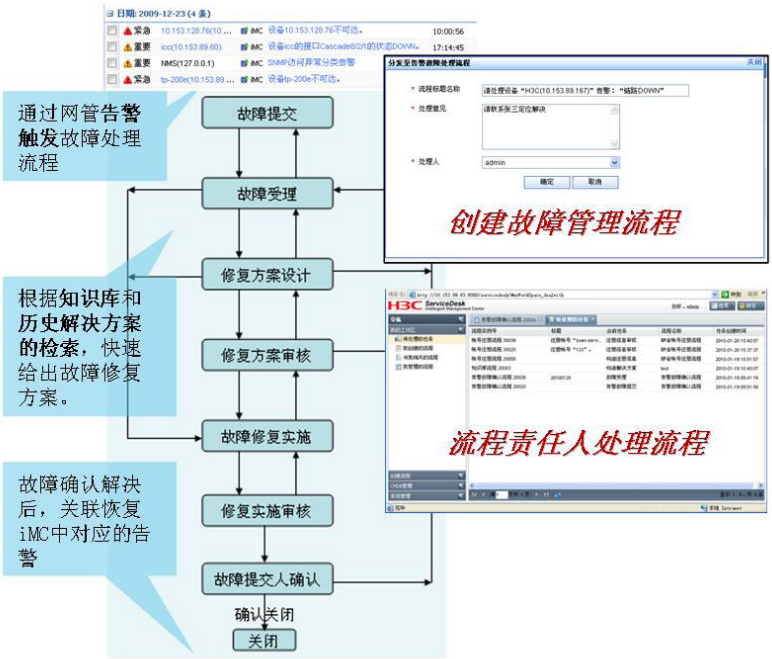


图11 iMC 故障处理流程

自动化业务流编排

编排的过程，就是网络业务/服务定义的过程，比如需要在客户接入设备配置用户认证信息、VPN资源，在承载网设备配置ACL、QoS资源、在数据中心设备配置VLAN、安全等。

iMC本身是以业务为导向的，在iMC的各个业务模块中，已经根据各业务不同的流程特点，预置了端到端的业务流程能力，比如端到端的VPN业务部署，从产生/分配/定位/解决的闭环的告警处理流程等。

iMC在智能化方面的设计

为达到自动化目的，需要对所有收集数据的综合分析能力和智能化能力。

业务内分析

iMC的各个业务组件或模块都会提供一定的智能数据分析能力，比如告警关联分析、Syslog/安全日志分析和联动、终端接入和绑定分析、无线/语音/VPN业务质量分析等等。

多业务综合分析

从App、用户、业务系统等多个角度对网络信息进行数据建模和综合分析。

比如iMC SHM系统提供了从业务系统视角的网络综合分析能力，使IT服务部门通过服务水平管理来保证其服务有效，建立服务健康水平监督体系，帮助IT服务部门做出正确的应对决策。SHM跨iMC系统的性能、告警、NQA链路监控，NTA流量分析等业务模块，提取关键性能指标（KPI），建立IT服务各个方面质量的度量指标（KQI）以及服务整体质量的度量模型（SLA），基于服务可用性、MTTR、MTBF等的监控和分析对服务的健康水平做出评价。安装的IMC业务模块越多，可参与到SHM管理的KPI数据就越丰富，对IT服务的监控水平评价就更为全面。

图 12 iMC SHM业务分析报表

智能分析报表

基于iMC收集、或分析处理后的数据，iMC提供丰富的BI报表。同时为满足用户不同的分析视角，iMC将这些数据作为数据源、结合业界领先的可视化的BI报表设计工具（水晶报表），实现可扩展的BI

分析能力和丰富的展现形式。

iMC服务于用户/App的设计

网络的最直接价值，就体现在连接用户和App。因此iMC聚焦于用户、APP的网络接入控制和网络分析能力。

用户网络接入控制

为使合法用户能够正常接入网络，并安全的使用网络，iMC的UAM/EAD组件和网络设备深度融合，以预定义的策略为行为基础，控制用户的网络接入，比如802.1x、Portal、VPN接入等，哑终端（IP电话、打印机）接入。EAD通过检测每一个接入网络的终端（包括PC、笔记本、平板电脑、智能手机）是否符合各类复杂的安全策略来提升网络的整体安全及权限控制，通过客户端iNode程序收集深入的终端资产信息，比如OS、软件、补丁、防病毒、网络配置、外设等确保所有接入网络的用户终端符合企业的安全策略。并提供多种数据防盗功能，如监视或阻止USB访问等。

应用网络接入控制

服务器/应用的接入控制，一方面可以通过交换机、IP、MAC的绑定关系进行合法性控制，另一方面考虑到计算虚拟化技术的广泛应用，网络管理需要适应服务器/应用的虚拟化和迁移特性，需要有新的管理技术。

iMC CRM特性一方面基于HP 提出的802.1Qbg （VEPA）技术，和VEPA vSwitch配合实现网络接入配置的随需迁移，另一方面基于VMware、Hyper-V等虚拟化管理软件的能力，动态感知服务器/应用的位置和迁移，主动实现网络的控制调整。

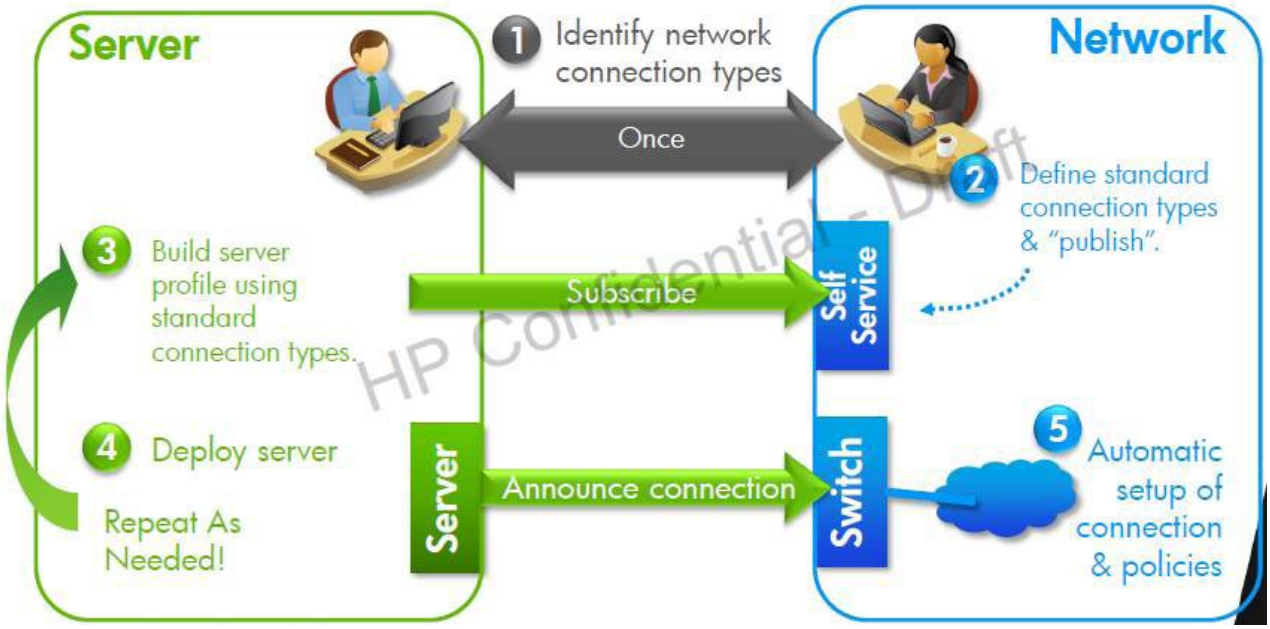


图 13 iMC CaaS

用户/App使用网络的分析

通过各种网流技术比如NetStream、sFlow、NTA、IPFIX、netFlow等采集网络流量，以及使用Probe/DIG直接抓取网络镜像流量，iMC NTA/UBA获得了用户、APP对网络使用情况的数据，NTA可以从源/目的/会话/应用等几个角度分析网络流量，UBA可以对用户使用网络的行为进行分析。

iMC APM对应用的运行状态进行了充分的监控分析，特别是通过网络访问App的性能（比如可达性、延时）等的监控和分析，从另一个角度补充了对应用的服务能力。

展望与未来的发展

随着虚拟化技术的落地和云计算技术的到来，网络作为基础设施的一部分必须面对IaaS对网络虚拟化和网络as a服务的要求。iMC将规划NaaS&SDN方案，借助传统网络虚拟化技术以及Openflow/overlay等可行技术实现网络资源的服务管理能力。

另外，随着iPAD等移动设备的普及，控制移动设备的网络接入BYOD方案也是iMC下一个阶段的重要解决方案。

总之，H3C iMC作为一个成熟的管理解决方案，实现复杂的综合方法、高度虚拟化的多厂商支持、跨多个功能领域的基础设备管理，其实现在单一的产品中覆盖绝大多数的管理任务，从而通过较短的学习曲线、更少的行政头痛，以及良好的数据利用，最终实现总体的优势成本价值。

缩略语

名称	解释
iMC	Intelligent Management Center
SDN	Software Define Network（软件定义网络）
BYOD	Bring Your Own Device
NaaS	Network as a Service
FCAPS	Fault Configuration Accounting Performance Security
ITIL	Information Technology Infrastructure Library
CRM	Connection Resource Management
VEPA	Virtual Ethernet Port Aggregator

iMC云数据中心管理方案

文/伊莉娜

云数据中心的管理需求

自从第一台计算机发明以来，IT行业每隔20年左右就会出现一次大的技术变迁，从早期的大型机，到后来的PC、互联网，莫不如此。而本世纪10年代，新的技术热点集中在云计算、数据中心身上，云的时代来临了。与之相应的，对云数据中心的管理也出现了新的需求，由此导致对云数据中心管理系统的变革。

具体看来，云数据中心的管理需求主要体现在如下方面：

第一大管理需求，体现在基础设备管理方面。云数据中心的基础设备更加规模化、标准化，由此带来了管理的复杂性。由于数据大集中的出现，数据中心管理设备的数量成倍增长，因此对设备的管理和性能、数据的采集提出了新的需求。除了面临设备数量增加的挑战，数据中心需要对传统的路由器、交换机、安全等网络设备进行管理外，还需要对存储、服务器等IT设备进行管理，实现资源多样性的统一管理。

第二大管理需求，体现在虚拟化资源管理方面。云数据中心为了节省成本、实现日益增多的业务，必须采用各种虚拟化技术。其中有“一虚多”，即一台服务器虚拟成多台服务器。有“多虚一”，即多

台服务器处理同一个业务。更多的是“多虚多”，即多个业务在多台虚拟服务器上运行。如此复杂的虚拟化，如何能以最经济、高效的方式让新增业务快速上线并运行？这同样是传统数据中心不存在的新管理问题。随着虚拟化的资源复用，数据中心资源分配更加的随心所欲，不再局限于死板的物理资源分配。而资源分配后的跟踪、执行、怎样为业务运营做支撑，也对数据中心管理的自动化提出新的需求。

第三大管理需求，体现在服务管理模式的转型。数据中心将从被动接活向主动服务转型。调查显示，24%的数据中心需要提升管理能力，希望简化管理并降低运营成本。这些数据表明，对很多企业来说，业务部门需求不断增加和变化，对数据中心挑战很大，增加数据中心的自动化和智能化程度，提高资源共享率，在有效控制成本的同时满足业务需求，是大多数企业对于其数据中心的下一步期望，这就要求数据中心从被动接活的角色向主动服务的角色转型，并改变整个IT部门的运行模式。

H3C iMC的数据中心管理实现

数据中心管理的发展路径和对应产品

正因为对云数据中心管理需求的深入理解，iMC智能管理中心规划并明确了数据中心管理的发展路径，并不断开发和生产出相应的管理产品。这让H3C的iMC智能管理中心在云数据中心时代闯出了一片新天地。

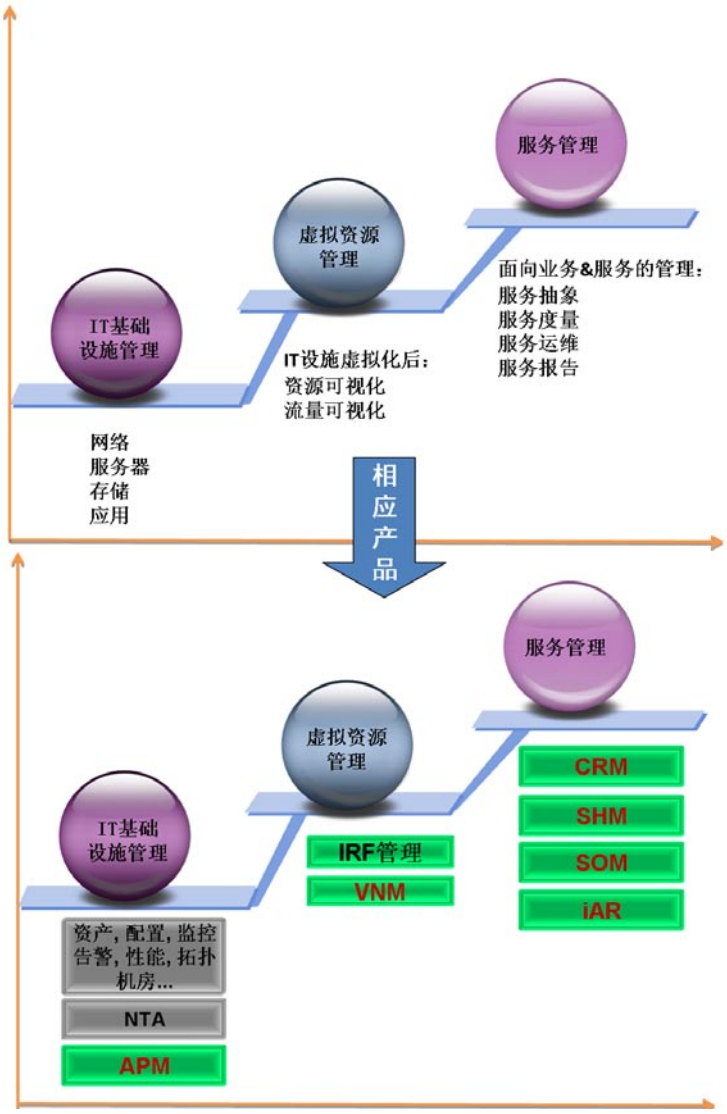


图1 数据中心管理的发展路径和对应产品

数据中心管理产品介绍

H3C iMC数据中心管理在融合SNMP、NetStream、ITIL等各种管理技术的基础上，结合现有的实际情况和管理工具，提供了融合的基础设施管理，虚拟化、自动化的资源管理，面向业务主动的服务管理，为实现基于用户、开放式、自动化、智能化的数据中心管理打下了基础，为数据中心资源的动态调配、最优化利用提供了保障。

融合的基础设施管理

就时间而言，融合管理的理念诞生要早于云计算，但云计算使融合管理成为必然。早在几年前，IT管理员们就发现，随着IT日趋成熟，其承载的企业业务系统也日益复杂化，单一、面向功能的管理系统由于标准不一、各自为政，一旦企业IT设施发生变化或用户核心业务进行调整，就很难与之相适应，由此融合的IT基础架构管理显得越来越重要。H3C通过业界领先的iMC平台，针对往往相互独立的流量分析、性能、配置、服务器应用等领域提供融合的基础设施管理。

1. 基础设备管理和配置

iMC 除了对传统的路由器、交换机进行管理外，更能对网络中的无线、安全、存储、语音、监控、视频、服务器、虚拟设备、打印机等设备进行管理，实现设备资源的集中管理。

同时配置管理帮助管理员方便的对设备配置文件和软件文件进行集中管理，包括配置文件的备份、恢复以及批量更新、设备软件的备份和升级等功能；提供设备配置的基线化版本管理，可以对配置文件的变化进行比较跟踪；提供设备软件的升级历史记录，可以全面审计设备软件版本的变化，并可快速的恢复历史版本，极大的方便了对设备的管理，提高了网络的可维护性。

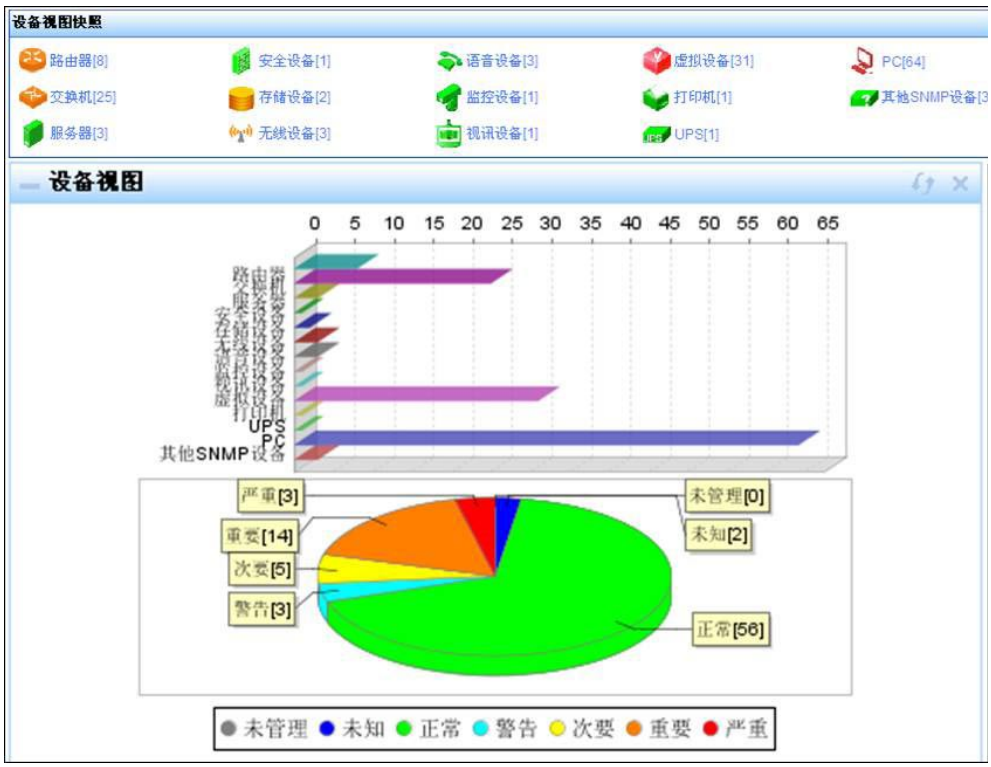


图2 基础设备管理界面

2. 拓扑管理

iMC专门提供了数据中心拓扑，满足数据中心基础设施集中部署、所见即所得的管理需求。

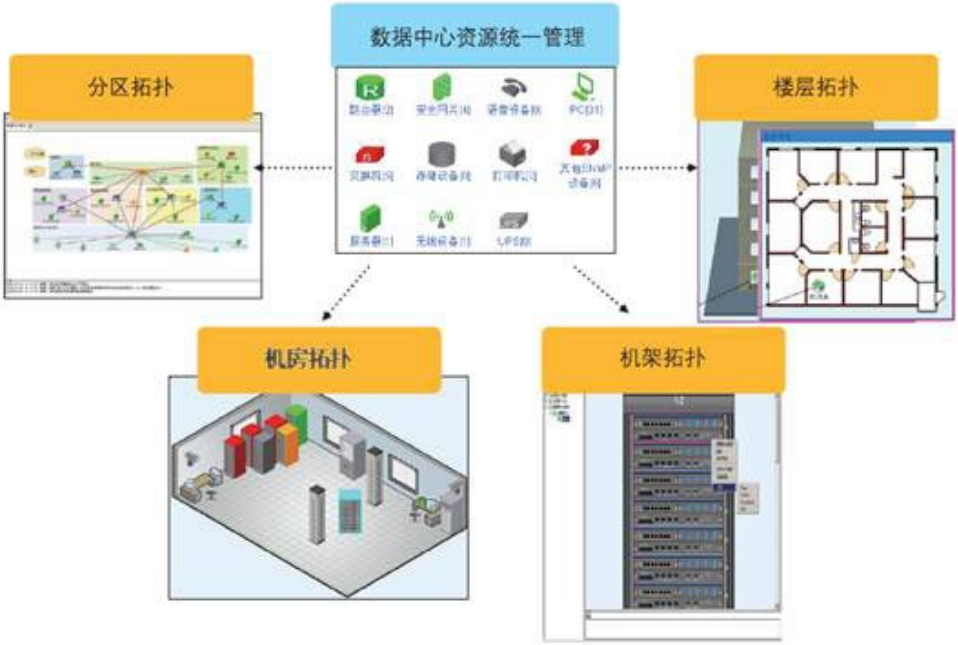


图3 拓扑管理界面

3. 性能管理

CPU利用率、内存利用率、带宽利用率、设备响应性能、设备不可达等是网络性能管理中用户最关注的几项，iMC通过TopN列表，使用户对当前网络中的性能瓶颈能够一目了然。

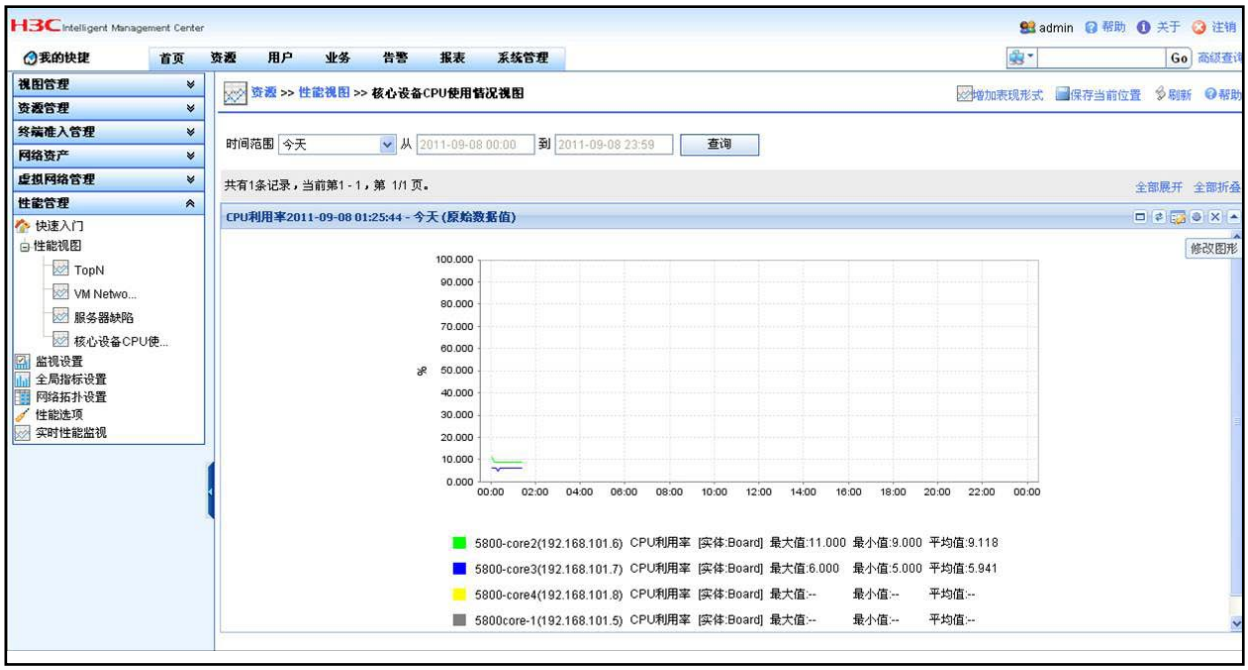


图4 性能管理界面

4. 告警管理

iMC能自动汇总全网中故障设备，形成故障设备列表，使管理员能快速、清晰的找到需要关注的故障设备。告警管理提供了对告警信息的管理功能，包括所有被管理设备上报的和智能管理中心自身各模块在运行过程中产生的告警信息。

图5 告警管理界面

5. 网络流量分析

NTA （Network Traffic Analyse），可以为数据中心提供网络流量信息统计和分析功能，能够让客户及时了解各种网络应用占用的网络带宽，各种业务消耗的网络资源和网络应用中TopN流量的源主机，可以帮助网络管理员及时发现网络瓶颈，防范网络病毒的攻击，并提供丰富的网络流量分析报表。帮助客户在网络规划、网络监控、网络优化、故障诊断等方面做出客观准确的决策。

图6 网络流量分析界面

6. 应用管理

APM （Applications Manager） 是为了帮助企业各种业务的监控管理需求而提供的应用监控管理解决方案，它提供了强大的系统与应用监控管理能力，可以对不同的业务系统、应用和网络服务，如：Web服务（如Apache服务器、IIS服务器）、应用服务器（如Microsoft .NET、WebLogic服务器、WebSphere服务器）、数据库、操作系统、中间件、邮件、其他关键应用等，对网络中的资源与应用进行远程管理，从而有效地帮助企业解决各种应用的监视与管理难题。

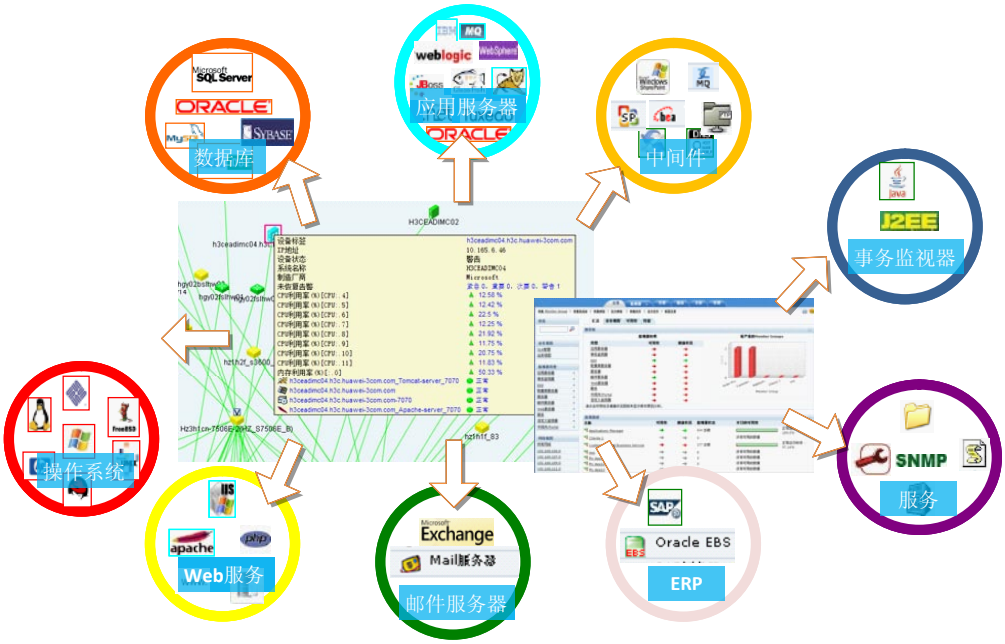


图7 应用管理界面

虚拟化、自动化的资源管理

在数据中心建设中，由于虚拟化技术所带来的成本降低和部署便捷，越来越多的公司开始将其数据中心转移到虚拟化环境中。iMC的虚拟化管理主要包括IRF管理和虚拟化网络管理两部分。

1. IRF管理

IRF（Intelligent Resilient Framework，智能弹性架构）是H3C自主研发的软件虚拟化技术。通过IRF将多台设备虚拟化成一台“分布式设备”，iMC在管理上实现一个IRF中多台物理设备的协同工作和统一管理，包括IRF拓扑展示、面板监控、配置和软件管理等。

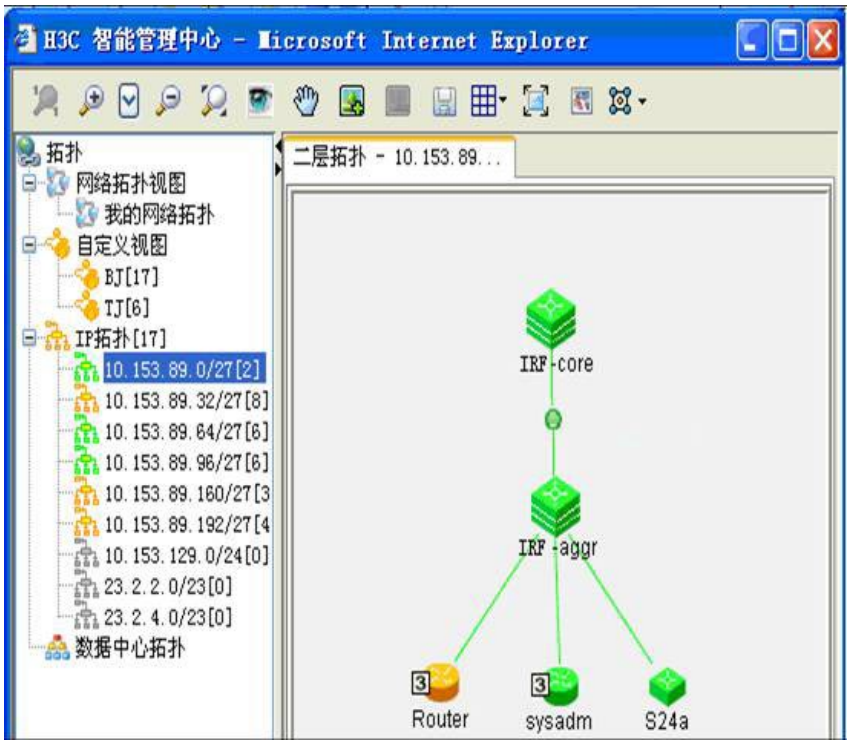


图8 IRF管理界面

2. 虚拟网络管理

VNM（Virtual Network Manager）是针对通过虚拟化软件构建的虚拟网络进行统一管理的系统。

系统提供对虚拟机(VM)、vSwitch、物理服务器和vManager的监控，并实现各虚拟网络设备间拓扑关系的展示，为帮助用户对虚拟网络进行管理提供有效手段。虚拟网络管理立足于智能管理中心，以统一的风格提供对虚拟网络设备的管理、监控等功能。

图9 虚拟网络管理界面

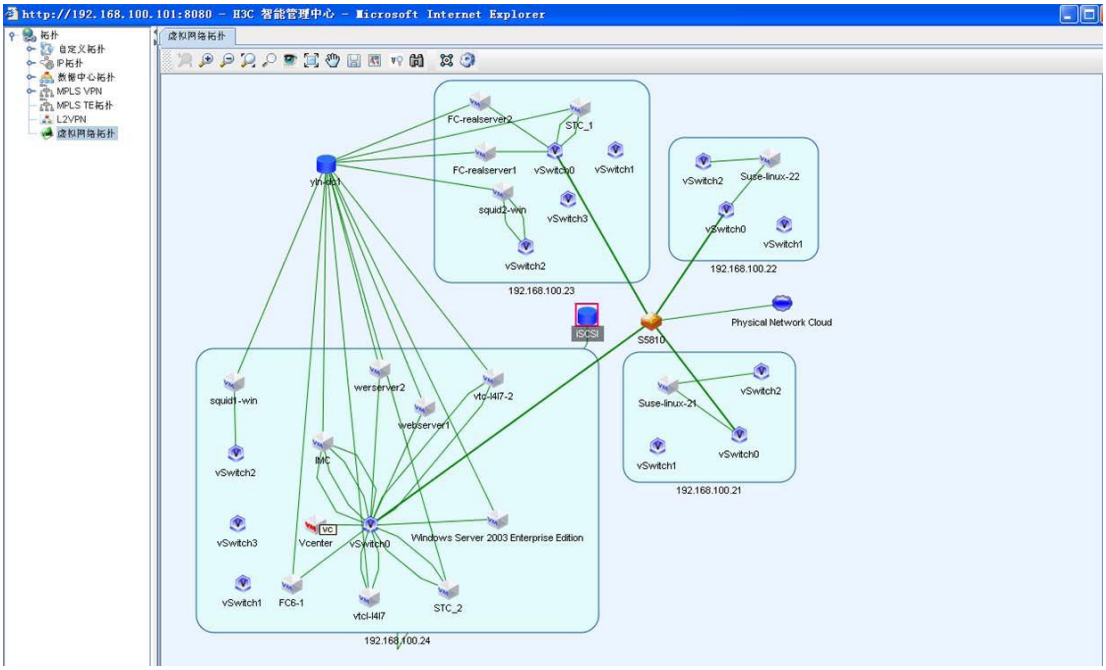


图10 虚拟网络拓扑界面

专业、主动的服务管理

1. 连接资源管理

在虚拟化数据中心环境中，为实现按需分配资源，需要计算、存储、网络资源的协同调度，才能完成服务/应用的创建部署。此过程中服务/VM要连接到网络，需要按服务类型的需求分配连接网络所需的资源。iMC CRM即用于服务/VM和网络之间连接的管理，从而实现匹配VM需求的网络资源动态调配。目前CRM有两种实现方案：1）基于802.1Qbg标准的CRM方案，该方案基于iMC CRM组件、802.1qbg交换机（H3C 58V2）和vSwitch (H3C vSwitch）实现。如下第一幅图中所示。2）基于VMware的

CRM方案。对于非EVB标准的VMware环境，基于iMC的拓扑分析能力、以及VMware事件实现。如下第二幅图中所示。

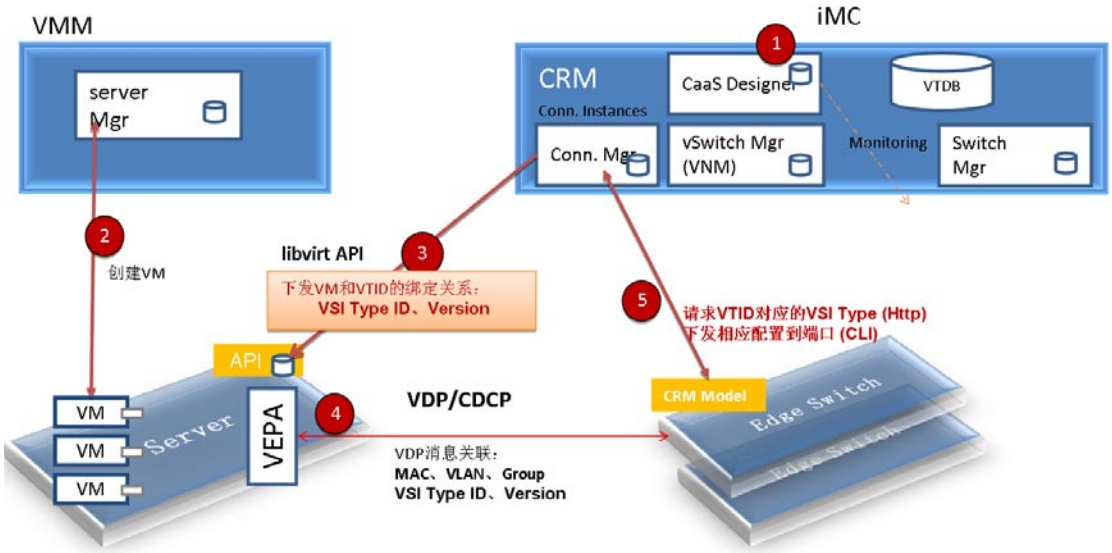


图11 基于802.1Qbg的CRM方案

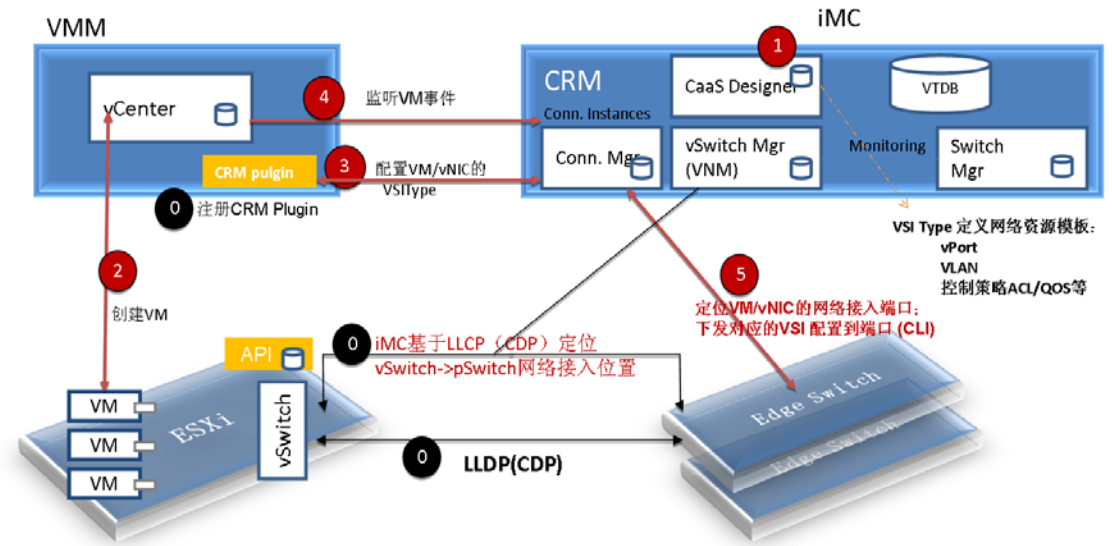


图12 基于VMware的CRM方案

2. 服务健康管理

SHM（Service Health Manager）基于iMC整体框架，融合告警、性能、流量、应用等数据，通过KQI（关键质量指标）的创建，来完成IT服务的质量监控，便于及时发现潜在问题、实时掌控IT服务的整体水平。

图13 服务健康管理界面

3. SOM

服务运维管理（SOM）是指在日常的网络和业务管理过程中，使用业务流程控制手段，对行为的过程和结果进行有效监管和控制，并在事后提供行为审计的能力。 服务运维管理与iMC中常用网络配置管理操作相互配合，并结合各种基本的可配置项（CI），为用户提供可运营维护的网络和业务配置管理环境，并最终提升管理软件的应用范围和价值。

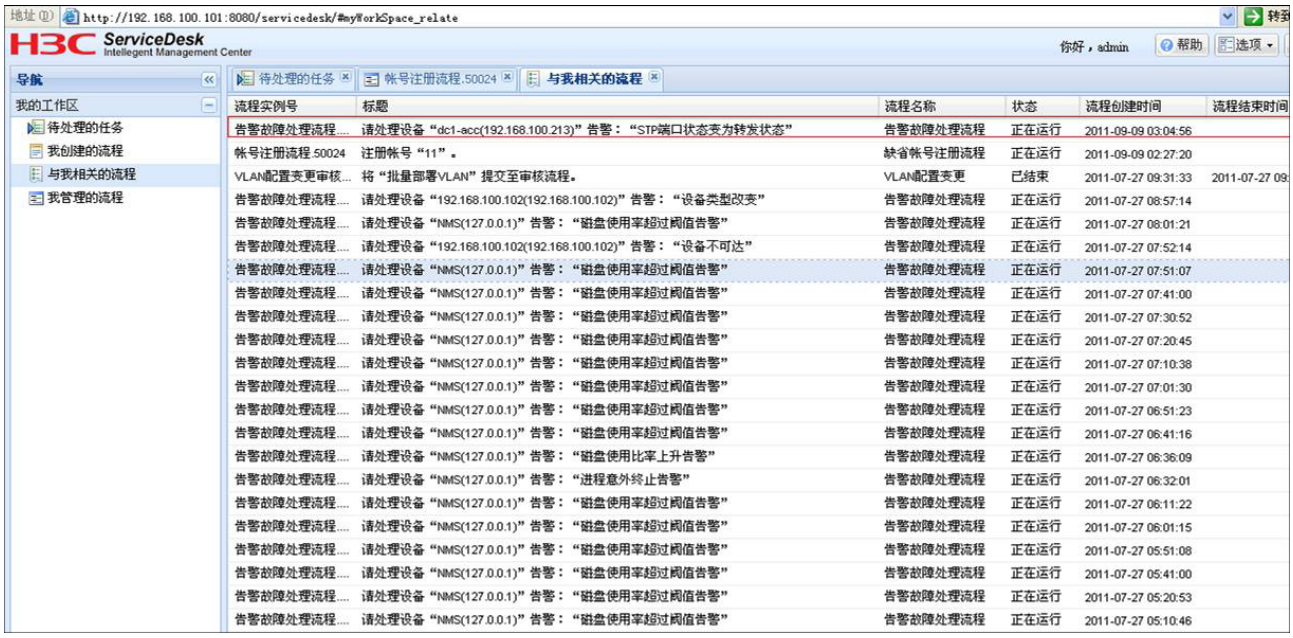


图14 SOM界面

4. 智能分析报表

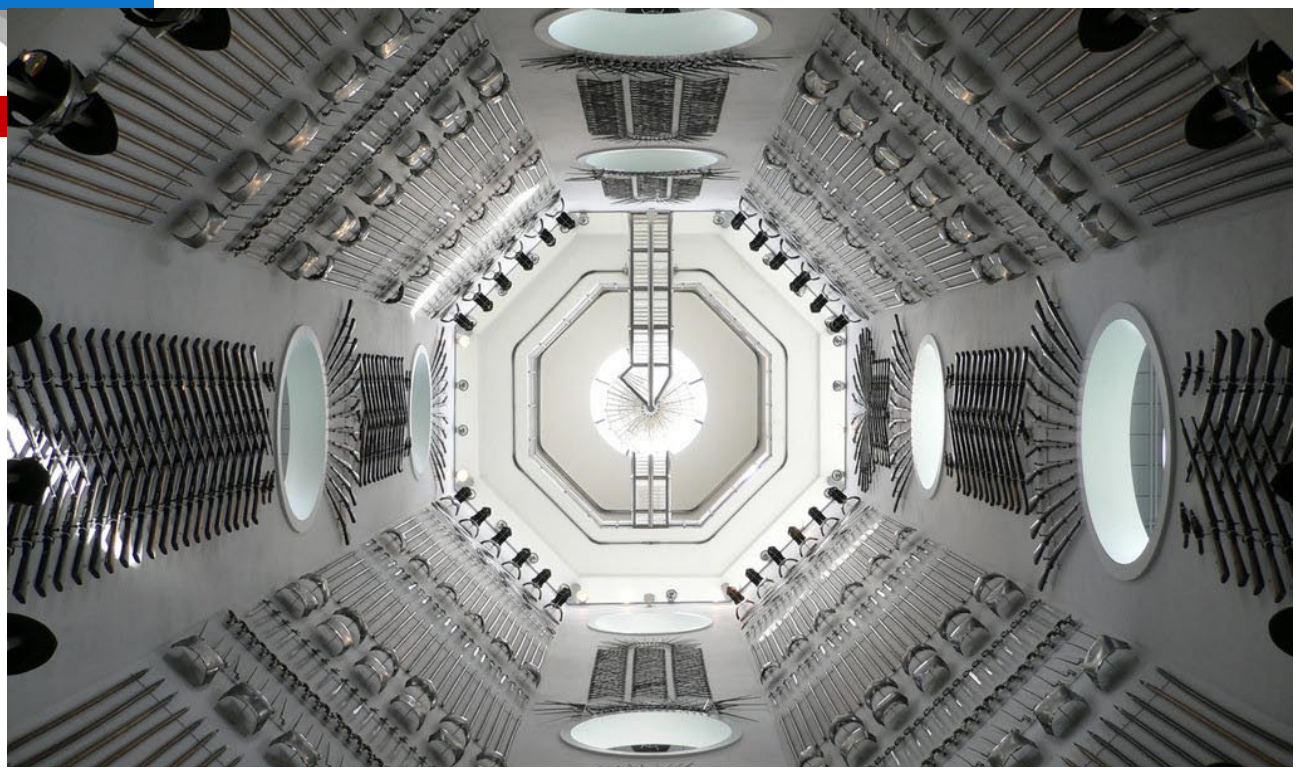
iAR（Intelligent Analysis Report）将报表分析和报表展示与iMC无缝集成，实现从数据提取、数据转换和数据展示等功能，提供“所见即所得”的有效报表系统解决方案。利用iAR可以方便地创建简单的报表，不仅如此，它还拥有生成复杂报表或专用报表所需的一整套工具，满足各行业用户的定制报表需求和iMC的专业报表设计人员的开发需求。

图15 智能分析报表界面

总结

H3C多年来在网络基础设施管理积累了丰富的管理经验和技术实践，并且积极参与国内云计算用户的网络建设和管理规划，充分探索并了解云数据中心的管理需求，相信这些可以为用户带来贴合实际、不断完善的云数据中心管理方案。

网络基础设施的管理



iMC的网络基础设施管理

文/袁亚屏

网络基础设施的管理由来已久，也是整个网络管理体系的基础。在数据通信网络中，通常情况下路由器、交换机、防火墙和服务器等网络设备被视为网络基础设施。下面我们来看一看iMC在网络基础设施的管理方面有什么独到之处。

iMC平台提供的管理功能

基础网管功能

iMC平台是整个iMC的根基，它提供了大量的网络基础设施管理功能，主要包括网元管理、性能管理、告警管理、日志管理等功能，同时还提供了VLAN管理、ACL管理、设备配置管理等比较有特色的功能。

可以说，iMC平台已经提供了很丰富的网络基础设施管理手段，能够满足用户的基本管理需求。包括功能管理、性能监视、告警管理和报表等等。

基础资源管理

除了传统的路由器、交换机外，iMC更能对网络中的无线、安全、语音、存储、服务器、打印机、UPS等设备进行管理，实现设备资源的集中化管理。

图1 基础资源管理

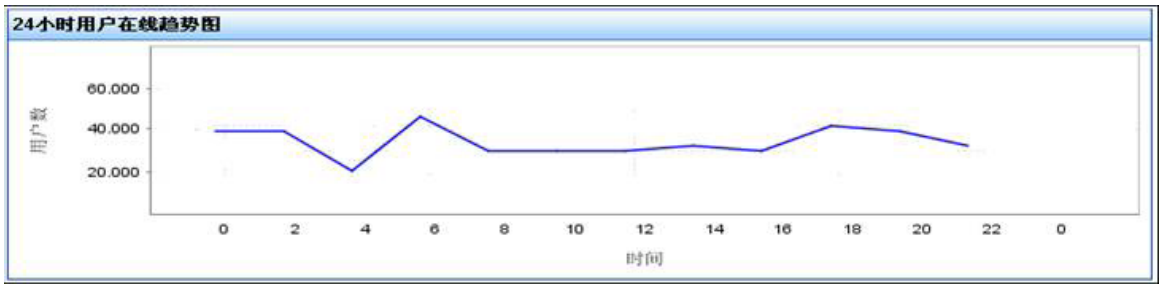


图2 用户在线趋势

设备面板管理

iMC支持设备面板管理，所见即所得的显示设备的资产组成和运行状态。

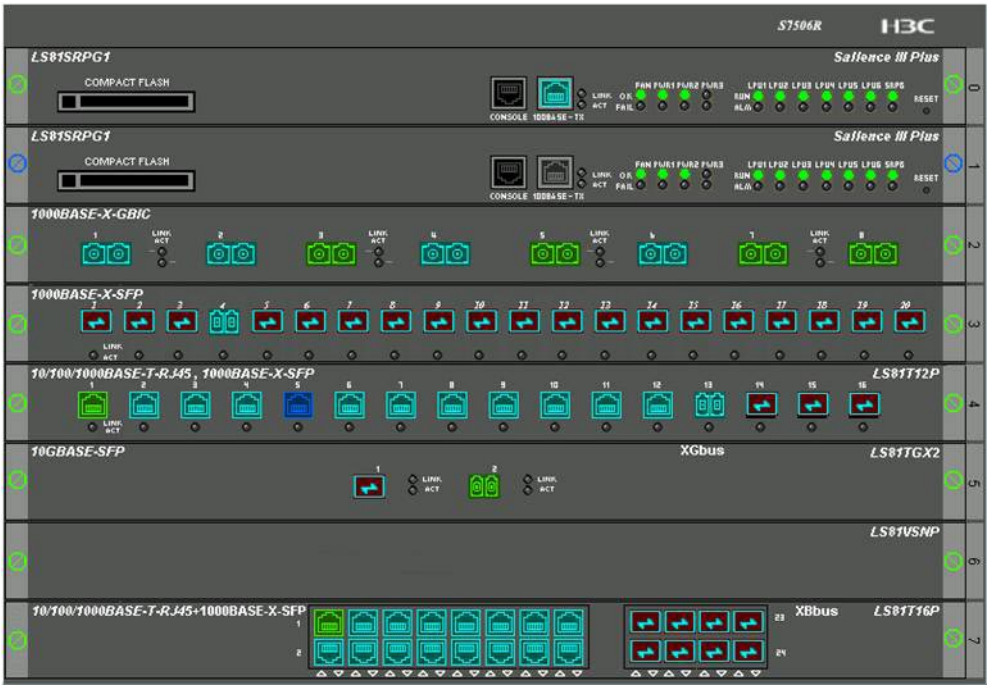


图3 设备面板管理

网络视图

iMC提供多种类型的视图，其中：

IP视图：从IP层协议的角度，对系统所管理的网络进行认识和分析所形成的拓扑，显示了三层设备之间的逻辑连接关系，这里所说的三层设备是指有两个或两个以上IP地址，并启动了IP转发的设备；

设备视图：使得用户对网络中设备类型和数量一目了然；

自定义视图：用户可以根据自己的管理需要，创建自定义视图，并将某些设备加入该视图中，以便进行管理。自定义视图中包含设备和子视图，其子视图又可以包含设备和子视图。同时还提供直观简便的预览功能，集中监控用户关心的重点设备和接口的状态。

状态	设备标签	子图	型号	IP地址	厂商	类型	CPU利用率(%)	设备响应时间(ms)	操作
正常	CORE_10508(185.100.0.254)		H3C S10508-V	185.100.0.254	H3C	交换机	11.0	0.0	
重要	Neocean(185.200.0.100)		H3C Neocean IX1000	185.200.0.100	H3C	存储设备	3.0	0.0	
重要	Neocean(101.3.200.100)		H3C Neocean EX1000	101.3.200.100	H3C	存储设备	4.0	0.0	
正常	S5800-FW1(202.102.30.27)		H3C SecBlade LSWM1FW10	202.102.30.27	H3C	安全设备	1.0	0.0	
正常	S5800-FW2(202.102.30.28)		H3C SecBlade LSWM1FW10	202.102.30.28	H3C	安全设备	1.0	0.0	
正常	S5830V2D(185.100.0.204)		H3C S5830V2-24S	185.100.0.204	H3C	交换机	2.0	0.0	
正常	S5830V2U(185.100.0.202)		H3C S5830V2-24S	185.100.0.202	H3C	交换机	2.0	0.0	
正常	TC-Gateway(202.102.30.10)		H3C SecBlade LSQ1FWBSC0	202.102.30.10	H3C	安全设备	1.0	0.0	
正常	VM-Duration(185.150.0.1)		H3C S5820X-28S	185.150.0.1	H3C	交换机	14.0	0.0	

图4 自定义视图

多样化的网络拓扑

显示设备、链路和CPU、链路流量等信息；融合显示告警故障状态；

提供完整的IP拓扑、二层拓扑、邻居拓扑，融合显示接入设备的接入情况；

用户可以根据实际组网情况，定义自己关注的自定义网络拓扑；

并对业务组件提供相应的业务拓扑和操作链接的平台支撑能力。

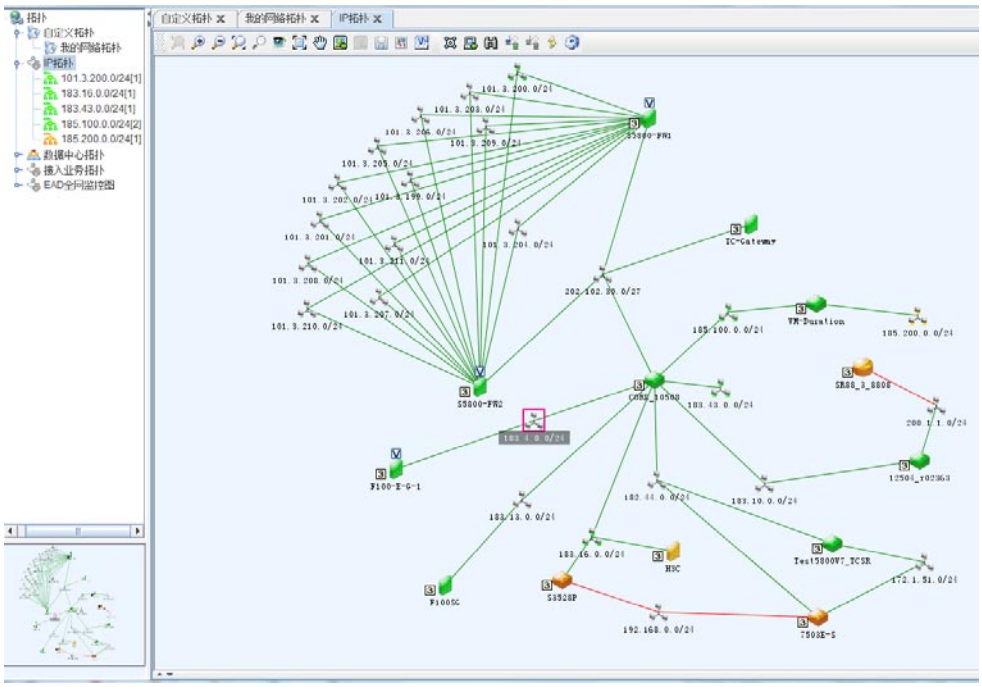


图5 网络拓扑

告警显示、过滤和关联

提供告警过滤，有效压缩海量网络告警；

汇总显示发生故障的设备，缩小管理员维护工作的关注范围；

为业务组件提供关联基本告警、产生业务告警的平台支撑能力；为网络的现状评估和优化提供数据基础。

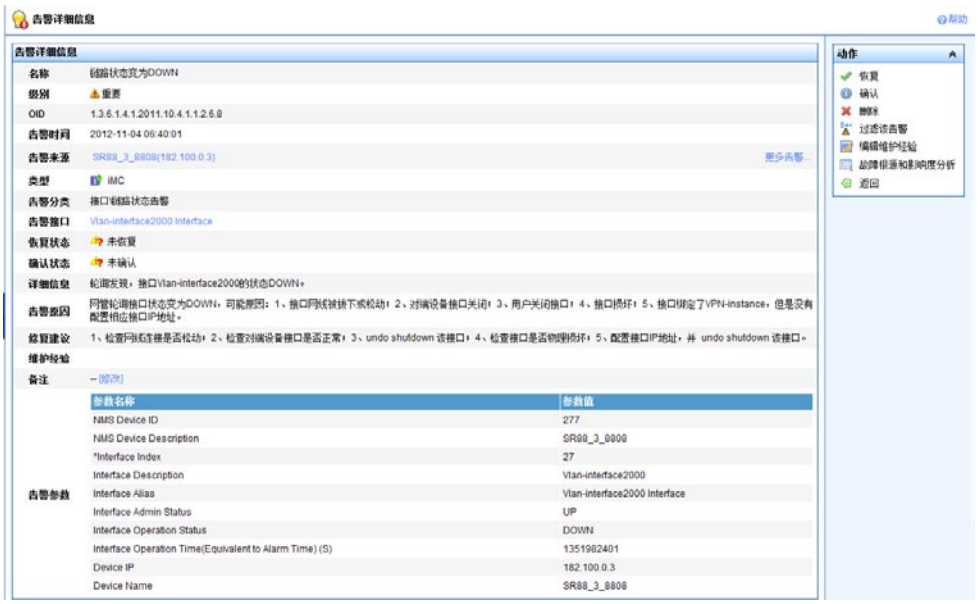


图6 详细告警

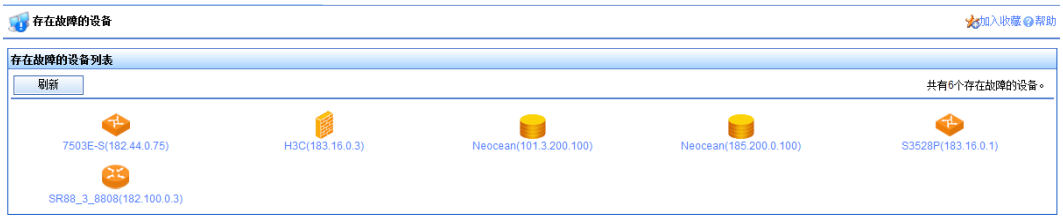


图7 故障设备汇总

性能管理

一目了然的网络TopN性能指标，性能与告警的深度结合，详实的性能统计报表。

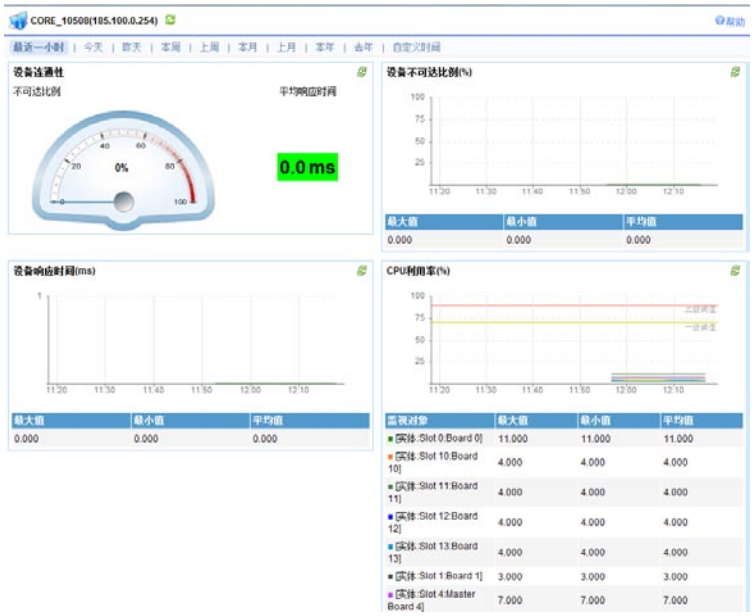


图8 性能数据汇总

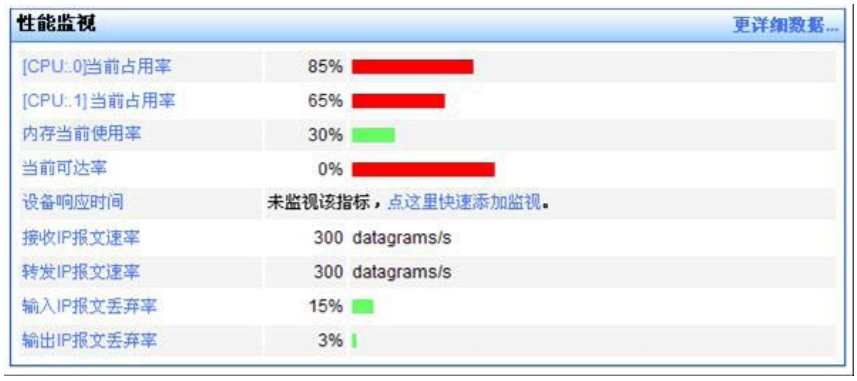


图9 性能监视

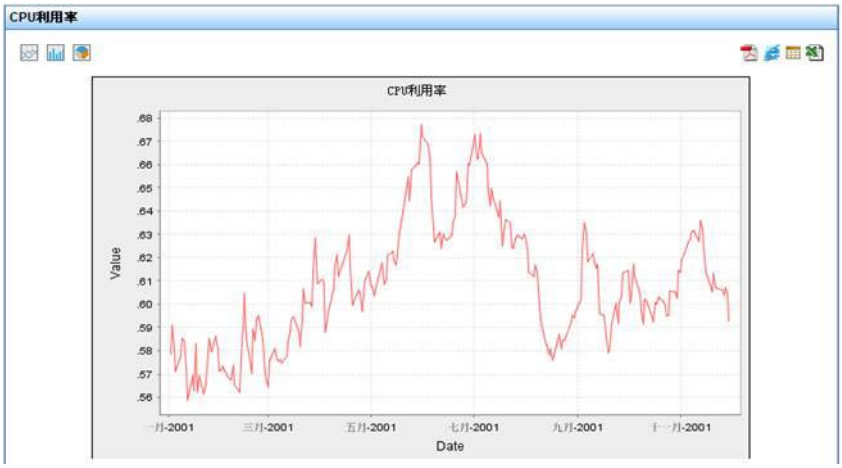


图10 性能统计报表

设备配置和设备软件管理

以资源管理的角度提供了配置文件库和软件文件库的管理，除了管理设备的版本软件，还支持设备上各种业务的软件管理。

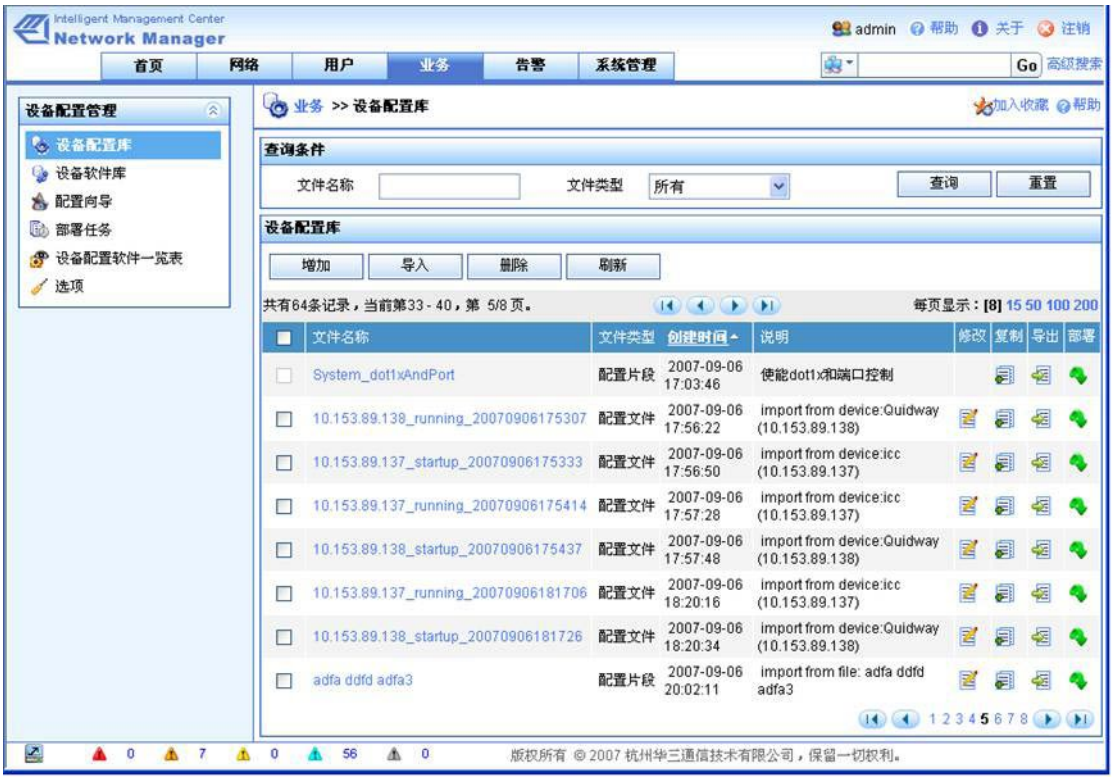


图11 设备软件与配置管理

特色功能

虚拟化管理

iMC提供了虚拟化管理功能，包括虚拟化网络的管理和虚拟化服务器的管理。

IRF构架就是一个比较典型的虚拟化网络的例子。iMC能够实现一个IRF中多台物理设备的协同工作和统一管理，使得多台参与IRF的设备可以被当作同一台设备来管理。

服务器虚拟化是近年来很流行的技术。目前iMC实现的虚拟化服务器管理主要实现基于VMware架构的管理，包括服务器(ESX/ESXi Server)、虚拟交换机(vSwitch)、虚拟机(VM)、集中管理平台(vCenter)等虚拟资源的管理及虚拟机迁移管理。

虚拟资源监控功能以树形结构，层次化地展示出ESX/ESXi Server、vSwitch、VM、端口组之间的从属或连接关系及相应的详细信息，可以监控虚拟机的CPU、内存、磁盘I/O、网络性能等使用情况；集中管理vCenter上收集的告警信息，包括ESX/ESXi Server主机状况，VM内存、CPU超载等信息。

图12 虚拟资源监控全局指标设置

图13 虚拟资源监控

虚拟网络拓扑功能以拓扑方式展示ESX/ESXi Server、虚拟交换机（vSwitch）、虚拟机（VM）之间的从属或连接关系，同时，通过ESX/ESXi Server和物理交换机之间的连接关系，展示ESX/ESXi 所在的物理位置。

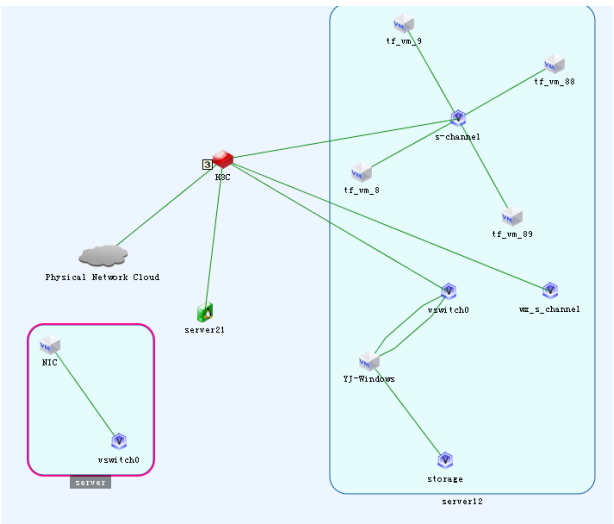


图14 虚拟网络拓扑

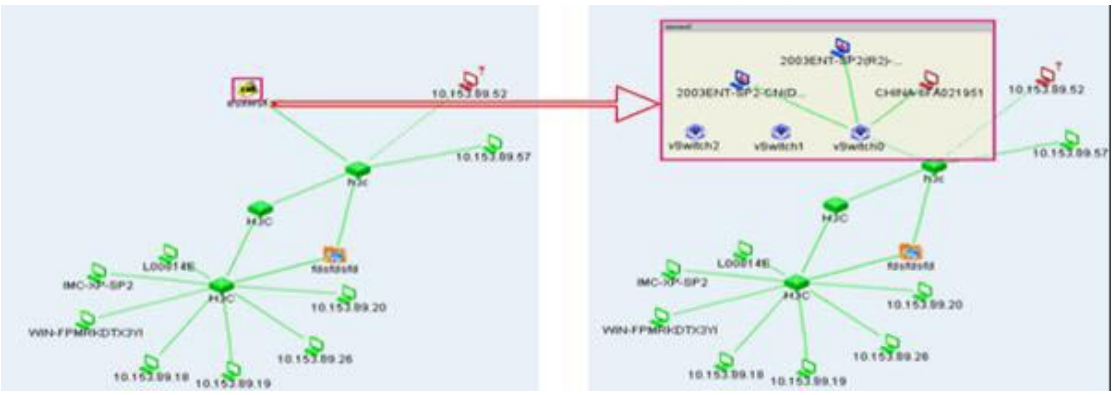


图15 ESX/ESXi物理位置展示

虚拟网络迁移

通过VM的配置文件可以查看VM网络配置内容。iMC会轮询vCenter上的迁移建议，管理员根据建议在iMC中手工执行迁移或设置参数自动执行迁移。

特殊设备的管理和特殊功能的实现

iMC平台的功能虽多，但是更多的是提供了通用功能，对于一些特殊设备的管理和特殊功能的实现，一般是使用组件的方式实现。

对于特殊设备和特殊网络的管理方面，iMC针对无线网络（WLAN）提供了WSM组件；针对语音设备和VoIP业务提供了VSM组件；针对存储设备的管理提供了UDM组件。这些组件和平台协同工作。

对于特殊功能的实现，iMC针对AAA（认证、授权和计费）提供了UAM/EAD/CAMS组件；针对VPN业务的管理提供了IVM和MVM组件；针对网络流量和用户行为的分析提供了NTA/UBA组件。这些组件和平台协同工作。

iMC在易用性上的特色

iMC在易用性方面也有一系列的特色。

WEB2.0

iMC v5版本开始使用了WEB2.0构架，使用更轻量级的REST接口，Web客户端采用AJAX技术，支持异步调用和自定义首页，由原来静态B/S升级为动态B/S。通过iMC V5，用户将获得全新的体验。

总结起来，iMC符合Web 2.0主要体现在：

SOA架构，SOAP及REST对外接口，Web客户端采用AJAX技术。

给用户带来的好处：

用户使用更便捷，Web客户端响应更快速，接口执行效率更高效。

自定义首页

从v5版本起，iMC通过AJAX技术支持全新的“自定义首页”功能。首页就像一个容器，管理员可以把自己关心的内容，如告警、拓扑、流量、WLAN等不同信息定制在首页上，或者改变页面的布局结构，各页面元素就像iGoogle一样可以拖拽到任何地方。同时支持RSS定制，管理员可以添加一些重要的外部信息的RSS源到首页，iMC展示的内容将变得更为丰富。

管理员A（关注流量）

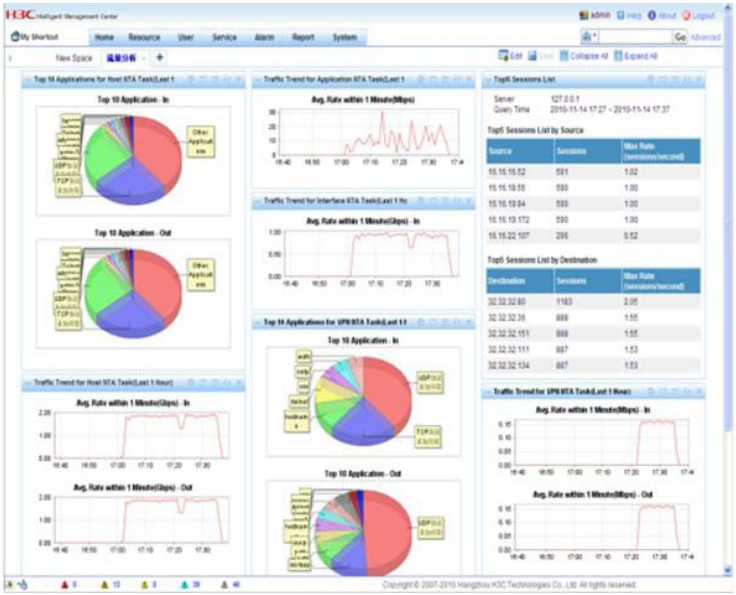


图16 自定义首页1

管理员B（关注告警）

图17 自定义首页2

管理员C：关注拓扑）

图18 自定义首页3

总结

iMC在网络基础设施的管理上，提供了丰富的功能和多样化的组件满足用户的需求，同时在易用性方面提供了很多特色功能。

——让“智能”飞

智能无线业务管理

文/王白辉

引言

如今，网络已经融入到社会的各行各业以及生活的方方面面，人们无时无刻不在使用或被使用网络。随着网络的飞速发展，传统有线网络已经无法满足层出不穷的网络业务需要，无线网络适应挑战满足人们随时随地能够接入网络的需求，更能适应变化无穷的无线终端接入，所以无线得到了爆炸式的发展。如此强势的发展带来了巨大的规模，作为灵活而又不可见的接入层网络，需要较大量的维护工作，这样对无线网络的管理需求也更加强烈。无线网络直接面向终端用户，对管理系统的稳定性、实时性、有效性都有很高的要求。传统的网络管理模式以及分布单点的无线设备管理都远远不足以满足当下神出鬼没、飞速发展、日益庞大的无线网络业务，“智能”的业务管理模式将更加有效，更加适应需要，也会变得更加重要！H3C iMC WSM适应市场需求，适应市场变化，适应市场发展，破世而出！

无线业务管理组件（WSM）依托智能管理平台（H3C iMC），实现有线无线一体化的管理，在iMC系统全面的智能的有线网络管理的基础上，为管理员提供无线网络管理能力。管理员无需重新搭建IT管理平台，即可在原有的有线网络管理系统中增加无线管理功能，与有线管理平台统一部署，节省用户投入，节约维护成本。可以实现但不仅限于以下功能：（批量）配置、网络监控、网络布局、定位管理、安全控制、网络规划、射频覆盖、准入策略、节能策略、网络评估、统计报表、业务扩展以及有线网络管理上实现的其他功能。无线业务管理组件（WSM）和智能管理平台（H3C iMC）的完美结合，让“智能”飞起来！

WLAN无线管理所面临的问题

设备数量大，种类多——难配置

无线网络的部署中，出现的第一个问题就是设备的数量非常大，动辄成百上千，在城域网中甚至上万数量级的无线设备。同时，无线网络部署带来了很多新的设备类型，比如说，无线控制器AC、胖AP（FAT AP）、瘦AP（FIT AP）等。这些造成了我们在建设无线网络的时候遇到“难配置”的问题。如图2–1所示：

组网复杂，分布广——难维护

无线网络的应用环境多种多样，易于变化。应用中从家庭、园区、街区、广场到大企业、商务楼、酒店，甚至地铁、公交，以及“无线城市”部署；分布范围也是从室内到室外，从家用到商用，从固定到移动。无线网络讲究信号覆盖，但由于地理情况不同，周围环境不同，分布广的同时造成组网复杂，一旦出了问题，很难对设备进行维护。 如图2–2所示：

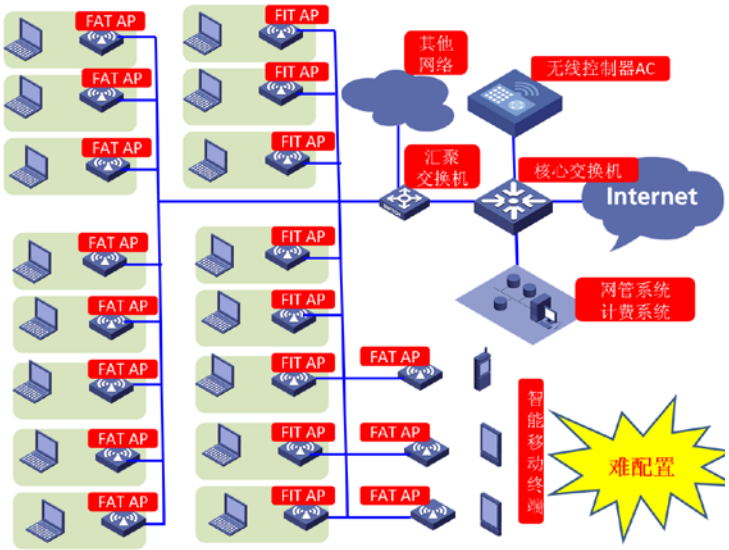


图 2–1 设备数量大，种类多——难配置

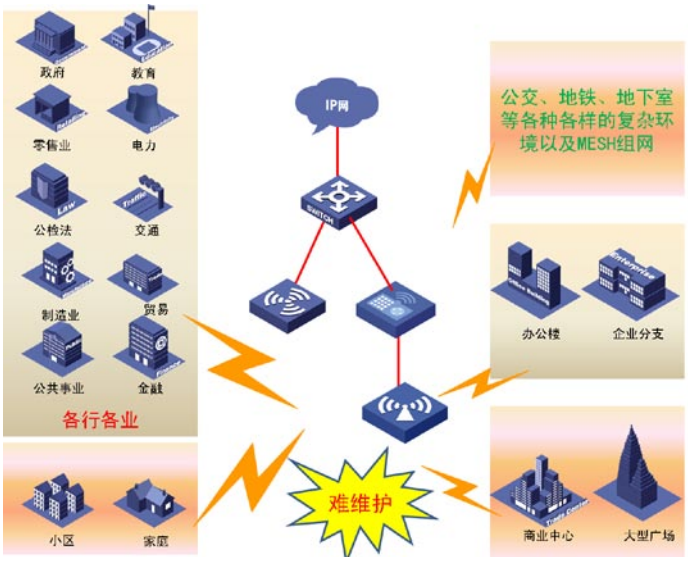


图 2–2 组网复杂，分布广——难维护

与有线配合，射频不可见——难管理

就无线网络的发展来看，很多对无线有需求的企业、单位和运营商，他们不会建一套完全独立的无线网络，无线网络还需要在现有有线网络的基础上进行扩展，这要求管理员同时具备有线网络、无线网络管理技术，并且同时维护两套网络，工作量大，效率低下。另外，无线信号看不见摸不着，并且遇到障碍物会有衰减，很难对“链路”进行部署预测，覆盖效果不能预先知道，即使正在使用的无线网络射频覆盖也缺乏直观稳定的数据。以上这些，给无线带来了“难管理”的问题。

业务单一，缺乏长期规划——难扩展

现在的大部分无线网络处于一个起步阶段，提供给用户一个宽带接入的手段，对于后期的高级应用顾及很少，更不要说更长远的新的应用。所以这种无处不在的无线网络要向可运营可管理的无线网络转变，将来要向无处不在的服务（业务）转变。如图2-3所示，更形象的说明了无线网络的现状和发展方向。但是当前的无线网络阶段缺乏长期规划，带来了“难扩展”的问题。

图 2-3 业务单一，缺乏长期规划——难扩展

智能无线业务管理组件iMC WSM

WSM管理模型

WSM是为实现有线无线一体化的管理理念而提出来的，借助有线网络设备的成熟的管理技术，引用到无线管理中，可以在同一个平台实现对有线无线的无缝管理，节省用户投入，减少维护工作。

如图3-1，WSM有线无线一体化管理模型，可以看出，有线无线一体化理念贯穿整个周期。管理模型中的五大步骤形成一个有机循环，始于部署，中间可以监控，然后运营，安全和优化之后，部署调整，如此往复网络逐渐走向稳定。在此，运营才是目的，其他步骤不可或缺，为运营提供更好的服务，

帮助运营以及整个生命周期的维护实现最小的投入和最大的收益。

WSM功能特点和优势

有线无线统一管理（智能的设备统一管理）

无线业务管理组件WSM作为iMC智能管理中心的无线业务管理核心，对于网络中的AC、FAT AP、FIT AP、移动终端等无线设备与有线设备进行一体化集中管理，全网设备信息和状态一目了然，如图3-2所示。

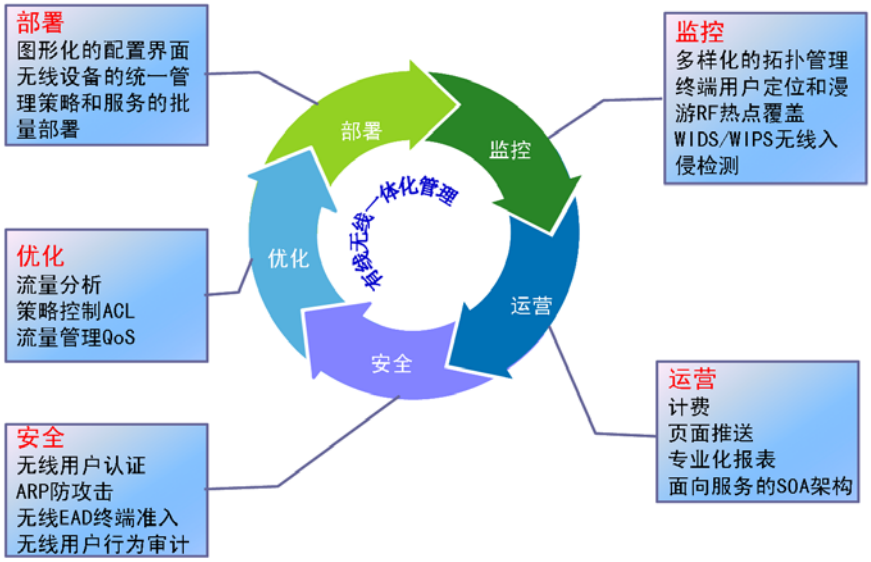


图 3-1 WSM有线无线一体化管理模型

无线业务管理概览页面，对无线设备运行情况直观呈现，包括无线资源状态、在线用户趋势、带宽趋势、告警等图表，并能通过相应链接进入资源信息、历史信息和TopN信息等页面，如图3-3所示。

智能的设备统一管理和直观的图表首页，直接呈现当前所有网络资源的状态，给管理员的管理工作带来了极大的方便。

有线网络管理成熟的EAD安全策略、流量策略、接入控制策略、授权认证策略等技术手段全部可以方便的移植到无线网络业务管理中，给无线网络的部署和维护节省大量投入。

图 3-2 iMC首页 有线无线设备一目了然

图 3-3 无线业务管理概览页面

多样化的拓扑管理

无线业务管理提供拓扑视图，在拓扑视图中可以选择不同的方式显示当前的网络部署情况和设备、链路的当前状态。系统根据不同的方式，有效的进行拓扑分组、真实的组织全网资源。并且管理员可以创建自己的位置视图和自定义视图，通过多维度、多层次的位置视图，可以扩展出更多非常直观的可视化功能，如射频覆盖显示、定位功能等都是在拓扑视图中基于位置视图实现，使呈现出的网络设备运行情况更逼近真实网络环境。

结构化的视图管理

首先视图分为三类：位置视图、自定义视图、GIS视图，如图3-4所示，不同的视图类型又有不同的组织形式和层次结构。

位置视图是基于真实的物理位置，由管理员创建。支持多层次的子位置视图，类似于Windows的文件夹系统，只能是高级别的包含低级别的位置视图，其中最高级的“区域”类型可以同级包含。一台无线设备只能属于一个位置视图，因为位置是基于真实的物理位置。位置视图中可以包含多台AP，包括FAT AP和FIT AP，FIT AP时只显示AP，不显示AC。

自定义视图是管理员根据自己需要而创建的，用于为定位到所关心的设备提供方便。它是由一台AC及其下的若干FIT AP组成。自定义视图不分级，一个视图只能包含一台AC，也只能包含一台AC下的多台FIT AP设备。并且一台AC或者FIT AP可以属于多个无线自定义视图。

GIS视图就是在系统提供的地图上创建与位置视图相对应的热点，然后可以对具体的AP设备进行定位。管理员可以定义热点在地图上显示的位置，方便掌握热点位置的分布，并快速定位所关心的热点的位置。GIS的核心是一个地理数据库，这里借用Google Map，需要管理员做相应设置。

图 3-4 视图管理

智能的射频覆盖管理及网络规划

在实际的无线网络环境部署和维护工作中，需要关注射频覆盖，以及无线网络后期的规划扩容问题。射频是看不见摸不着的，遇到障碍物会有衰减，并且在空间传播会有多径效应。针对以上问题，无线业务管理组件可以智能的在拓扑视图直观显示射频覆盖状况，并可以精确显示由于遮挡、障碍等对射频造成的衰减情况。射频覆盖可以设置比例尺，调整AP Radio功率、天线类型等更逼近真实物理环境的显示射频覆盖状况，可以分别按照信号强度、速率和信道显示射频覆盖情况。如图3-5所示，按信号强度显示射频覆盖，射频覆盖直接呈现，可以看到由于遮挡对信号造成的衰减，不同颜色的分布呈现信号的

具体强度区间。在此可以操作：增加/删除背景图、设置比例尺、增加障碍物、增加/删除设备、增加/删除位置、设置射频覆盖颜色、显示信号覆盖（按强度、信道、速率）等。

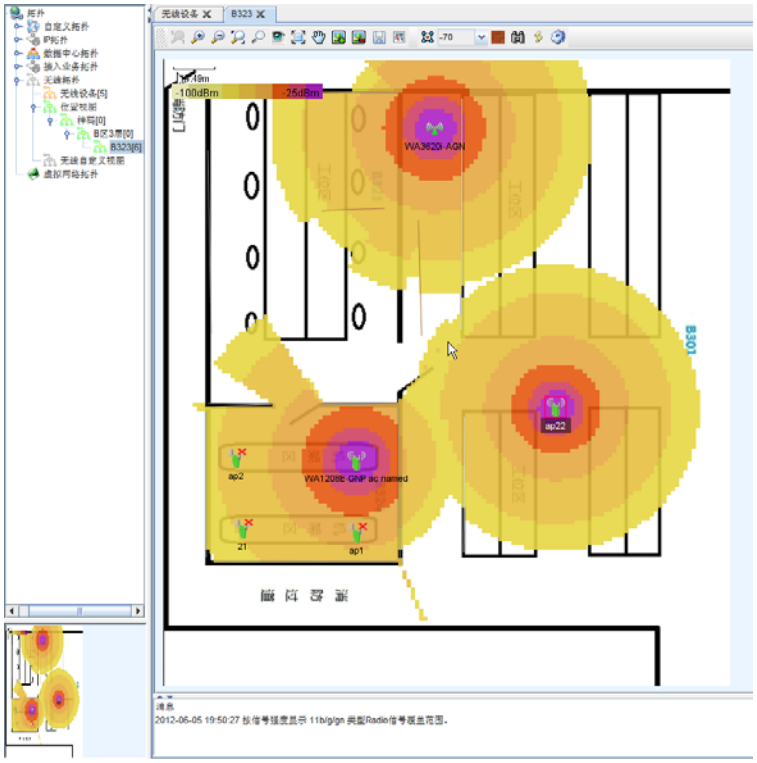


图 3-5 按信号强度显示射频覆盖

真实的呈现物理设备的射频覆盖情况给当前环境的维护带来方便，WSM还提供虚拟AP来为无线网络规划和无线网络扩容服务。可根据需求，把虚拟AP加入到拓扑视图相应的位置中，并查看信号覆盖范围和强度，帮助用户在建设和扩容WLAN之前，通过评估具体位置中AP的信号覆盖情况，对AP型号的选择和布局进行详细的规划。如图3-6所示，假设在一块儿很大的广场区域规划无线网络，防止信号覆盖不足而又因重叠浪费资源，可以使用虚拟AP预先模拟射频覆盖，做无线网络规划。图中AP为虚拟AP。

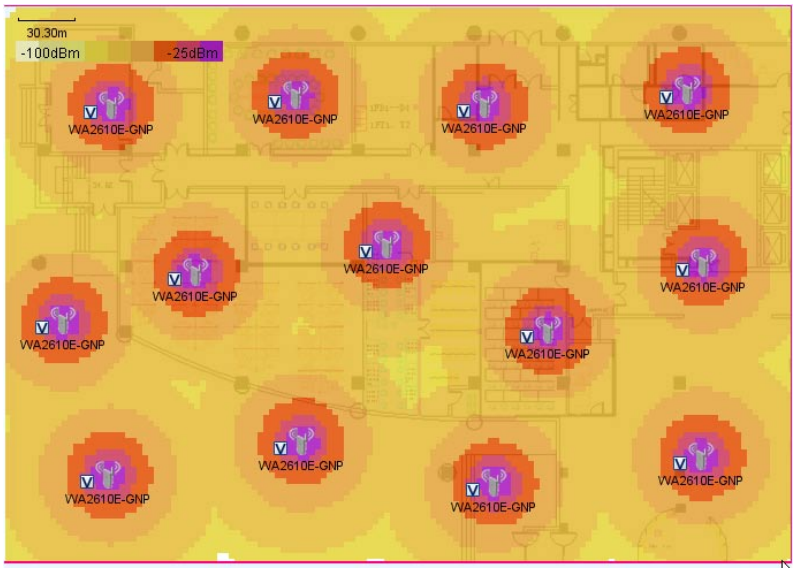


图 3-6 无线网络规划：虚拟AP射频覆盖

无线定位和基于iNode的实时定位

在对无线网络进行管理时，需要无线定位功能。通过无线定位功能，可以实现对在线STA以及非法STA、非法AP进行定位，方便管理员第一时间了解无线用户和非法STA、非法AP的物理位置，第一时

间解决问题。如果在线STA、非法STA或者非法AP所关联的AP设备处于位置视图下，并与热点进行关联，还可以定位到GIS视图中。

STA安装H3C iNode客户端以后，还可以实现基于iNode采样的无线定位，也称为实时定位。基于iNode采样的无线定位，可以快速、精确、实时的定位当前STA的物理位置，所以可以同时实现iNode无线客户端的实时跟踪、对用户的历史轨迹进行记录，并可以对用户历史轨迹进行动态展示，如图3-7，基于iNode采用的无线定位用户的历史轨迹动态展示。

基于物理位置的无线终端准入策略

在基于iNode采样的无线定位的基础上，借助于定位的实时性、精确性，可以实现基于物理位置的准入策略功能。通过设置准入区域和准入策略，可以对准入控制用户分组中的用户实施禁止或允许的控制，对规则违反的无线终端进行通知、告警、强制下线处理，如图3-8所示，设置了禁止类型、强制下线处理的准入策略，在其生效以后，准入区域和准入控制用户分组中的用户会被强制下线。通过准入策略功能，可以对某一区域实行控制，允许或禁止特定客户端上线，做到安全、有效、精确的管理无线网络环境，减少许多不必要的麻烦和故障的发生。

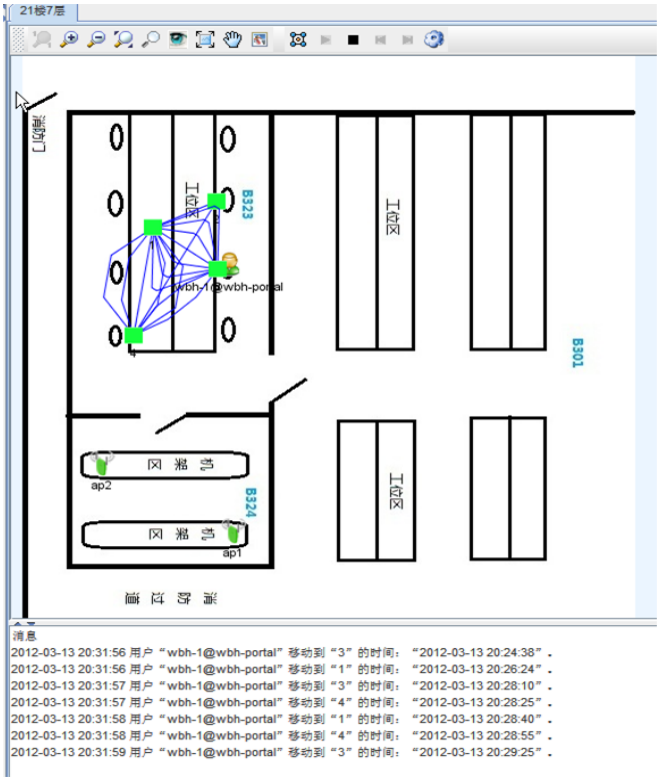


图 3-7 基于iNode采用的无线定位用户的历史轨迹动态展示

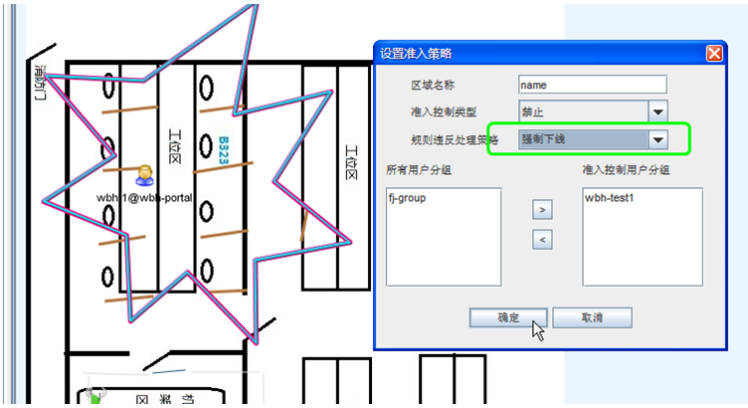


图 3-8 基于物理位置的准入区域和准入策略

强大的无线网络配置部署

如图3–9，无线配置管理分为网管配置、无线控制器配置管理和FAT AP批量配置管理。

图 3–9 无线网络配置部署

网管配置包括无线性能监视设置、FIT AP分组、主备AC分组、策略模板管理、AP型号管理、天线管理。可以批量启动或停止无线报表、FIT AP分组分权、管理主备AC组、管理AP型号和天线参数、预定义策略模板等操作，为之后的配置部署以及维护做好准备工作。

无线控制器配置管理，是以配置向导的方式呈现，操作依次进行，简单快捷而清晰，配置过程直观显示；而且在配置过程中可以使用预定义模板，可以进行批量操作，大大加快了配置部署的速度。在操作中还可通过“相关操作”跳转到下一步或者需要进行的操作页面，既方便又能防止遗漏操作步骤。

FAT AP批量配置管理同样是通过向导方式呈现。在配置BSS接口、服务策略、Radio接口、端口安全、绑定Radio的时候，都可以进行批量操作，这样在部署和维护大规模的FAT AP组网环境时，非常方便和快捷。

另外，进入到设备的详细视图以后，还可以对AC、AP进行配置管理，对策略和MESH进行配置；在资源管理首页，可以看到多种无线资源，可以对各种无线资源进行管理，如图3–10所示，无线资源管理首页，通过链接进入相应的页面进行具体的无线资源配置管理和维护。

图 3–10 无线资源管理首页

绿色节能管理

WSM可以对全网无线设备制定绿色节能策略，支持对AP、Radio按计划启动和停止，支持对Radio的功率按计划动态调整，支持对Radio提供的无线接入服务按计划启动和停止；以达到节约能源，减少辐射，改善环境的目的。如图3–11所示，配置节能策略，策略类型包括AP启动停止、Radio启动停止、Radio功率调整、SSID启动停止，执行方式包括一次性和周期性，再设置不同执行周期的相应起止时间。绿色节能策略对加入AP列表中的AP生效。

图 3–11 节能策略管理

智能的主备AC管理

WSM可以提供强大的主备AC管理功能。在界面中，可以看到各个AP的主备连接状态，并且可以对相同序列号的AP进行合并，从而实现了全网级别的AP管理。同时，在处理报表等性能数据时，自动对主备下的性能数据进行整合，极大提高了性能数据的可用性、移动性、准确性。同时，通过主备AC分组的配置，用户可以方便的将配置同时下发到主备AC上，方便了用户的使用。 如图3–12所示，在配置AP模板时，同时选择主备AC分组、选择是否同步主备AC、设置主备AC优先级等。

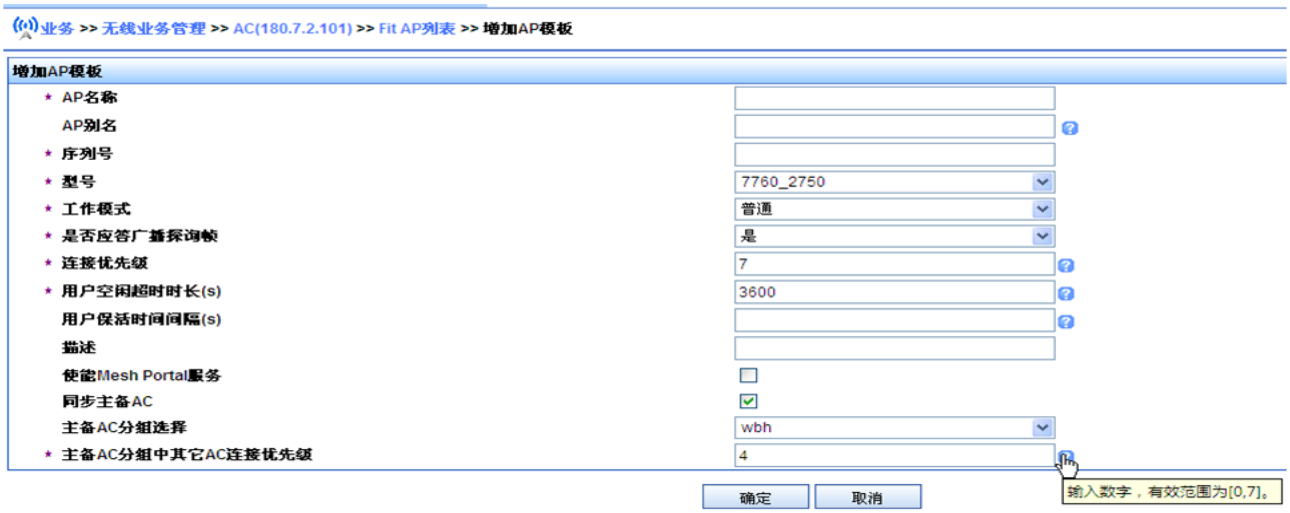


图 3–12 主备AC管理

无线入侵检测和防护

无线网络中时常有非法设备，对此，WSM提供了非法设备检测的功能，可对无线入侵的STA和AP进行检测，可明确显示非法接入设备，并对其进行信息查询、位置定位，可以将其加入攻击列表或准许列表，及对其采取反制措施。

智能化的无线网络质量评估

无线网络环境复杂，信号覆盖不可见，无线设备工作情况和用户体验数据难以直接收集，对此，WSM提供了智能化的无线网络评估功能。网络评估功能为用户提供了评估无线网络质量的途径，方便用户了解某区域内的AP工作情况及用户体验情况，根据评估结果及数据记录，用户可采取有效措施进行网络优化，改善网络质量。

网络评估功能是通过创建网络评估任务实现的，而网络评估任务是基于位置视图创建的。根据任务设定对采集到的数据进行汇总计算，并根据任务阈值设置的AP及用户的评价标准对AP及用户进行评价，完成评估后可查看网络评估报告，了解评估期间AP的工作情况及用户网络使用情况。评估报告中会显示各位置视图下AP设备的总评信息、评估期间AP及用户各项统计指标的历史及汇总记录、以及相应的评价结果，可通过总评信息了解某位置下AP的整体工作情况，通过各查询条件迅速找到关心的AP及用户。如图3-13所示，为一AP设备的网络评估结果。

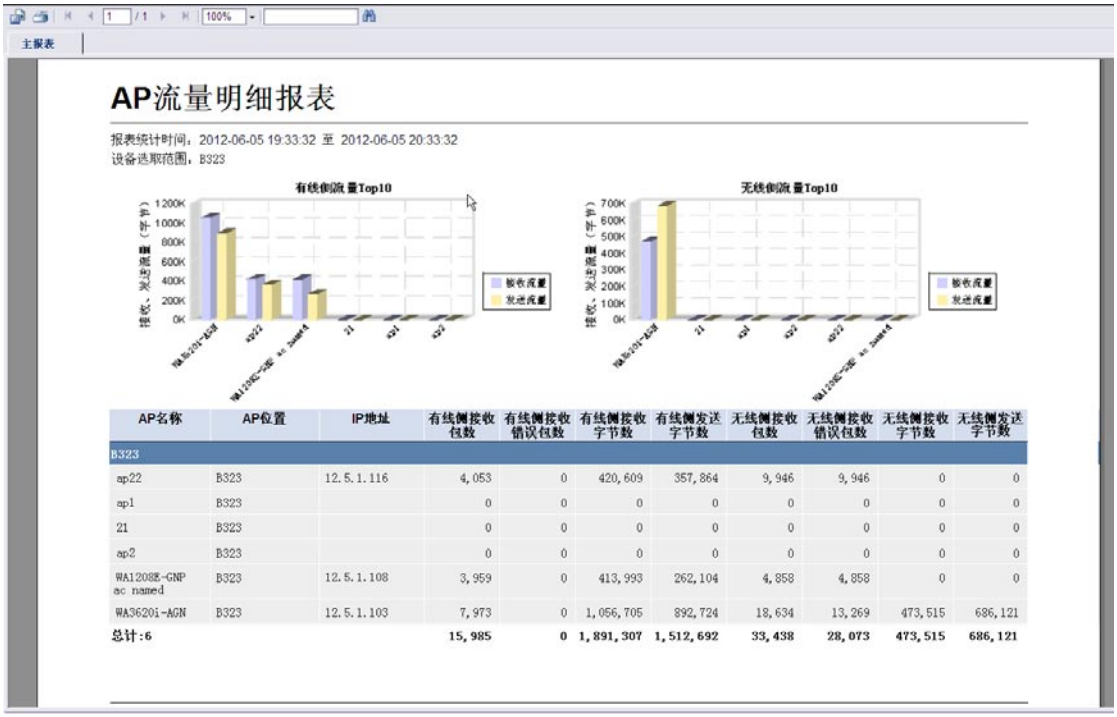
图 3-13 AP无线网络评估结果

丰富的无线统计报表

无线网络业务管理，需要对网络进行全方位的监控，从网络各种性能指标、告警指标中进行智能的统计和分析，才能有效的从整体对网络状况进行衡量。WSM提供了丰富的无线统计报表查询和定制功能，以帮助管理员对网络进行综合而全面的管理。通过配置分级报表，可以实现针对大规模无线网络的报表系统，从而可以满足运营商级别的报表统计需求。如图3-14所示，WSM预定义的30种无线业务报表，管理员还可以通过iMC报表设计器组件自定义自己的报表。如图3-15所示，为最近一小时的AP流量

明细表。B323位置中的AP没有承载大的流量，图3–15仅仅示意报表的呈现状态。

图 3–14 预定义的无线业务报表



AP名称	AP位置	IP地址	有线侧接收包数	有线侧接收错误包数	有线侧接收字节数	有线侧发送字节数	无线侧接收包数	无线侧接收错误包数	无线侧接收字节数	无线侧发送字节数
B323										
ap22	B323	12.5.1.116	4,053	0	420,609	357,864	9,946	9,946	0	0
ap1	B323		0	0	0	0	0	0	0	0
21	B323		0	0	0	0	0	0	0	0
ap2	B323		0	0	0	0	0	0	0	0
WA1208E-GNP ac named	B323	12.5.1.108	3,959	0	413,993	262,104	4,858	4,858	0	0
WA3620i-AGN	B323	12.5.1.103	7,973	0	1,056,705	892,724	18,634	13,269	473,515	686,121
总计:6			15,985	0	1,891,307	1,512,692	33,438	28,073	473,515	686,121

图 3–15 最近一小时AP流量明细表

多样化的业务开放

WSM整体实现继承iMC思想，采用主流SOA架构实现，从无线定位到广告推送再到数据开放，WSM不仅能和iMC家族中其他组件完美配合，并且将数据提供出来供第三方系统调用，符合运营商的管理模型和管理思路。SOA架构的开放性使得WSM方案可支持多样化的业务。

结束语

智能无线业务管理H3C iMC WSM迎接挑战，有效解决了WLAN管理所面临的主要问题。WSM的功能、特点和优势已经摆在面前，给无线业务管理带来了不仅仅是一场革命，也能给“智能”插上翅膀，让它在无线的天空中飞的更高更远！无线网络在飞速发展，iMC WSM智能无线业务管理也会永不止步！WSM拥有美好的今天，也必有美好的明天！

EPON和EoC的管理

文/史计达

EPON和EoC技术介绍

EPON技术介绍

EPON(以太无源光网络)是一种新型的光纤接入技术，它在物理层采用PON技术，在链路层使用以太网协议，利用PON的拓扑结构实现了以太网的接入。因此，它综合了PON技术和以太网的优点：低成本、高带宽、扩展性强、灵活快速的服务重组、与现有的以太网的兼容性、方便的管理等等。

EPON采用点到多点结构，无源光纤传输方式，在以太网上提供多种业务。目前，IP/Ethernet应用占到整个局域网通信的95%以上，EPON由于使用上述经济而高效的结构，从而成为连接接入网最终用户的一种最有效的通信方法。10Gbps以太主干和城域环的出现也将使EPON成为未来全光网中最佳的最后一公里的解决方案。

EoC技术介绍

对于广电而言，进行双向网改造产用传统的LAN入户方式而言，成本昂贵、工程浩大、还需要解决能否入户的问题；而广电网络中从小区光节点到用户端的同轴线资源是可以直接借用的，采用基于同轴线缆的入户方案是广电双向改造的较好选择，而EoC技术可以很好的保护原有的同轴接入网资源，有效的节省投资。

EoC是在同轴电缆上传输以太网数据的技术统称。根据早期区分习惯，EoC技术分为无源EoC和有源EoC。

无源EoC直接把以太网的基带信号通过无源器件耦合到同轴电缆中传输。该方案要求：局端数据信号必须到楼道，从楼道到用户端CABLE网络必须为星型，EoC经过的CABLE网络不能有分支分配器。

有源EoC技术，现在业界方案多种多样，规模、成熟度不一，大多是基于调制技术。比如有：Moca、HPNA、Homeplug1.0、WLAN降频等技术，均将数据信号调制到能在CATV同轴网传输的某一频段上，然后将CATV信号和调制后的数据信号混合传输，下行方向传输CATV和数据调制信号，上行方向传输数据调制信号，为双向数字电视平台提供回传通道。

如何管理EPON和EoC网络?

EPON和EoC网络管理的难点

作为接入网络，EPON ONU、EoC的头端/终端设备数量庞大，分布复杂，对网络的部署、监控、故障排查要求极高，如果像对待其它网络设备一样即对每个EPON和EoC设备单独进行管理，即浪费IP地址又对网络和网管服务器的性能造成压力，更多的是如此巨大的管理工作量的不可实施性。

解决思路

要想解决EPON和EoC中涉及的大量终端设备的管理问题，必须从其EPON和EoC本身具备的特性和原理出发，需要我们来分析一下EPON技术本身的特点（我司EoC采用和EPON类似的技术）。与其它PON技术一样，EPON技术采用点到多点的用户网络拓扑结构，利用光纤实现数据、语音和视频的全业务接入的目的。

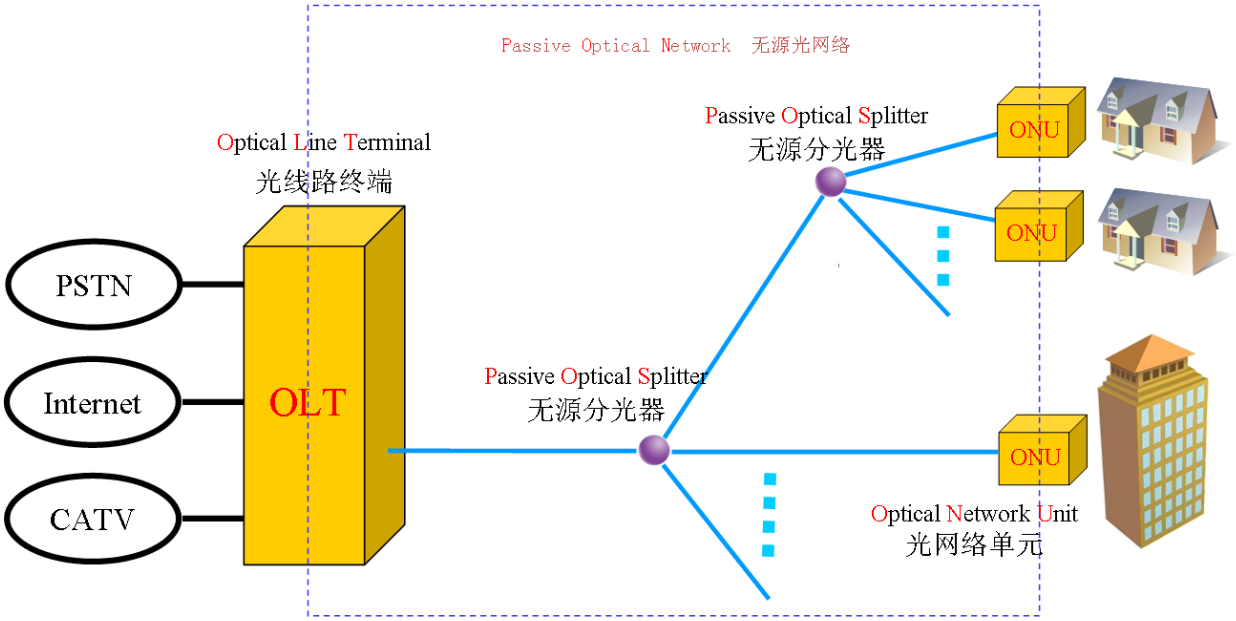


图1 EPON原理图

EPON的系统结构如图1所示。 一个典型的Ethernet over PON系统由OLT、ONU、POS组成。OLT（Optical Line Terminal）放在中心机房，ONU（Optical Network Unit）放在用户设备端附近或与其合为一体。POS（Passive Optical Splitter）是无源光纤分支器，是一个连接OLT和ONU的无源设备，它的功能是分发下行数据，并集中上行数据。

当OLT启动后，它会周期性的在本端口上广播允许接入的时隙等信息。ONU上电后，根据OLT广播的允许接入信息，主动发起注册请求，OLT通过对ONU的认证（本过程可选），允许ONU接入，并给请求注册的ONU分配一个本OLT端口唯一的一个逻辑链路标识（LLID），LLID的作用包括：

- 在ONU注册成动后分配一个唯一的LLID
- OLT接收数据时比较LLID注册列表
- ONU接收数据时，仅接收符合自己的LLID的或者广播包

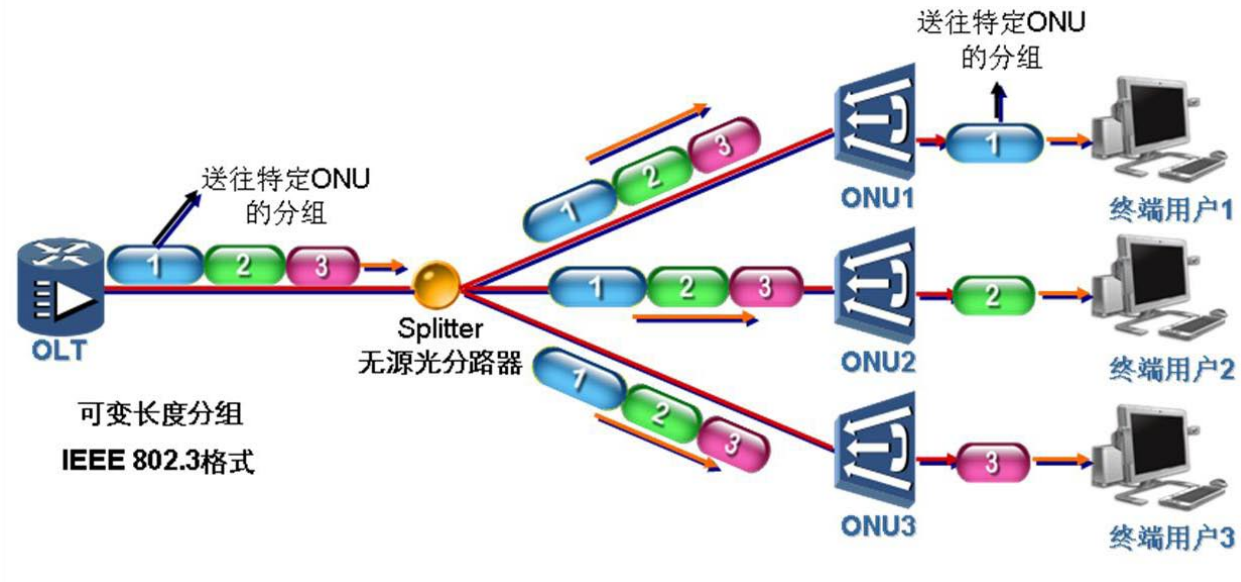


图2 EPON传输原理图

注册也就是OLT和ONU之间如何建立联系的一个过程，OLT控制ONU之前必须先找到ONU。所以

只要当ONU成功注册到OLT上，我们就可以通过OLT读取到该OLT节点下绑定的所有ONU信息（注册成功和不成功都可以），即通过OLT实现对ONU的管理，可以解决海量ONU终端的管理问题。

H3C智能管理中心EPON管理系统（EPM）和EoC管理系统（EoCM）基于iMC智能管理平台，既可以为用户提供专有业务的配置、监控等管理功能，也可以提供互连网络设备的网络管理和网元管理，同时还集成用户管理功能以及VLAN管理、ACL管理等相关业务功能，实现EPON和EoC网络的综合业务保障。

EPON业务管理系统（EPM）和EoC管理系统（EoCM）是iMC智能管理中心的业务组件之一。

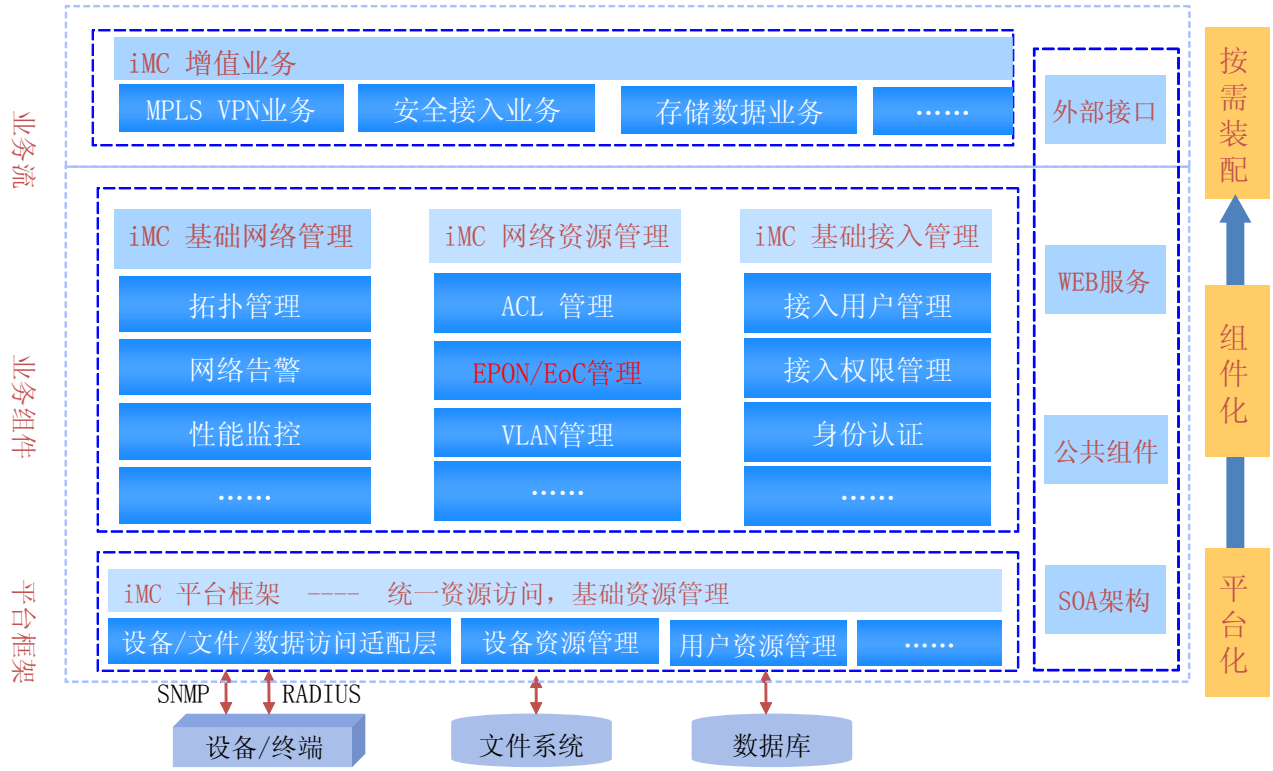


图3 EPON/EoC组件在iMC架构中的位置

iMC的EPON/EoC管理

EPON管理组件EPM

EPM解决方案的实现思路，是通过以组件化的方式提供EPON业务管理，通过多组件集成在管理平台上，提供用户所需要的功能。在网管系统中，应该包括如下基本功能：

- 故障管理（FAILURES）－－检测、隔离、更正网络问题并从这些问题中恢复。
- 性能管理（PERFORMANCE）－－分析和控制整个网络的数据吞吐，为终端用户提供连续的可靠的服务。
- 配置管理（CONFIGURATION）－－从网络中获取信息并根据这些信息对设备进行配置，通过它，可以实现对网络设备的配置的集中管理。。
- 安全管理（SECURITY）－－控制对网络资源和敏感信息的访问。这种控制包括对网络设备的访问限制，对给定设备上某种应用的访问控制以及对网络协议的访问控制。

EPM网管主要包括EPON设备管理，拓扑管理，ONU设备管理，分光器管理，升级管理，业务部署管理，静默ONU管理，可控组播管理等几个部分。

EPM管理组件作为iMC智能管理中心的EPON业务管理核心，对于网络中的OLT，ONU设备提供一个集中管理的平台，提供直观的EPON资源管理功能，可以对OLT设备信息、OLT设备单板信息、ONU设备信息、UNI信息进行集中展示，并直观展示运行状态。通过Web页面的超级链接，用户可以方便的进行关联信息查询，方便了解EPON网络运行的各种状况。与iMC智能管理平台及其它组件配合，系统还能提供ONU设备的故障、性能监控等基本管理功能和其它业务，实现无缝融合管理。

基于iMC，通过选择安装EPON业务组件EPM，用户可以获得EPON接入网全面的业务管理功能，实现EPON的设备管理、通用配置管理、EPON设备软件升级、EPON拓扑管理、EPON网络性能和故障管理等功能。通过iMC开放的体系框架，EPM可以与iMC其他业务组件无缝集成，如用户管理组件、VLAN管理组件、ACL管理组件等；也可以通过开发的接口与第三方业务管理系统进行对接，实现综合业务支撑。满足基于EPON技术的各类光接入方案的管理要求，保证对数据、IPTV、VoIP等多业务的支撑。

EoC管理组件EoCM

EoCM解决方案的实现思路，是通过以组件化的方式提供EPCN业务管理，通过多组件集成在管理平台上，提供用户所需要的功能。

EoC管理组件主要包括EoC设备管理、CNU设备管理、EoC用户管理、EoC套餐管理、CNU配置任务管理、EoC拓扑管理、EoC性能监控与告警管理等几个部分。

EoC解决方案中的头端设备CLT是针对于楼宇间的交换机，因此在小区中数量会比较多，CNU设备是需要进入最终进户家中的设备，数量更为巨大，因此EoCM提供了EoC设备管理与CNU设备管理功能，管理员可以以列表的形式对CLT设备与CNU设备进行浏览与管理，同时还提供了多种条件组合的查询功能，可以方便快速定位设备。

鉴于一般运营商不会提供完全由用户自己定制的业务套餐，只是会定制若干套餐由用户选择，EoCM提供了EoC套餐管理功能，管理员可以事先规划好可以提供的业务参数并通过EoC网管定制套餐，当用户开户时选择了某一套餐时，直接选择预先定义好的套餐即可，而不必再记忆与输入复杂的参数了。

EoC解决方案是利用同轴电缆来做传输介质，因此也带来了一个问题就是当CLT设备与用户家中的CNU设备距离过远时传输的信号会发生衰减，当衰减达到一定程度后将导致信号无法正确传输进而用户无法正常使用的严重后果，因此对于用户CNU设备线路的衰减情况的监控是极为重要的，EoC网管在EoC拓扑管理中提供了直观的观察手段：在拓扑图中CNU与上级设备的链路以颜色来表示其线路的衰减状态；另外设备上可以设置两档衰减阈值，当线路衰减变化跨越阈值时，设备会主动上报告警报文通知网管；管理员可以通过查看EoC拓扑图或查看告警信息，快速定位线路衰减严重的线路。

CNU设备是需要进入用户家中的，因此对于CNU设备的管理必然需要关联到用户，因此EoC网管引入了EoC用户的概念，用来做CNU设备与用户关联的中介，用户的配置参数是与EoC用户相绑定的，当用户更换了CNU设备后，可以保证用户的配置不会更改，只需要重新下发用户的配置到新的CNU设备即可，同时EoC网管还提供了EoC用户与CNU设备配置比较的功能，使得EoC用户与CNU设备配置不一致的EoC用户与CNU设备一目了然，便于管理员的日常维护。

终端用户数量巨大，如果采用单独设备配置的方式来操作工作量会非常大，EoC网管针对此问题提供了CNU配置任务管理功能，管理员只需要通过配置任务向导简单地进行任务参数配置，就可以一次性对大量的用户CNU设备进行配置下发操作，由于采用了任务的方式，还可以定时执行一些操作，例如在

统一在月末的凌晨为用户批量升级带宽等操作。

在实际运营环境中，某些中小运营商的规模比较小，对于用户的管理也不是很严格，并且没有多种资费标准，则可以采用匿名设备接入的方式，即运营商制只负责用户终端的发放，用户拿到家中接入EPCN网络即可使用，不需要在运营处进行开户、套餐选择等操作，可以最大程度地节约运营商的管理成本。对于匿名设备接入方式，EoC网管提供了信息查询等常用功能，但由于用户是匿名接入的，无法提供配置功能。

总结

通过iMC的EPM和EoCM组件，可以方便的实现对海量ONU、EoC头端和终端进行设备管理、配置、监控；其提供的批量操作大大简化了繁琐的重复性工作，节省时间和劳动力；简介明了、可伸缩的拓扑管理以及和告警信息的关联让管理员对于网络和设备的故障一目了然，快速定位；iMC的开放性架构让EPM和EoCM组件和iMC的其它组件无缝连接（通过开发接口，也可以实现和第三方软件的对接），为网络管理员提供了更全面的管理手段。

分支网点的管理

文/袁 江

在这个信息爆炸的时代，互联网无论是规模还是应用，都在急剧的增长着。大量的多业务路由器、网关、WLAN设备等接入设备被广泛的应用于工业园区、企业内部、运营商边缘、家庭等分散的广域网络中，需要对这些用户侧设备（CPE：customer premises equipment）进行有效的远程集中管理。然而，传统的远程管理方式（如Telnet、SSH、SNMP、Web管理等）具有很多的局限性，如：设备命令行、SNMP实现因厂商不同而不一致，设备的IP地址因使用场景而需要经常变化，Web管理的界面及配置方式各异等，无法高效的对大量CPE进行批量、自动化的管理。企业迫切的需要一种新的网络管理系统，满足对广域网中的大量CPE进行远程管理的需求。为此，数字用户线(DSL：digital subscriber line)论坛专门制订了用于终端的网管协议--TR069。

TR069

TR069（TECHNICAL REPORT 069）即CPE WAN Management Protocol，是由DSL论坛（www.dslforum.org）所开发的技术规范之一，DSL论坛的文档编号为TR069，其全称为“CPE广域网管理协议”。它提供了对下一代网络中用户侧网络设备进行管理配置的通用框架和协议，用于从网络侧对用户侧网络中的网关、路由器、机顶盒等设备进行远程集中管理。

TR069协议是一个位于IP之上的应用层协议，这使得该协议的适用性很广，对接入方式没有限制。基于不对称数字用户线(ADSL)、以太网、无源光网络(PON)等接入方式的CPE均可以使用此协议。在TR069定义的网管模型中管理服务器称为自动配置服务器(ACS)，负责完成对用户终端设备(CPE)的管理。基于TR069的网管架构如图1所示。

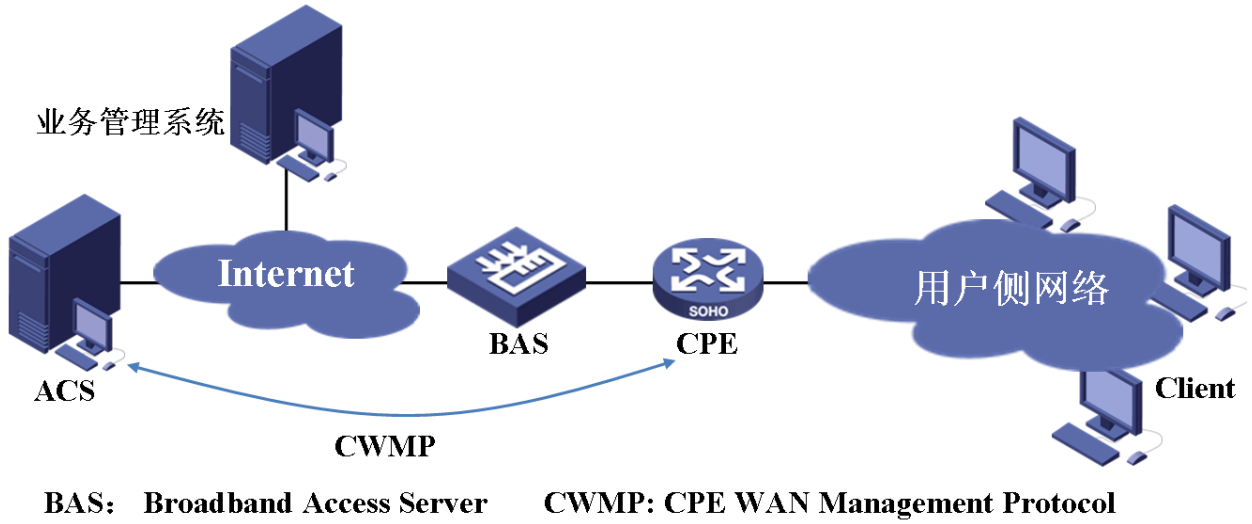


图1 基于TR069的网管架构

TR069协议在架构设计上使用超文本传输协议(HTTP)的客户机/服务器(C/S)模型，并充分借鉴了很多Web的成熟技术，使得协议的实现相对简单，并且具有很好的扩展性。其中ACS作为HTTP服务器，CPE作为客户机，对于终端产品来说，降低了开发、实现的难度。

iMC BIMS

基于TR069，H3C针对企业网和运营商等多种网络运营环境开发出分支网点智能管理系统iMC BIMS（Branch Intelligent Management System），可以对CPE设备进行远程集中管理，能够解决

CPE设备数量大、动态IP等管理困难，节约维护成本，提高问题解决效率。

iMC BIMS基于iMC架构开发，在涵盖TR069协议的资源管理、业务管理、配置管理、告警管理和系统管理等ACS功能的基础上，提供了权限控制平台，具有简单易用、高性能、可扩展的特点，可以帮助网络管理员轻松完成网络的资源、业务和配置等管理任务，极大提高网络的安全性、可管理性和可维护性，能够满足企业、园区和运营商等多种网络解决方案中的TR069管理需求。

BIMS应用场景

企业网

分支机构的网络通过广域网接入总部网络，各分支设备支持TR069协议，设备的IP可以固定，也可以是动态IP；总部通过iMC BIMS可以对各分支设备进行统一管理。

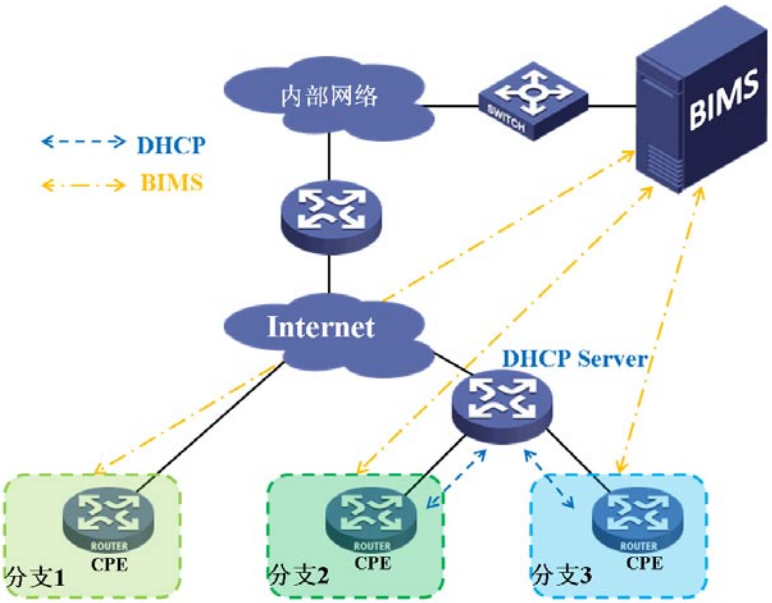


图2 企业网应用场景

BIMS提供了查看和查询系统中的设备，支持认证、增加、删除、同步和刷新设备等功能，可以查看、修改设备的参数和配置信息，支持设备导入导出，能够对设备进行远程重启和恢复出厂设置等操作。

图3 BIMS资源

BIMS提供丰富的配置管理功能，包括配置文件库管理、设备软件管理、统一的部署向导、部署任务管理、设备配置一览表、备份设备配置和备份历史记录管理等功能。

图4 BIMS配置管理

设备软件库管理：对系统中的设备软件进行统一有效地管理，支持导入、导出、修改和删除设备软件。

图5 BIMS软件库管理

设备配置备份管理：支持增加、删除、修改设备配置文件备份任务，可以定制备份任务的执行方式和执行时间。

图6 BIMS配置备份

运营商

运营商通过广域网为企业、家庭等接入点提供宽带服务，各企业、家庭使用支持TR069协议的终端设备（CPE）作为网络接入点，各CPE的IP可以是固定IP，也可以是动态IP，这种网络具有物理位置分散、设备数量大、动态IP等特点；在管理中心，通过iMC BIMS可以对广域网中的大量CPE进行远程集中管理。

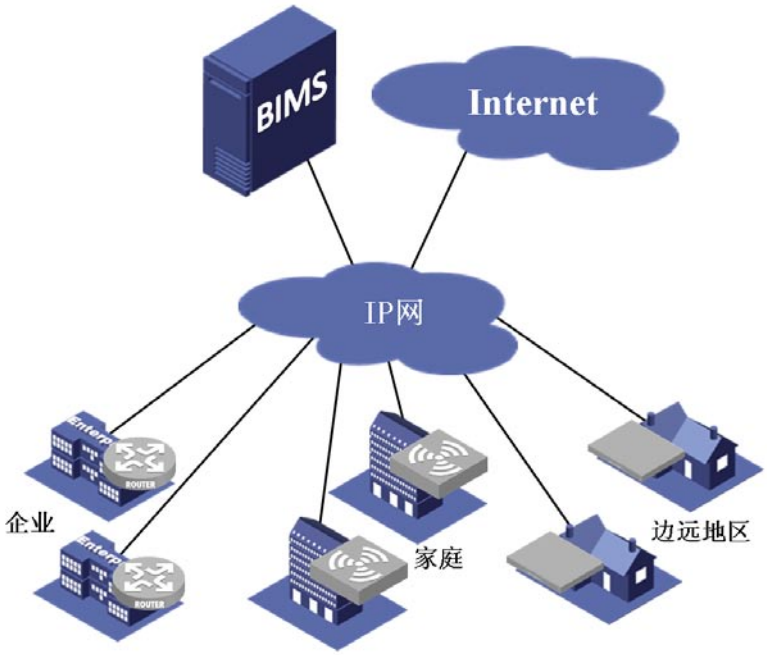


图7 运营商网场景

BIMS提供对单个设备或者同时对多个设备批量执行IP Ping测试的功能，可以对所选设备的相关业务情况进行诊断；可以对WAN DSL链路、WAN IP连接、WAN PPP连接进行管理，使管理员能够清晰的了解广域网的链路及连接状况。

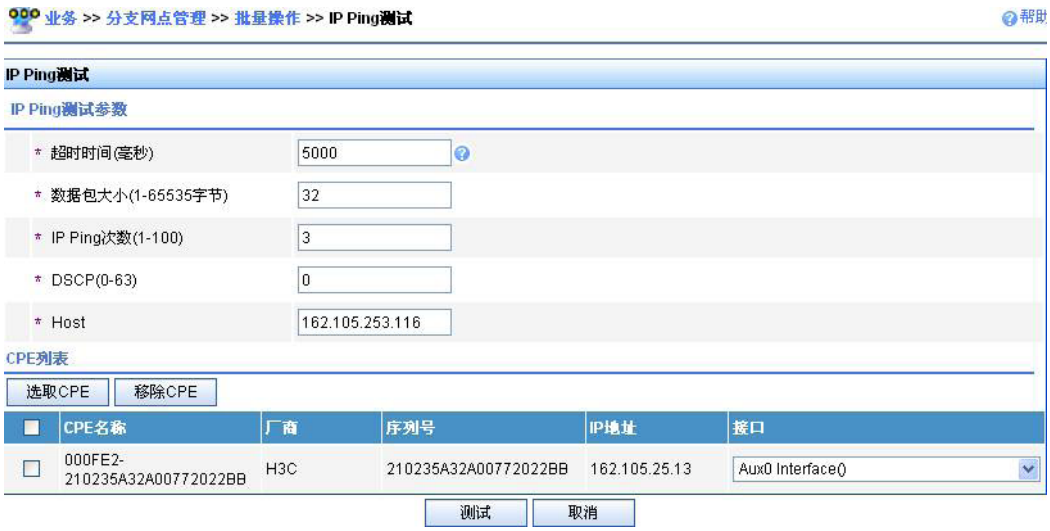


图8 IP Ping测试功能

BIMS支持增加、删除和修改、CPE认证用户，用于认证CPE设备，实现网管的防攻击保护。

图9 CPE认证用户功能

小结

TR069采用了成熟的通信协议、开放的面向对象的管理信息架构，具有强大的灵活性和可扩充能力，可以满足各类远端用户的设备管理和配置需求。

H3C iMC BIMS基于TR069，实现了对用户侧设备的远程管理，使管理员可轻松对设备进行批量升级，全面监控边缘设备，快速定位故障和恢复，简单易用，是一种完全满足市场需求的端到端的解决方案。

针对特定类型设备的专用管理软件

文/袁亚屏

当前，通用网络管理软件大行其道，在大多数场合能够很好的满足用户的需求。但是在管理一些特殊的设备或网络的时候，还是需要为其量身定做一套专用的管理软件才行。

通用网管软件面临的难题

通用网络管理软件的好处显而易见，成本低、上手容易、管理方便等等都是其优点。但是在遇到一些比较特殊的设备或者组网的时候，还是暴露了一些缺点。

1. 强调适用性，个性不足

通用网管软件为了强调自己的适用性，一般会采用主流的管理接口，对于一些使用比较特殊的设备往往不能支持。比如一个通用网管软件可能支持比较流行的SNMP等接口，但如果想实现类似HTTP等接口就相对比较困难。主要原因是HTTP接口并没有统一的标准，不具有普遍适用性，在通用网管软件上实现起来不划算。

2. 灵活性不足

网络设备千差万别，有些设备的管理接口变动比较频繁，需要管理软件能够有相适应的灵活性，这是通用网管软件难以做到的。

3. 组件化不是解决所有问题的方法

以H3C iMC为代表的网管软件使用组件化的方式进行开发，一定程度上解决了通用网管软件灵活性不足的缺点，但是对于一些比较少见的设备和网络，还是存在开发成本过高，不够灵活等问题。

同时，组件化的网管软件体系中，任何组件都不能摆脱对平台的依赖，即使用户基本上并不使用平台的功能，也要为这个没有用处的平台付出额外的服务器硬件资源。

以H3C的防火墙和IPS产品为例，这些产品的核心功能目前主要通过WEB配置，管理接口自然是HTTP。同时这些设备有很多其它网络设备所没有的功能，产品的功能变化也比较频繁。对于这类产品，专用的管理软件更为适合。

专用网管软件的特点

一般来说，和通用网管软件相比，专用网管软件有如下几个特点：

1、轻量化。专用网管软件一般都是为了实现一些特定的功能，无论是软件的体积和对硬件资源的消耗都比通用网管软件小很多。

2、功能精细化。由于专用网管软件的开发目标比较明确，很多功能都会做的比较细致，和被管理设备贴合的更好。

3、响应快速化。一般来说专用网管软件的开发团队和被管理产品的开发团队结合比较紧密。双方的需求，对方都能比较迅速的加以响应。

为安全产品量身定制的SecCenter

SecCenter（安全管理中心）是H3C为旗下的安全产品（防火墙、入侵防御系统、应用控制网关、统一威胁管理系统）量身定制的专用网管软件。在常见的网络基础设施管理功能之外，针对安全产品的特点和需求开发了很多特色功能。

1、日志的收集和管理

SecCenter集成日志采集器、数据库、大容量存储、日志分析、审计、报表等功能部件，可对H3C Firewall、IPS、UTM、ACG、AFC等安全设备进行集中管理，利于网络的快速部署、全面了解设备的运维信息，能够同时支持NetStream、NetFlow、cFlow、Syslog、Windows WMI、ODBC等国内外主流日志采集方式，并对H3C网络、安全产品进行统一安全信息与事件管理，能实时、全面地了解全网安全状况。

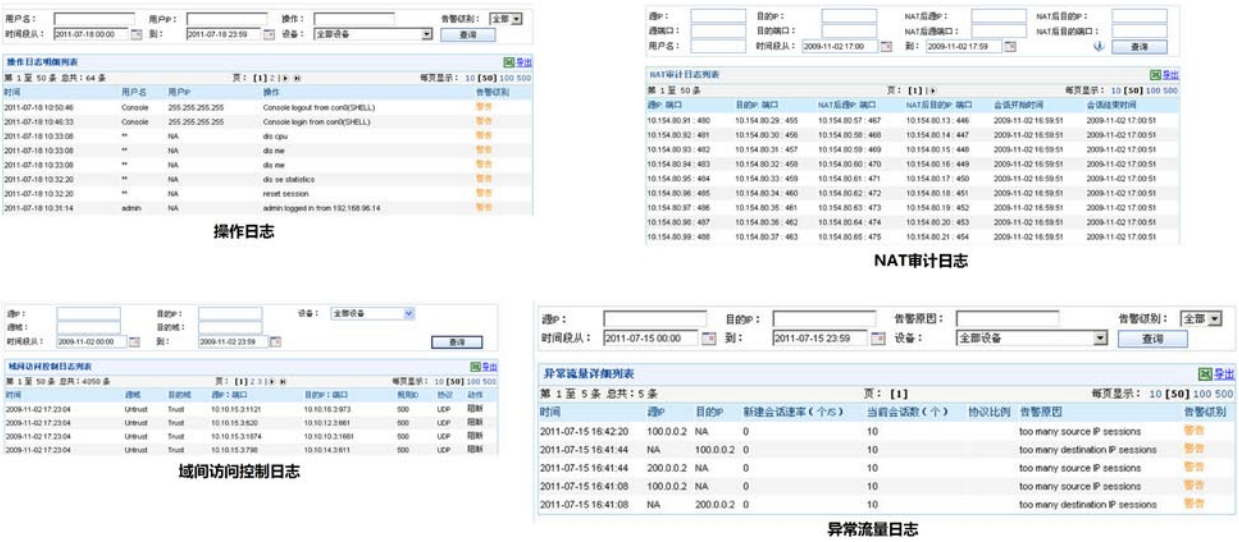


图1 SecCenter可以收集从不同渠道上送的日志信息

通用网管软件提供通用的日志报表功能，由于框架限制很难提供个性化的信息。但是对于安全产品来说，日志的收集管理审计是很重要的功能，因此SecCenter在这方面有所增强，提供丰富的功能。

2、安全事件智能分析

SecCenter能够对来自于网络、安全等设施的安全信息与事件进行分析，关联和聚类常见的安全问题，过滤重复信息，发现隐藏的安全问题。事件智能分析使管理员能够轻松了解突发事件的起因、发生位置、被攻击设备和端口，并能根据预先制定的策略做出快速的响应，保障网络安全。

安全产品的日志信息非常丰富，其中包含的信息很多，在海量的日志中迅速的发现用户所关心的内容并呈现出来，是对SecCenter的基本功能要求之一。SecCenter在这方面又体现出了专用网管软件精专的一面，将日志分析和网络基础设施管理紧密的联系起来。

图2 事件快照功能，对日志信息进行分析归纳的结果

3、完善的配置管理功能

H3C安全产品的配置方式以WEB为主，配置接口为私有，且变化相对比较频繁，通用网管软件难以很好的进行适配，专用网管软件就可以为其量身定制。SecCenter完整的实现了配置文件管理和特色配置的下发（资源、域间策略等等）。

图3 域间规则的管理

4、特征库的统一管理

特征库对于IPS、ACG和UTM产品非常重要，SecCenter能够自动检测网络中上述类型的设备的特征库版本和当前应用状态，可对整网的设备实施统一的特征库升级管理。只有安全产品对此功能有需求，使用专用网管软件来实现是再合适不过了。

图4 特征库管理

此外，SecCenter和iMC相比有着软件体积小，对服务器性能要求低等特点，安装使用也更为容易。

总结

以SecCenter为实例，我们可以归纳专用网络管理软件的几个特点：

1、软件体积小，安装方便，对硬件性能要求相对较低；

2、针对被管理设备的功能和需求进行适应性的功能开发；

3、快速响应产品需求。

文/徐泽新

用户身份识别和访问控制

前言

业界传统的网络管理、用户管理软件各自发展已经较为完善，然而网络管理系统关注于网络基础资源的管理，包括路由器、交换机、服务器等；而用户管理则关注于对当前正在使用网络基础资源的用户的管理，包括对用户身份的认证、授权、用户信息的组织管理等，但实际上网络设备和用户是有机融合的整体，最好是能够进行统一规划管理。

同时网络管理中的另一大问题是安全问题。随着网络技术的应用与发展，人们对信息网络的应用需求不断提升，对网络的依赖性也越强，伴随而来的信息安全威胁也在不断增加。而传统的网络防御系统往往是一种单点的被动防御的系统，在企业网络中任何一台受病毒感染或者易感染的终端接入网络都可能将威胁扩展到整个企业网。那么如何能够从源头上控制威胁的引入以及即时升级整个网络的防御能力就尤为重要。

EAD整体方案介绍

为了解决现有的网络管理中存在的不足，我司推出了端点准入防御（EAD，Endpoint Admission Defense）解决方案，旨在整合孤立的单点防御系统，加强对用户的集中管理，统一实施企业安全策略，提高网络终端的主动抵抗能力。EAD方案通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，对网络设备及接入用户进行统一管理，可以将不符合安全要求的终端限制在“隔离区”内，防止“危险”终端对网络安全的损害，避免“易感”终端受病毒的攻击。

其中EAD解决方案的核心安全策略服务器由我司的iMC服务器来提供，其主要功能由以下三个方面功能的联动来实现：

接入用户管理及准入控制：由iMC中UAM组件来实现。iMC所提供的接入用户管理功能具有接入用户信息集中管理、与网络设备管理及拓扑管理相融合等特点，在简化接入用户管理复杂度的基础上，又强化了管理效果。接入与准入控制功能是为用户对接入业务的使用进行认证、授权控制。可以针对不同的用户群提供不同的服务、授予不同的权限。它通过与用户管理功能以及网络资源管理、接入服务管理的协同，使的接入业务管理的方便性得到提升、管理效果得到增强。

端点准入防御：由iMC中EAD组件来实现。EAD安全管理组件是终端准入控制解决方案（EAD）的核心，在对接入用户进行身份认证的基础上要求接入用户进行安全认证，实现对其安全状态的准入控制。 智能管理中心支持针对不同检查项的检查结果的下线、隔离、提醒、监控等多种控制方式；支持安全状态评估、网络中安全威胁定位、安全事件感知及保护措施执行等；预防操作系统补丁、病毒、间谍软件、网络攻击、钓鱼网站、硬盘数据攻击、ARP攻击、异常流量、敏感软件安装/运行、系统服务的启动状态、注册表、共享目录、资产未注册、操作系统密码等因素可能带来的安全威胁。这些功能从端点接入上保证每一个接入网络的终端的安全，从而保证整个网络安全。它提供完备的安全状态评估和实时的“危险”用户隔离。

桌面资产管理：由iMC中DAM组件来实现。在客户端中加载DAM组件即桌面资产管理组件后可，用户通过iNode认证上线时主动注册资产，在iMC中可以监控以上线的资产，包括资产的硬件信息、软件信息、开启的服务、进程、监控的端口、注册表、补丁信息。并可监控终端外设使用情况、进行绿色节能处理定时关机、对资产变更提供监控告警。同时可以对桌面资产进行审计，包括USB监控记录、打印机监控、外围违规查询、终端文件审计。批量进行软件分发，大大的减少了管理员的工作量。

EAD工作原理

组成结构

EAD端点准入防御方案是一个整合方案，其基本部件包括安全客户端、安全联动设备、安全策略服务器以及防病毒服务器、补丁服务器等第三方服务器。EAD方案中的各部件各司其职，由安全策略中心协调与整合各功能部件，共同完成对网络接入终端的安全状态评估、隔离与修复，提升网络的整体防御能力。

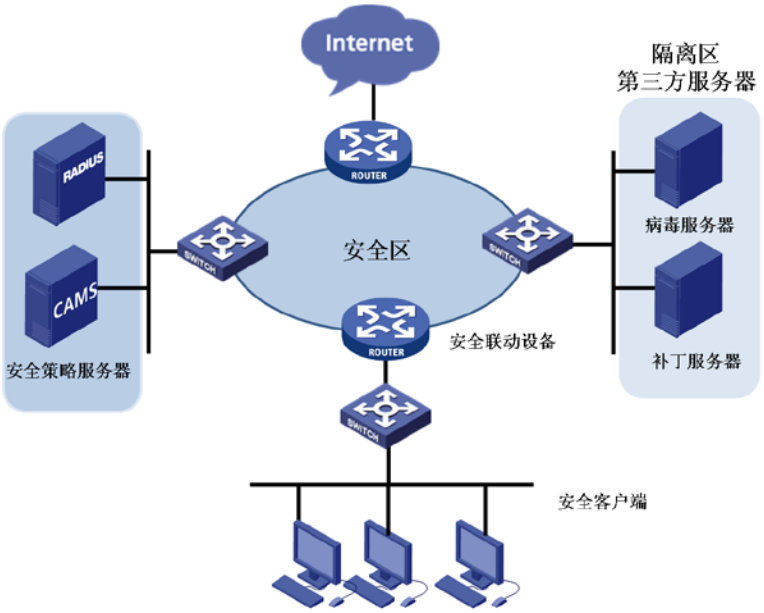


图1 EAD解决方案基本组网图

安全客户端

安全客户端是安装在用户终端系统上的软件，是对用户终端进行身份认证、安全状态评估以及安全策略实施的主体，其主要功能包括：

支持802.1x、Portal、VPN等多种认证方式，可以与我司的交换机、路由器、VPN网关等配合实现接入层、汇聚层以及VPN的端点准入控制。

◆ 检查用户终端的安全状态，包括操作系统版本、系统补丁等信息；同时提供与防病毒客户端联动的接口，实现与第三方防病毒客户端的联动，检查用户终端的防病毒软件版本、病毒库版本、以及病毒查杀信息。这些信息将被传递到安全策略服务器，执行端点准入的判断与控制。

◆ 安全策略实施，接收安全策略服务器下发的安全策略并强制用户终端执行，包括设置安全策略（是否监控邮件、注册表）、系统修复通知与实施（自动或手工升级补丁和病毒库）等功能。不按要求实施安全策略的用户终端将被限制在隔离区。

◆ 实时监控系统安全状态，包括是否更改安全设置、是否发现新病毒等，并将安全事件定时上报到安全策略服务器，用于事后进行安全审计。

安全联动设备

安全联动设备是企业网络中安全策略的实施点，起到强制用户准入认证、隔离不合格终端、为合法用户提供网络服务的作用。根据应用场合的不同，安全联动设备可以是我司的交换机、路由器、VPN网关、无线接入设备等，分别实现不同认证方式（如802.1x、VPN和Portal等）的端点准入控制。不论是哪种接入设备或采用哪种认证方式，安全联动设备均具有以下功能：

◆ 强制网络接入终端进行身份认证和安全状态评估。

◆ 隔离不符合安全策略的用户终端。联动设备接收到安全策略服务器下发的隔离指令后，可以通过VLAN或ACL方式限制用户的访问权限；同样，收到解除用户隔离的指令后也可以在线解除对用户终端的隔离。

◆ 提供基于身份的网络服务。安全联动设备可以根据安全策略服务器下发的策略，为用户提供个性化的网络服务，如提供不同的QoS、ACL、VLAN等。

安全策略服务器

EAD方案的核心是整合与联动，其中的安全策略服务器是EAD方案中的管理与控制中心，它作为一个软件的集合可运行在Windows、Linux平台下，兼具用户管理、安全策略管理、安全状态评估、安全联动控制以及安全事件审计等功能。

◆ 安全策略管理。安全策略服务器定义了对用户终端进行准入控制的一系列措施，包括用户终端安全状态评估配置、补丁检查项配置、安全策略配置、终端修复配置以及对终端用户的隔离方式配置等。

◆ 用户管理。企业网中，不同的用户、不同类型的接入终端可能要求不同级别的安全检查和控制。安全策略服务器可以为不同用户提供基于身份的个性化安全配置和网络服务等级，方便管理员对网络用户制定差异化的安全策略。

◆ 安全联动控制。安全策略服务器负责评估安全客户端上报的安全状态，控制安全联动设备对用户的隔离与开放，下发用户终端的安全策略。通过安全策略服务器的控制，安全客户端、安全联动设备与防病毒服务器才可以协同工作，配合完成端到端的安全准入控制。

◆ 日志审计。安全策略服务器收集由安全客户端上报的安全事件，并形成安全日志，可以为管理员追踪和监控网络的整个网络的安全状态提供依据。

第三方服务器

在EAD方案中，第三方服务器是指处于隔离区中，用于终端进行自我修复的防病毒服务器或补丁服务器。网络版的防病毒服务器提供病毒库升级服务，允许防病毒客户端进行在线升级；补丁服务器则提

供系统补丁升级服务，当用户终端的系统补丁不能满足安全要求时，可以通过补丁服务器进行补丁下载和升级。

EAD解决方案工作原理

EAD解决方案的核心部件为安全策略服务器。安全策略服务器的角色由iMC服务器来承担，其中涉及到用户接入管理、EAD安全管理、桌面资产管理三个部分。通过这三个组件间的配合使用来实现客户端的安全接入。

用户接入管理

用户接入管理由iMC的用户接入管理组件UAM来实现，它提供对接入网络的终端用户进行认证和授权的功能。UAM支持LAN、WLAN、VPN认证接入、实现对接入用户的统一集中管理。

UAM组件可以支持的主要业务特性如下：

◆ 支持多种接入认证方式：包括802.1x认证、Portal认证、移动用户VPN接入认证，并支持多种验证方式（PAP、CHAP、EAP-MD5、EAP-TLS、PEAP、WAPI证书）等。

◆ 支持多种用户身份认证方式：包括快速认证、用户名密码认证、证书认证、LDAP用户统一认证，IP、MAC、接入设备、物理端口、VLAN等多因素绑定认证。

◆ 支持对基于用户的上网权限控制：接入时段、区域控制，用户黑名单，下发访问控制列表（ACL）、VLAN、QOS、限制用户使用代理、修改MAC地址、IP地址设置方式。

◆ 采用用户-服务-策略模式，并实现用户分组管理，方便管理员针对不同类型的用户采取不同的认证和授权方式。

◆ 提供用户附加信息的定制功能，管理员可根据自身网络的特点定制接入用户的属性信息，如：所在部门、职称、岗位等。

◆ 用户管理与设备管理相融合，突破了传统的网络管理理念，可直接对接入设备进行查看信息、配置命令、部署ACL等操作。

◆ 用户管理与拓扑管理的融合，实现接入业务的终端用户拓扑，可通过网络拓扑对接入设备和接入用户进行操作、监控用户的在线状态。

用户认证接入基本流程如下图所示：

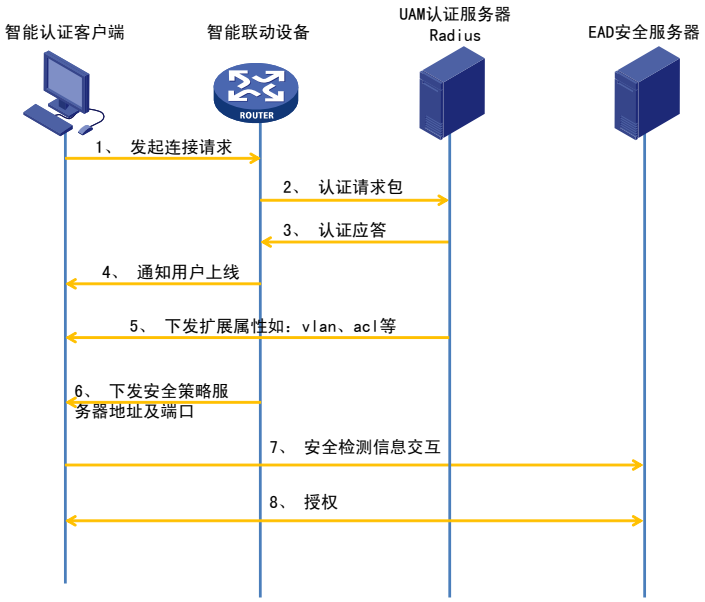


图2 用户接入认证基本流程图

EAD安全管理

EAD安全策略组件为EAD解决方案提供接入用户安全策略管理平台，设置各种影响终端和网络安全的检查项及针对不合格检查项的处理措施，包括终端安全软件管理、可控软件组管理、软件补丁管理、终端异常流量监控策略管理、注册表监控策略管理、目录共享策略管理、资产注册状态监控、操作系统密码监控、用户网关信息设置、安全策略和安全级别管理等。

EAD组件可以支持的主要业务特性如下：

◆ 终端安全软件管理：终端安全软件包括防病毒软件、防间谍软件、防火墙软件、防钓鱼软件和硬盘加密软件。设置接入用户需要安装和运行的终端安全软件的种类，以确保终端用户接入网络后最大限度的免受攻击和侵害。

◆ 可控软件组管理：设置接入用户必须或禁止安装的软件、必须或禁止运行的进程、必须或禁止启动的服务、存在或不存在文件，以确保接入网络的终端用户安装的软件、运行的进程、启动的服务和存在的文件符合操作员制定的安全标准，避免不安全终端接入网络。

◆ 补丁管理：针对Windows各类操作系统发布的修复安全漏洞的补丁，可以根据安全漏洞的危害程度，将其修复补丁分级，按照级别可以设置缺省的处理策略，以确 保接入网络的终端用户不存在影响网络安全的漏洞。针对Linux和Mac OS操作系统，采用两级管理的方式来确保用户的网络安全。即iMC EAD仅检查要求的补丁管理软件在操作系统中的安装和运行情况，而由补丁管理软件负责检查操作系统补丁是否合格。

◆ 流量监控策略管理：当接入网络的终端用户的流量发生异常变化时，智能管理中心可以及时感知并做出相应的处理。流量监控策略可以设置终端用户IP流量异常阈值/严重异常阈值、广播报文异常阈值/严重异常阈值。

◆ 注册表监控策略管理：设置接入用户需要的注册表监控策略，以确保接入网络的终端用户的注册表符合操作员制定的安全标准，避免不安全终端接入网络。注册表监控策略可以设置注册表监控项是否必须存在、注册表监控项键值是否必须符合操作员定义的值等。

◆ 目录共享策略管理：监控用户终端的共享目录是否符合操作员制定的安全标准，如果iMC EAD系统认为共享目录不安全，可以对接入用户进行提醒、隔离、下线等处理。

◆ 资产注册状态监控：iMC EAD系统可以在用户上线时检测用户使用的资产是否已注册。如果资产未注册，可以对接入用户进行提醒、隔离、下线等处理。该功能需要与iMC DAM联动。

◆ 操作系统密码监控：iMC EAD系统可以判断登录操作系统的密码的安全性，如果iMC EAD系统认为密码不安全，可以对接入用户进行提醒、隔离、下线等处理。

◆ 用户网关信息设置（UAM组件特性）：网络中常见的ARP攻击是攻击者仿冒网关的IP地址，在局域网内广播ARP报文，告知其他终端网关的MAC为攻击者自身或其他的MAC，导致其他终端无法正常访问网络或者网络流量被重定向造成安全隐患。智能管理中心可以通过设置用户网关的IP/MAC对应信息并下发给接入用户，与iNode认证客户 端配合保证接入用户ARP表中的网关MAC地址不会被恶意修改，使接入用户免受ARP攻击的影响。

◆ 安全策略和安全级别管理：安全策略和安全级别是EAD安全管理组件的功能核心，用户申请的接入服务中必须应用了安全策略后才能使用该业务，用户安全认证时的各检查项、检查方式、修复策略，用户在线时实时监控的项和处理策略都在安全策略中设置。而安全级别应用于安全策略，用来设置每个检查项如果不合格时要采取的安全措施（下线、隔离、提醒、监控），当一次安全认证有多个检查项不合格时，按最严格的安全措施处理。

EAD安全接入认证基本流程如下图所示：

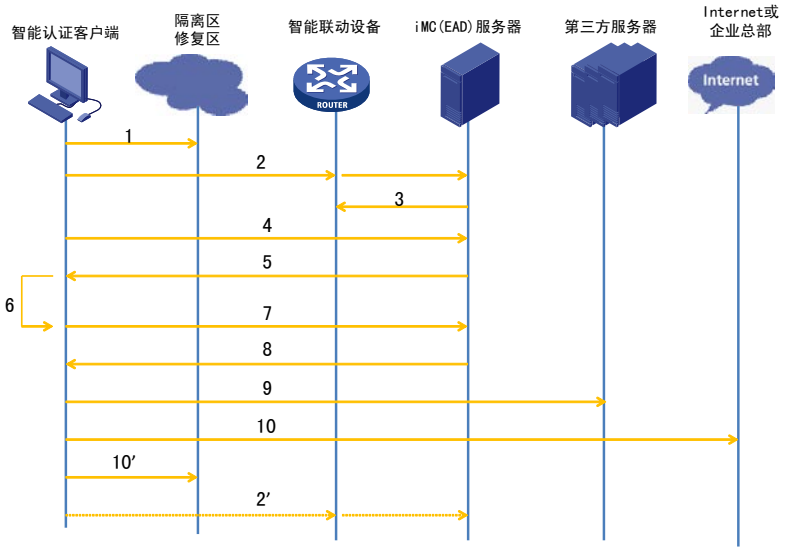


图3 EAD方案用户认证基本流程图

EAD方案认证流程详细描述如下：

1、用户在通过认证前只能访问隔离区资源；用户客户端在首次使用http访问Internet或安全网络时，会被重定向到隔离区。在隔离区内，用户可以获取客户端安装程序如iNode，当用户下载并安装安全客户端后，就可以进行安全认证。

2、当需要访问核心资源时，用户终端使用iNode发起认证请求

3、用户在iMC 服务器上认证成功，通知接入设备用户上线，并下发代理IP和端口，通知用户进行安全认证；

4、用户通过iNode客户端上传登录信息、请求安全检查项；

5、EAD安全策略服务器下发用户安全策略（是否检查补丁、杀毒）及其他控制信息；

6、iNode客户端与第三方软件或定制插件联动，执行安全策略检查及其他功能；

7、iNode收集终端计算机本地安全检查结果并安检结果上报EAD安全策略服务器；

8、安全策略服务服务器根据预先设置好的安全策略进行对比，下发对比结果到iNode客户端，显示修复策略以及设置监控任务等；

9、当用户终端的安全性不符合要求时，设备对iNode客户端做下线或隔离处理。终端可以依据iNode的安全检查信息访问第三方服务器进行补丁升级或病毒库更新等修复任务；

10、EAD安全策略服务器经过分析，如果认为终端用户满足安全要求，则提醒iNode客户端可以正常访问网络；

10’、 EAD安全策略服务器进行实时监控，当客户端实时在线时感染了病毒时，iNode客户端安全状态发生改变，EAD服务器通知iNode主动下线，用户只能访问隔离区进行自我修复；

2’、用户完成修复后可再次进行安全认证请求上线。

DAM桌面资产管理

桌面资产管理组件DAM提供了对资产全方位的管理和监控的功能。这里所涉及的资产是指接入网络的各类终端，如PC、服务器等。基于获取的 资产软硬件信息，DAM实现了对资产软硬件使用情况、变更情况的监控；基于对资产的配置和软件分发，DAM实现了对资产的有效管理；DAM还提供了多元化的统计报表，让网络管理员对资产的监控数据分析的更加充分。

DAM主要提供三大类功能：资产硬件管理、 资产软件管理、资产管理策略配置。

◆ 资产硬件管理

◆ 资产硬件管理提供了对资产的硬件部分（如CPU、硬盘等）的全面管理，其功能包括：资产分

组、资产管理、资产硬件变更、USB监控、桌面控制方案、外设管理策略、外设违规查询及资产统计。

◆ 资产分组：使管理员可以对资产进行层次化、个性化管理。它属于辅助功能，不直接对资产硬件进行管理。

◆ 资产管理：提供了查询桌面资产的功能。可以快速查询资产及其硬件信息，并快捷地执行相关操作。

◆ 资产硬件变更：记录了资产硬件的变更情况。通过该功能，管理员可以查询到资产的相关历史记录，全面了解资产硬件变更情况。

◆ USB监控：详细记录了USB接口的使用情况。其中包括使用时间、相关文件操作等。

◆ 桌面控制方案：能够给指定的资产或指定分组下的所有资产应用具体的管理策略进行控制管理。

◆ 外设管理策略：提供了对资产的外设（如存储设备或通讯设备）进行管理功能。

◆ 外设违规查询：详细记录了外设违规的具体情况。其中包括违规设备的类型、设备范例ID、违规操作时间等。

◆ 资产统计：提供了灵活多样的统计方式，可以对全部或部分资产进行统计，也可以对特定的硬件信息进行统计。让管理员轻松统计所关注的信息。

◆ 资产软件管理

◆ 资产软件管理提供了对资产的软件部分（如操作系统、IP地址、软件安装与卸载等）的全面管理，其功能包括：资产分组、资产管理、资产软件变更、软件分发及资产统计。

◆ 资产分组：使管理员可以对资产进行层次化、个性化管理。它属于辅助功能，不直接对资产软件进行管理。

◆ 资产管理：提供了查询桌面资产的功能。可以快速查询资产及其软件信息，并快捷地执行相关操作。

◆ 资产软件变更：记录了资产软件的变更情况。通过该功能，管理员可以查询到资产的相关历史记录，全面了解资产软件变更情况。

◆ 软件分发：能够给指定的资产或指定分组下的所有资产自动批量分发和安装软件，满足大型分布式网络中软件统一安装、升级的需求。 每一个分发都有清新的过程跟踪和记录，并可以实时查看分发状态。

◆ 资产统计：提供了灵活多样的统计方式，可以对全部或部分资产进行统计，也可以对特定的软件信息进行统计。让管理员轻松统计所关注的信息。

◆ 资产管理策略配置

◆ 通过业务参数配置，可以满足不同的管理需求。例如可以使能或禁止资产的自动注册功能等。

桌面资产管理工作基本流程如下图所示：

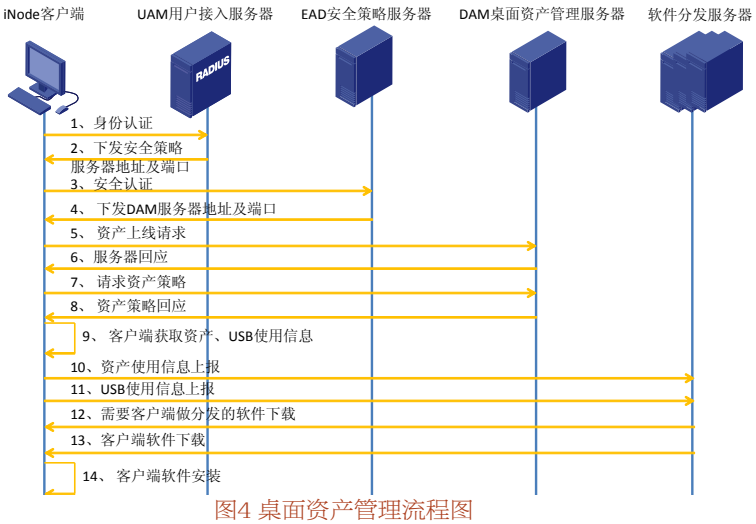


图4 桌面资产管理流程图

小结

EAD是一种通用接入安全解决方案，具有很强的灵活性和适应性，实现对局域网接入、无线接入、VPN接入、关键区域访问等多种组网方式的端点防御，从源头上减少威胁因素的引入，大大提高了企业网络的安全性。通过http报文的重定向功能可以实现客户端的快速部署功能，减少网络管理员的工作量。当企业网络范围较大时或分散在多个物理区域时，EAD提供分级节点管理模式来对网络进行分级管理。

网络流量和用户行为分析

文/袁 江

随着互联网的迅速发展，网络应用、业务越来越丰富，巨量的资源、众多的用户群体为我们的工作和生活带来了极大的便利。但与此同时，网络的繁华盛世也带来了激增的流量、越发复杂的应用构成、多样化甚至破坏性的用户行为等亟待解决的问题，在这种情况下，对网络流量、用户行为进行全面、深入的分析，从而了解流量的分布与变化趋势、用户的访问和操作记录就显得十分必要了。

网络管理的挑战

网络流量的复杂性、用户行为的多样性给网络运营维护带来了巨大的挑战，企业在管理网络中普遍遭遇了如下一些问题：

◆ 网络的规划构造：网络利用率如何？出口流量、公司分支之间的流量多大？流量都由哪些协议、应用构成？主要用户有哪些？流量变化趋势如何？网络带宽是否需要扩容？

◆ 应用业务的部署：当前网内有哪些应用？分别产生了多少流量？企业内部重要应用的运行状况如何？各应用、业务之间的流量比率如何？

◆ 网络安全的监控：网络中是否有攻击？是否包含病毒异常流量？是否有非法用户接入？攻击流量的来源是哪里？有哪些攻击、病毒存在于网络中？

◆ 用户使用网络的监管：哪些用户产生的流量最多？分别使用了哪些应用？用户是否使用了P2P应用占用资源？是否访问了非法网站？

从这些问题来看，网络管理者需要分析流量的源和目的、流量的组成、流量大小、应用层信息等多方面来获知当前网络的使用状况。面对海量的流量数据信息，管理人员是无法通过人工完成流量分析的，为了解决这一棘手且亟待解决的问题，H3C公司推出了基于iMC平台的网络流量分析（NTA）组件和用户行为审计（UBA）组件，NTA注重网络流量信息的统计与分析，UBA关注网络日志的查询审计。两个组件可单独部署使用，也可统一部署满足网络管理员更细化的需求。

NTA/UBA解决方案可以使网络管理人员了解企业内部网络的运行状况，及时发现并解决网络中的性能瓶颈问题、网络异常现象，完成对网络用户的行为监管，帮助完成对网络的优化。

NTA/UBA简介

iMC NTA网络流量分析组件为客户提供了一种简便、直观的流量分析解决方案。客户可以使用支持NetStream/NetFlow/sFlow等技术的网络设备提供网络流量信息，也可以使用DIG探针采集器对网络流量信息进行采集（若现有设备不支持NetStream等技术）。同时，不需要改动现有网络结构，NTA可根据需求灵活的在不同层面（接入层、汇聚层、核心层）的网络设备上进行流量信息采集，可以为企业网、校园网、园区网等各种网络提供网络流量信息统计和分析功能，让客户及时了解各种网络应用占用的网络带宽，各种业务消耗的网络资源和网络应用中TopN流量的源主机等相关信息。

iMC UBA用户行为审计组件提供对NAT1.0日志、FLOW1.0日志、NetStream v5/v8/v9日志、DIG日志的查询审计功能，用来对终端用户的上网行为进行事后审计，追查用户的非法网络行为，满足相关部门对用户网络访问日志进行审计的要求。

两个组件通过定制特定条件的分析审计任务，可以分类细化流量，对分析结果进行图表化的显示，简单、直观的呈现客户分析审查的网络数据。

NTA/UBA解决方案及实现机制

流量分析的过程大概可以分为三个环节：数据采集、分析统计、结果显示。相应的，NTA/UBA解决方案架构包括：流量采样设备（NTE，NetTraffic Exporter）、网流集结服务器（NTC，NetTraffic Collector）、分析处理服务器（NTP，NetTraffic Processor），三个部件之间的关系如图1所示：

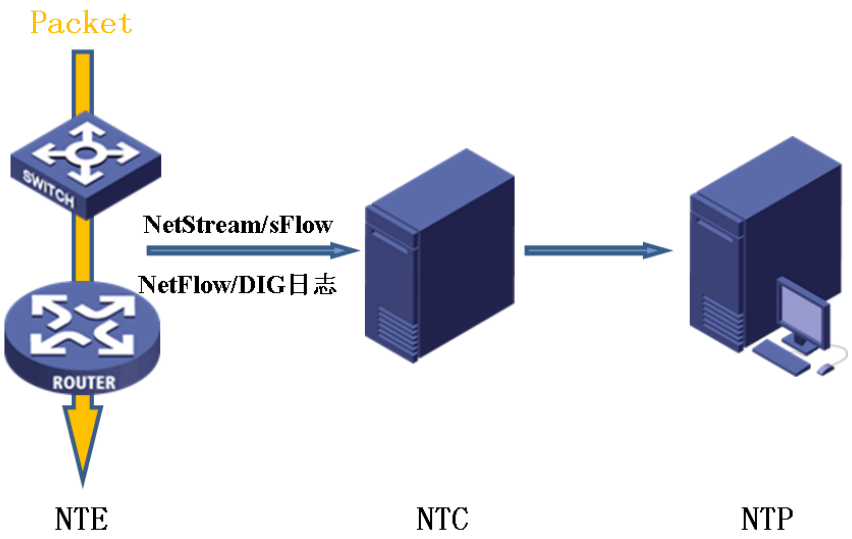


图1 NTA/UBA各组成部件的关系

各部件的功能

NTE包含支持NetStream、sFlow、NetFlow等技术的路由器和交换机等网络设备以及DIG探针采集器，负责对设备各个端口进出的网络报文进行流分类统计，然后将NetStream/sFlow/NetFlow/DIG日志以UDP包的形式发送到NTC设备监听的端口。

NTC接收到一个或者多个NTE设备源源不断发送过来的日志信息，对这些数据进行过滤与聚合，并将数据存储在数据库中供NTP分析处理。

NTP是一个网络流量的分析工具，对NTC生成的数据进行二次聚合、统计分析。为便于网络管理人员的操作，采用基于Web形式访问，提供直观的、图形化的管理界面，所有数据输出都以友好的形式直接在Web页面中显示。

DIG探针采集器

针对一些不支持NetStream/NetFlow/sFlow等技术的网络设备，H3C提供了DIG探针采集设备（DIG在组网中的位置如图9所示）。DIG采集器直接获取网络设备接口上的镜像数据或者分流器TAP数据进行处理（ TAP，测试接入端口，是一个硬件设备，它直接插入到网络电缆和发送一份网络通信给其它设备），生成DIG日志提供给NTC/NTP进行分析统计。

DIG日志又称为探针日志，目前1.0的版本包含这些内容：开始/结束时间、源/目的IP地址、 源/目的端口号、协议类型、输入/输出包个数、输入/输出字节数。

DIG日志探针组件对采集到的原始网络报文进行实时处理，对报文进行过滤处理，过滤掉一些不希望继续处理的报文；然后进行聚合处理，即按照预置聚合条件将多条报文聚合成一条，减少后续处理以及归档的日志数据量。聚合之后，DIG日志探针组件将会形成DIG日志，并将DIG日志发送给NTC/NTP进行处理。

NTA/UBA功能特点

任务式多角度分析

NTA网络流量分析组件通过定制任务方式实现对接口/接口组、探针、特定应用、特定主机组的流量信息实时监控，流量信息包括流入、流出速率以及当前速率相对于链路最大速率的比例等。全任务式的自动跟踪，大大简化了管理员监控网络流量的工作。

UBA用户行为审计组件提供基于任务的自动跟踪审计功能，可以根据接入用户名、用户访问网页的URL等各种查询审计条件灵活制定审计任务。任务一旦制定，组件将自动跟踪审计当前时间段内满足查询条件的所有用户及日志信息。审计任务包括：地址转换、Web访问、文件传输、邮件、通用等多种类型。

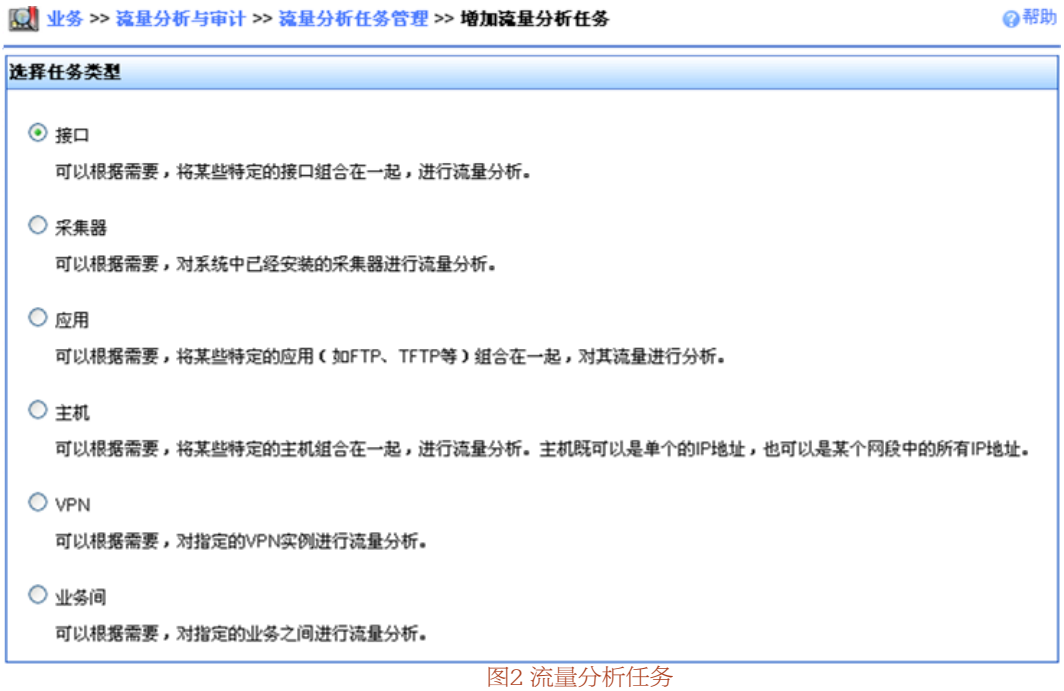


图2 流量分析任务

细化实用的深入分析

NTA/UBA对接收到的网络流量信息和网络日志信息进行详细的分析，对分析出来的结果进行统计，呈现出流量趋势、应用流量、操作对象等各个网络管理员关心的数据。

◆ 总体流量趋势分析反映被监控对象（如一个接口、接口组、IP地址组）的入、出流量随时间变化的趋势。图形化的统计一览表提供了指定时间段内总流量、采样点速率最大值、采样点速率最小值和平均速率的信息。对于设备接口，还可提供带宽资源利用率的统计。同时还支持流量明细报表，可提供各采样时间点上的流量和平均速率值。

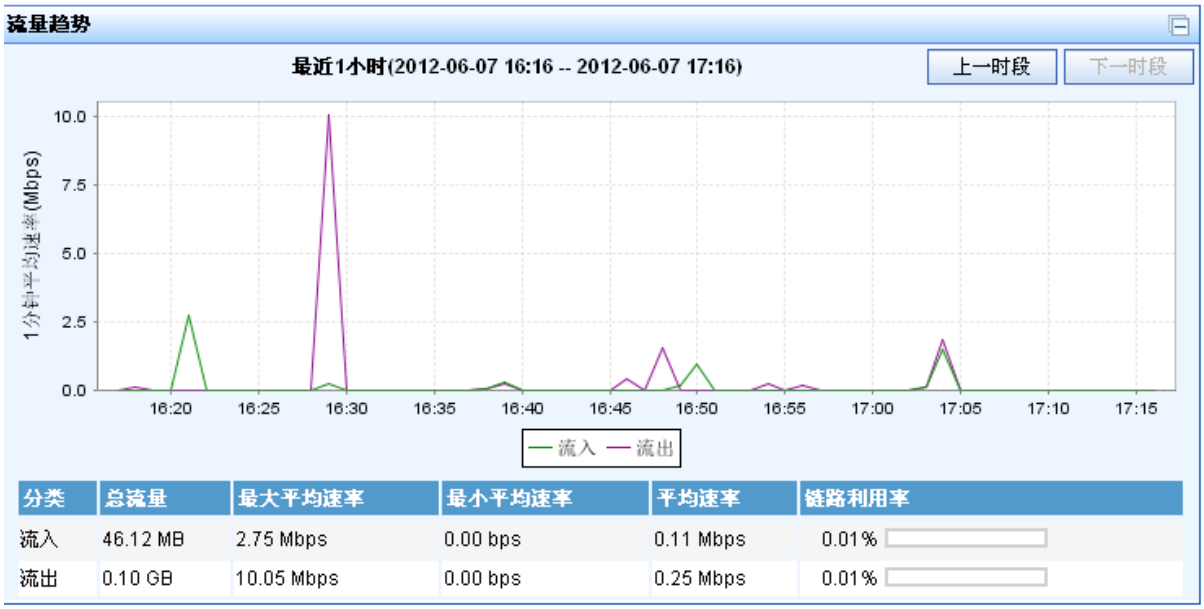


图3 整体流量趋势

◆ 应用流量分析反映被考察对象（如一个接口）的流入（或流出）方向上，带宽被各种网络应用占用的比例随时间变化的趋势，包含报表统计时间内的该应用的总流量、平均流速和占所有应用总流量的百分比等。同时还支持对该应用的流量信息进一步的数据挖掘，分析使用该应用流量的最大源主机和目的主机地址TopN列表。

图4 应用流量分析

◆ 源主机\目的主机\会话流量分析反映被考察对象（如一个接口）的流入（或流出）方向上，在指定时间范围内总流量最大的网络节点（源、目的主机）、以及网络节点间会话的排名。同时还支持对节点、会话流量进行进一步的数据挖掘，分析节点流量中使用最多的应用和与该节点通讯最多的节点、分析会话流量中双方节点使用应用的排名信息。

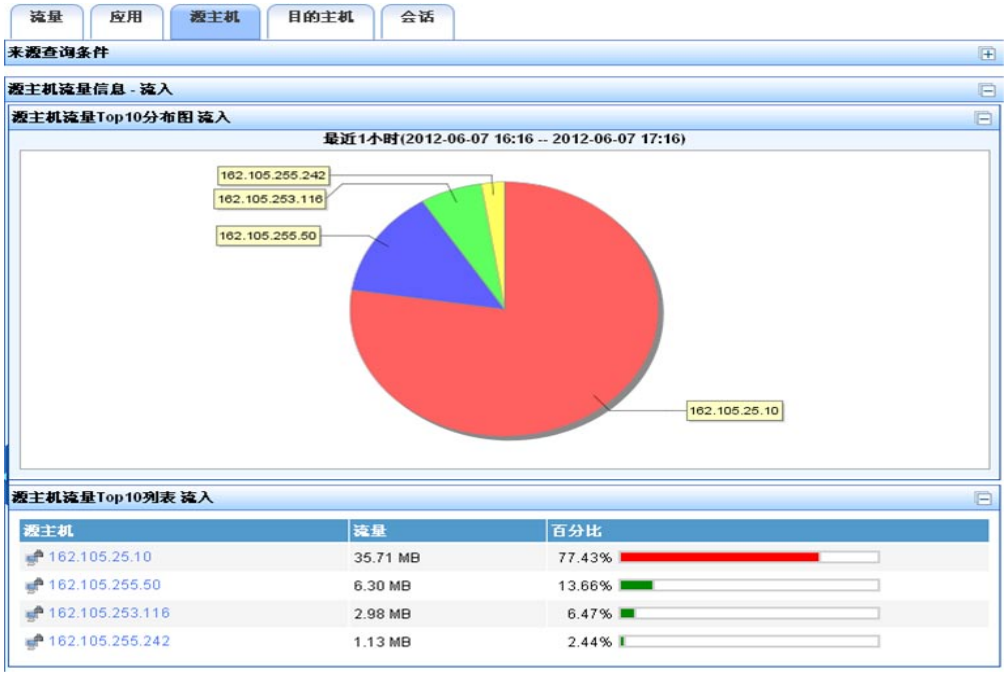


图5 源主机流量分析

◆ 智能基线及自动告警：采用了独创的坏值剔除技术和高精度的基线构造算法，以周为单位整理历史流量信息，智能化自动生成流量基线，准确反映网络总体流量基准，动态衡量网络总体流量水平。基于基线实时检测流量突变状态，并采用零均值化、二阶自回归模型AR(2)等高准确性的数学模型，在无序的流量运行状态中准确分辨网络异常流量，流量发生异常偏离时自动告警。同时NTA依托iMC平台支持

丰富的告警方式，通过声光、短信、邮件等多种方式通知管理员，及时发现网络中的异常流量。

◆ 未知应用流量分析对组件中没有定义的TCP、UDP应用进行了深入的分析，提供按照端口号、源IP和目的主机IP分组的未知应用流量信息，并可查看到某一个端口、源IP和目的主机IP的详细通信信息，提供按源、目的主机分类的流量TopN情况。可以按协议和端口将统计到的未知应用定义为已知应用，方便将网络中用户特有的应用进行识别和统计。

◆ 七层应用流量分析：端口不固定的应用，如BT、eDonkey等应通过报文应用层数据的特征进行识别。基于七层应用的识别和分类，NTA可针对百兆链路提供对常见P2P、BT、eDonkey等应用的网络占用带宽趋势图和流量趋势图及应用的详细信息列表等报表，实现对此类应用流量的监控。组件已经将大部分常见的端口不固定的应用设定为组件预定义的应用，如：BT、DC、eDonkey、Gnutella、Kazaa、MSN、QQ、AIM等。用户可根据需要定义其它的应用识别。七层应用识别只对DIG日志有效，对其他类型的日志无效。

◆ 基于用户的流量分析：组件提供了根据IP地址获取对应的主机名称/域名和MAC地址的功能，并可与iMC EAD进行联动，获取特定时间段内使用该IP地址的用户上网明细信息。

◆ MPLS VPN流量分析：VPN流量分析通过NTA对NetStream V9中VPN日志模板的支持，可以接收和处理MPLS VPN流量日志，并基于VPN进行流量分析，供用户了解网络中各VPN内部的流量使用情况，对规划VPN网络提供帮助。分析内容包括VPN的总体流量趋势情况、VPN内的业务（应用）流量情况、VPN内各节点（源、目的IP）的流量及业务使用的情况、VPN内会话流量情况、VPN组合分析等；同时支持智能基线及告警功能。

◆ 支持网络应用的自定义。通常情况下，网络应用由一组（或多组）固定的网络协议和通讯端口的组合进行标识，如HTTP应用对应TCP协议和80端口。网络流量分析组件预定义了近三百种常用应用定义，管理员可以直接使用。根据网络的实际使用情况，管理员也可以自定义关心的应用来进行数据的统计分析。例如将FTP应用定义为TCP/21和UDP/21，NTA网络流量分析组件就会依据协议类型和端口号信息统计符合FTP应用定义的流量信息，帮助管理员获取更为实用的网络流量统计结果。

强大的日志审计功能

◆ UBA用户行为审计组件可根据用户需要，通过接入用户名、上网时间、用户访问网页的URL、ftp操作文件及发送邮件的主题等各种条件的组合对网络日志进行快速审计，并对审计结果提供灵活的排序、分组、保存等功能。

◆ 网络管理员可以从海量的网络日志中精确审计终端用户的上网行为。终端用户何时访问了某网站、何时访问了某网页、发送了哪些Email、向外发送了哪些文件等信息均可通过日志审计得出结果，日志审计包括：

◆ 通用日志审计：审计内容包括接入用户名、用户上网起止时间、来源/目的IP地址、来源/目的端口、使用的协议及应用名。

◆ Web访问审计：审计内容包括接入用户名、用户上网起止时间、来源/目的IP地址、端口、用户访问的站点、用户访问的网页等。

◆ 文件传输审计：审计内容包括接入用户名、用户传输文件起止时间、来源/目的IP地址、端口、FTP用户名、传输文件名、传输方式（上传/下载）等。

◆ 邮件审计：审计内容包括接入用户名、邮件发送时间、来源/目的IP地址、发件人、收件人、邮件主题等。

◆ 地址转换审计：审计内容包括接入用户名、用户上网起止时间、来源/目的IP地址、来源/目的端口、使用的协议及应用名、NAT转换后IP地址/端口等。

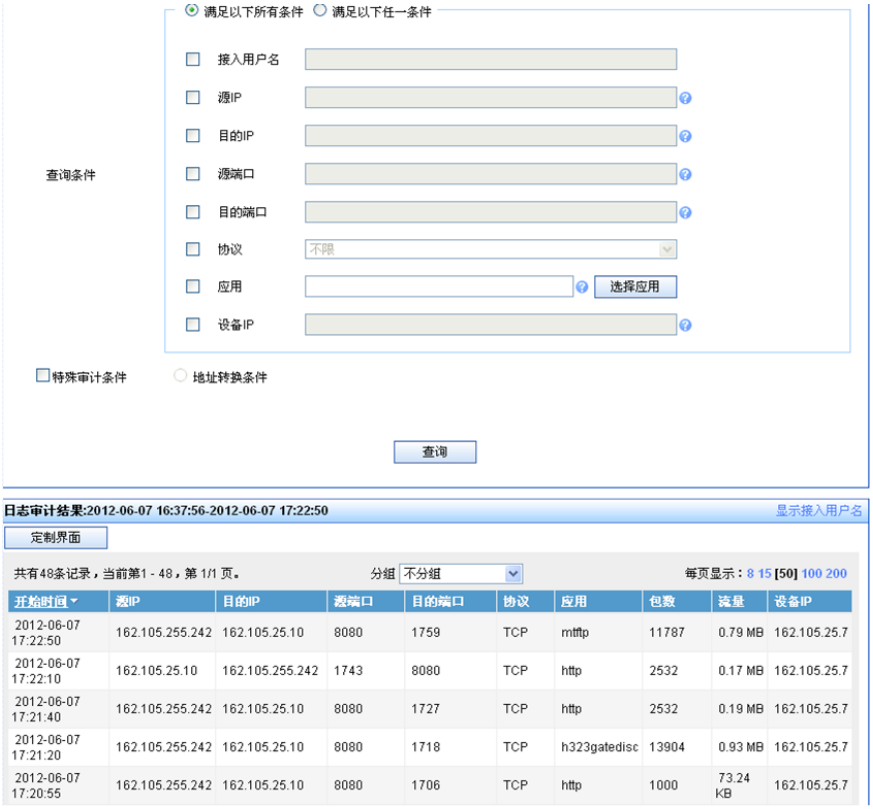


图6 日志审计界面

提供专业的报表

NTA/UBA可以生成专业的报表，包括基于接口的总体流量趋势分析报表、应用流量分析报表、节点（包括源、目的主机IP）流量报表、会话流量报表、访问站点、会话数、应用分布、未知应用的TopN报表，SMTP、HTTP、FTP的应用分析报表，每种报表都可以按照天、周等周期和图形、列表等形式输出。通过使用这些自带的报表，管理员可以非常清楚的了解当前用户对网络的使用情况。

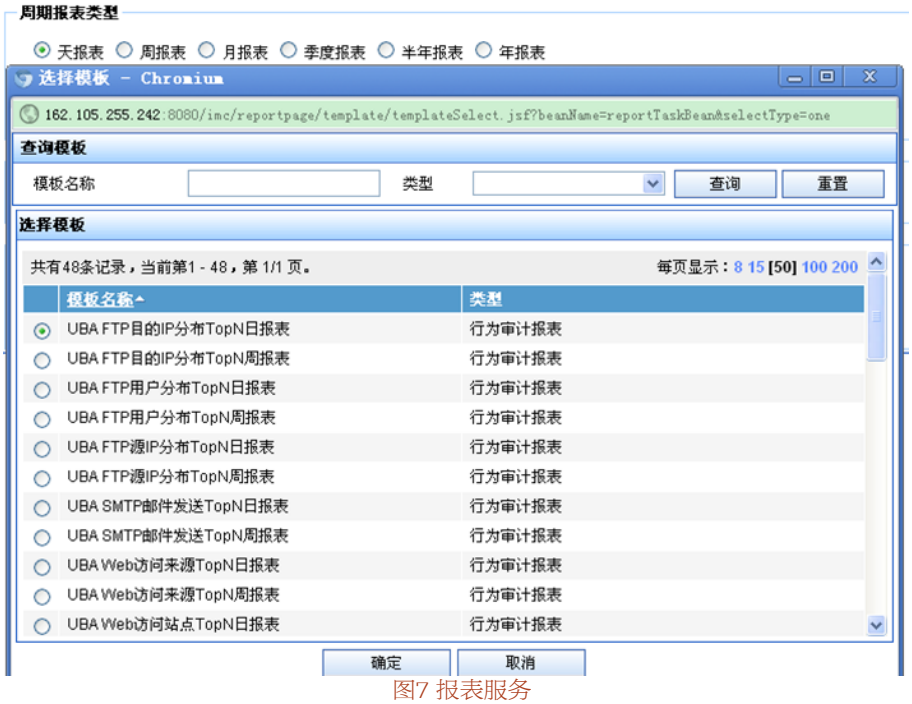


图7 报表服务

NAT/UBA典型组网

NetStream/sFlow/NAT组网方式

该组网方式下，需要设备支持NetStream、sFlow、NAT等技术，能输出相关日志。NAT/UBA接收日志并进行分析，可区分4层流量信息，实现多种方式的日志记录与审计功能，可提供丰富的报表供查阅。

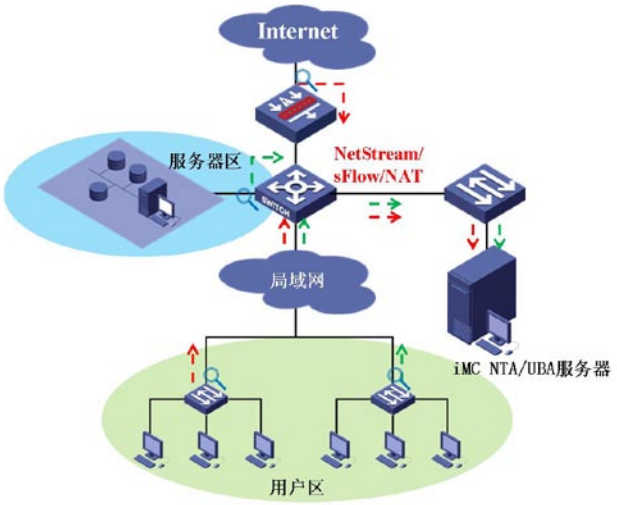


图8 NetStream/sFlow/NAT组网方式

DIG探针组网方式

探针式采集器能够与任何支持端口镜像功能的交换机或集线器配合，采集网络中的报文信息。

该组网方式最大的优点在于不依赖于具体厂商的设备，从而可以更有效的保护用户的已有投资，主要面向出口容量不大的行业用户，为管理提供更深入的用户行为审计，同时提供了对端口或链路进行流量分析、网络优化和异常监控的手段。

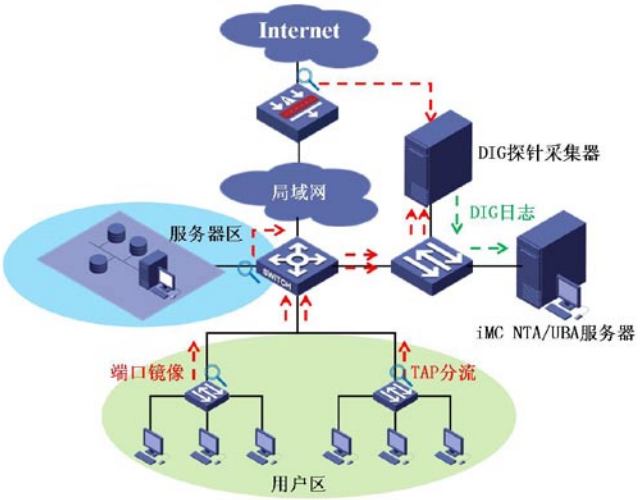


图9 DIG探针组网方式

小结

综上所述，NTA/UBA解决方案可用于监控流量日益增大、业务日益增多、高速发展的网络，帮助网络管理员及时发现、解决网络异常现象；了解网络资源负载情况、应用使用的趋势状况、用户操作的行为记录，方便网络管理员及时进行网络优化调整，防止有害的网络行为，避免进行无效的带宽投资；同时NTA/UBA专业的报表功能为网络管理员提供多样全面的网络流量分析报表，为网络规划提供有力参考。

IPsec VPN业务管理

文/其其格

引言

今天，随着企业网、校园网、园区网等各式各样网络的建设步伐不断加快，分支机构及边界网络的规模也扩得越来越大，选择远程办公的人也日益增多。如何保障网络的安全性，稳定性，为网络中大量的设备提供便捷、高效的管理是网络管理者急需考虑的问题。

IPsec VPN组网配置多，技术复杂，需要管理员掌握VPN的配置命令及实现情况。 但对于用户而言，需要的只是一个能够满足企业业务需求的管道服务，不需要去关注VPN的内部实现。

H3C iMC IPsec VPN管理系统，从用户角度入手，为用户提供了完善的解决方案，方便用户监控、维护和管理各自的网络。

VPN的管理变革需求

难部署

IPsec VPN配置命令多，参数专业性强，对其应用程序文件及配置文件进行升级管理困难，人力管理成本过高。如何快速完成业务规划部署给网络管理带来了巨大的挑战。

难监控

VPN网络比较复杂，运营商网络边缘设备数量巨大，很难对每一台设备进行吞吐量、丢包率统计，无法掌握IPsec VPN网络的整体性能及运行状态。 然而网络的稳定性要求越来越受到重视，管理员和用户希望轻松了解和掌控通道的状况和网络的吞吐情况。

难管理

企业网络往往会部署多个厂商的网络设备，根据业务的差别还会部署不同的VPN技术。这就给VPN的管理变革提出的第三个需求：如何将多个厂商，多种VPN业务统一进行管理，方便进行部署和业务开通？

智能VPN业务管理组件 IVM介绍

IVM管理架构

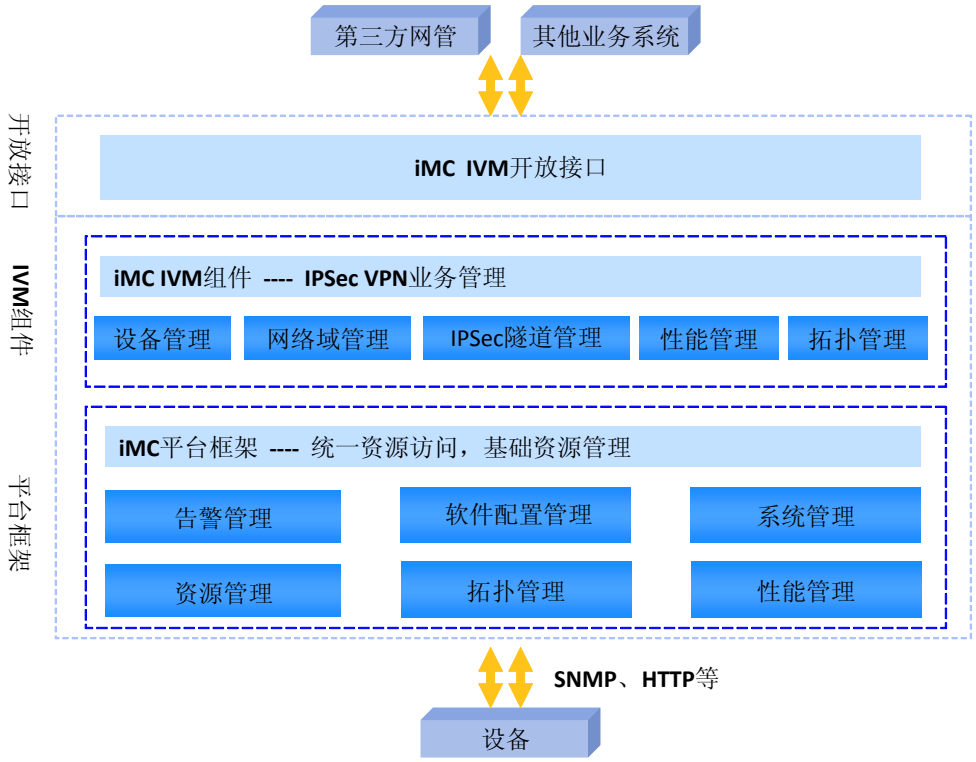


图 1 IVM架构管理图

IPsec VPN管理（IPsec VPN Management）组件简称为IVM，IPsec VPN管理系统基于强大的iMC平台，可进行多业务的融合管理，提供统一资源访问、告警管理、软件配置管理、拓扑管理、系统管理、性能管理等基础资源管理。

IVM是智能IPsec VPN管理系统的核心,具有IPsec网络规划部署、隧道管理、性能管理等功能。通过可视化的管理界面可以清晰的了解全网设备的信息和状态，并实时掌控具体业务分布和流量状态。

设备与iMC之间可以基于SNMP、Telnet/SSH或TR069等协议自动发现方式发现网络设备，使用简单的操作将其纳入iMC IVM管理。既可以实现对固定IP地址网络设备的业务下发，也可以实现对NAT后、动态IP设备的业务下发，并满足用户对安全、性能、可靠性等方面的要求。

IVM的功能特点

智能的网络域管理平台

为了更好地帮助用户划分业务逻辑，简化管理员部署工作量，统一管理VPN业务，iMC IVM在业界首先提出基于网络域的管理模式。

网络域是抽象出来的概念，是具有一些类型安全提议、策略应用的隧道集合。便于统一规划、部署、性能监控。

网络域中的网络类型可以是IPsec VPN 、DVPN、GRE VPN 等，但每一个网络域只能是一种类型的VPN。

用户可以根据各自的业务将网络设备划分为不同的网络域，并应用不同的安全策略，增强IPsec VPN网络的安全性。

图 2 智能的网络域管理界面

固化的策略模板管理系统

安全提议是安全策略或者安全框架的一个组成部分，它用于保存IPsec需要使用的特定安全协议、加密/认证算法以及封装模式，为IPsec协商SA提供各种安全参数。

IKE安全提议定义了一套属性数据来描述IKE协商怎样进行安全通信。用户可以创建多条不同优先级的IKE提议，优先级由IKE提议的序号表示，数值越小，优先级越高。

用户只要在选项栏中选择需要配置的安全协议、加密算法等参数就可以直接调用固定模板，然后通过网络域部署到所有设备上，部署完成之后这个网络域才算是建成的，之后打通隧道就可以了。

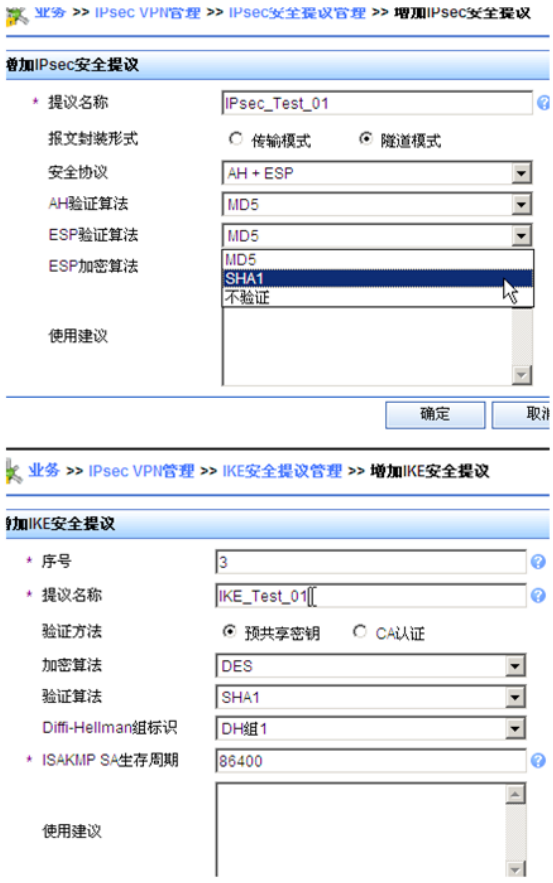


图 3 固化的模板管理界面

轻松构建IPsec VPN网络

大型企业网中，随着接入节点规模庞大，维护部署工作量也越来越大，IVM组件是能满足这种困扰的重要技术之一，iMC IVM组件部署在总部，管理员可以基于网络域和模板的方式快速直观的实现对中小型分支机构、移动用户、家庭用户等端到端VPN业务管道的规划。

总部的设备可以作为Hub设备，其他分支节点的设备均作为Spoke设备，一个网络域中只能有一个Hub设备，但Spoke设备可以有多个，组成从一个中心节点到星型网络的抽象体，并实现统一配置，统一管理。

通过IVM构建IPsec VPN网络需要有以下六个步骤完成：

1、创建网络域；

2、选择网络域中的Hub设备和Spoke设备；

3、选择配置IPsec的指定网络接口；

4、使用策略模板配置IPsec安全提议，IKE安全提议；

5、策略模板关联部署到网络域中；

6、增加Spoke设备到网络域，系统会自动为其配置网络域中共同的配置信息；

管理员也可以对模板形成的配置文件进行审核，并批量下发到网络域对应的设备上。极大程度地简化了设备的配置部署工作，管理员从总部轻松几个步骤就可构建IPsec VPN网络。

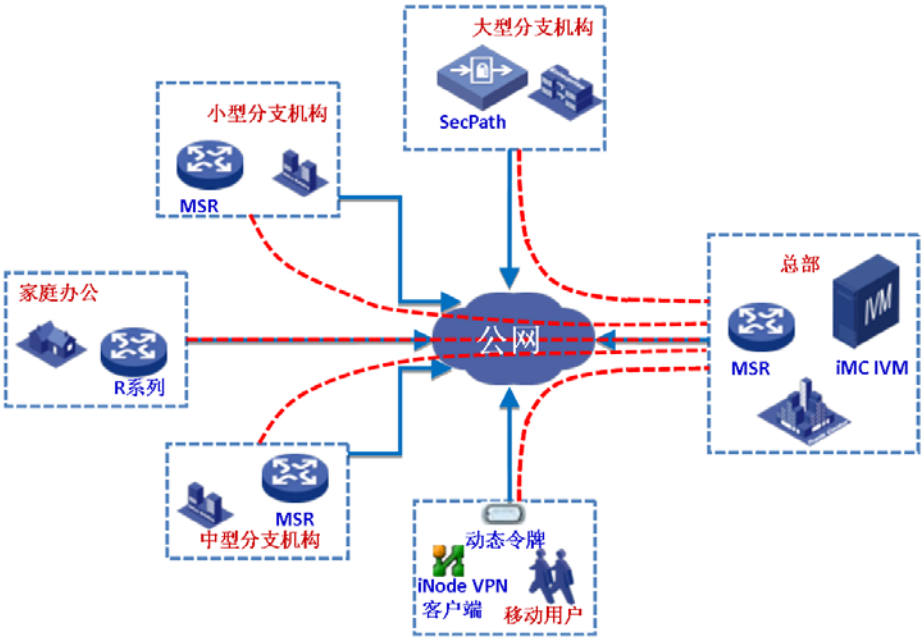


图 4 轻松构建IPsec网络

可视化的IPsec VPN网络性能评估界面

IVM管理首页可清晰地了解到整体网络的服务质量，VPN管理系统可以展示隧道最近24小时流量趋势图、网络域流量分布情况、IPsec接收速率TOP5等信息，管理员和用户通过此界面可以轻松的了解和掌握IPsec通道的运行状况和网络吞吐情况。

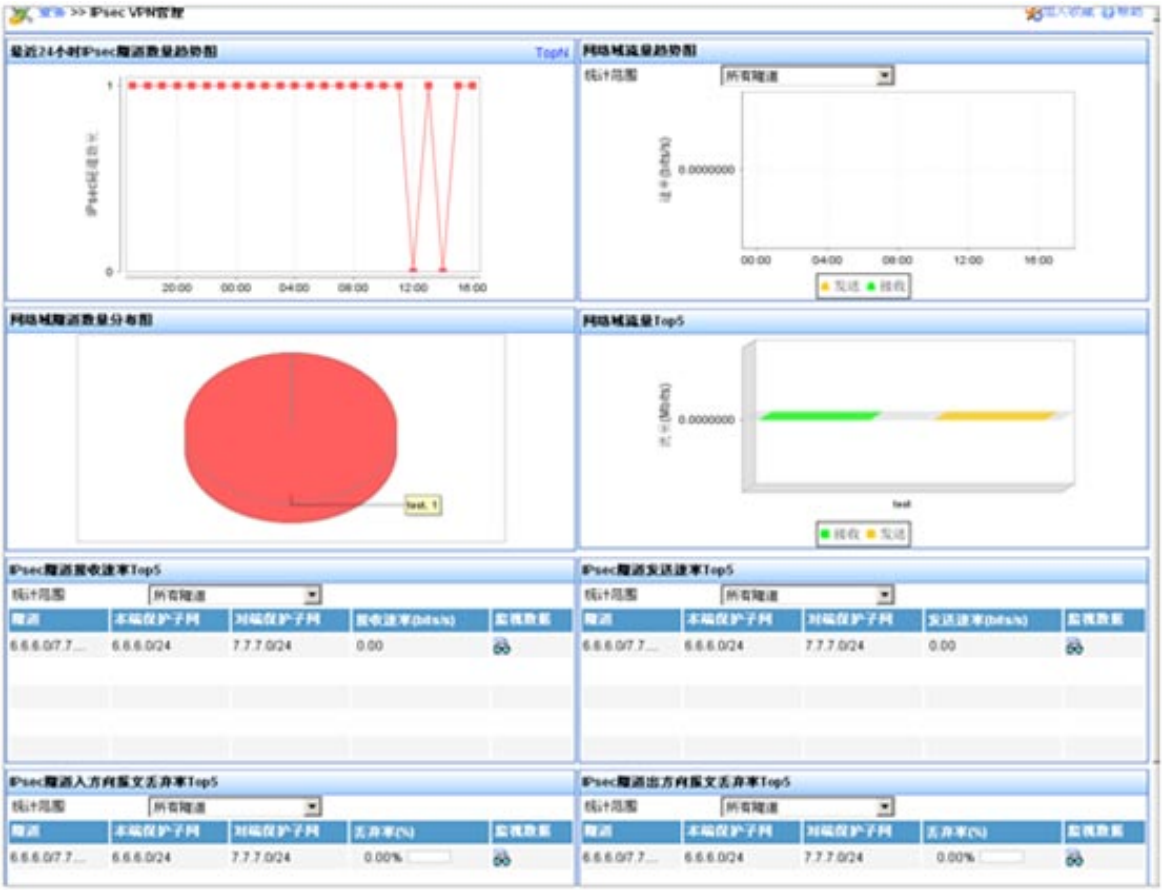


图5 可视化性能管理界面

直观的拓扑管理

IVM拓扑管理实现查看IPsec VPN设备拓扑和查看网络域拓扑功能，设备拓扑快照用于查看IVM设备管理中的IPsec设备上的隧道拓扑，网络域拓扑用于查看指定网络域的逻辑拓扑。

iMC IVM以网络域为单位自动构建并显示IPsec VPN业务拓扑，用户在拓扑上可以直观查看IPsec VPN网络布局，并提供拓扑背景变更、拓扑拖拽、拓扑缩放、自动布局等拓扑管理功能。

iMC IVM拓扑还实时关联告警信息，直观反映网络设备及隧道的运行状态，并在显示设备及隧道的IP地址、流量情况等详细信息 。

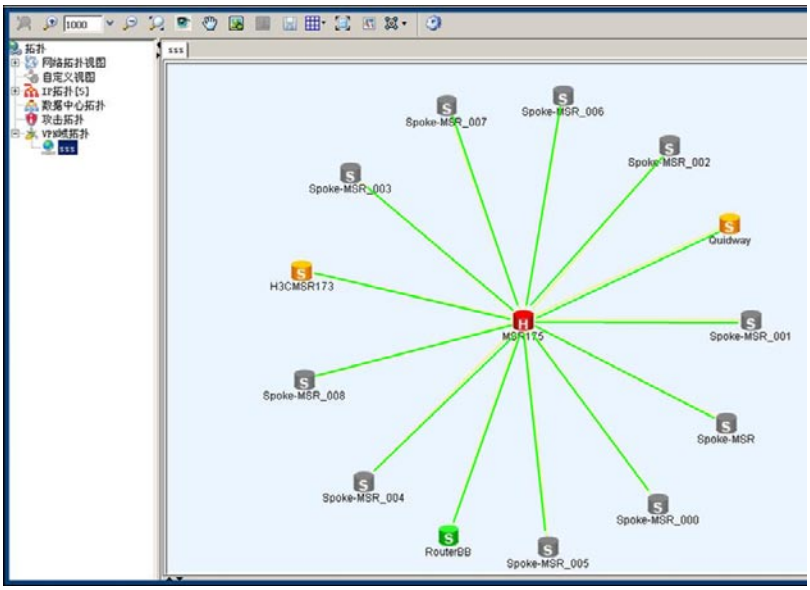


图6 清晰的拓扑管理界面

全面的隧道管理系统

在实际的IPsec VPN网络环境部署和维护工作中，通过IVM可实现查询隧道信息、查看隧道详细信息、查询历史隧道信息、导出历史隧道信息功能。

图7 全面的隧道管理界面

强大的iMC BIMS融合技术

通过IVM融合iMC BIMS技术总部VPN管理系统可保存分支企业的关键设备的业务配置，一旦分支关键设备出现问题，分支企业启动设备通过TR069等协议请求配置，实现零配置业务下发，远程解决设备容灾问题，大大提高了企业的运维能力，有效解决了分支企业IT维护人员薄弱的管理短板。

一直困扰IPsec VPN网络管理的难题：

◆ 运营商网络需要将大量NAT后、ADSL后、DHCP后的接入设备管理起来纳入全网管理；

◆ 运营商网络边缘设备数量巨大，对其应用程序文件及配置文件进行升级管理困难，人力管理成本过高；

◆ 当通过SNMP、Telnet等方式管理网络设备时，一般需要知道设备IP地址等信息，增加了网管主动管理设备的难度；

◆ IPsec VPN网络管理只能对已建立的IPsec VPN网络进行监控；

◆ H3C推出了iMC IVM、iMC BIMS的融合管理方案，真正做到IPsec VPN全流程管理：

◆ iMC BIMS通过TR069协议发现全网Spoke设备；

◆ iMC IVM对全网Spoke设备进行预配置，建立虚拟IPsec隧道，并将配置下发到iMC BIMS；

◆ Spoke设备上线后，iMC BIMS通过TR069协议将IPsec隧道设置下发到Spoke设备上，真正建立起IPsec隧道，完成IPsec VPN网络的建立；

◆ IPsec VPN网络建立后，由iMC IVM进行全面的IPsec VPN网络管理功能，提供向导性的批量资源管理、隧道管理、性能管理、拓扑管理等能力；

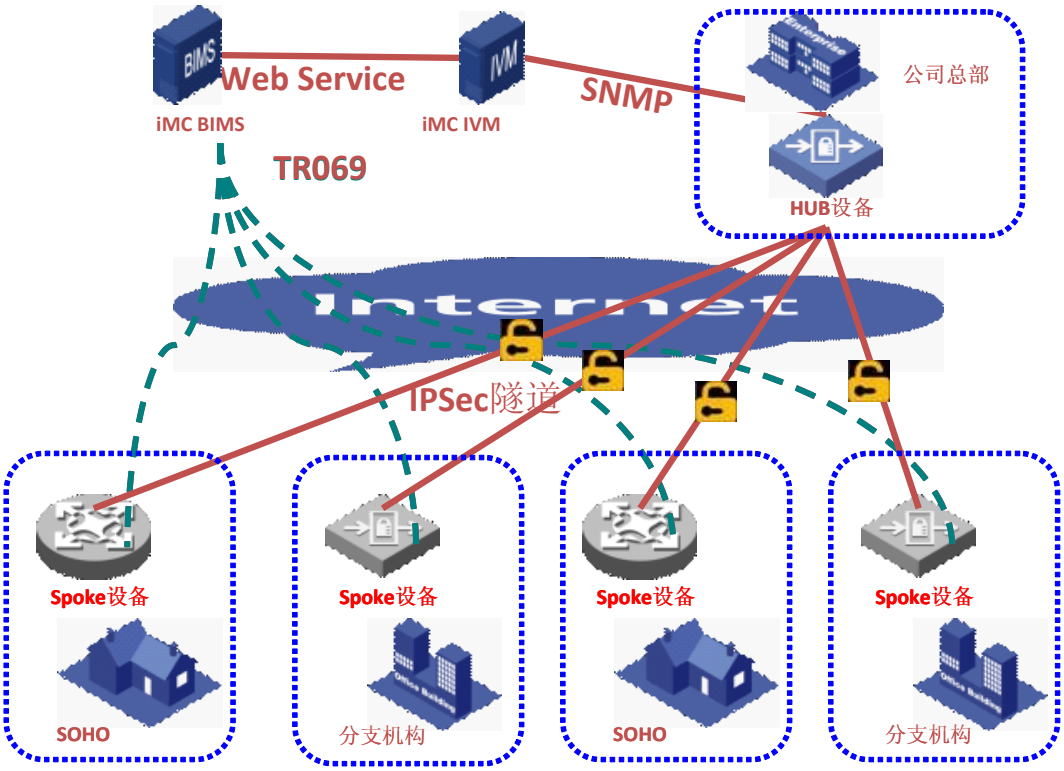


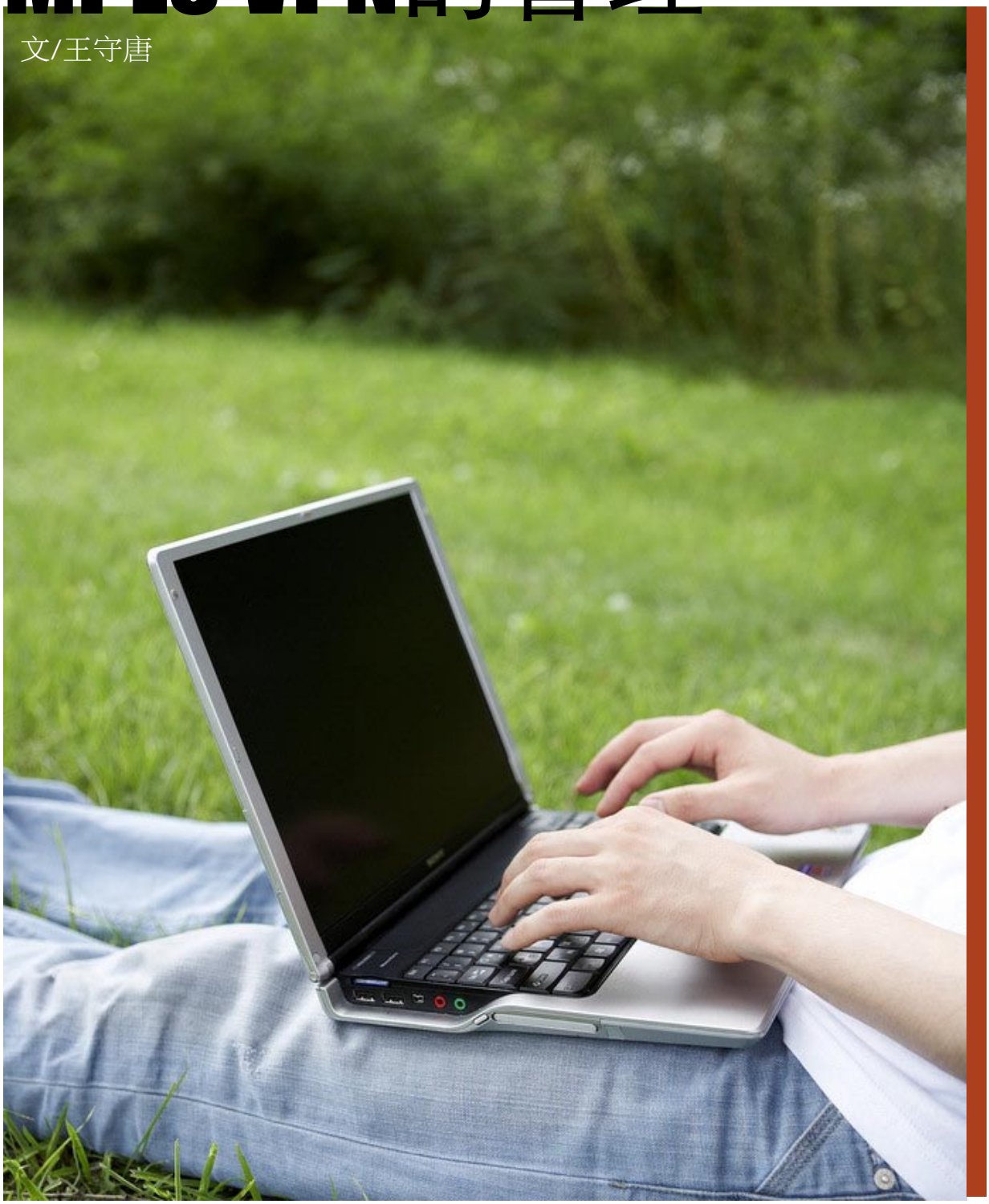
图8 强大的BIMS融合技术

结束语

IPsec VPN业务管理组件与iMC平台完美融合，提供从分级分权的基础资源管理到不同VPN的融合，轻松部署，以及可视化的流量性能监视和可灵活定义的业务报表展示，使我们的网络管理员从此不用再穿梭于机房的各个角落，坐在办公室里可轻松掌握、把控未来。IPsec VPN业务管理组件使复杂的IPsec VPN网络管理更加智能化、简单化、个性化，为确保承载高效、可靠的VPN网络做出了重大的贡献。

MPLS VPN的管理

文/王守唐



MPLS VPN管理需求

在大型企业网中，接入节点规模庞大，对接入点的互访控制要求越来越迫切。尤其对电力、政务、金融等跨地域的大型企业，为不同业务提供安全可靠的专用网络，更是安全生产、提高经济效益的有效手段。MPLS VPN就是能够满足这种需求的重要技术之一，得到大量主流设备厂商的支持，关键技术都已标准化；但是MPLS VPN涉及技术多而且复杂，增加了业务运营、部署、监控、服务水平检验等方面的管理难度。因此一个有效的MPLS VPN管理解决方案是大型企业网络运维中不可缺少的一环。

在大型MPLS VPN网络中，每一次业务的变更、新的部门的接入，都会对全网的路由、设备数量及配置产生影响，这就需要网络管理人员在进行业务部署之前，对网络变更进行深入的评估。管理员面临的第一个问题是：网络中正在运行着哪些业务？

传统的解决方法往往是管理员先通过查看设备、网络的配置了解现有网络已经部署的业务。此方法完全依赖于操作人员的经验。但在大型企业网络中，一个业务的调整往往会涉及十几台、甚至几十台设备，完全基于经验来进行业务规划的方式实现起来将会非常困难，不具有可操作性。因此MPLS VPN管理系统应该能够自动采集PE设备上的信息，从而发现网络中实际存在的VPN及VPN链路，形成VPN拓扑，使现有网络上的业务部署一目了然。

管理员面临的第二个问题是：如何方便快捷地部署新的MPLS VPN业务？

传统的业务部署中，需要依靠管理员对逐台设备进行手工配置，一旦出现误配置，问题的排查和定位工作将会耗费大量时间；因此，MPLS VPN管理系统需要实现业务的自动部署功能，而且最好使用图形化的界面的部署，增加用户的友好性，减少使用复杂的命令以降低错误的可能。

管理员面临的第三个问题是：如何感知网络中MPLS VPN的运行是否出现问题？如何定位问题？

MPLS VPN管理工具需要实现对网络中VPN业务的有效监控。监控的手段需要多种多样，如管理系统可以通过设备自动上报的告警信息和定期的状态轮询来发现业务的故障。发现故障后，管理系统会自动分析该告警对业务的影响，并及时向管理员通知业务告警信息，在拓扑图中实时显示故障信息，使网络运维人员在故障发生后可以快速定位网络故障。

另外需要从流量上对VPN进行监控。相比传统的基础网管，VPN管理系统需要更加关注对VPN业务接入的流量管理，然后通过图形化方式，按照日、月、年的方式进行报表输出。从而方便管理员对可能存在性能问题的业务进行处理。

为了保证客户业务的开通和正常运营，管理系统需要对已经部署的VPN业务进行定期审计，包括两个方面的内容，配置审计和VPN连通性审计，当设备上相关配置发生变化和VPN不能正常通信的时候，需要及时通知管理员进行处理。

H3C iMC MVM简介

针对MPLS VPN市场需求，H3C公司推出了MPLS VPN业务管理解决方案——iMC MPLS VPN Manager，简称MVM

MVM在iMC平台的基础上，定位于为各种规模的企业MPLS VPN网络提供管理方案。提供对MPLS VPN网络的业务发现、拓扑显示、状态监控、连通性审计、性能管理和业务部署等管理功能。因此MVM既具有基础网管能力同时又具备MPLS VPN业务管理能力。

MVM不仅可以配合H3C的设备，也可以配置Cisco和华为的VPN网络设备。

MVM的主要部件包括MPLS L3 VPN管理，L2 VPN管理和MPLS TE等相关内容。另外还有MPLS

TP和PBB相关部署内容，本文内容以MPLS L3/L2 VPN的介绍为主。

MVM的部署位置

根据管理要求的不同，MVM在网络中的部署位置基本有三种：

MVM接到核心网的PE/P设备上

将MVM接到核心网的PE/P设备上，用户可以从本地局域网或者Internet远程访问MVM服务器。基础网管能够管理P和PE设备的基本网络属性，MVM可以管理PE设备的MPLS VPN特性，这种方式的缺点是MVM不能管理到CE设备。如图1所示：

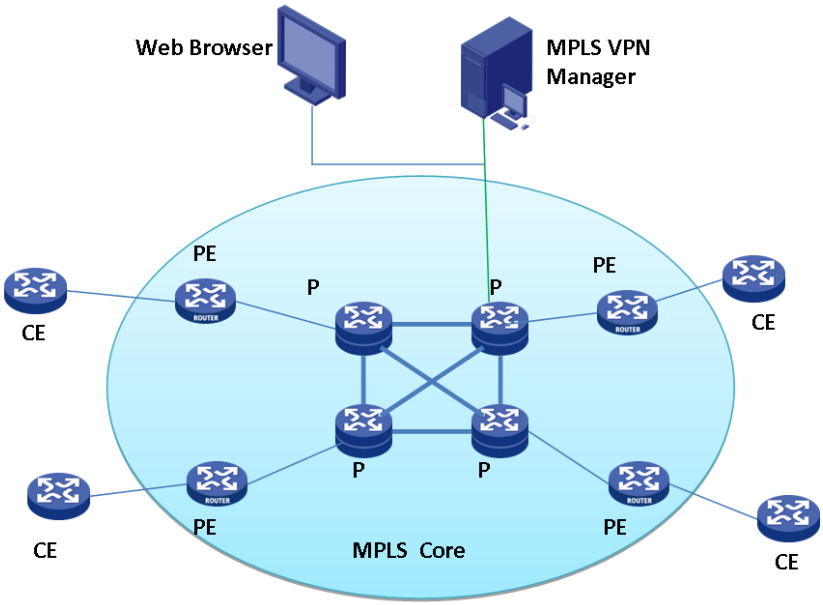


图1 MVM接入方式1----直接连接到核心网PE/P设备

管理VPN方式

管理VPN的方式可以同时管理PE和CE设备。同时管理PE和CE不仅是MVM的需求，也是设备网管管理PE和CE设备的要求。

如图2所示，MCE、MPE之所以增加一个M字母，是因为他们充当了管理VPN中的CE和PE的角色。通过管理VPN，VPN Manager连接在MCE上，可以访问所有VPN的CE设备；另一方面，MCE和MPE之间还存在一个IPv4的通路，通过这条通路，可以管理所有PE甚至是核心网中的P设备。

这样，MCE和MPE之间应该有两个逻辑接口。建议VPN Manager采用公网地址，在管理VPN中应该引入到达该公网地址的路由。需要注意的是：所有希望被VPN Manager管理的CE的地址空间不能重叠。

这种方式主要用于L3 VPN的管理中

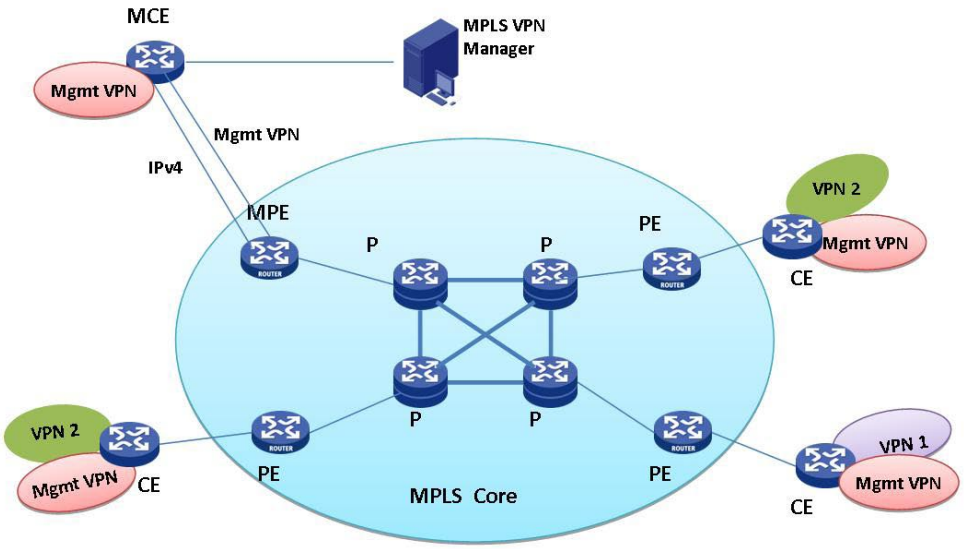


图2 MVM接入方式2----管理VPN方式

管理VPN的CE（Site）之间的互连可采用Hub-Spoke(Central Services)方式，这样就可以保证各VPN之间的隔离性。

双链路方式

双链路方式是指PE和CE之间存在两条链路：一条用于VPN的接入，另一条接入到核心网中，用于CE的管理。

MVM接入到公网的PE/P设备上，可以同时管理PE和CE设备。

这种管理方式的优势是简单。缺点是要占用一个CE的接口/子接口，一个核心网IP地址资源，适合接口和IP地址资源比较丰富的情况下使用。

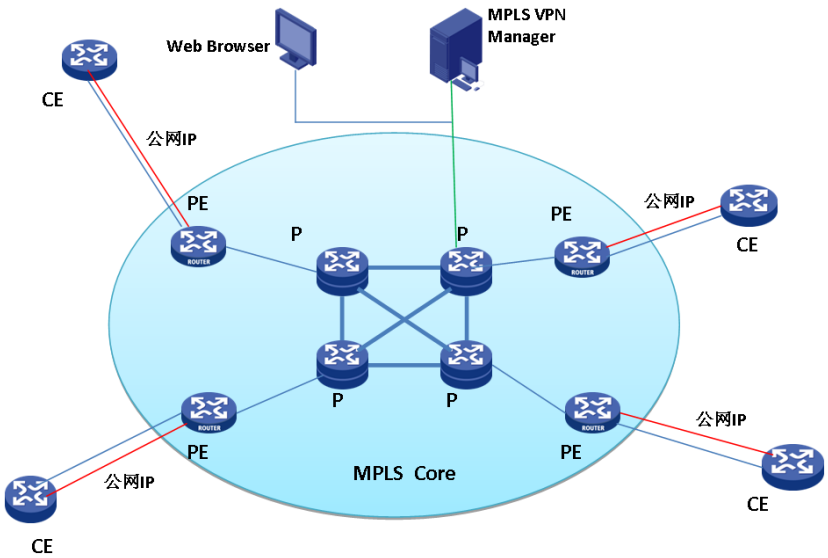


图3 MVM接入方式3----双链路方式

MPLS L3 VPN管理组件

基本概念

基础VPN

实际应用中，用户的任何一种业务都可以对应其网络中某些Site之间的互通关系。而复杂的互通关系最终可以分解为三种基本形式的VPN：

1. Full –Mesh VPN（也称为Simple VPN ）

一个VPN的所有用户形成一个闭合用户群，相互之间能够进行流量转发。对于这种组网，需要为每个VPN分配一个VPN Target，作为该VPN的Export Target和Import Target。

2. Hub–Spoke (Central Services) VPN

一个VPN存在一个Hub Site，放置有服务器，其它Site作为Spoke Site，需要都与Server互通，但Spoke之间不能互通。Hub和Spoke形成一组相反VPN Target。Spoke间的Export Target相同，Import Target也相同。

3. Hub and Spoke (Central Transit) VPN

在这种VPN中，设置中心访问控制设备，其它用户的互访都通过中心访问控制设备进行。此时，需要设置两个VPN Target，一个表示“Hub”，另一个表示“Spoke”。各Site在PE上的VPN实例的VPN Target设置规则为：

◆ 连接Spoke站点的Spoke–PE：Export Target为“Spoke”，Import Target为“Hub”；

◆ 连接Hub站点的Hub–PE：Hub–PE上需要使用两个接口或子接口，一个用于接收Spoke–PE发来的路由，对应VRF的Import Target为“Spoke”；另一个用于向Spoke–PE发布路由，对应VRF的Export Target为“Hub”。

Service Community

Service Community简称为SC，是VPN的最小组网单位，一个SC对应一个由若干Site组成的且共享相同一组RT值的集合，是一组具有最基础的业务连通性的团体。简单的理解，SC就是一个业务，使用一组RT，对应一类基础组网。

举例来说：在一个VPN中，有7个Site，Site 1、3、5形成了一个Full–Mesh的组网；而Site 2、4、6形成了另一个Full–Mesh组网；而Site 1、2、3、4、5、6都需要访问位于Site 7中的服务器。这样整个VPN需要建立3个SC：

1) Site 1、3、5组成了SC 1，Full–Mesh类型，import–RT和export–RT都定义成100:1

2) Site 2、4、6组成了SC 2，Full–Mesh类型，import–RT和export–RT都定义成100:2

3) Site 1、2、3、4、5、6、7组成了SC3，Hub–Spoke类型，Site 7是Hub节点，import–RT定义为100:3，export–RT定义为100:4，其它节点为Spoke节点，import–RT和export–RT的定义正好相反。

这样：

1) 在Site 1、3、5定义VRF时，加入的SC选择SC1和SC3，就是说为该VRF有SC1和SC3两项服务。对SC3是以Spoke方式加入；

2) 在Site 2、4、6上定义VRF时，加入的SC选择SC2和SC3。对SC3是以Spoke方式加入；

3) Site 7定义VRF时，加入SC选择SC3，并使用Hub方式加入。

在实际应用的时候，不同业务采用不同的SC，各个业务的RT值分开设置，不要交叉。

Service Access

简称SA，服务接入，表示CE接入到PE的一条被VRF绑定的链路

主要功能

业务发现

对于已经部署了VPN业务的网络，MVM可以实现自动发现。

自动发现功能利用当前组网环境中的各个PE设备上VRF的RT值特征和接口的VRF绑定关系，生成三种基本类型的SC。然后分析各个SC下的SA所在接口，将存在相同接口的SC合并成VPN，最终将网络中存在的VPN以及VPN链路发现出来，为管理员快速获取当前网络结构提供了一条便捷的途径。

发现过程中系统自动创建VPN和SC，用户也可以先手工创建VPN和SC，然后执行自动发现，此时会根据RT关系把链路归类到合适的VPN下。

发现链路后，如果没有配置CE接口，系统可以自动创建非管理CE来补充链路。

业务部署

对于没有部署VPN业务的网络，MVM提供了BGP MPLS VPN部署功能，向导式的操作步骤简单直观，无需记忆枯燥的命令行，大大节省了管理员的配置工作量。支持VPN链路的部署和批量拆除。

VPN的网络部署主要表现为SA的部署，包括选择PE和VPN，选择SC，选择接口，选择VRF，配置路由等步骤，一步步地引导用户进行配置。最后根据用户要求形成对应的配置命令，下发给对应的设备。

拓扑管理

MVM可以生成VPN的拓扑图，方便了对VPN的直观监控。不仅能够实时显示网络对象的状态，包括VPN配置是否发生变化、PE设备同步结果、以及PE设备是否存在链路配置缺失等，而且可以实时显示CE之间的连接关系和连通状态。

MVM包含两种拓扑：接入拓扑和业务拓扑。

1. 接入拓扑

接入拓扑反映PE和CE之间的连接关系。全网拓扑也是一种接入拓扑，反映全网的PE和CE之间的连接关系。

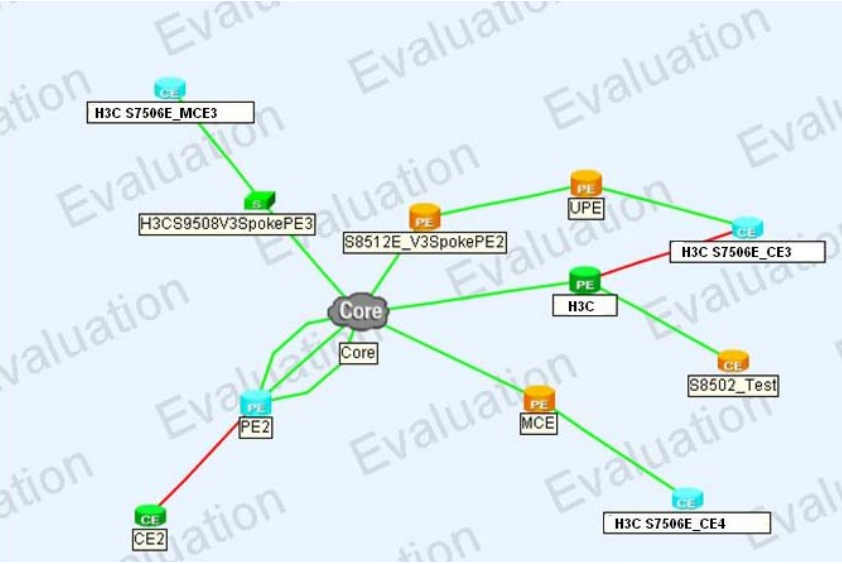


图4 L3 VPN：接入拓扑示例

在接入拓扑（包括全网拓扑）上能够进行系统的大部分操作，如查看链路信息、添加链路、部署以及拆除部署、设备同步、查看配置变更信息、连通性审计，针对某个PE进行自动发现等。

2. 业务拓扑

业务拓扑反映VPN中CE之间的连通性关系。如果两个CE之间有链路，则表示这两个设备应该互通（从RT关系看），而链路颜色代表了实际的连通状态。

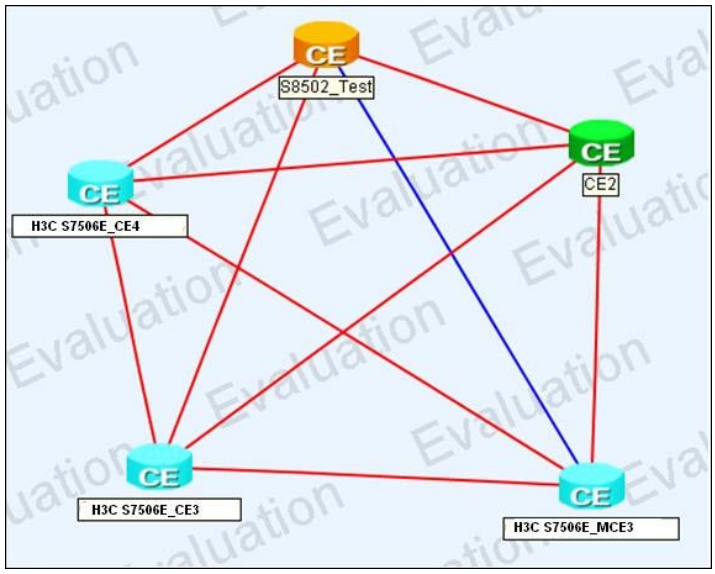


图5 L3 VPN：业务拓扑示例

在业务拓扑上能够针对链路或者整个VPN进行连通性审计，可以查看链路的连通性审计信息

流量监控

包括设置VPN流量监控和SA流量监控。

SA的流量监控对象是PE上绑定VRF的接口流量。

VPN的流量实际上是VPN下的各SA的流量进行汇总从而得到VPN的流量。

MVM提供了对VPN和SA流量的流量统计和报表功能，为用户提供流量概况和精细化两个角度的趋势分析能力。

对于已经设置监控的VPN和SA，能够通过多种形式查看流量报表。 如流量提供柱图、折线等图表显示方式，为预测资源的利用情况和发展趋势提供了方便的手段。流量统计结果可以按照日、月、年的方式进行报表输出，支持Html、PDF等多种格式，满足各种汇报和分析数据的需要。

图6 L3 VPN：流量监控示例

审计管理

审计包括配置审计、连通性审计和故障定位功能

1. 配置审计

当进行设备同步时（立即同步或自动同步），自动触发配置审计功能，比较网管配置和设备当前配置的差异，对业务差异产生配置审计告警，并在拓扑上直观显示

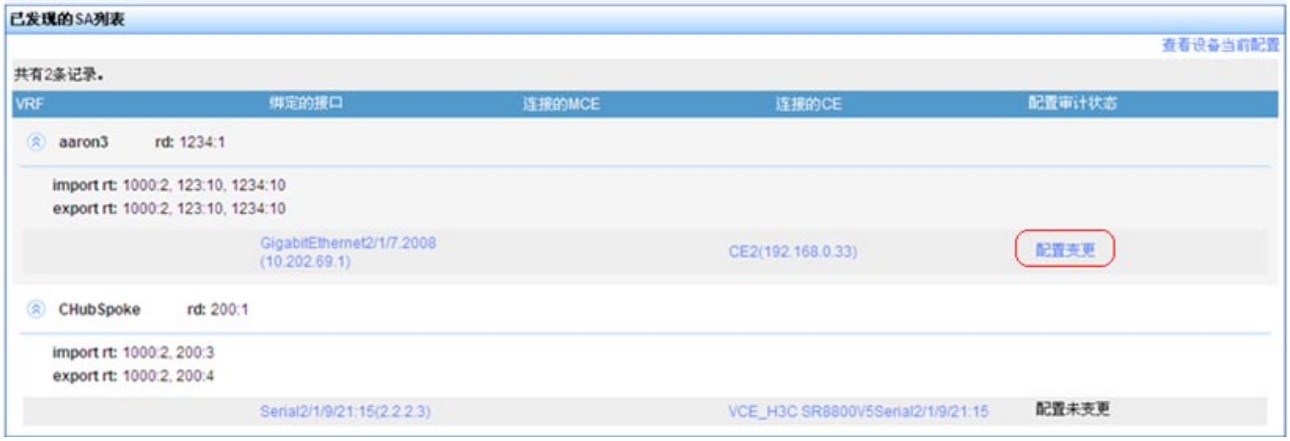


图7 L3 VPN：配置审计示例

2. 连通性审计

对于VPN或指定的CE－CE链路能够进行连通性审计，用户可以根据审计结果直观地看到连通性是否和预期一致。对于与预期不一致的，系统将生成连通性审计告警。用户可通过该功能判断业务运行是否正常。

连通性审计的原则是：先进行一段式Ping，若Ping不通再进行三段式Ping；双归属链路直接采用三段式Ping。

一段式Ping的条件：本端CE和对端CE都可管理；本端CE可管理，对端CE不可管理但接口配置了IP地址。

采用三段式Ping的链路，审计包括三段：

◆ 本端PE到本端CE；

◆ 本端PE到对端PE；

◆ 本端PE到对端CE。同时支持多路径审计（双归属的情况），当CE接口未配置IP地址时连通性通过所连接PE接口的状态确定。

图8 L3 VPN：联通性审计示例

3. 故障定位

主要是通过各种检测手段进行故障定位（Trouble Shooting）。用户能够准确快速的定位出MPLS网络中OSPF、MPLS、BGP的故障信息。例如，OSPF没有建立Peer，某个接口down或者没有绑定VRF等故障信息，维护人员可以根据定位信息去检查网络，排除故障。

定位检测可以分为三个部分：CE-PE 之间的检测，PE-PE之间的检测和边缘PE设备之间的检测。

CE-PE间的检测包括：

1、VRF绑定

2、链路层检测

3、OSPF层检测

PE-PE之间的检测包括：

1、MPLS层检测

2、BGP层检测

边缘PE设备检测，主要是指PE本身功能的检测，其中包括：

1、VRF匹配

2、路由引入

3、多个下一跳

主要检测手段包括ping (LSP Ping)，提取协议的状态信息，如BGP/OSPF/LDP的协议状态信息，提取接口信息，配置检查等等方式。

故障定位

故障定位完成。

时间	源设备	目的设备	结果
2012-02-21 17:38:35	--	--	故障定位结束。
2012-02-21 17:38:35	H3C (10.153.146.141)	H3C (10.153.146.143)	设备H3C(10.153.146.143)发现故障，设备上接口Vlan-interface1没有绑定VRF。
2012-02-21 17:38:34	ssssssssssss (10.153.146.145)	H3C (10.153.146.143)	未发现故障。
2012-02-21 17:38:33	qqqqqqqqqqqqqqq (10.153.146.146)	ssssssssssss (10.153.146.145)	未发现故障。
2012-02-21 17:38:29	--	--	故障定位开始。

图9 L3 VPN：故障定位示例

告警管理

包括设备告警、VPN连通性审计告警、配置审计告警；可以查看VPN的告警、设备告警，对未确认告警进行确认（支持批量确认VPN告警）；告警能够在拓扑上直观反映

告警级别	告警来源	告警信息	确认状态	告警时间
警告	S8508-V5_H3C(192.168.0.1)	MPLS VPN Manager发现设备"S8508-V5_H3C (192.168.0.1)"新增VRF:yb RD:70:60 ImportRT:25:25 ExportRT:25:25。	未确认	2008-02-27 11:48:17
警告	S8508-V5_H3C(192.168.0.1)	MPLS VPN Manager发现设备"S8508-V5_H3C (192.168.0.1)"新增VRF:vrf_57572:2367 RD:57572:2367 ImportRT:1000:1 ExportRT:1000:1。	未确认	2008-02-27 11:48:17
警告	S8508-V5_H3C(192.168.0.1)	MPLS VPN Manager发现设备"S8508-V5_H3C (192.168.0.1)"新增VRF:vrf_55563:30967 RD:55563:30967 ImportRT:100:30 ExportRT:100:50。	未确认	2008-02-27 11:48:17
警告	S8508-V5_H3C(192.168.0.1)	MPLS VPN Manager发现设备"S8508-V5_H3C (192.168.0.1)"新增VRF:vrf_48289:56965 RD:48289:56965 ImportRT:1000:2 ExportRT:1000:2。	未确认	2008-02-27 11:48:17

图10 L3 VPN：告警管理示例

其它功能

1. MPLS VPN资源管理

系统提供了便捷的方式增加VPN资源。VPN资源包括：PE、CE、VPN。PE和CE资源可以直接从基础网络资源导入，而VPN资源用户既可以手工增加，也可以利用自动发现功能构建。

2. MPLS VPN分组管理

MVM支持将已发现的VPN按照网络的实际情况或者用户希望的方式进行组合。这在网络非常庞大时，可以按客户、按种类等分组方法，把VPN分到不同的分组中。

3. 支持管理VPN

通过建立管理VPN，可以把CE设备纳入网管系统。此时能够支持对CE进行拓扑、告警、性能等与PE设备类似的网管功能。为了使管理VPN的建立不干扰业务VPN的发现和管理，MVM提供对管理VPN的设置和过滤，使两者互不干扰。

MPLS L2 VPN管理组件

简介

iMC L2 VPN管理模块实现对各种L2 VPN组网类型的管理支持，包括：VPLS、分层VPLS、VLL、PBB（MAC-in-MAC），以及VLL与VPLS混合组网方式，PBB与VPLS的混合组网（H3C特有双栈方案）等组网形式。

主要功能

业务发现

通过智能自动发现可以帮助用户快速发现当前VPN各种组网状况，实现业务还原。

支持多种方式的L2 VPN业务发现，包括VPLS（支持分层VPLS业务发现）、VLL、PBB以及各种混合组网的业务发现。能够自动计算PE与CE的连接关系。某些情况下，网管如果无法管理到CE，可以在自动发现过程中，提供自动创建CE的功能。

如图11所示，指定对应的PE设备后，进行“自动发现”，能够迅速发现网络中的L2 VPN业务。

图11 L2 VPN：业务发现

业务部署

通过基于拓扑向导的端到端的部署流程，帮助用户快速开通E-Line、E-LAN等L2 VPN业务。在部署过程中，支持部署向导化，部署导航可视化。提供良好的操作体验。

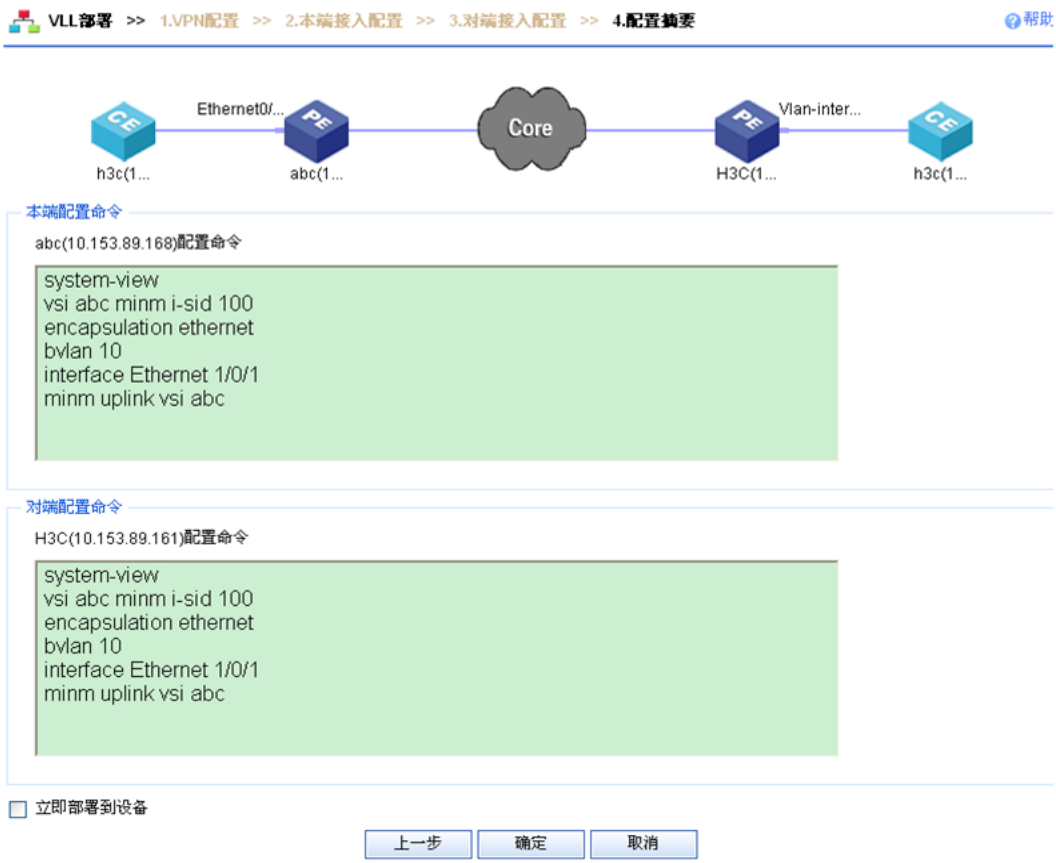


图12 L2 VPN：业务部署

不仅支持VPN部署，而且支持VPN业务拆除。部署结束后，能够通过在VPN拓扑上查看设备之间的连通性状态，充分验证部署的正确性。

支持设备预部署功能，可以根据规划在网管系统中进行部署演习，对于不合适的配置信息进行修改、删除操作，而不影响实际业务运行，经过确认后对各个VPN部署信息统一下发到设备上。

拓扑管理

通过业务拓扑，用户能够实时观测VPN链路状况；支持L2 VPN拓扑业务展示，能够展示PE与PE之间PW关系以及PE与CE之间的链路连接关系。

在L2 VPN的拓扑上，可以体现各种监控状态，如：PE、CE的告警状态、PW审计状态、PE和CE间链路连通状态、PE设备配置状态等。

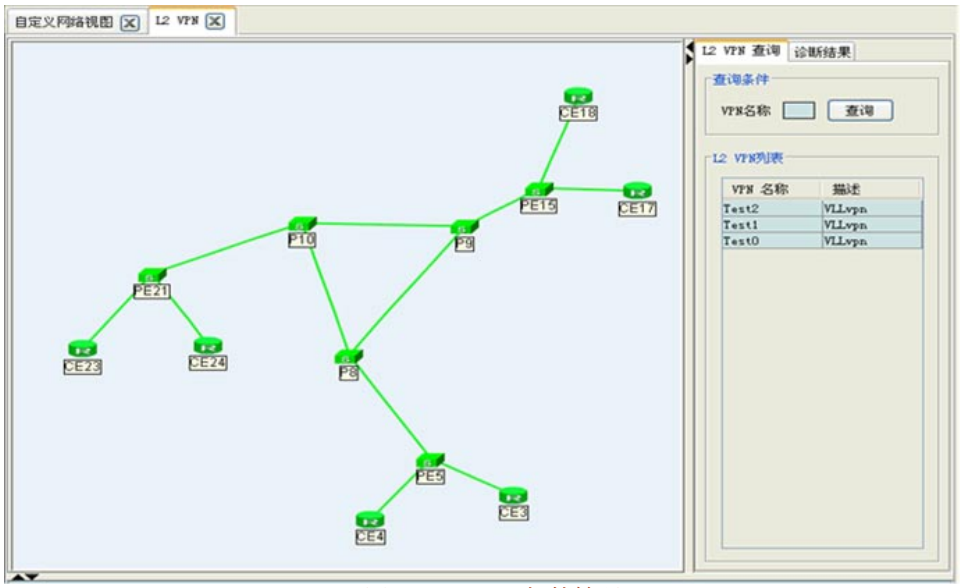


图13 L2 VPN：拓扑管理

业务审计和监控

业务审计模块可以实现对VPN故障进行检测和分析。

PW连通性审计，帮助用户方便快捷地了解网络中PE设备间连通情况。审计发现的问题，可以在VPN拓扑上实时反映。

通过PE设备配置审计，可以有效管理PE设备配置信息，提高网络访问安全。配置审计将设备当前的实际配置信息与网管上的配置信息进行比较，审计结果会在变更信息页面进行显示，也会直观的反映在视图中。

其它功能

1. 设备管理

iMC L2 VPN提供统一的设备管理功能，包括PE设备管理和CE设备管理。提供统一的管理界面，能够对网络中的设备类型和数量有总体的了解。同时提供状态列，反馈设备当前状态信息，便于了解VPN网络中设备情况。

在设备管理中，提供导入设备功能，能够方便地将PE、CE设备加入到网管中。同时在PE设备列表中，能够方便地检查设备配置信息是否发生改变。

支持虚拟CE。由于CE设备的多样性，部分CE设备可能是不可管理的，管理员可以创建虚拟CE。虚拟CE同样代表了一个客户接入点，利用虚拟CE设备不仅能够体现PE设备和客户站点之间的连接关系，而且能够体现客户接入点之间的连通性。

支持直接查看PE、CE设备的详细信息。除了基础网络资源的信息，还可以查看PE设备的VPN配置信息，包括VPLS、VLL以及PBB的配置相关信息。

2. VPN资源管理

iMC L2 VPN将L2 VPN网络中的VPN信息、AC信息统一作为网络资源管理起来。用户既可以手工增加VPN和AC资源，也可以利用自动发现功能构建这些网络资源。

针对VPLS网络，以VSI ID作为VPN唯一标识；对于VLL类型VPN，以PW ID作为发现VPN的关键指标；对于PBB网络，以I-SID作为VPN特征点。

AC资源信息主要描述网络中PE的接入信息。

3. 安全策略

iMC L2 VPN提供严格而灵活的访问控制策略，支持密码复杂度设置。iMC L2 VPN还引入了角色概念，管理员可以定义每种角色具备的操作权限和管理范围，使得特定客户只在合理授权下管理网络。完善的操作日志记录，为事后审计提供了丰富的信息。

MPLS TE简介

MPLS TE Manager提供了一个简单、高效的可视化管理工具，帮助管理员管理网络的运行状况，合理分配网络资源。如：为某条重要业务在网络上开拓一条专用隧道，从而保证沿途的带宽，保障业务运营的稳定性。管理员可以通过拓扑查看全网TE设备的分布连接情况。增加设备的隧道并将其发布到路由中，这些隧道只有特定业务的流量可以通过，从而保证特定业务通畅稳定。

MPLS TE Manager提供七大类功能：TE拓扑、资源管理、RSVP-TE高级特性、MPLS TE隧道管理、显式路径管理、保护管理、流量接入管理。

1. TE拓扑

实现MPLS TE Tunnel信息的图像化管理，直观地反映了网络的性能状况，为管理员优化网络性能

提供了依据。

该功能除了可以查看TE链路信息，还具有Tunnel过滤、链路管理组属性过滤等功能。

◆ 选择“按设备Tunnel过滤”时，在拓扑图上将突出显示指定设备上的隧道；

◆ 选择“按链路管理组属性过滤”时，在拓扑图上将突出显示符合链路组管理属性的所有链路。

2. 资源管理

该功能用于管理MPLS TE系统的资源，包括设备资源和接口资源。

◆ 设备管理：用于导入、同步支持MPLS TE特性的设备，查看已导入设备的信息，并对已导入设备进行CR-LSP仲裁方法、流量转发参数、FRR扫描间隔、自动带宽调整使能等操作。

◆ 接口管理：可以完成MPLS TE设备的所有接口配置，实现了MPLS TE功能。该功能也可以设置设备接口上的流量参数。当链路带宽发生变化时，可能导致重新计算路径，这样会消耗大量资源。因此可以通过限定当带宽变化到达一定限度时才进行泛洪。

3. RSVP-TE高级特性

◆ 设备RSVP-TE：实现MPLS TE设备的RSVP-TE功能，进行MPLS TE设备的RSVP-TE的配置。

◆ 接口RSVP-TE：实现MPLS TE接口的RSVP-TE功能，进行MPLS TE接口的RSVP-TE的配置。

4. MPLS TE隧道列表

用于对MPLS TE隧道进行查询、增加、修改、删除操作，同时可以查看某条隧道相关的保护信息及拓扑信息，包括静态隧道和动态隧道。

5. 显式路径管理

配置设备的显示路径，供动态Tunnel引用。

6. 保护管理

该功能提供对隧道保护的查询、绑定、拆除、自动发现操作。包括路径保护和节点保护。

7. 流量接入管理

该功能提供对流量接入的查询、增加和删除操作。配置流量接入后，可以将流量引入到特定的隧道上。

附录：参考文档

[1]《H3C智能管理中心 MPLS VPN Manager介绍》

[2]《iMC L2 VPN管理产品概述》

[3] iMC帮助文档

应用与服务健康管理

文/曾劼

前言

随着Web2.0、云计算、数据中心等信息技术的飞速发展，企业的各种业务已经越来越紧密地与Internet结合在一起，IT在办公及生产应用系统的重要性越来越高，业务部门要求IT服务部门通过服务水平管理来保证其服务有效，建立服务健康水平监督体系，来保证服务达到规定的健康水平等级，同时由于服务器、数据库、中间件等组成的应用信息系统越来越复杂，对IT技术人员的要求变得越来越高，各种突发故障排除起来也越来越困难。

场景一：国内某大型汽车制造商，ERP 是其至关重要的生产业务管理系统，该公司平均每1到1.5 分钟下线一台车，运行一段时间后发现ERP 系统反应变慢，已经跟不上生产节奏，如果因ERP 系统造成停产，企业一天就将损失几千万元。

场景二：某大型在线旅行服务公司，其在线旅行订购系统作为最重要的业务系统，要求在高性能下不间断地运行，这套在线订购系统运行一段时间后，维护人员发现系统运行很慢，性能上出现了问题，而且资源占用率非常高，但找不出瓶颈在什么地方。

因此，很多企业急需一套易于部署、功能全面、扩展灵活的IT运维管理解决方案，满足其不同层次的应用管理需求，一旦服务出现故障，可以快速并正确地分析原因，帮助IT服务部门做出正确的应对决策。

应用管理

常用监控方式对比

目前常用的监控方式分为Agent方式和Agentless方式，Agent方式需要维护人员在每台主机上部署一个监控代理，然后监控代理负责采集数据并传输给服务器。Agentless方式则不需要部署监控代理，服务器通过一些通用的协议和接口去直接采集主机的信息。

国外主流应用监控厂商常采用Agent方式进行监控。下表是Agent与Agentless在应用监控方面的一个对比。

监控方式 对比项	Agent方式	Agentless方式
对监控资源的影响	占用一定的CPU和内存运行Agent代理软件本身。	除了Telnet/SSH/WMI对CPU和内存的影响，其他几乎可以忽略。
对监控服务器的影响	大部分工作通过监控资源端的Agent代理软件完成，对监控服务器的影响相对较小。	所有工作通过监控服务器远程连接监控资源端实现，对监控服务器的影响相对较大。
通讯对网络带宽的影响	在监控资源端采集的数据，经过压缩处理后，传输给监控服务器，故对网络带宽的占用较低。	监控服务器直接采集监控资源端的数据，并传输回监控服务器，数据都未经压缩和汇总，故数据量相对较大。
监控指标	Agent代理监控方式一般都支持二次开发，监控用户关心的独特指标。	提供了二次开发接口，通过脚本语言等方式自行开发获取监控数据，按指定格式输出实现监控。
部署方式	部署相对麻烦，需要每台主机部署安装。	只需要开通相应的协议和端口，几乎不需要部署。

通过对比可以发现，Agentless在功能、资源影响上并不逊色于Agent方式。从部署的简易性、对业务系统的影响程度、监控的安全以及稳定性等多方面考虑，Agentless方式无疑更为通用。

iMC应用管理组件

iMC应用管理组件（iMC Applications Manager，iMC APM）是为了满足企业各种业务的监控管理需求而提供的应用监控管理解决方案，采用易于部署的Web架构，基于最新的 Agentless技术，无需在被监控的服务器上安装监控代理，就可以通过Telnet、命令行等方式，对关键应用或资源进行远程监控，避免安装监控代理后对服务器造成的影响。iMC APM提供强大的系统与应用监控管理能力，可以对不同的业务系统、应用和网络服务（如服务器、操作系统、数据库、Web服务、中间件、邮件、其他关键应用等），进行远程监控和管理，从而充分满足用户对各种关键业务和数据中心的监控管理需求。在应用监控的基础上，结合告警、报表等功能，对网络中的所有应用进行可用性和健康度评价，帮助网络管理员了解网络应用的运行状况，并及时发现网络应用的隐患。

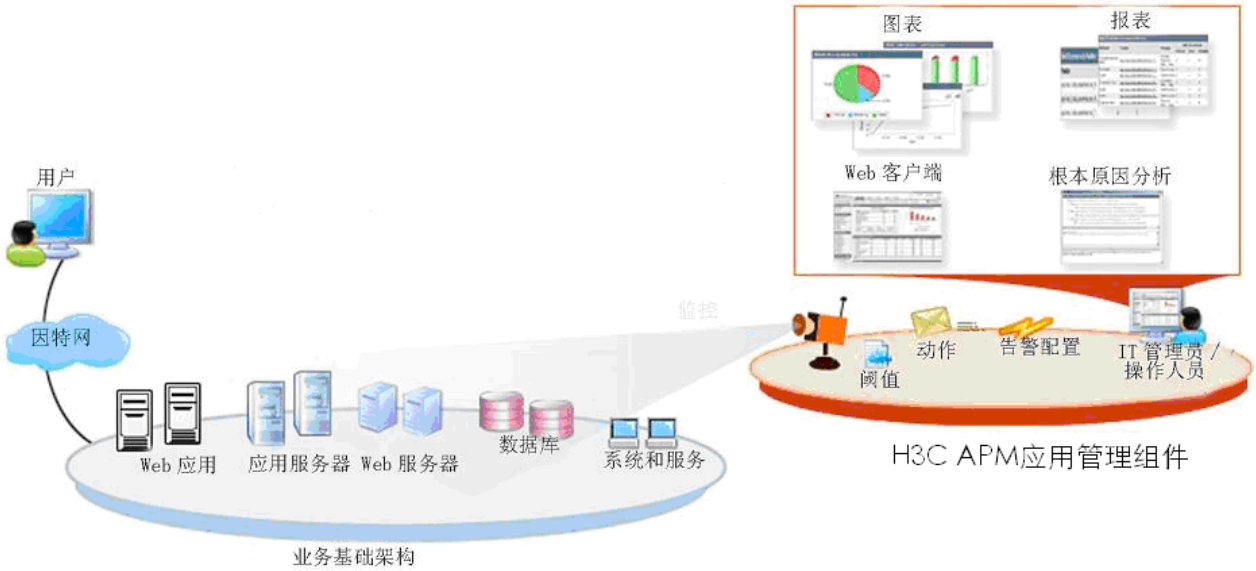


图1 应用管理功能示意图

iMC 应用管理组件系统结构

如图2所示，APM系统从架构上分为三个层次：性能采集器、数据处理层和性能展示层，系统支持的监视器类型和对应的指标控制信息通过指标配置文件进行说明。

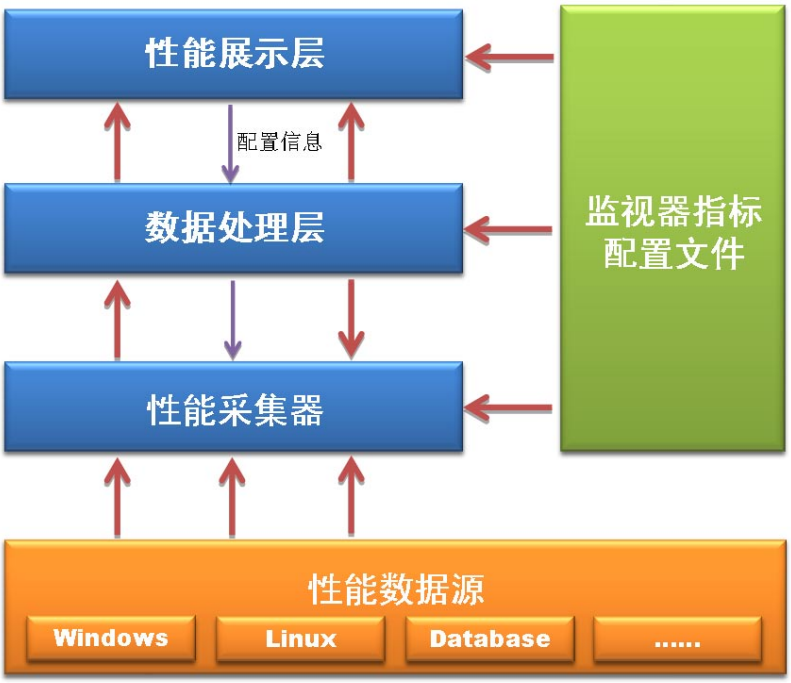


图2 应用管理组件系统结构

iMC 应用管理组件包括APM模块和APM-Server模块，其中APM模块主要是APM的应用管理和应用监视部分，APM-Server模块主要负责APM自动发现和APM指标数据获取。

iMC应用管理组件特点

APM具有应用监视、主机监视、融合管理等诸多特点，下面将主要几个特点展示给读者。

◆ 应用监视

应用监视能够监视各种应用程序和服务器，包括：Windows服务器、Unix服务器、Linux服务器、数据库、应用服务器、Web服务器、邮件服务器、Web服务、LDAP服务等。

图3 应用监视

◆ Windows服务器包括：Windows XP、各版本的 Windows Server。

◆ Unix服务器包括：AIX、FreeBSD、OpenBSD、Solaris、Mac OS、HP-UX。

◆ Linux服务器包括：Linux。

◆ 数据库服务器包括：Oracle（8.x/9i/10g/RAC/11g）、MySQL（3.23.x/4.x/5.x）、MS SQL Server（2000/2005/2008）。

◆ 应用服务器包括：.Net服务器、JBoss服务器、Tomcat服务器。

◆ Web服务器包括：Apache 服务器、IIS服务器。

◆ 邮件服务器包括：Exchange 服务器（2003/2007）。

◆ Web服务包括：REST服务、SOAP服务。

◆ LDAP包括：Active Directory服务。

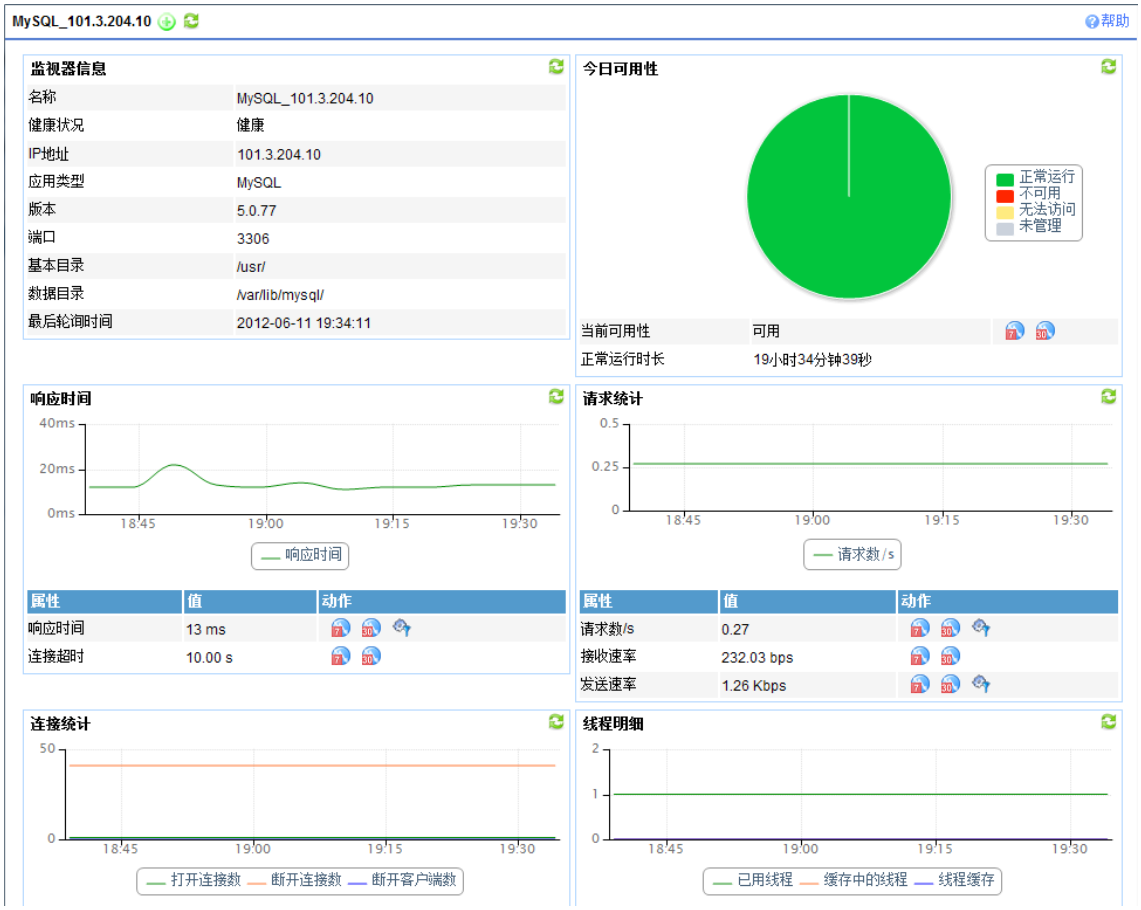


图4 MySQL应用监视

MSSQL_101.3.202.30 帮助

监视器信息

名称	MSSQL_101.3.202.30
健康状况	健康
IP地址	101.3.202.30
应用类型	SQL Server
版本	Microsoft SQL Server 2008 - 10.0.4000
端口	1433
最后轮询时间	2012-06-11 19:32:37

今日可用性

正常运行
不可用
无法访问
未管理

当前可用性	可用
正常运行时长	19小时37分钟31秒

内存使用情况

500MB
250MB
0MB
18:45 19:00 19:15 19:30

SQL缓冲内存 优化内存 锁内存 连接内存

属性	值	动作
内存总数	5.89 GB	
SQL缓冲内存	27.22 MB	
优化内存	1.04 MB	
锁内存	339.16 MB	
连接内存	1.44 MB	
分配工作区内存	0.00 KB	
内存分配未决进程	0	
内存分配成功进程	0	

缓冲区管理

100%
0%
18:45 19:00 19:15 19:30

缓冲区命中率

属性	值	动作
缓冲区命中率	100.00 %	
每分钟查找页数	57,883	
每分钟已读页数	0	
每分钟已写页数	0	
总页数	771,673	
数据库页	395,423	
空闲页	278	

连接统计

50ms

缓存明细

100%

图5 SQL Server应用监视

ActiveDirectory_101.3.200.10 帮助

监视器信息

名称	ActiveDirectory_101.3.200.10
健康状况	健康
IP地址	101.3.200.10
应用类型	Active Directory服务
最后轮询时间	2012-06-11 19:37:20

今日可用性

正常运行
不可用
无法访问
未管理

当前可用性	可用
正常运行时长	19小时40分钟15秒

网络监控

5
0
18:45 19:00 19:15 19:30

AB客户端会话数

属性	值	动作
AB客户端会话数	4	
DS通知队列大小	0	

数据库

50MB
25MB
0MB
18:45 19:00 19:15 19:30

文件大小

属性	值	动作
文件大小	36.02 MB	

NTFRS进程

100%
0%
18:45 19:00 19:15 19:30

CPU利用率(%)

属性	值	动作

LSASS进程

100%
0%
18:45 19:00 19:15 19:30

CPU利用率(%)

属性	值	动作

图6 ActiveDirectory应用监视

从图4、图5、图6可以看出，iMC APM不但可以监控多种应用，还可以根据应用的不同选择不同的性能指标展示给用户。

◆ 主机监视

iMC APM从应用所在服务器/PC的角度提供了应用监视的功能，可方便地查看到各服务器/PC自身和部署应用的运行情况。图7和图8分别展示了iMC APM对于WindowsServer以及Linux的主机监视功能。

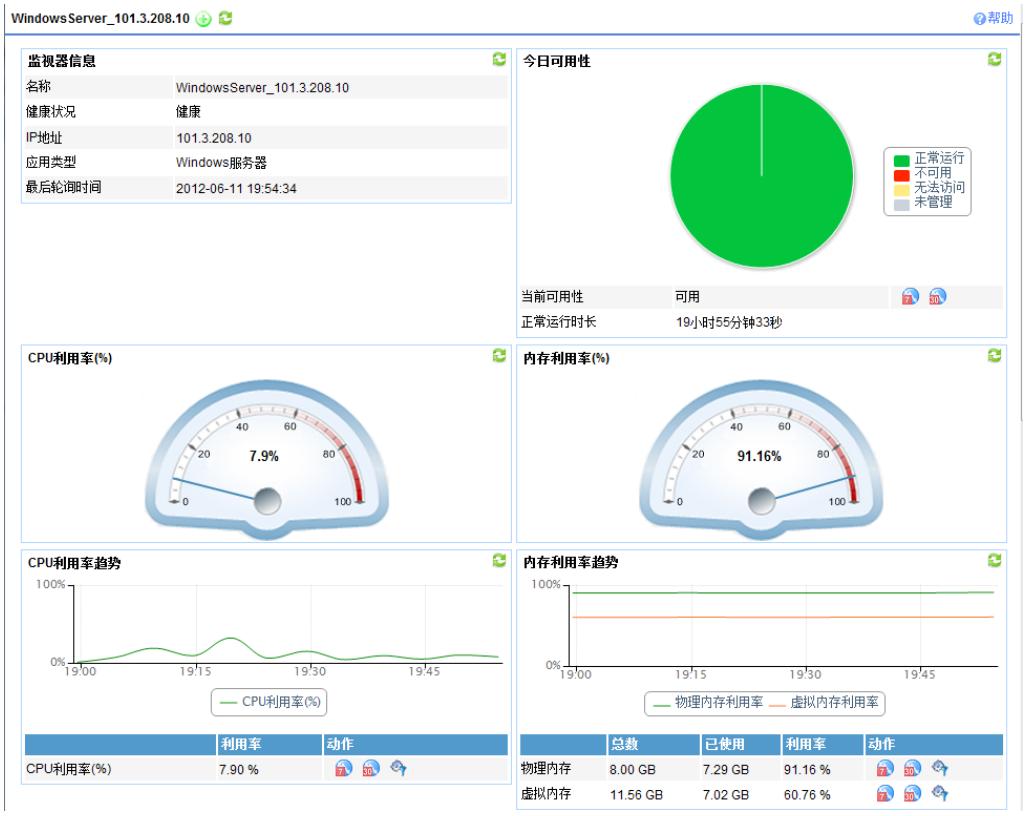


图7 WindowsServer主机监视

图8 Linux主机监视

◆ 融合管理

APM作为iMC的一个组件，与iMC智能管理中心平台无缝融合，监控的应用所在主机均被 iMC管理，不仅可以从业务的角度进行管理，也可以从网络的角度直接监控业务。

首页查看：可在iMC首页查看资源的简要状况，包括应用名称、可用性、健康状况等，点击超链接，可进入应用性能详细情况。

图9 首页查看

告警联动：查看APM告警的详细信息时，点击告警分类的链接可直接联动到该应用的报告页面。

图10 告警联动

小结

iMC应用管理产品主要应用于企业数据中心网络，对数据中心涉及应用服务器、数据库、操作系统、邮件服务器、Web服务器、服务等应用进行数据采集和监控。提供了自动发现应用、应用监视、主机监视、分类监视、应用分组等模块，同时拥有报表功能。当被监视的应用出现异常时，iMC应用管理就会产生告警，通过这些告警，可以鉴别出问题的根本原因。

服务健康管理

IT运维的现状

根据IDC的数据分析，自1999年至2010年，全球各公司对于IT部门的投入从1140亿美元增长到了2150亿美元，随着新设备采购成本的降低，越来越多的资金投入到了管理和维护中去，2010年管理和维护的成本已经占到了全年总投入的71%。

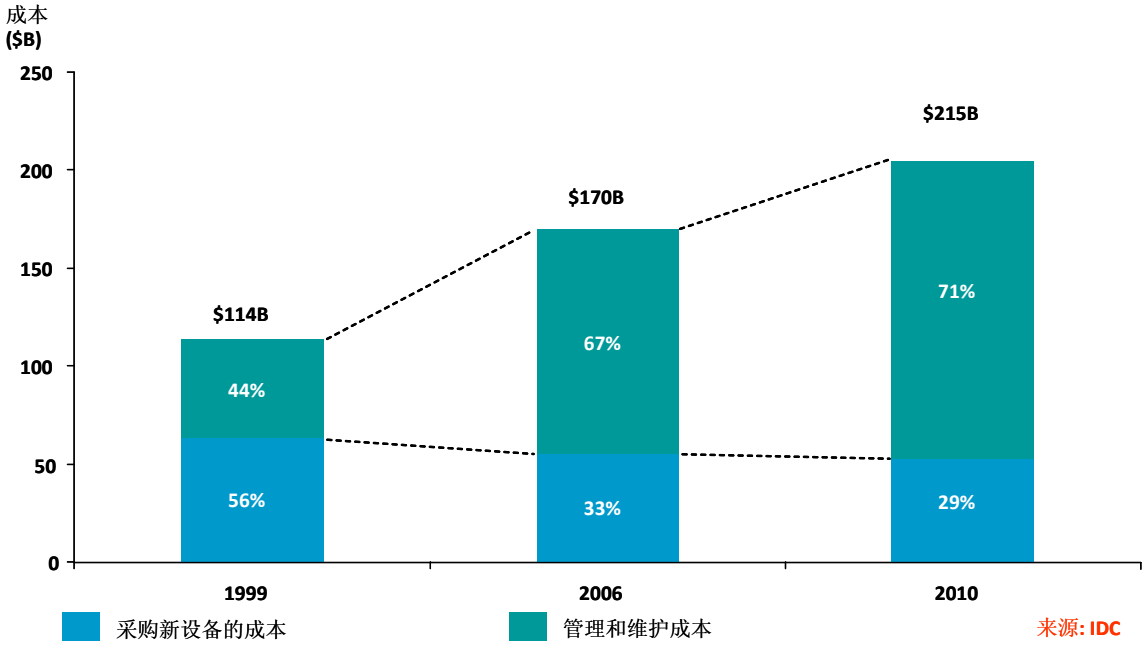


图11 IT部门成本分析

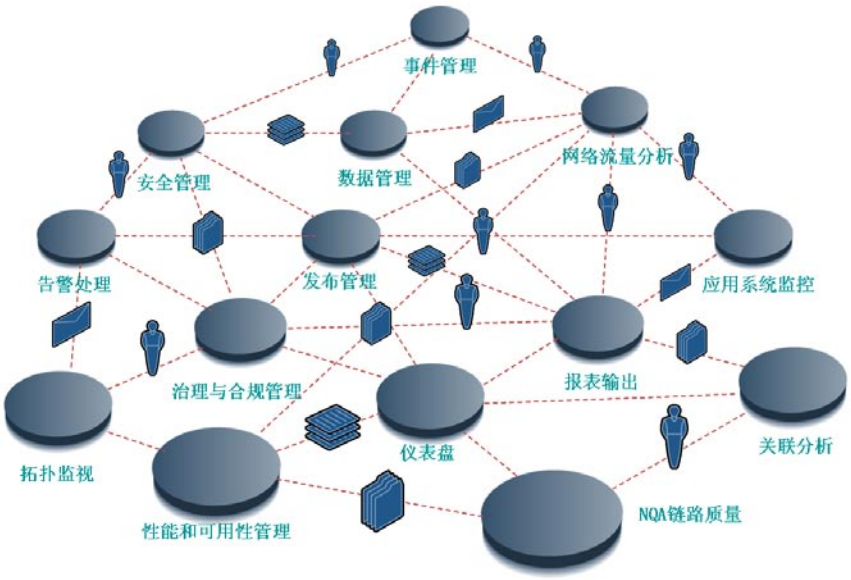


图12 割裂的管理孤岛

目前，IT运维的现状就像一个个被割裂的管理孤岛，IT管理员只能被动的响应。如何降低IT成本、提升服务质量、控制风险、增加对业务的影响并提供可视性成为了众多IT管理者思考的问题。

iMC服务健康管理组件

iMC SHM服务健康管理组件（iMC Service Health Manager，iMC SHM），定位于IT服务的健康监控管理方案，基于iMC系统的性能、告警、NQA链路监控，NTA网络流量分析等业务模块，提取关键性能指标（KPI），建立服务各个方面质量的度量指标（KQI）以及服务整体质量的度量模型（SLA），基于服务可用性、MTTR平均修复时间、MTBF平均无故障时间等的监控和分析对服务的健康水平做出评价。

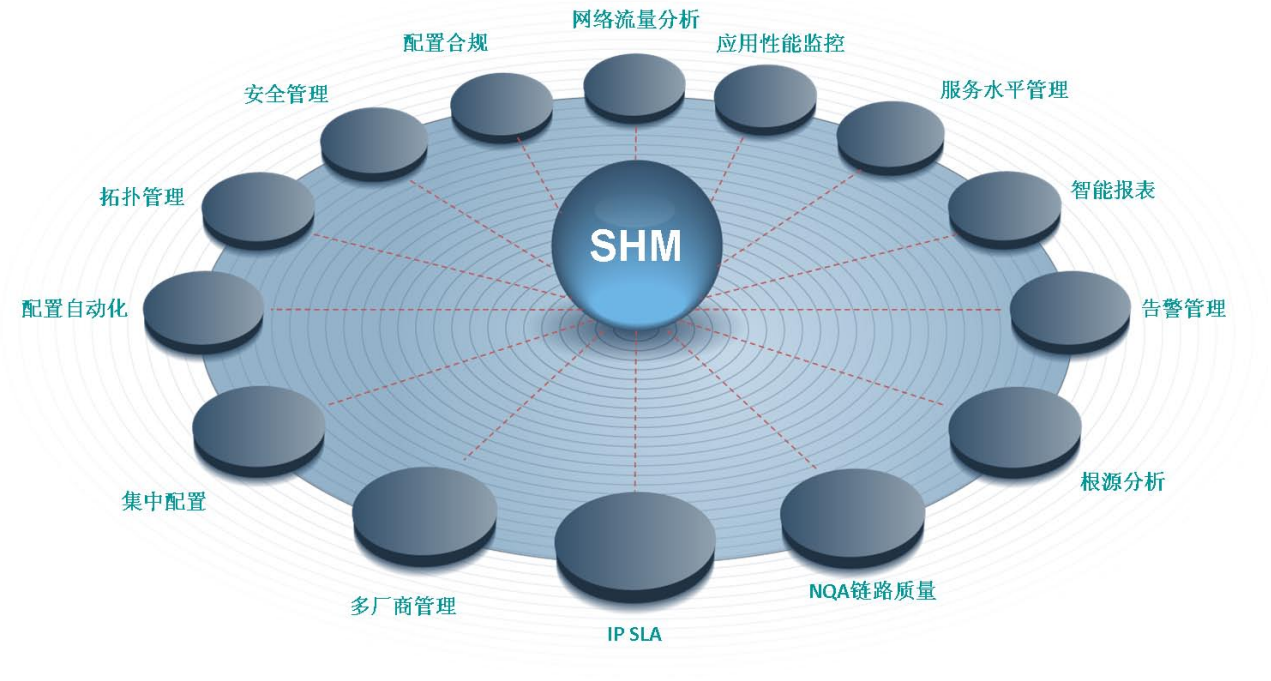


图13 iMC SHM服务健康管理组件

SHM组件包含NQA管理和服务健康管理两大部分，定位于IT服务的健康监控管理方案。

NQA管理

使用NQA配置管理功能定义系统的基本资源，包括NQA设备、NQA种类、NQA等级和基本指标的配置，用户可在系统预定义的NQA种类和NQA等级的基础上增加需要的配置项，然后在NQA管理中利用前面定义的配置，选择合适的监控设备，明确网络中需要度量目标，建立用户关注的NQA实例，系统将对这些实例定期进行采集，以便用户对网络当前的运行情况给出评价。

NQA管理支持H3C、Cisco、Huawei等多厂家设备，同时支持语音、视频、网络链接、VRF等业务的时延、抖动、丢包、吞吐量等质量指标的监控，并且允许管理员对各项基本指标的参数进行修改；可以测量UDP响应时间、单项延时、抖动、丢包率、设备连通性、DNS查询、TCP链接、每一跳ICMP响应时间和抖动、HTTP处理时间等多项质量指标。

基本指标

刷新

共有15条记录。

基本指标名称	基本指标描述	所属指标组
ICMP Echo	ICMP Echo 指标	基本特性组
UDP Echo	UDP Echo 指标	基本特性组
TCP Connection	TCP Connection 指标	基本特性组
HTTP	HTTP 指标	高级特性组
DLSw	DLSw 指标	高级特性组
DHCP	DHCP 指标	高级特性组
FTP	FTP 指标	高级特性组
UDP Jitter	UDP Jitter指标	高级特性组
Voice	Voice指标	高级特性组
HW UDP Echo	HW UDP Echo 指标	HW特性组
HW TCP Connection	HW TCP Connection 指标	HW特性组
H3C UDP Echo	H3C UDP Echo 指标	H3C特性组
H3C TCP Connection	H3C TCP Connection 指标	H3C特性组
Cisco UDP Echo	Cisco UDP Echo 指标	Cisco特性组
Cisco TCP Connection	Cisco TCP Connection 指标	Cisco特性组

图14 NQA管理基本指标

服务健康管理

服务健康管理包括KQI管理，服务等级以及SLA服务。

KQI管理用于提供服务管理中关于KQI的相关配置信息。KQI作为服务质量可视化评价的参考原型，提供了选择不同的KPI、应用不同的计算方式及划分不同的评分规则等功能。KQI的类型包括预定义和自定义的。

KQI列表

增加 删除 刷新

共有8条记录，当前第1 - 8，第 1/1 页。

名称	描述	类型
NQA链路质量	NQA链路质量类KQI	预定义
NQA语音质量	NQA语音质量类KQI	预定义
接口流量	接口流量	预定义
接口性能	接口性能	预定义
设备告警状态	设备告警状态	预定义
设备状态	设备状态	预定义
应用流量	应用流量	预定义
主机流量	主机流量	预定义

图15 预定义KQI列表

服务等级用于定义服务的级别，并在创建SLA过程中进行引用。

图16 自定义服务等级

SLA服务以树表格的形式展示各服务及服务度量指标的健康状态。列表内容包括：服务名称、服务健康状况、违例、状态、当前可用性，今天健康状况、本周健康状况、本月健康状况、本年健康状况。其中服务和KQI以6种健康状态展示服务健康状况及4种可用性状态展示服务和KQI的当前可用性。健康状况包括：优秀、良好、一般、较差、极差、无数据。可用性状态包括：可用、部分可用、不可用、无数据。并且提供服务的查询功能，查询条件包括：服务名称、评价状态，可用性。

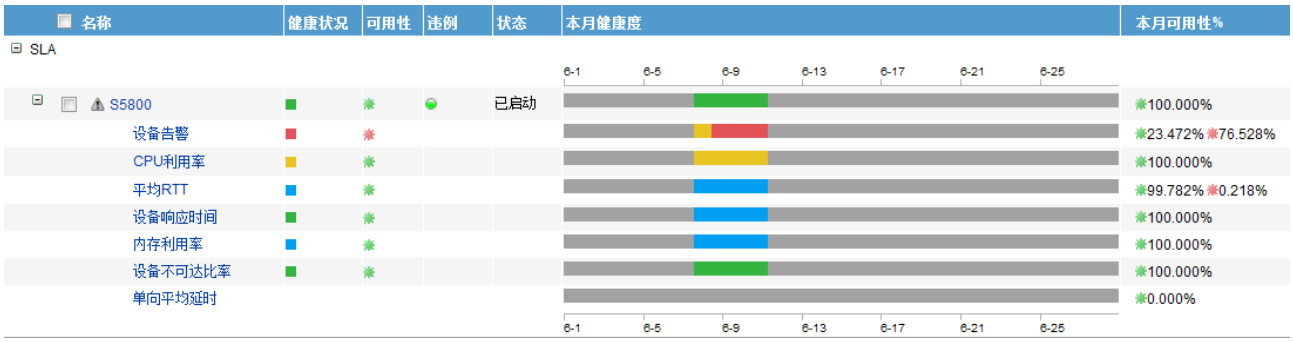


图17 SLA服务中设备健康状态评价

SLA建模流程如图18所示。

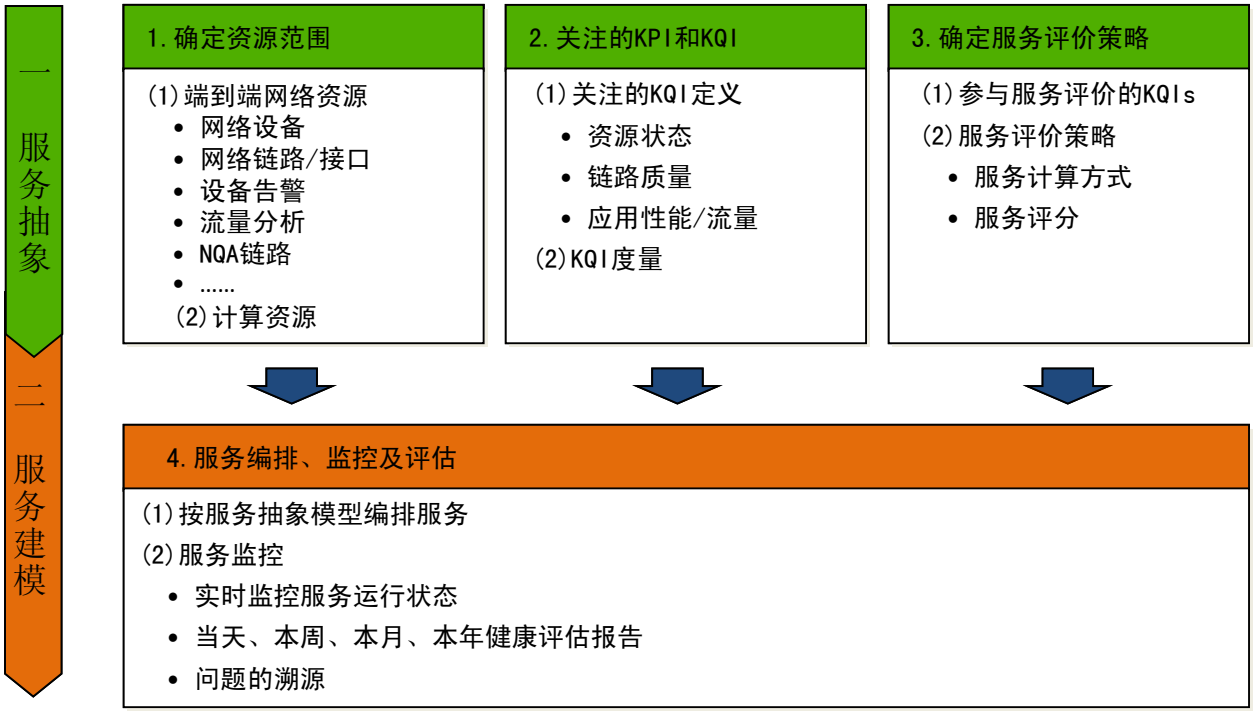


图18 SLA建模流程

小结

iMC SHM的出现，解决了IT运维中管理孤岛的问题，该组件基于iMC各个业务组件，包括平台（告警、性能）、NQA、NTA及APM等提炼KPI指标，预定义设备监控、接口监控、NQA语音、NQA链路、NTA流量分析等五类KPI；在KPI的基础上，SHM提供NQA链路质量、NQA语音质量、接口流量、接口性能、设备告警状态、设备状态、应用流量、主机流量、主机应用等九大类KQI，并提供各业务组件扩展机制，真正实现iMC平台及各组件对网络各角度性能数据的可度量定义。

前言

IT网络运维服务的管理随着ISO20000、ITIL v3.0的发布和推广，已经形成了事实上的标准，在当今企业IT管理领域已经是非常迫切的需求。特别是ISO20000的认证要求，已经成为企业越来越普遍的需求。

iMC服务运维管理产品（iMC Service Operation Manager，iMC SOM）是面向企业IT网络运维服务的管理解决方案，关注ITIL服务生命周期中关键的服务转换和服务运营部分，聚焦于和IT网络基础架构管理关系紧密的运维流程的支持能力。SOM通过流程化管理能力，使所有的IT运维活动（比如配置的变更、故障问题的处理）做到可控、可度量、可审计。

ITIL

ITIL概念

ITIL (Information Technology Infrastructure Library) ——IT基础架构库，IT服务管理的最佳实践框架（ISO 20000是对IT服务管理体系的要求&标准、或者说是IT服务管理实践的要点）。

ITIL强调基于“以流程为中心，以客户为导向”的IT管理理念，将传统的IT管理活动按照流程的方式重新加以组织，并强调根据客户和业务需求提供质量可靠、成本合理的IT服务。基于ITIL提供IT服务，可以确保企业充分利用其技术和人力资源，并确保业务需求能够以最低的成本得到满足。

ITIL简史

◆ 在20世纪80年代末期， ITIL由CCTA（英国国家计算机和电信局）提出，英国商务部（OGC）发布了ITIL并在英国得到应用；

- ◆ 20世纪90年代初期，ITIL被引入欧洲其他国家；ITIL成为欧洲事实上的IT服务管理标；
- ◆ 1998年，国际ITSM论坛成立，在澳大利亚举办第一次itSMF会议；
- ◆ 2001年，英国商务部（OGC）发布了ITIL 2.0版本；并被接受为英国国家标准BS15000；
- ◆ 2002年，BS15000被国际标准化组织（ISO）接纳，启动了ITSM的标准化历程；
- ◆ 21世纪初，ITIL引入中国，在中国掀起了IT服务管理热潮；
- ◆ 2005年， 国际标准组织（ISO）接纳BS15000，并命名、正式发布为ISO20000；
- ◆ 2007年5月30日 ITIL v3核心读物正式发布。

ITILv3.0

ITIL v3.0包含了对IT服务从战略、设计、到转换、运营、改进的全生命周期的管理，业界厂商提供的方案往往覆盖了多个领域和多个产品，使得方案的统一规划实施和工具的选择使用非常困难。因为往往一种产品无法进行完整的服务全生命周期管理，而多重产品结合使用有可能会产生功能重叠和冲突。

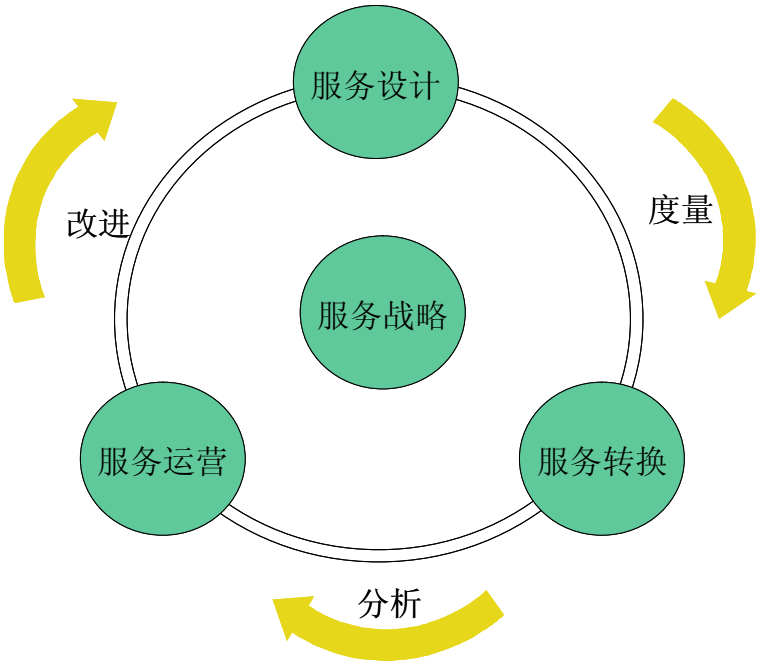


图1 ITIL v3.0生命周期图

SOM与ITIL的对应关系

ITILv3包含了对服务从战略、设计、到转换、运营、改进的服务全生命周期的管理，往往覆盖了复杂的管理工具；IMC SOM 产品关注于其中关键的服务转换和服务运营部分，聚焦于和IT运维工作关系紧密的运维流程的支持能力。

SOM与ITIL v3.0的对应关系如下表：

表1 SOM与ITIL v3.0对应关系

ITIL v3流程作用	SOM映射	
服务台	服务台	SOM
Service Strategy 服务战略	制定服务战略	
	服务财务管理	
	服务投资组合管理	
	需求管理	

Service Design 服务设计	服务目录（V3）	SLA
	服务级别管理	SLA
	能力管理	PLAT、APM、SLA
	可用性管理	SLA
	服务连续性管理	SLA
	信息安全管理	EAD、UAM
	供应商管理	
Service Transition 服务转换	规划与支持（V3）	
	变更管理	SOM
	服务资产和配置管理	SOM
	发布管理	SOM
	服务检查和测试（V3）	
	评估（V3）	SLA
	知识管理（V3）	SOM
Service Operation 服务运营	事件管理（V3）	SOM
	事故管理	SOM
	请求实现（V3）	SOM
	问题管理	SOM
	访问管理（V3）	SOM、UAM
Continuous Service Improvement 持续性服务改进	服务报告（V3）	SLA、 iAR

SOM简介

iMC SOM整体架构

iMC SOM组件在统一的配置管理数据库（CMDB）、自定义流程框架、自助服务台框架所提供的自动化运维能力基础上，提供了ITIL服务运维领域完整的资产管理、配置管理、变更管理、请求/事件/故障管理、问题管理、知识库管理等功能，并提供Service Desk作为IT网络服务的统一管理门户。

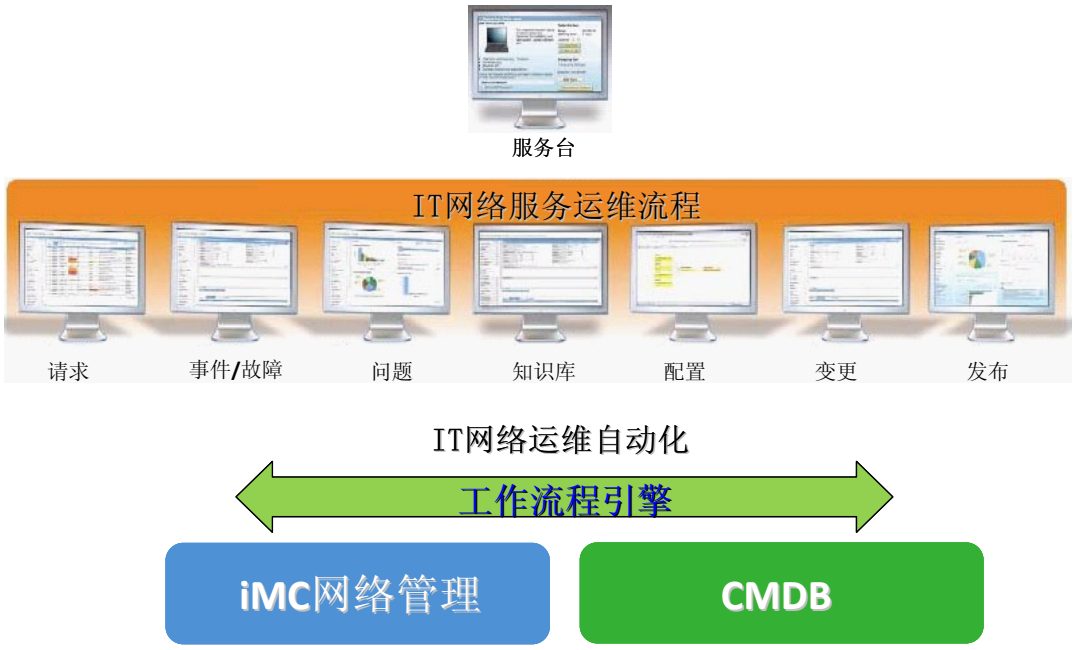


图2 iMC SOM整体架构图

iMC SOM组件通过与iMC告警、配置、软件管理等特性的融合联动，使iMC对IT网络的所有配置和变更、故障定位处理活动都被纳入到可控、可审计、可度量的运维能力要求之中。关于SOM组件与其他组件的联动在后面的几个典型流程介绍中会详细描述。

SOM功能简介

iMC运维服务管理组件由配置管理数据库（CMDB）管理和服务台管理两个模块组成，同时依赖于iMC智能管理平台的用户自助服务管理模块。

◆ CMDB管理用于维护流程过程中使用的基本数据；

◆ 服务台则提供基于Web的用户操作界面，用户使用服务台完成各种流程操作；

◆ 用户自助服务管理组件提供了访问iMC中用户资源的数据访问接口，该组件的部署基于智能管理中心平台。

用户自助服务管理

SOM的使用者为iMC智能管理平台的用户，即通过登录平台的用户再登录到SOM服务台中执行流程操作。用户自助服务管理组件提供了访问iMC中用户资源的数据访问接口，该组件的部署基于智能管理中心平台。

增加用户及自助账户

图3为增加自助用户的界面，在iMC智能管理平台的用户页面左侧导航树上有增加用户的功能项，点击该项可进入如下界面：

图3 增加自助用户界面

增加用户本身是平台组件的一个功能，开通自助账户是用户自助服务管理组件添加的功能；在此处添加一个用户，并开通了自助帐户之后，就可以通过自助账户登录SOM服务台了。

自助账户名称与用户姓名可以不一致。群组可选择性添加，群组的一个重要用途就是为用户划分自助权限。创建群组时，可以为群组分配权限。当一个用户加入一个或多个群组后，该用户的最终权限为用户开通自助服务时配置的自助服务功能权限以及所属所有群组的自助服务功能权限的并集。

SOM的用户分为如下两类：网络及业务的规划和管理人员、运维服务人员。在创建自助帐号时应区分用户的角色，分配给相应的权限，规划好权限管理。

网络及业务的规划和管理人员：负责规划如何使用iMC管理平台及SOM业务，对网络运维工作进行整体设计和管理。例如规划运维人员的角色、权限，各自职能等；创建不同类型的用户并划分到相关群组，使其各司其职；建立各种运维流程，使其能够支撑企业的IT运行；分析不同的配置项类型，并纳入CMDB的统一管理；分析和审计各种流程记录和日志，对运维过程进行监管等。

运维服务人员：SOM中使用流程的用户。根据需要启动不同类型的流程，或处理流程中的特定环节。根据权限划分，可执行不同的流程操作：普通运维人员只能按照正常步骤启动或执行特定环节；高权限维护人员可对流程过程进行监管。

登陆到SOM服务台

在创建了自助用户之后就可以登录SOM服务台了，在登录iMC智能管理平台之后在首页的左侧导航树上有iMC服务运维管理控制台的链接，点击此链接后会根据目前登录iMC智能管理平台的用户的自助账户自动登录到SOM服务台。

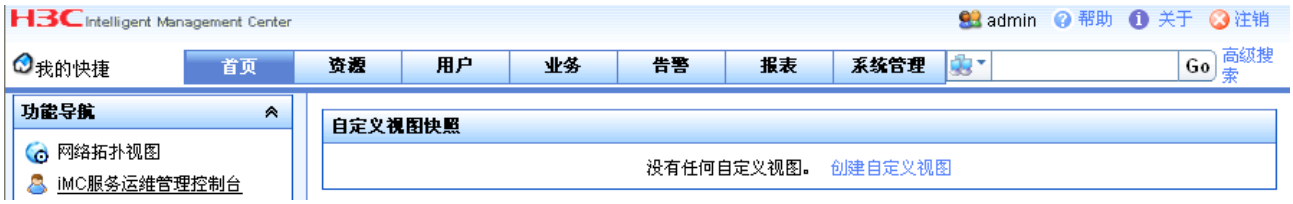


图4 SOM服务台入口

另一种登录SOM服务台的方法是在浏览器上使用：http://ip:port/servicedesk/直接进入，此时会提示输入自助账户的用户名和密码登录。

SOM上的用户账户管理

用户登录到SOM之后，根据其权限的设置，SOM服务台左侧的导航树会出现不同的功能项，没有权限的功能项在此就不会显示了。

拥有帐号管理权限的自助账户登录后可以在SOM控制台左侧的导航树上找到系统管理->用户帐号功能项，如图5所示：

图5 SOM服务台上的用户管理

该界面上已经提供了与用户管理相关的所有基本功能，需要注意的一点是，虽然在iMC智能管理平台和在SOM服务台上都有用户帐号管理功能，但其结果并不冲突，在SOM上对用户的修改在iMC智能管理平台上也能体现出来，反之亦然。

只是如果在SOM上对用户进行销号处理的话，只会销掉自助帐号，而iMC智能管理平台上的用户还会被保留，其自助帐号信息会被销掉；这是因为iMC智能管理平台的用户可能还会拥有其他组件的权限或信息，因此SOM不能注销iMC智能管理平台的用户。

网络运维流程

iMC SOM组件从关注服务运维流程的角度出发，提供了配置管理、变更管理、请求/事件/故障管理、问题管理等IT网络运维流程的全生命周期管理。

流程权限设置

触发流程的权限

目前，iMC智能管理平台能够触发的流程分为4种：iCC配置变更流程、VLAN配置变更流程、ACL配置变更流程、告警故障处理流程。

前三种配置变更流程触发需要在操作员权限处进行设置，告警故障处理流程需要创建自动分发规则或者手工分发才会触发流程。前三种流程都是有相应权限的操作员进行配置变更时触发流程建立的，告警故障处理流程是接收到告警后根据规则或者由操作员手工分发而触发流程建立的，这四种网络运维流程都不能在SOM服务台上手工创建，只能在触发建立流程之后在SOM服务台上对流程进行处理。

操作员即登录iMC智能管理平台的用户，在系统管理页面左侧导航树操作员管理–>操作员功能项处设置，如图6所示：

图6 触发流程权限设置

在需经流程审核操作处勾选相应的流程后，该操作员如果进行相应的操作就会触发网络运维流程待审批；如果此处不勾选，那么即使操作员进行相关操作也不会触发流程。如果对相关配置变更需要进行审核，那么操作员的该项配置必须进行妥善处理。

告警故障处理流程与配置变更流程不同，不需要进行特别的权限设置；但是默认情况下，告警上报之后并不会触发告警故障处理流程。触发告警故障处理流程有两种方法：手工分发和自动分发。

先讲一下手工分发的过程：操作员登录iMC智能管理平台后转到告警页面，点击左侧导航树的告警浏览->实时告警功能项，可以看到实时未恢复的告警，选中告警点分发，或者直接点击告警后面的未分发链接即可开始手工分发，如图7所示：

图7 手工分发告警

点击分发之后会弹出如下界面，在此处填写对告警的处理意见，选择处理人，确定后就会创建一个告警故障处理流程，相关的SOM用户就可以开始处理该流程了。

图8 分发至告警故障处理流程

已经恢复的告警不能够再进行分发，因为分发流程的目的之一也是要恢复告警。上面讲的是手工分发，下面介绍自动分发，自动分发需要创建告警自动分发规则并启用该规则。在告警页面左侧的导航树上点告警设置->告警自动分发规则功能项，点击告警自动分发规则界面上的增加按钮，即可转到增加自动分发规则界面，如图9所示：

图9 增加自动分发规则

填写必要的信息后点确定即可完成规则的创建并默认启用该规则，规则启用后，告警模块收到告警信息后先进行规则匹配，匹配到任何一条告警自动分发规则后就触发告警故障处理流程，从而完成告警的自动分发。

请注意，以上四个流程的触发都是在iMC智能管理平台上完成的，在此阶段还没有需要SOM用户处理的流程。

处理流程的权限

当iMC智能管理平台上触发创建了一个流程后，SOM用户就可以处理该流程了，但是哪些用户可以处理流程的哪个阶段呢？这是需要在SOM服务台上进行设置的。

使用具有流程管理权限的账户登录SOM服务台，在服务台左侧导航树流程管理–>网络运维流程中选择想要配置权限的流程，在该流程上点击鼠标右键，弹出右键菜单，再点击右键菜单中的配置流程即可进入配置流程界面，如图10所示：

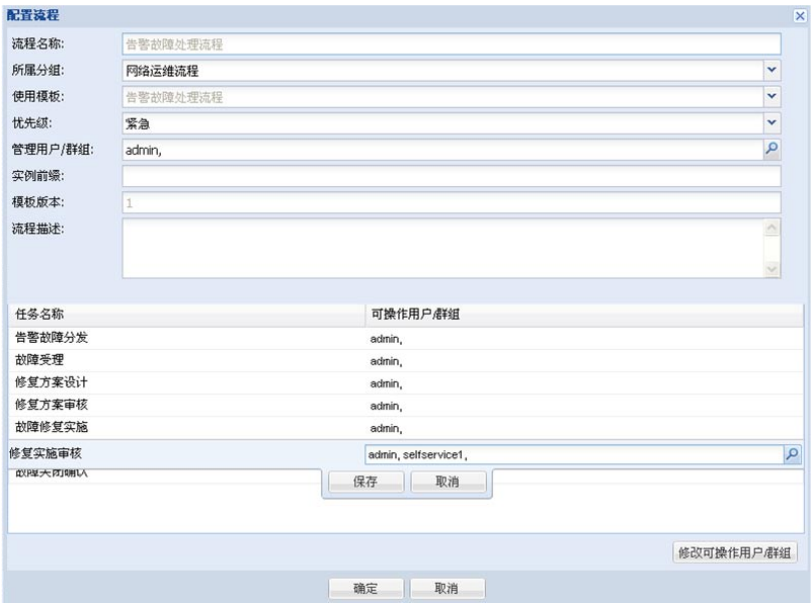


图10 配置流程权限

图10以告警故障处理流程举例，在不同的流程环节后面的可操作用户/群组中输入用户名或群组名，该用户和群组即可获得对该流程此环节的操作权限。

告警故障分发流程

iMC SOM的告警故障分发流程，实现了与iMC故障告警功能的融合，为用户提供了一个从定位、审核、修复到确认关闭的闭环过程，保障网络故障得到及时有效处理。

告警故障分发流程由告警故障分发、故障受理、修复方案设计、修复方案审核、故障修复实施，修复实施审核和故障关闭确认7个环节构成。流程处理一般是7个环节顺序执行，在有些环节中可以指定跳转的环节。

图11 告警故障分发处理流程

进行SOM服务台之后在待处理的任务中可以看到已经创建好的告警故障处理流程，为了区分多个流程，每个流程都有唯一的编号，该编号顺序增长，如图中流程的编号为：11571。选中流程后双击即可打开该流程进行处理。

网络运维流程都有由iMC智能管理平台侧触发，因此进入SOM服务台后默认都是从第二个流程环节开始处理的，但是通过图11展开的第2个流程环节可以看到，这里也是可以进行环节的跳转，也可以返回至第一环节处理。一般来讲，告警故障恢复流程创建后可以根据告警的复杂度和修复方案的成熟度对该告警进行处理；如果有成熟可实施的修复方案可以直接到故障修复实施环节，实施完成后审核，然后关闭并恢复告警；如果该告警没有比较成熟的修复方案可以直接选择，那么可以进行修复方案设计，然后审核方案后再实施。当然，也有一些可以忽略或不需要进行修复处理的告警，可以返回或直接关闭。灵活的指定环节跳转功能为各种不同情况的告警提供了不同的处理办法，但是也只能按照不同环节给出

的选择进行跳转，不能跳转到任意环节，这也是出于流程处理规范化的考虑。如果在此告警故障处理流程的关闭环节选择了恢复告警相关的选项，那iMC智能管理平台侧告警模块上对应的实时告警会自动恢复，不需要手工再去恢复。

iCC配置变更流程

iMC SOM的iCC配置变更流程可以和iMC 配置管理相融合，使IT管理人员通过iMC所做的所有网络变更操作都满足受控、可审计的要求，提高企业用户对网管操作的透明度和信任度。

iCC配置变更流程用来对受限的操作员提交的配置文件变更请求进行流程化的管理。iCC配置变更流程包括提交配置变更申请、变更审核、关闭确认三个环节。

首先看一下触发的过程，当一个设置图6中的触发权限的操作员进行配置变更操作时，完成一个配置变更的最后一个页面会提示提交审核，点击提交审核后即创建了一个iCC配置变更流程，如图12所示：

图12 触发iCC配置变更流程

iCC创建部署任务的其他环节和相关技术在这里没有进行介绍，需要了解此方面知识请查阅iCC相关文档，本文主要介绍与SOM相关的部分操作。

如果该用户没有设置如图6中的触发审核流程权限，那么此处的按钮是完成字样，提交后即直接创建了配置变更任务，而没有创建审核流程。点击提交审核后，会弹出如下窗口需要对标题和审核人进行确认修改，填写处理建议，确定后即创建了iCC配置变更流程。

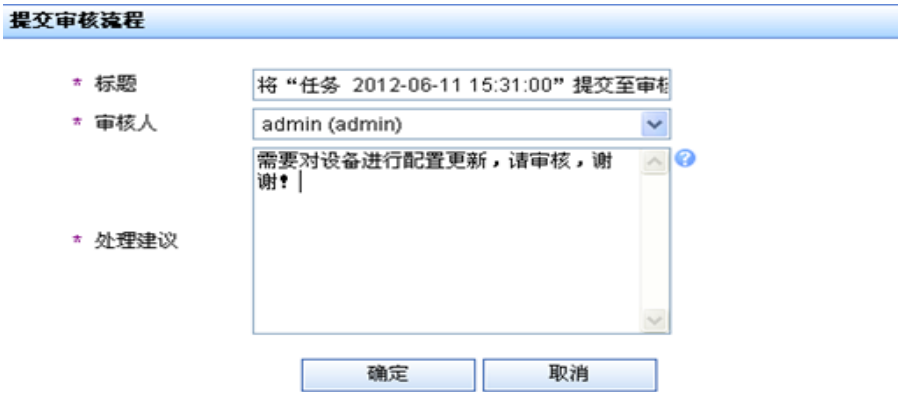


图13 iCC提交审核

iCC配置变更流程创建之后相关处理责任人在SOM服务台的待处理任务中即可看到，双击之后可以进行审核处理；该流程相对简单，审核之后即可关闭。

图14 iCC配置变更流程

流程在提交后，相关人员按照指定的环节进行处理，直到流程关闭。如果在变更审核环节审核通过，相关的任务就开始执行；如果审核不通过，相关的任务状态就是审核不通过。

如图15所示，第一个任务为审核通过并且执行完成的任务，第二个任务为审核不通过的任务。

状态--执行结果	任务名称	任务子类型	调度类型	创建者	上次开始时间	下次开始时间	修改	复制	审核流程
完成--成功	任务 2012-06-11 16:10:42	部署设备配置	一次性	admin	2012-06-11 16:11:58	--			
审核不通过--未完成	任务 2012-06-11 15:31:00	部署设备配置	一次性	admin	--	--			

图15 审核之后的iCC配置任务

ACL配置变更流程

该流程需要iMC智能管理平台安装了ACL组件才有可能触发，ACL组件对设备进行ACL配置，实现网络数据的流控管理。

ACL配置变更流程用来对受限的操作员提交的部署ACL请求进行流程化的管理。ACL配置变更流程包括提交配置变更申请、变更审核、关闭确认三个环节。

创建ACL部署的最后一个页面上有提交审核按钮，如图16所示：

图16 ACL部署任务

ACL创建部署任务的其他环节和相关技术在这里没有进行介绍，需要了解此方面知识请查阅ACL相关文档，本文主要介绍与SOM相关的部分操作。

如果该用户所使用的操作员设置触发流程的权限的页面没有勾选ACL配置变更流程，那么此处<提交审核>的按钮是<完成>字样，提交后即直接创建了ACL部署任务，而没有创建审核流程。点击提交审核后，会弹出如下窗口需要对标题和审核人进行确认修改，填写处理建议，确定后即创建了ACL配置变更流程。

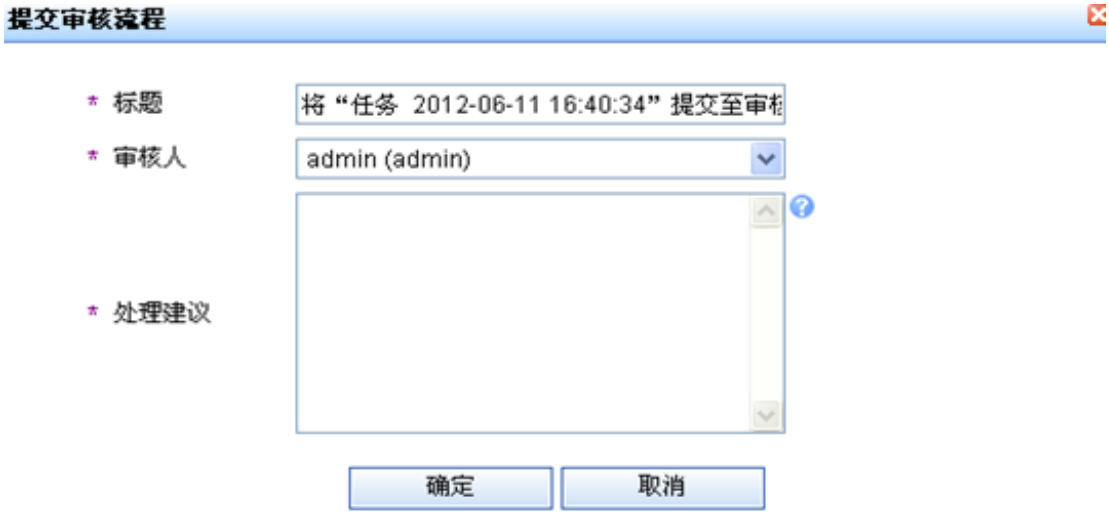


图17 ACL提交审核流程

ACL配置变更流程创建之后相关处理责任人在SOM服务台的待处理任务中即可看到，双击之后可以进行审核处理；该流程相对简单，审核之后即可关闭。

图18 ACL配置变更流程

流程在提交后，相关人员按照指定的环节进行处理，直到流程关闭。如果在变更审核环节审核通过，相关的任务就开始执行；如果审核不通过，相关的任务状态就是审核不通过。

如图19所示，第一个任务为审核通过并且执行完成的任务，第二个任务为审核不通过的任务。

	任务状态	任务名称	创建时间	创建者	任务类型	预定执行时间	任务结束时间	执行结果	审核流程	修改
☐	完成	任务 2012-06-11 17:17:56	2012-06-11 17:18:07	admin	立即执行	--	2012-06-11 17:18:37	全部成功		
☐	审核不通过	任务 2012-06-11 16:40:34	2012-06-11 16:46:57	admin	立即执行	--	--	未完成		

图19 审核之后的ACL任务

VLAN配置变更流程

该流程需要iMC智能管理平台安装了VLAN组件才有可能触发，VLAN组件对网络中VLAN资源进行管理。

VLAN配置变更流程用来对受流程管理限制的操作员提交的批量VLAN变更请求时，进行流程化的管理。实际网络应用中，通常只有网络管理人员有权限修改设备配置，而普通用户不能修改。然而，很多情况下，没有VLAN管理权限的操作员也希望通过修改设备上的VLAN配置来达到目标，这些变更请求需要向网管员发起申请。VLAN配置变更流程就是帮助这些没有变更权限的操作员向网管员发起申请的途径。VLAN配置变更流程包括流程配置、发起请求、处理请求，如下章节将逐一进行介绍。

创建VLAN部署任务的最后一个页面上有提交审核按钮，如图20所示：

图20 VLAN部署任务

VLAN创建部署任务的其他环节和相关技术在这里没有进行介绍，需要了解此方面知识请查阅VLAN相关文档，本文主要介绍与SOM相关的部分操作。

如果该用户所使用的操作员设置触发流程的权限的页面没有勾选VLAN配置变更流程，那么此处<提交审核>的按钮是<完成>字样，提交后即直接创建了VLAN部署任务，而没有创建审核流程。点击提交审核后，会弹出如下窗口需要对标题和审核人进行确认修改，填写处理建议，确定后即创建了VLAN配置变更流程。

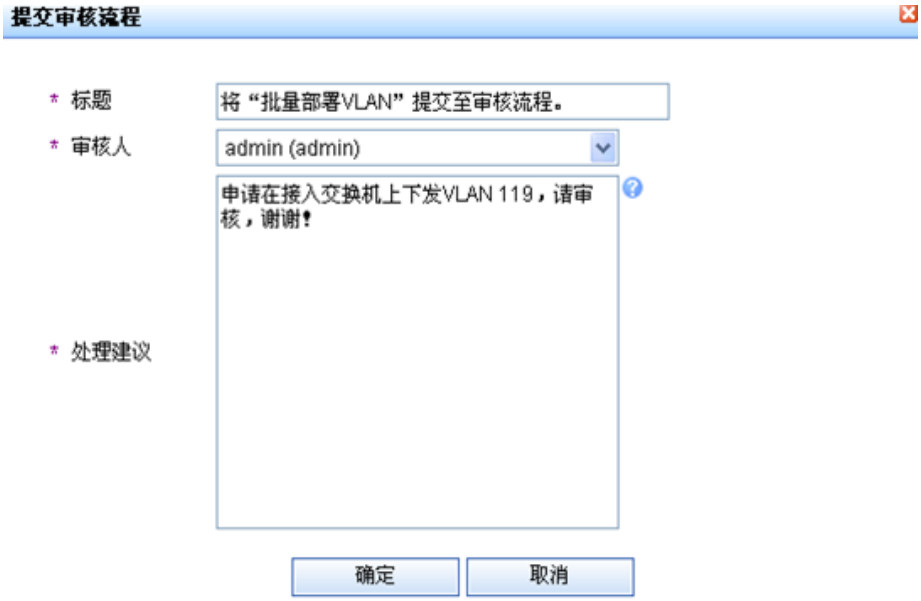


图21 VLAN提交审核流程

VLAN配置变更流程创建之后相关处理责任人在SOM服务台的待处理任务中即可看到，双击之后可以进行审核处理；该流程相对简单，审核之后会自动关闭。

图22 VLAN配置变更流程

流程在提交后，相关人员按照指定的环节进行处理。如果在变更审核环节审核通过，相关的任务就开始执行；如果审核不通过，相关的任务状态就是审核不通过。

如图23所示，第一个任务为审核通过并且执行完成的任务，第二个任务为审核不通过的任务。

	操作	结果	时间	详细信息	审核流程
	部署VLAN	成功	2012-06-11 17:32:23		
	部署VLAN	审核不通过	2012-06-11 17:28:49		

图23 审核之后的VLAN任务

定制流程

不同的企业对实际运维流程有各自习惯和强制要求，为了适应这种差异，SOM组件提供了从流程各个步骤到流程模板的灵活定制能力。

基于系统预置的流程模板，定义适用的流程；在流程定义中，可以指定流程的优先级、各阶段任务的可操作用户。 流程模板中定义了流程的各个步骤和转接关系，但没有绑定具体的责任人；基于流程模板创建流程定义时，需要指定各步骤有权处理的责任人或用户群组。

对于高级用户，可以使用脚本语言创建或定制流程模板；在创建新的流程步骤、或创建新的流程模板时，可以通过配置模板的能力，自动生成流程各步骤的界面，在界面中可以将界面元素绑定到CMDB中的CI数据，使用户在处理流程时，自动从CMDB中过滤相关CI作为输入选择。编写流程模板对于脚本语言编程能力和对系统的了解要求较高，一般用户不建议使用此功能，本文中就不详细介绍该功能了。

定制流程的过程

在SOM左侧的导航树上点击流程管理->定制流程后，会弹出流程的定制窗口，如图24所示：

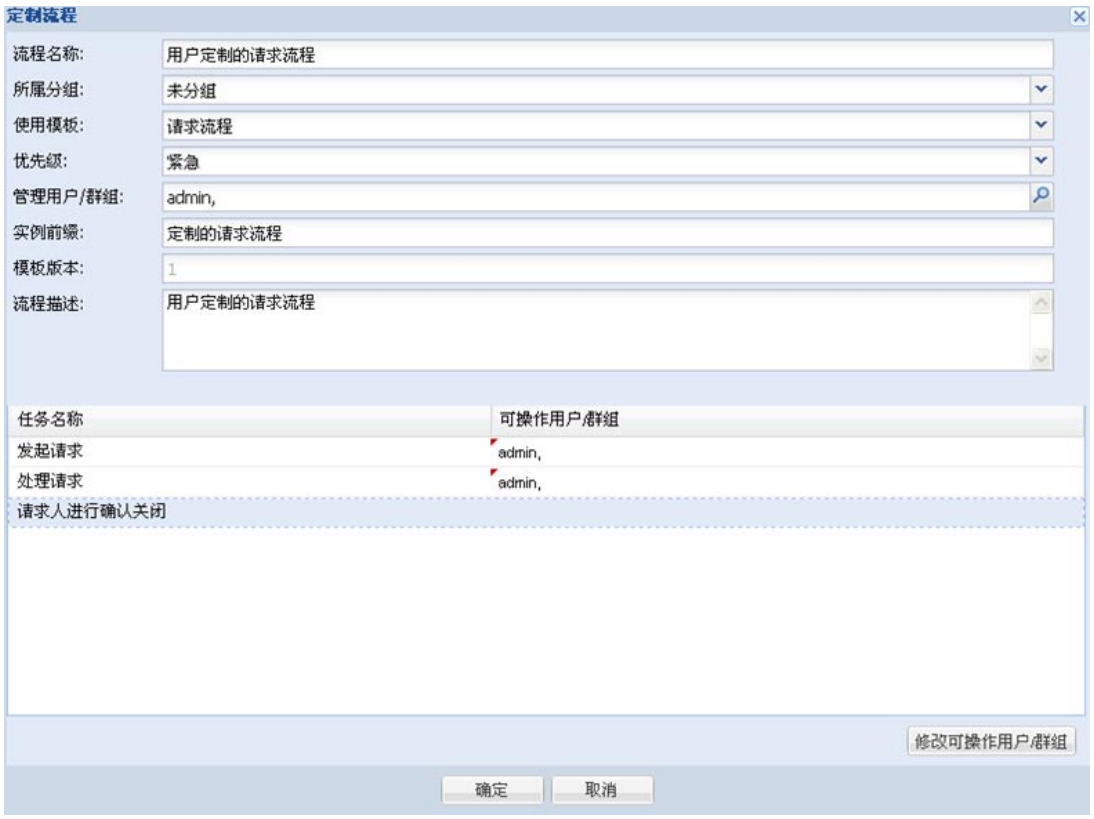


图24 定制流程

如图24中填写流程名称，选择使用的流程模板，对管理用户/群组和每个流程环节的可操作用户/群组进行填写后即可完成流程的定制。个别的流程环节不能指定可操作用户/群组，如图24中的请求人进行确认关闭环节就不能指定可操作用户/群组，因为该环节会直接返回给发起请求的用户进行确认关闭，所以不需要再指定可操作用户/群组。

系统预定义了四种流程模板，分别是：请求流程、问题流程、帐号注册流程和知识库流程。不同的模板设置的流程环节也不同。如图24中的请求流程包含了发起请求、处理请求和请求人进行确认关闭三个环节；问题流程则包括提交问题、问题分类、问题诊断和诊断后审核四个环节；帐号注册流程包含构造注册信息和注册信息审核两个环节；知识库流程包括构造解决方案和解决方案确认两个环节。

当定制的流程较多时，可以通过在导航树流程管理->更多…中选择创建新分组，然后在定制流程时在所属分组中进行选择，对流程进行分组管理。

创建流程实例

网络运维流程不能在SOM服务台上手工创建实例，但是定制的流程是需要用户手工创建实例的。以上一小节定制的流程为例，在SOM服务台左侧导航树流程管理->未分组->用户定制的请求流程上双击，或者在该节点上点鼠标右键，再选择右键菜单中的创建实例，即可完成一个流程实例的创建。创建的实例，如图25所示：

图25 创建流程实例

流程实例的名称由定制流程时填写的流程前缀和流程的编号组成，实例创建后，相关责任人可以开始对该流程的处理。

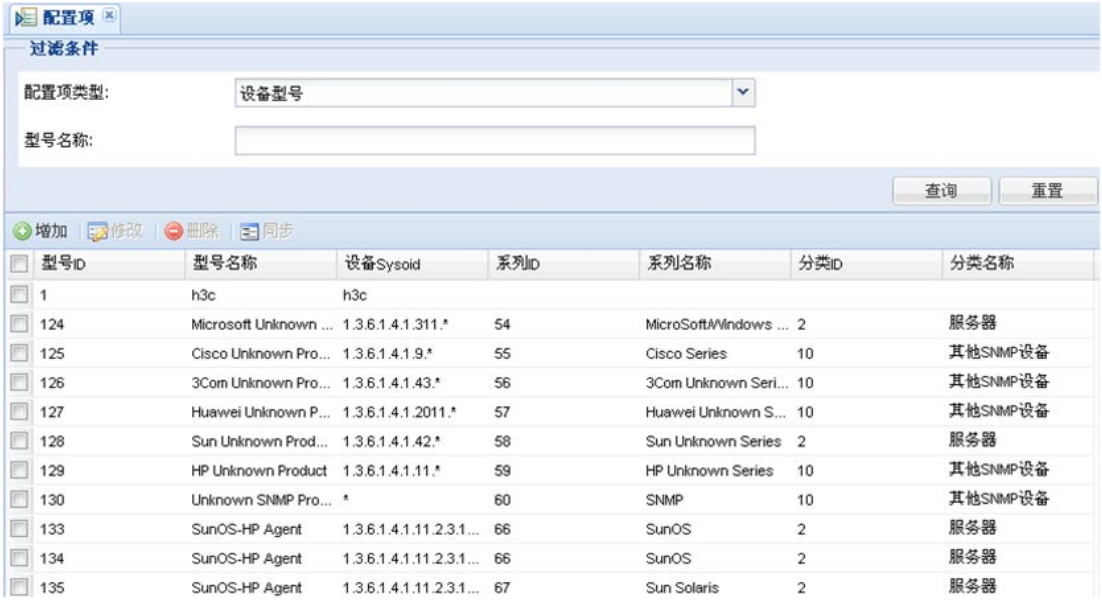
CMDB

CMDB是IT运维服务管理的核心部件，和一般的资产管理相比，除了资产配置项本身信息，还维护各配置项之间的关系、当前状态和变更情况。iMC SOM CMDB采取“CMDB核心数据”加“原始业务资产数据”的管理组织方式，通过联合的CMDB，可以帮助用户度量企业IT资产的价值，为服务管理流程提供有关IT基础设施的准确信息，为故障管理、问题管理、变更管理和发布管理等的运作提供后台支持。

CMDB由配置项、配置项关系、知识库、问题库和管理菜单组成。

配置项

在SOM服务台左侧的导航树上选择CMDB管理->配置项，双击该选项，打开了配置项的操作页面，选择一个配置项类型，点查询，即可查询出该配置项的所有数据：



型号ID	型号名称	设备Sysoid	系列ID	系列名称	分类ID	分类名称
1	h3c	h3c				
124	Microsoft Unknown ...	1.3.6.1.4.1.311.*	54	MicroSoftWindows ...	2	服务器
125	Cisco Unknown Pro...	1.3.6.1.4.1.9.*	55	Cisco Series	10	其他SNMP设备
126	3Com Unknown Pro...	1.3.6.1.4.1.43.*	56	3Com Unknown Seri...	10	其他SNMP设备
127	Huawei Unknown P...	1.3.6.1.4.1.2011.*	57	Huawei Unknown S...	10	其他SNMP设备
128	Sun Unknown Prod...	1.3.6.1.4.1.42.*	58	Sun Unknown Series	2	服务器
129	HP Unknown Product	1.3.6.1.4.1.11.*	59	HP Unknown Series	10	其他SNMP设备
130	Unknown SNMP Pro...	*	60	SNMP	10	其他SNMP设备
133	SunOS-HP Agent	1.3.6.1.4.1.11.2.3.1...	66	SunOS	2	服务器
134	SunOS-HP Agent	1.3.6.1.4.1.11.2.3.1...	66	SunOS	2	服务器
135	SunOS-HP Agent	1.3.6.1.4.1.11.2.3.1...	67	Sun Solaris	2	服务器

图26 配置项

配置项类型可以是iMC基础配置项，例如：设备、设备型号等，也可以是用户自定义的，例如：会议室、公司组织结构。

默认的配置项类型有：设备、设备型号、设备类别、设备系列、设备软件、配置模板。在CMDB管理->管理菜单->配置项类型中可以查看到这些默认的配置项，在配置项类型页面还可以增加用户自定义的配置项类型。配置项中的数据有两个来源，一是用户手工增加，在图26中可以看到增加按钮；二是从iMC智能管理平台的数据库中同步。但是用户自定义的配置项类型无法从iMC智能管理平台的数据库中同步数据，因为该数据库中并没有用户自定义的这部分配置项的配置数据。

如图26所示，选择了配置项类型后，该配置项类型的关键列会出现在配置项类型的下方，可以输入数据进行查询；不同的配置项类型关键列不同，例如型号名称就是设备型号的关键列，而设备的关键列是设备IP。

在图26中用户可以增加自定义的配置项，还可以选择一个配置项进行修改或删除，如果是从iMC智能管理平台的数据库中同步过来的数据可以选中然后进行同步，此处只会同步勾选的部分数据。如果想从数据库中同步所有数据则需要到CMDB管理->管理菜单->配置项类型页面选中需要同步的配置项类型选择同步，并保存同步后的数据。需要注意的是同步数据会覆盖用户对此数据之前进行的修改。

配置项关系

要想建立配置项之间的关系，首先要有可供选择使用的配置项关系类型。配置项关系类型用于描述配置项之间的关联关系，例如：父子关系、包含关系、从属关系等。系统没有预定义配置项关系类项，因此要到CMDB管理->管理菜单->配置项关系类型页面去定义要使用的配置项关系类型。

创建配置项关系类型的过程很简单，在CMDB管理->管理菜单->配置项关系类型页面点增加，输入名称和描述即可。

下面介绍如何增加配置项关系，在SOM服务台左侧导航树CMDB管理->配置项关系页面点击增加，弹出界面如下：

图27 增加配置项关系

选择左配置项类型之后，左节点的选项会随之自动转换成该配置项的关键列；选择左节点，关系类型，右配置项类型后，下方会自动查询出右配置项类型中的所有数据，可以根据需要进行勾选，然后点击确定，即可建立配置项关系。

在CMDB管理->配置项关系页面上还可以对配置项关系进行查询和删除。

知识库/问题库

知识库/问题库主要用于保存SOM使用过程中的经验和问题记录。

iMC SOM集中的知识库保存解决方案避免了重复工作，并通过有效的知识共享，提高了整体生产效率，不管是哪个技术人员处理请求，用户都能得到一致的回答。

要填加知识库/问题库必须首先填加知识库/问题库分类，在SOM服务台左侧导航树上选择CMDB管理->管理菜单->知识库/问题库分类双击，在页面上点增加就会弹出增加知识库/问题库分类的页面，填入名称和描述，选择分类确定即可创建一个知识库/问题库分类。在分类处如果选择共享，则知识库和问题库都可以使用该分类，如果选择仅知识库适用或者仅问题库适用则只在对应的库中可见。

在SOM服务台左侧导航树上选择CMDB管理->知识库双击，点增加按钮即可弹出如下界面：

图28 增加知识库

输入必要的元素即可完成知识库的创建。在CMDB管理->知识库页面还可完成修改、删除、过滤、刷新等操作。

问题库的操作方法与知识库基本相同，在此不做赘述。

管理页面的三个功能配置项类型、配置项关系类型、知识库/问题库分类已经在上面配置项、配置项关系、知识库/问题库中进行了简单介绍，不再重复介绍了。

需要说明的一点是在介绍SOM的其他文档中可能会看到名为CI的简写，CI即配置项。

总结

iMC SOM服务运维管理组件在IT服务管理的最佳实践——ITIL规范的基础上，提供用户服务台、CMDB配置管理数据库、知识库等流程管理功能，并结合iMC智能管理平台的基础设施管理能力和IP资源配置能力，打通了IT运维流程与网络配置管理之间的界限，帮助用户整合IT服务与业务流程，提高了数据中心信息部门的IT服务交付能力与服务支持能力，为用户实现以流程为导向、以客户响应为中心的IT运维服务奠定了基础。

基于LoadRunner实现iMC的高质量压力测试

文/刘宇征

前言

我们知道，iMC是一款有强大后台服务支撑的WEB应用，能够支持大量用户并发访问。对于这样的一款web应用程序进行压力测试，测试流程通常由以下四个基本步骤组成：

◆ 步骤 1 – 创建脚本。通过测试工具捕获在应用程序上执行的用户业务流程，根据client与server之间交互的底层协议内容，创建可重复执行的交互脚本。在脚本中需要对server的返回结果进行判断，对需要变化的输入项做参数化处理。

◆ 步骤 2 – 设计模拟场景。通过定义测试期间发生的事件，设置负载测试环境。在此阶段需要根据被测试对象的特性和性能基线设计好并发的Vuser数量，并发时机及并发执行的持续时长等等。

◆ 步骤 3 – 运行场景。运行、管理并监控负载测试。此阶段是产生测试压力的真正阶段，通过测试工具按照场景的设计运行测试脚本，给被测系统造成真实的压力。测试工具实时监控被测系统的响应时间、cpu/内存使用率、流量吞吐等性能指标，可初步得到被测系统的性能瓶颈所在。

◆ 步骤 4 – 分析结果。根据测试工具提供的执行日志及测试报表等数据分析在负载测试期间被测系统的性能表现。

然而我们发现，对iMC进行压力测试是相当困难的。iMC由大量功能页面构成，每个页面又包含许多动态变化的页面元素，如动态列表、图等等。如何适应这种内容动态变化，准确判断出一个页面是否显示正常，成为测试的难点之一；对iMC的功能测试需要模拟用户的操作，主要通过测试脚本编写实现。编写复杂的测试脚本费时费力，且页面一旦做了少量变化，原先的脚本就可能出错，导致测试无法顺利进行。如何减少脚本编写和修改的复杂度，成为iMC测试的另一个难点；iMC的许多组件可支持大量用户并发访问，如何有效模拟规格数量的用户的并发访问行为，提供足够的测试压力，是又一个测试难点。

工欲善其事，必先利其器。选用一款合适的测试工具，可以大大减少我们遇到的测试困难。

HP LoadRunner就是这样一款测试利器。HP LoadRunner是业内使用相当广泛的自动化测试工具，其组件之一的HP Virtual User Generator (VuGen)组件可以快速简单地录制用户的web页面操作过程，并自动形成测试脚本。当被测页面发生变化时，只需要对脚本做少量的修改，有效缩短了测试人员的脚本编写和修改、调试时间。通过可视化的脚本回放操作，以及更详细的脚本回放过程记录log文件，LoadRunner可以将脚本测试过程直观的展现在测试人员面前，便于判断页面功能正常与否。LoadRunner的另一组件HP LoadRunner Controller组件可将之前录制的脚本通过多线程的方式同时执行，从而在系统上施加负载。合理设置并发执行的线程数及各线程持续时间，可对iMC形成足够的测试压力，以测试出其中可能隐藏的BUG。

下文中我们通过一个测试例介绍使用LoadRunner完成iMC性能测试的过程。在这个测试例中我们模拟10并发用户创建账户的行为，测试iMC用户管理模块新建账户的能力。具体过程是，模拟10个用户，以每3秒1个用户的速度登录iMC，每个用户在iMC上连续创建10个帐户，10用户共创建100个帐户。创建成功后，所有用户退出登录。

在正式开始这个测试例的配置步骤之前，我们先对LoadRunner做一个简要介绍。

LoadRunner简介

HP LoadRunner是一款业界广泛使用的性能测试工具，它通过模拟多个用户同时在应用程序中工作的场景，对应用程序进行负载测试，并对被测系统的性能进行监控。

使用 HP LoadRunner 可以创建模拟场景，并定义性能测试会话期间发生在场景中的事件。在场景中， LoadRunner 会用虚拟用户（简称 Vuser）代替物理计算机上的真实用户。这些 Vuser模拟典型用户的操作，对系统施加负载。

HP LoadRunner 由如下执行组件构成：

◆ HP Virtual User Generator (VuGen)。用于创建脚本。

VuGen 通过录制用户在应用程序上执行的操作来生成虚拟用户（或称Vuser）。然后 VuGen 将这些操作录制到自动化 Vuser 脚本中，将其作为负载测试的基础。

◆ HP LoadRunner Controller。用于设计并运行场景。

Controller 是用来设计、管理和监控负载测试的中央控制台。使用 Controller 可运行模拟真实用户操作的脚本，并通过让多个 Vuser 同时执行这些操作，从而在系统上施加负载。

◆ HP Analysis。用于分析场景。

HP Analysis 提供包含深入性能分析信息的图和报告。使用这些图和报告可以找出并确定应用程序的瓶颈，同时确定需要对系统进行哪些改进以提高其性能。

在本测试例中我们重点使用前两个组件，录制脚本并创建负载，对iMC施加一定负载以完成性能测试。

测试步骤

上文简单介绍了LoadRunner的功能组件，下面我们就按照测试步骤，一步步利用LoadRunner完成对iMC用户管理模块的压力测试。

创建测试脚本

创建负载测试的第一步是使用 VuGen 录制用户业务流程。VuGen 以“录制–回放”的方式工作。

当我们在iMC页面上执行业务流程步骤时， VuGen 会将我们的操作录制到自动化脚本中，并将其作为负载测试的基础。

录制业务流程以创建脚本

首先打开 VuGen 并创建一个空白脚本。

选择开始 > 程序 > HP LoadRunner > LoadRunner。将打开 HP LoadRunner 窗口。

在 LoadRunner Launcher 窗格中，单击Create/Edit Scripts。这时将打开 VuGen 起始页。

在 VuGen 起始页，单击<New Vuser Script…>”按钮。将打开新建虚拟用户对话框，其中显示了新建单协议脚本选择框。

协议是客户端用来与系统后端进行通信的语言。iMC 是一个基于 Web 的应用程序，因此我们将创建一个 Web 虚拟用户脚本。

在“Category”框选择“All Protocols”后，将列出适用于单协议脚本的所有可用协议。

向下滚动列表，选择 Web (HTTP/HTML) 并单击<OK>按钮，创建一个空白 Web 脚本。如图1所示：

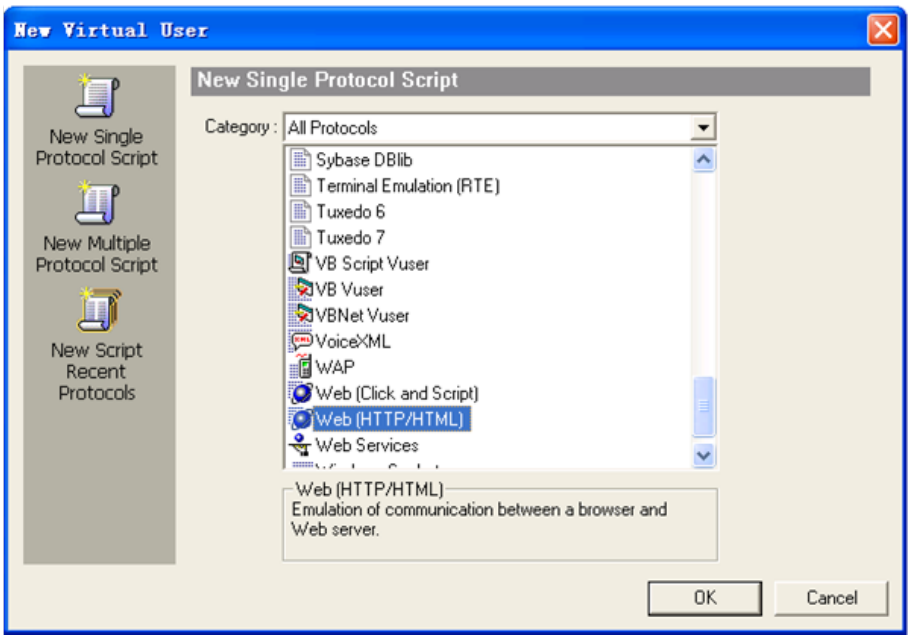


图1 新建虚拟用户对话框

在工具栏上点击“Start Record”按钮，如图2，打开“Start Recording”对话框。如图3。

图2 Start Record按钮

在 URL 地址框中，输入iMC登录页面的地址 “http://210.1.1.253:8080/imc”。在“录制到”操作框中，选择 vuser_init。单击确定。

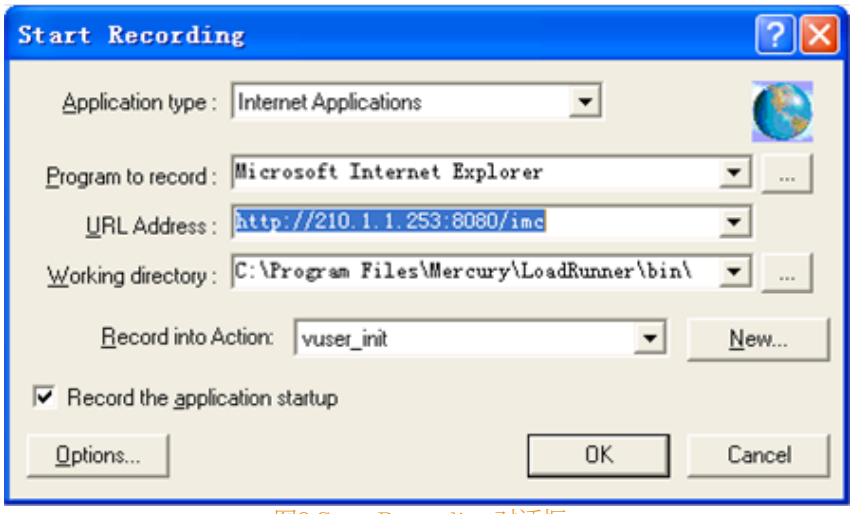


图3 Start Recording对话框

这时将自动打开浮动的“正在录制”工具栏。

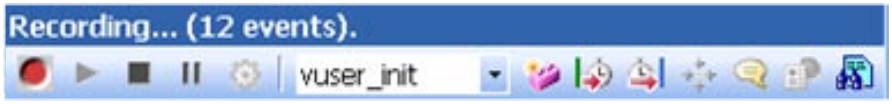


图4 录制工具栏

经过短暂等待后，将会打开一个新的 Web 浏览窗口并显示iMC登录页面。

随着IE页面中元素的逐渐显现，我们可以观察到上述浮动工具栏顶部的数字在不断增加。这说明LoadRunner记录了越来越多的client与iMC server之间的通讯内容。等该数字不再增加之后，我们开始在iMC登录页面中输入用户名/密码登录。

在IE的iMC登录页面上，以用户名admin，密码admin登录。如图5：

图5 iMC登录窗口

随着成功登录iMC并在IE上显示出iMC的首页，我们可以看到LoadRunner录制的元素越来越多，浮动工具栏顶部的数字越来越大。等浮动栏顶部的数字不再增加之后，说明我们登录iMC的步骤已经全部完成。我们按浮动栏上的暂停按钮暂停录制，如下图：

图6 录制工具栏

通过上面的步骤，我们已经将iMC登录过程录制到vuser_init环节中。

LoadRunner脚本回放通常有三个阶段，分别是脚本初始化（Init）阶段、脚本运行（Run）阶段和脚本结束（End）退出阶段，三个阶段缺省对应的脚本分别为“vuser_init”、“Action”和“vuser_end”，如图7所示：

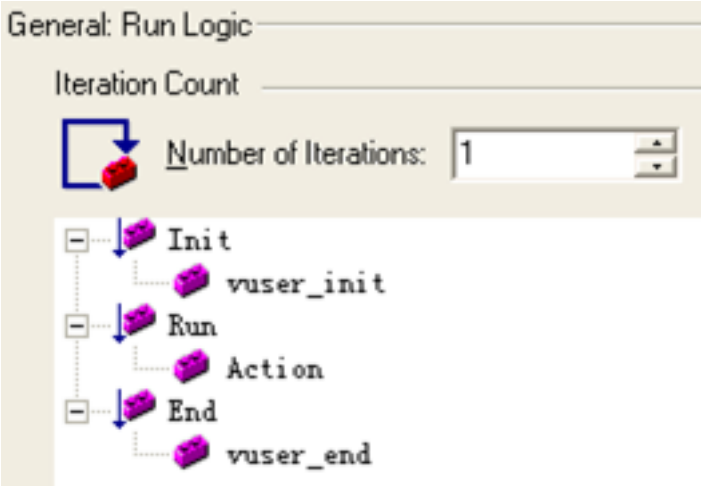


图7 脚本运行逻辑

其中的Run阶段可以根据用户定义，重复迭代执行任意次，其他两个阶段只能执行一次。因此，如果测试目的并非测试iMC登录的话，我们可以把登录过程录制在Vuser_init脚本中，把注销iMC登录过程录制在Vuser_end脚本中，减少由于登录给iMC造成的压力。

按照这个思路，我们在上述步骤中，已成功将iMC登录过程录制在了Vuser_init脚本中。接下来，我们将需要重点加压测试的部分录制在Action脚本中。

在浮动工具栏上选择Action后，点击红色录制按钮，继续录制下面的步骤：

图8 录制工具栏

接下来，我们进入iMC的用户管理页面，新建用户user01，密码也设置为user01，如图9所示：

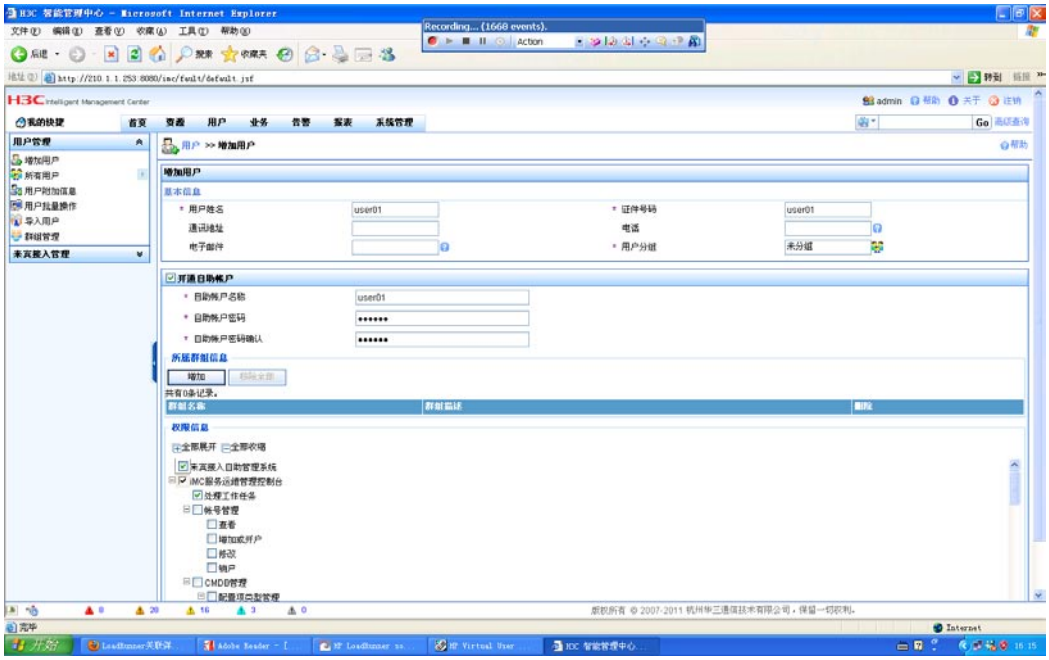


图9 iMC新建用户页面

用户新建完成后，与录制Vuser_init脚本的步骤一样，待浮动工具栏上的数字稳定后，点击暂停键，停止Action脚本录制工作。

在浮动工具栏上选择Vuser_end，点击红色录制按钮，继续录制退出iMC登录的步骤，点击注销退出iMC，如图10所示：

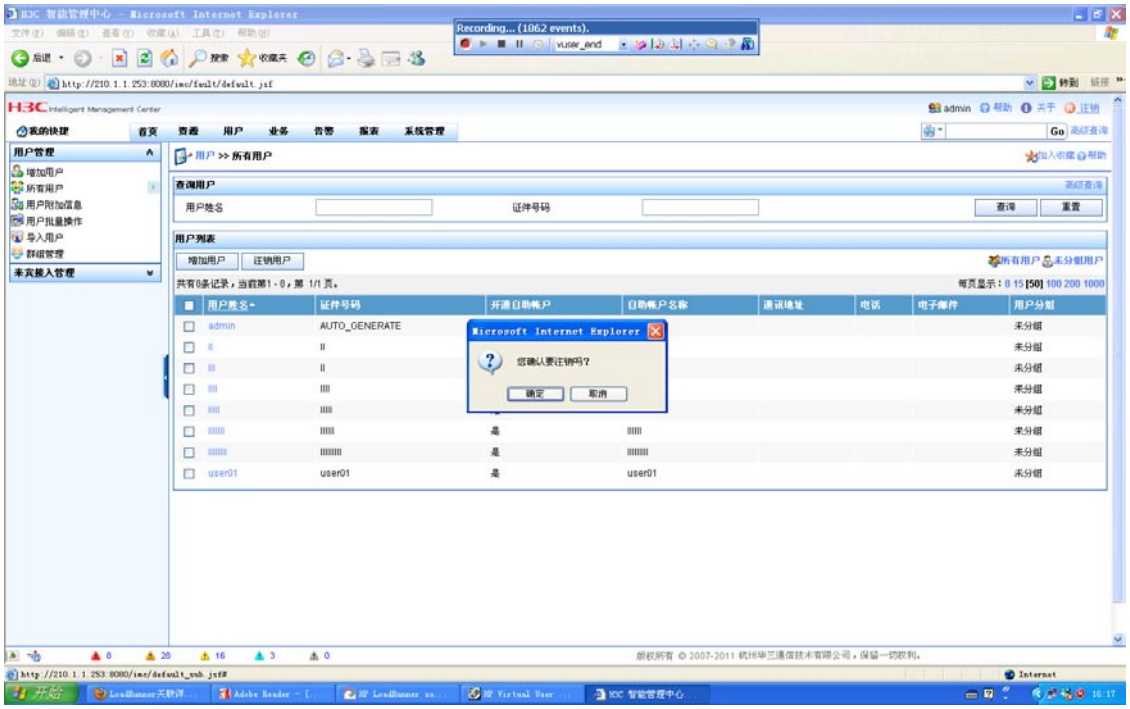


图10 iMC退出登录页面

完成退出iMC后，待浮动工具栏上的数字稳定，点停止按钮，如图11，完成整个脚本录制过程。

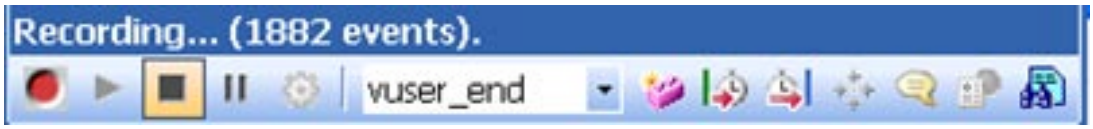


图11 录制工具栏

LoadRunner会弹出下图这个对话框，并自动生成整个Vuser脚本。

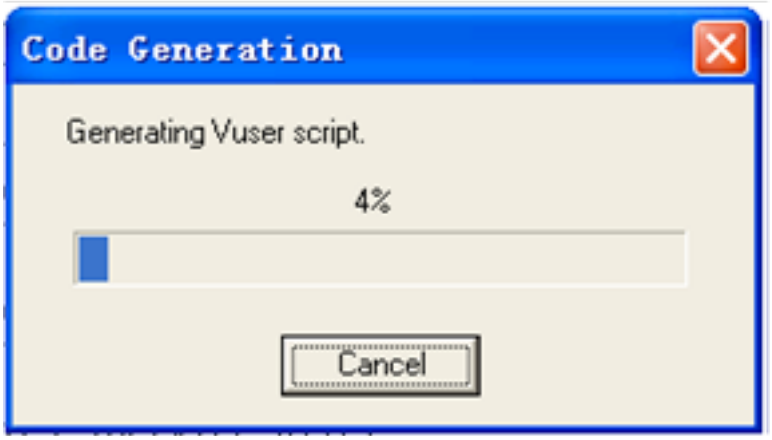


图12 脚本生成进度框

生成 Vuser 脚本后， VuGen 向导将自动继续执行任务窗格中的下一个步骤，并显示录制摘要信息（包括协议信息和会话期间创建的一系列操作）。VuGen 为录制期间执行的每个步骤生成一个快照，即

录制期间各窗口的图片。这些录制的快照以缩略图的形式显示在右窗格中。（由于格式问题，多数缩略图都可能无法正确显示，不必管它）。

从菜单中选择[File >> Save]，在文件名框中输入脚本名称，比如imc_user_add，并单击<保存>按钮。VuGen 将该文件保存到 LoadRunner 脚本文件夹中，返回“Recording Summary”页面，并在标题栏中显示脚本名称。如图13：

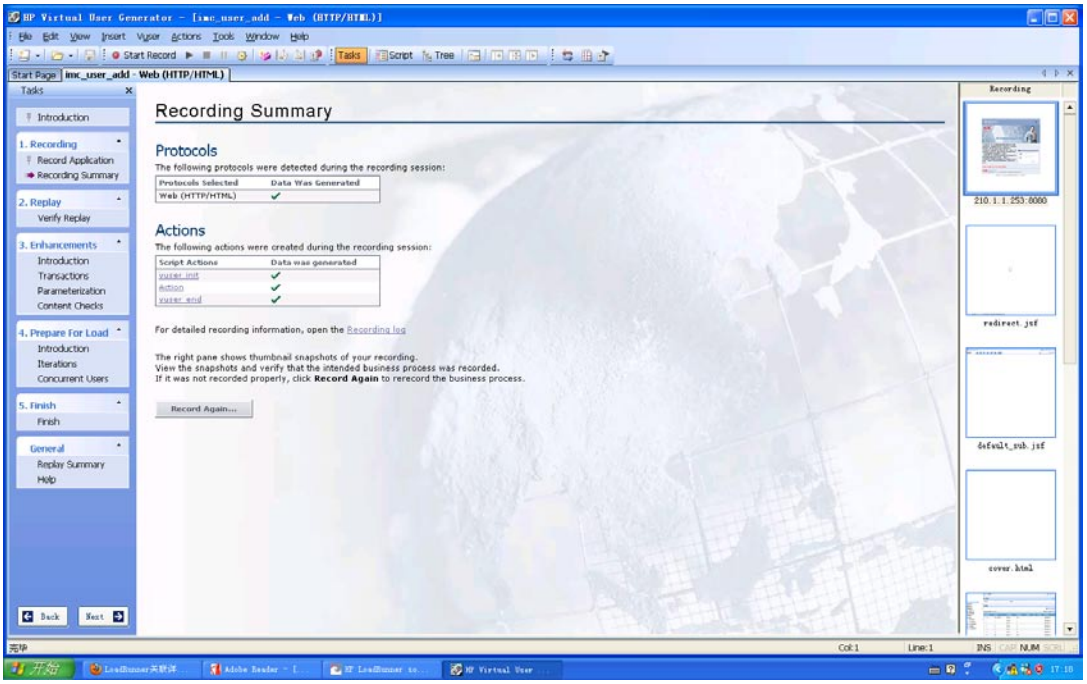


图13 脚本录制、保存完毕，显示Recording Summary页面

查看录制好的脚本

我们可以在 VuGen 中查看已录制的脚本。可以在树视图或脚本视图中查看。树视图是一种基于图标的视图，将 Vuser 的操作以步骤的形式列出，而脚本视图是一种基于文本的视图，将 Vuser 的操作以函数的形式列出。

1 树视图

要在树视图中查看脚本，请从菜单栏中选择[View >> Tree View]，或者单击工具栏上的树按钮。对于录制期间执行的每个步骤， VuGen 在脚本树中为其生成一个图标和一个标题。如图14所示：

2 脚本视图

脚本视图是一种基于文本的视图，以 API 函数的形式列出 Vuser 的操作。要在脚本视图中查看脚本，请选择[View >> Script View]菜单，或者单击工具栏上的脚本按钮。

在脚本视图中，VuGen 在编辑器中显示脚本，并用不同颜色表示函数及其参数值。

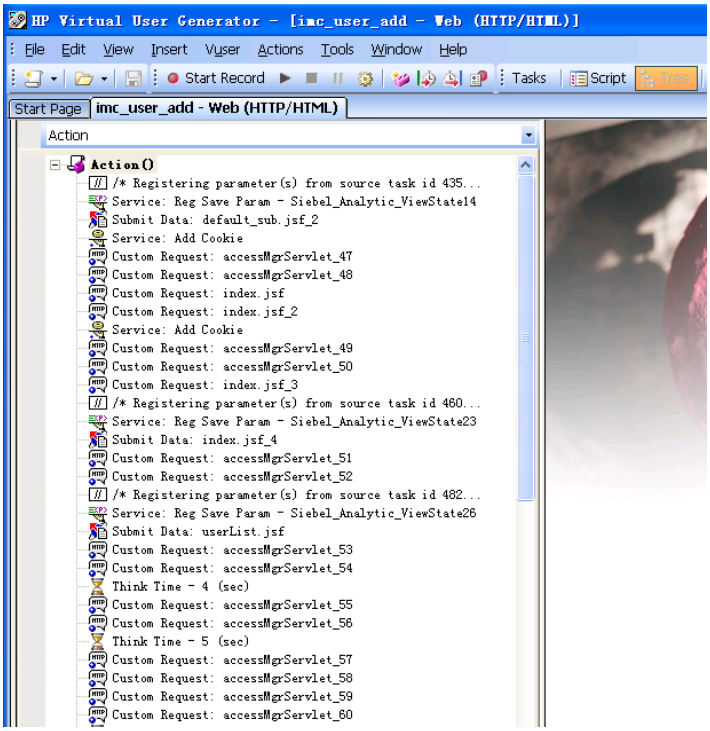


图14 树视图

可以在窗口中直接输入 C 或 LoadRunner API 函数以及控制流语句。如图15所示：

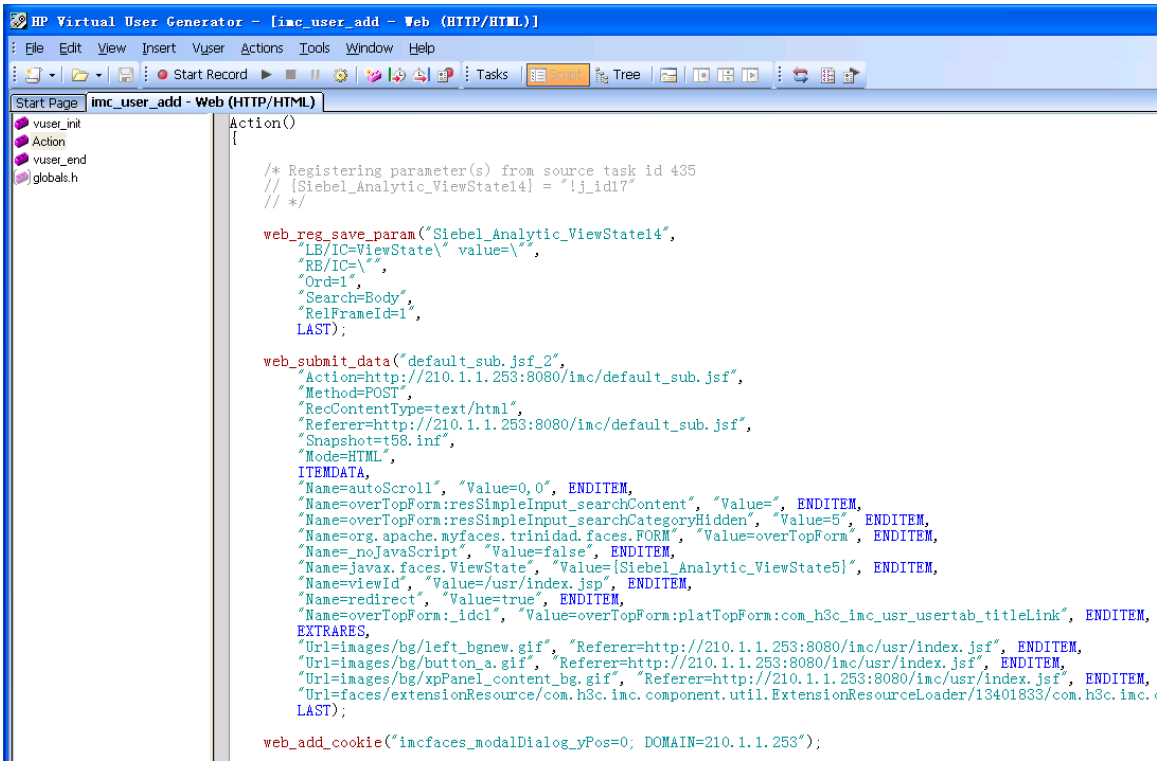


图15 脚本视图

在完成了脚本录制以后，我们需要对脚本做验证，以证明脚本录制正确，对录制过程中的问题予以修改，需要对录制的部分信息用参数替代（比如用户名、密码等部分）。

验证脚本已录制的操作

完成录制后，我们需要回放脚本以验证其是否准确模拟了录制的操作。要回放脚本，应执行下列操作：

1 点击工具栏中的回放按钮，LoadRunner开始脚本回放操作。

2 在任务窗格中单击“Verify Replay”链接，以查看关于上次回放的概要信息。

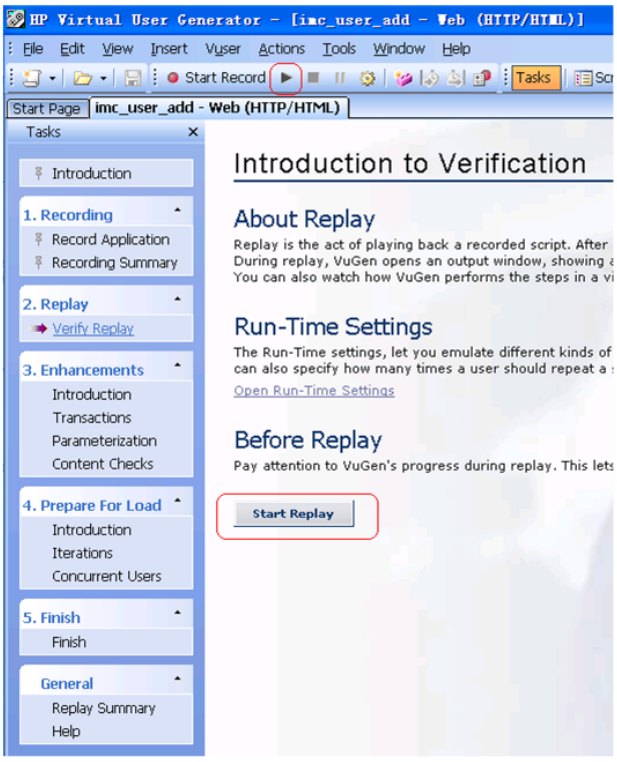


图16 脚本验证回放

在回放之前，我们可以通过[Tools >> General Option]菜单，打开LoadRunner的脚本回放过程显示，这样，回放过程中LoadRunner会打开一个浏览器，将回放过程中的所有页面显示在该窗口中，这有助于我们对回放过程产生的错误进行定位（不过由于回放速度太快，窗口中的很多内容可能来不及显示）。打开脚本回放过程显示功能需要勾选的选项如图17所示：

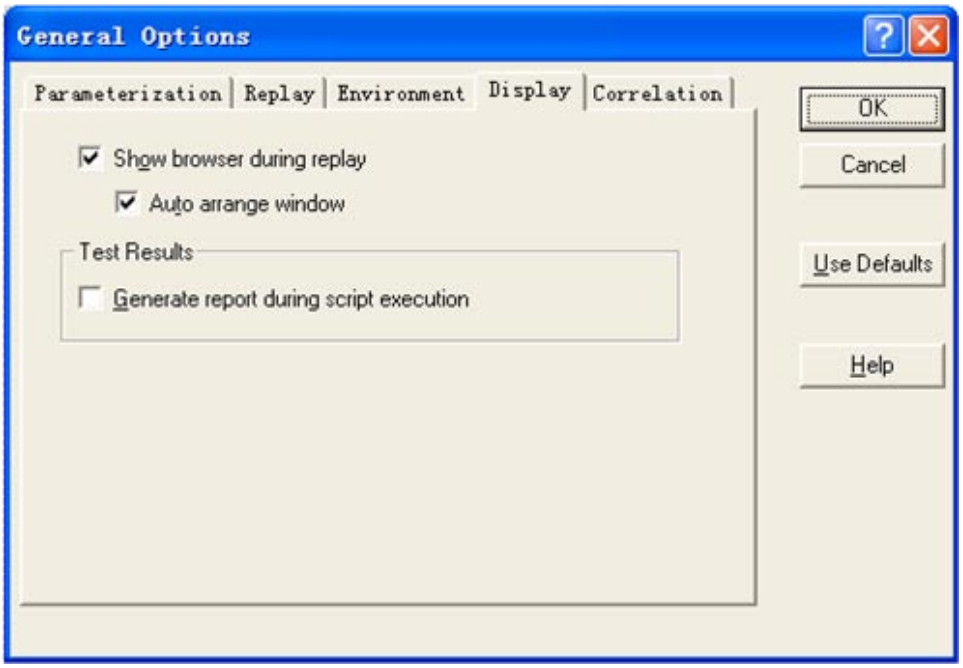


图17 Display选项

在“上次回放概要”页面列出了检测到的所有错误，并显示录制和回放快照的缩略图。如图18所示：

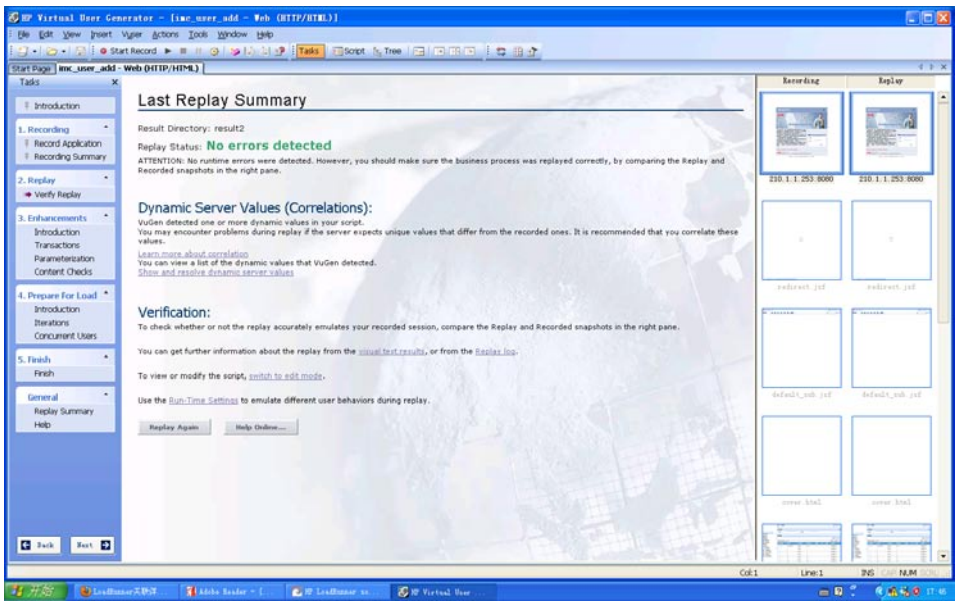


图18 回放概要

图18所示的这些信息说明我们录制的脚本在回放中未产生错误，也就是说我们可以用这个脚本进行负载测试了。但不要忘了，上面这个脚本中，我们输入的用户名、密码是固定的，如果我们用LoadRunner模拟N个user执行新建用户操作，这些虚拟用户（Vuser）新建的用户名/密码都是同样的user01，这是不符合我们预期的。我们希望新建不同的用户，用户名从user01一直到user100。因此我

们需要对脚本进行修改，让LoadRunner在执行负载测试的时候，填入的用户名/密码字段每次都不一样。这就需要使用参数替代技术。

参数化已经录制的脚本

我们用脚本视图浏览先前录制的脚本，在Action脚本中，通过按Ctrl＋F键查找“user01”关键字，我们发现脚本中存在5处。高亮第一处的“user01”，右键并选择“Replace with a Parameter”菜单，如下图所示：

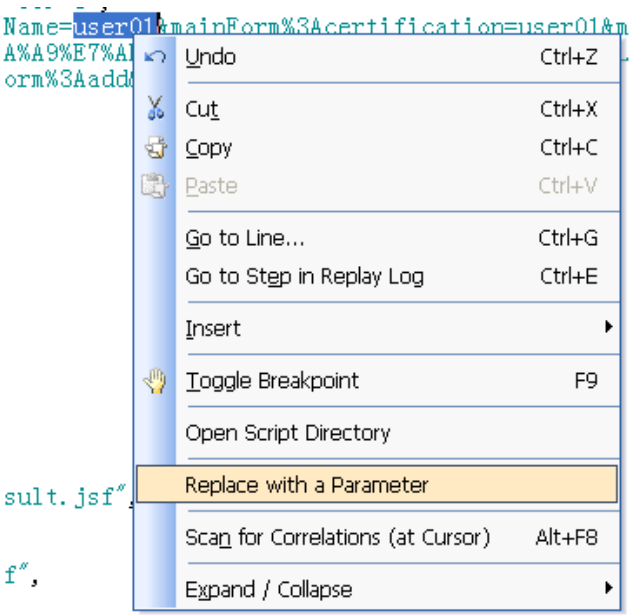


图19 “参数替换”右键菜单

在打开的对话框中输入参数的名称，比如“username”，如图20：

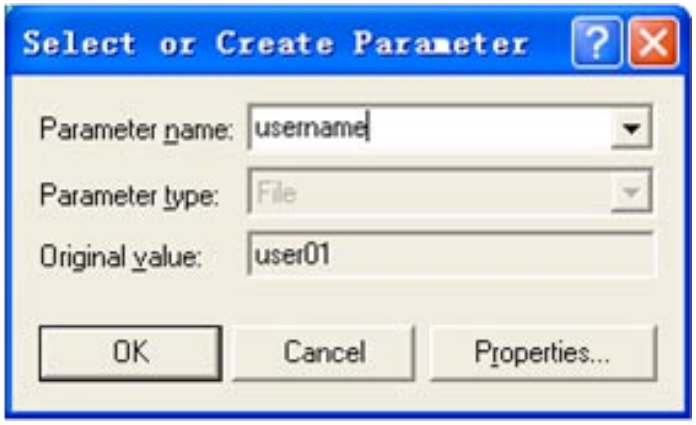


图20 创建参数对话框

点“属性”按钮打开参数属性对话框，如果中间的表格没有数据就新建一个表格，如果已有数据则可通过增加列的方式将我们希望的“user01”到“user100”共100个数据输入其中。当然我们也可以通过notepad编辑这些数据，这样做会使得数据增加更为简单。我们甚至可以通过查询数据库的方法构造参数值，这属于较高级的应用技巧，我们这里不深入介绍。

还有两个需要调整的地方，“Select next row”应该选择“Unique”，“When out of value”应该选择“Continue in a cyclic manner”。调整后的参数属性对话框如图21所示：

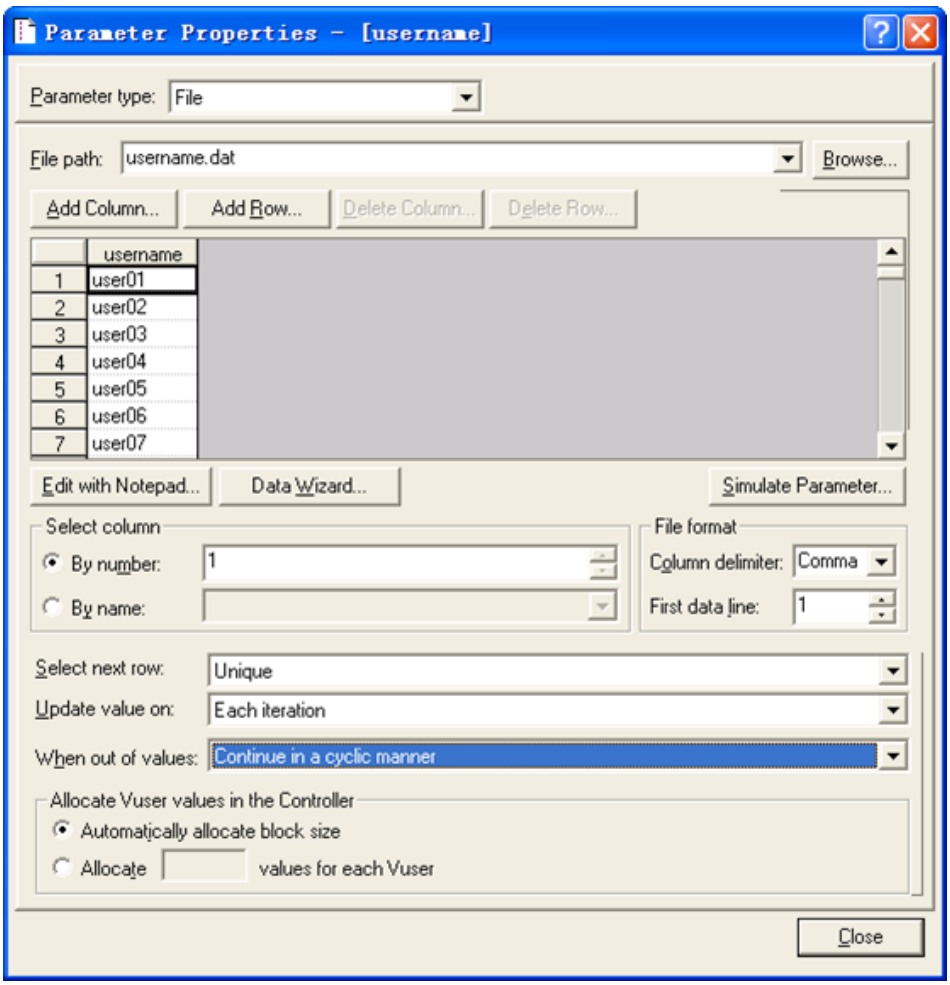


图21 参数属性

参数替换后，脚本的相应位置已替换为紫色的以花括号包围的变量参数。对于剩余部分的user01，我们选择鼠标右键菜单的use existing parameter并用刚刚建立的变量参数“username”替代。如图22：

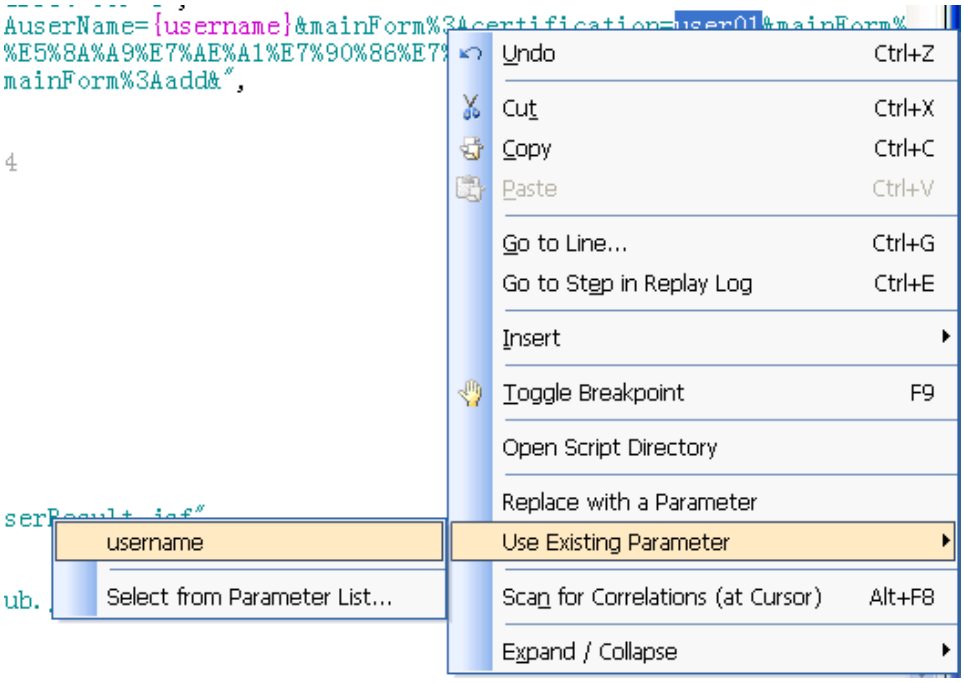


图22 参数替换右键菜单

至此，脚本录制和修改工作全部完成。

下面，我们用controller设计场景，并利用前面录制修改得到的脚本进行负载测试。

创建测试场景

创建场景

按照我们文首提到的测试例，我们创建一个场景，在场景中模拟10用户登录iMC并创建共100个账户，具体操作如下：

1 打开 Controller。

选择开始 > 程序 > HP LoadRunner > LoadRunner。将打开 HP LoadRunner窗口。

在 LoadRunner Launcher 窗格中，单击Run Load Tests。这时将打开 LoadRunner Controller。默认情况下， Controller 打开时将显示“新建场景”对话框。

2 选择场景类型。

选择手动场景。

3 向负载测试中添加脚本。

单击浏览按钮找到我们前面录制的脚本imc_user_add，单击确定，如图23所示。

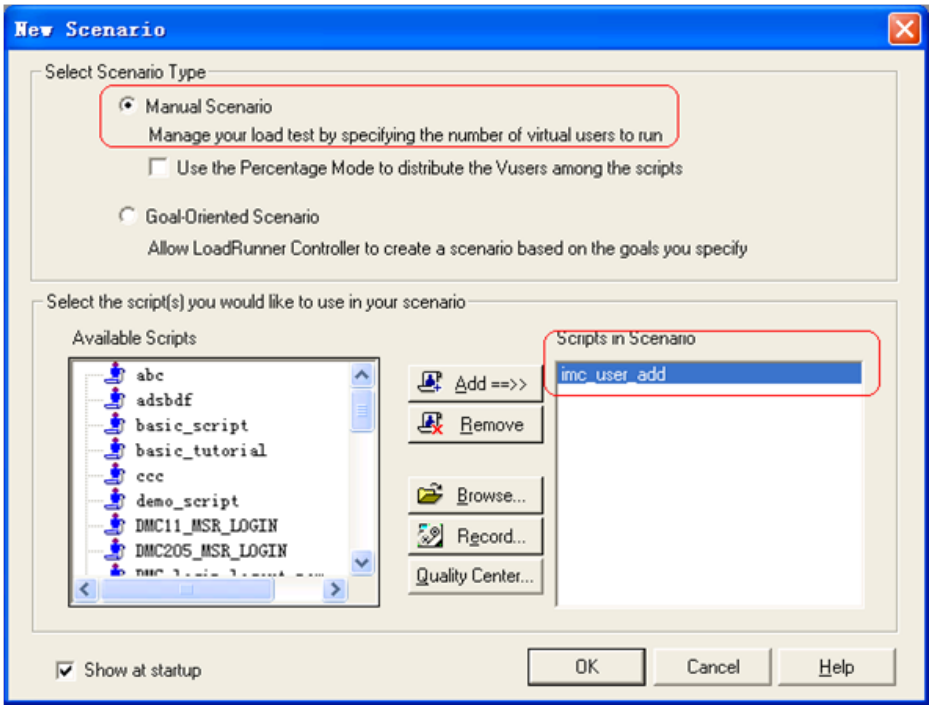


图23 新场景对话框

LoadRunner Controller 将在“设计”选项卡中打开场景。

生成负载

LoadRunner通过在应用程序中运行Vuser生成负载。LoadRunner支持分布式结构，当单机性能不足时可以使用多个Load Generator协同测试。在本测试中因为单机性能可满足要求，我们只需要在如图24所示之处选择localhost即可。如果此处是空白，可以自己添加一个名为localhost的Load Generator，系统会自动建立连接。

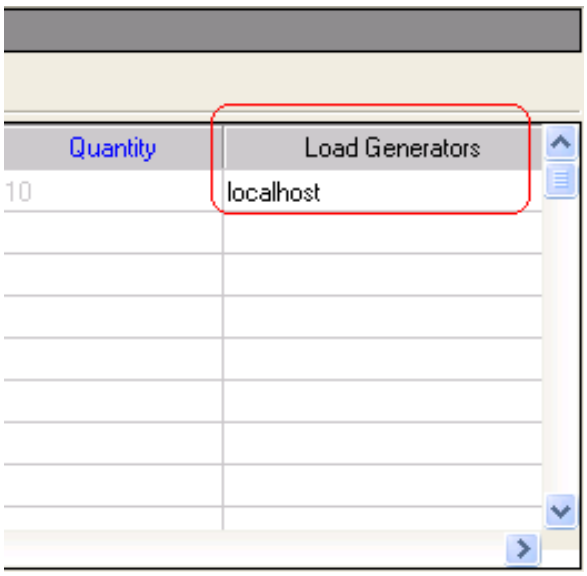


图24 Load Generators

模拟真实负载行为

在正常使用iMC的时候，用户不会正好同时登录和退出系统。利用 Controller 窗口的“场景计划”窗格，可创建能更准确模拟典型用户行为的场景计划。

例如，创建手动场景后，我们可以设置场景的持续时间或选择逐渐运行和停止场景中的 Vuser。

我们可以更改默认负载设置并配置场景计划。

1 选择计划类型和运行模式。

在“场景计划”窗格中，选择计划方式：场景，运行模式选择：Run until comlete。

2 设置计划操作定义。

在“操作”网格中，配置下列设置：

a 设置 Vuser 初始化。

在“操作”网格中双击初始化。这时将打开“编辑操作”对话框，显示初始化操作。此步骤指定用怎样的强度运行我们在Vuser_init中录制的登录iMC的脚本。为避免10个用户同时登录iMC造成iMC处理负担过重，我们将其改为每隔3秒初始化一个Vuser。

b 指定逐渐启动。

在“操作”网格中双击启动 Vuser。这时将打开“编辑操作”对话框，显示“启动 Vuser”操作。

在启动Vuser 框中，输入 10 个 Vuser 并选择第二个选项：每隔 3 秒启动1 个 Vuser。此步骤指定如何运行我们在Action录制的脚本。

由于我们在运行模式中选择了Run until complete，我们在Action中录制的脚本运行完就会自动运行Vuser_end中的脚本，并自动结束，不需要设置Vuser运行持续时间和Vuser停止顺序。

3 查看计划程序的图示。

交互计划图显示了场景计划中的“启动 Vuser”、“持续时间”和“停止 Vuser”操作。

设置好的负载参数如图25所示：

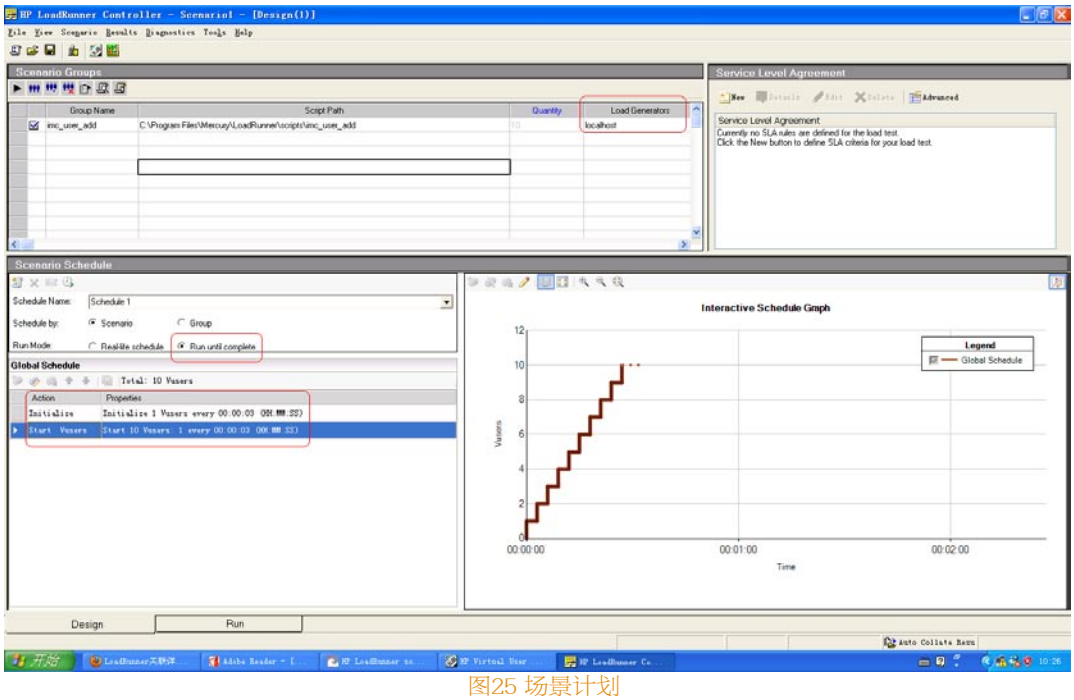


图25 场景计划

4 设置脚本运行次数

我们的测试目标是让10个用户只登录一次iMC，但每个用户在登录完成后都需要新建10个帐户。这可以通过设置Vuser运行脚本的迭代次数来实现。

点击Scenario Groups窗口中工具条上的Run-time Setting按钮，如图26所示，可打开设置窗口。

图26 场景组工具栏

在Run Logic页面将Number of Iterations次数设置为10，这样每个Vuser在运行Action脚本时就会运行10次，也就是新建10个帐户。如图27所示：

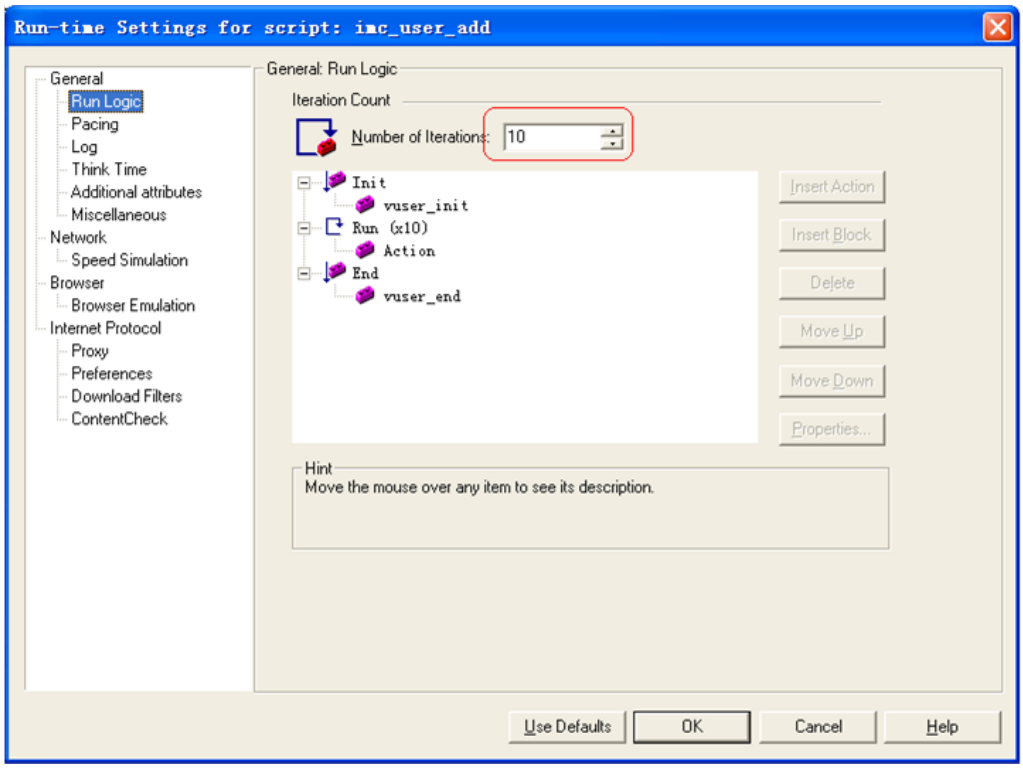


图27 脚本运行参数设定

至此，设置方面的工作我们就都完成了，接下来可以产生负载了。

运行测试场景

通过上面的步骤，我们已经完成了负载测试场景的设置，接下来就可以运行该测试并观察iMC服务器在负载下的性能。在开始测试之前，我们先来熟悉 Controller 窗口的“运行”视图。“运行”视图是用来管理和监控测试情况的控制中心。

单击运行选项卡，打开“运行”视图。

视图简介

“运行”视图包含下面几部分：

◆ “场景组”窗格。

位于左上角的窗格，我们可以在其中查看场景组内 Vuser 的状态。

使用该窗格右侧的按钮可以启动、停止和重置场景，查看各个 Vuser 的状态，通过手动添加更多 Vuser 增加场景运行期间应用程序的负载。

◆ “场景状态”窗格。

位于右上角的窗格，我们可以在其中查看负载测试的概要信息，包括正在运行的 Vuser 数目和每个 Vuser 操作的状态。

◆ 可用图树。

位于中间偏左位置的窗格，我们可以在其中看到一列 LoadRunner 图。要打开图，我们可以在树中选择一个图，并将其拖到图查看区域。

◆ 图查看区域。

位于中间偏右位置的窗格，我们可以在其中自定义显示画面，查看1 到 8 个图。

◆ 图例。

位于底部的窗格，您可以在其中查看所选图的数据。选中一行时，图中的相应线条将突出显示，反之则不突出显示。

运行负载测试场景

我们已经完成了脚本录制和场景设置工作，下面我们正式开始负载测试，也就是利用Controller来运行场景。我们按照如下步骤进行：

1 开始场景。

在“Run”选项卡上选择[Scenario >> Start]菜单，开始运行测试。Controller 将开始运行场景。

2 利用 Controller 的联机图监控性能。

当测试运行时，可以通过 LoadRunner 的一套集成监控器实时了解应用程序的实际性能以及潜在的瓶颈。我们可以在 Controller 的联机图上查看监控器收集的性能数据。联机图显示在“运行”选项卡的图查看区域。默认情况下，将显示下面几张图：

“运行”选项卡显示下列默认的联机图：

◆ “正在运行 Vuser – 整个场景”图。显示在指定时间运行的 Vuser 数。

◆ “事务响应时间 – 整个场景”图。显示完成每个事务所用的时间。

◆ “每秒点击次数 – 整个场景”图。显示场景运行期间 Vuser 每秒向 Web 服务器提交的点击次数（HTTP 请求数）。

◆ “Windows 资源”图。显示场景运行期间评测的 Windows 资源。

通过以上几张图表，我们可以看出Vuser的运行数量和iMC的响应时间及iMC服务器的资源消耗。如果资源消耗过大，或者iMC响应时间过长，就表示存在性能瓶颈，需要具体分析优化。

下面是测试图表的示例：

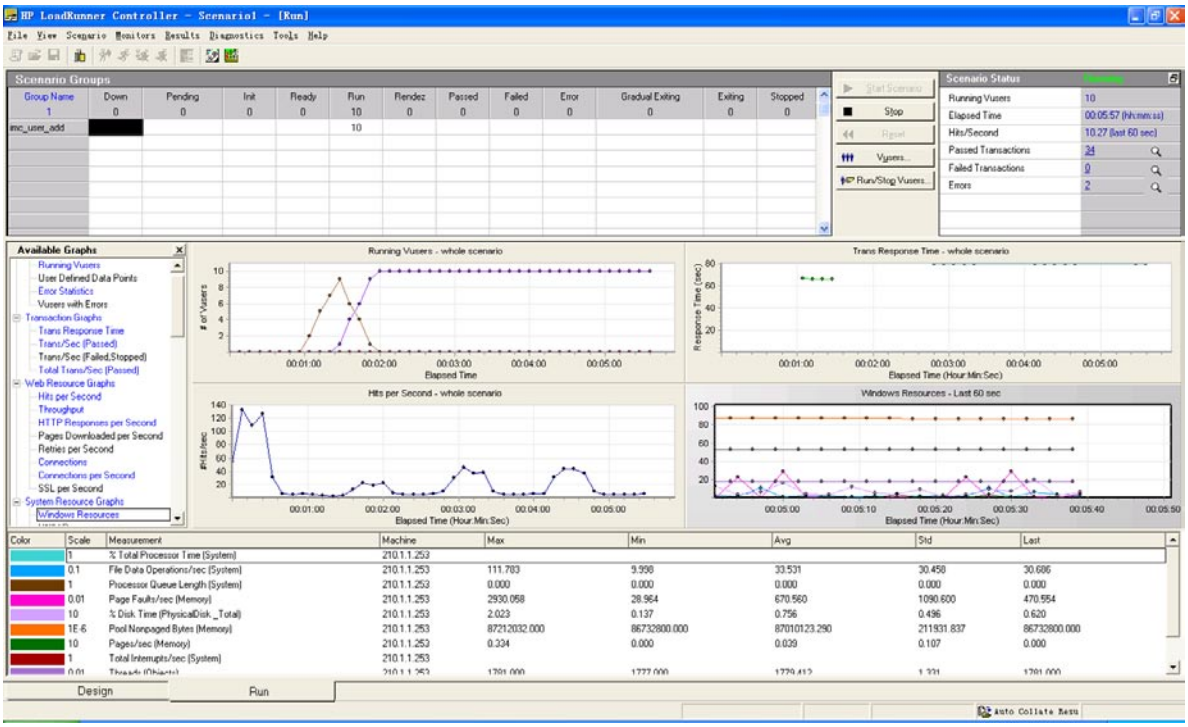


图28 场景运行界面

点击<Vusers…>按钮，可以在弹出的窗口中看到所有10个Vuser的运行状态，如图29：

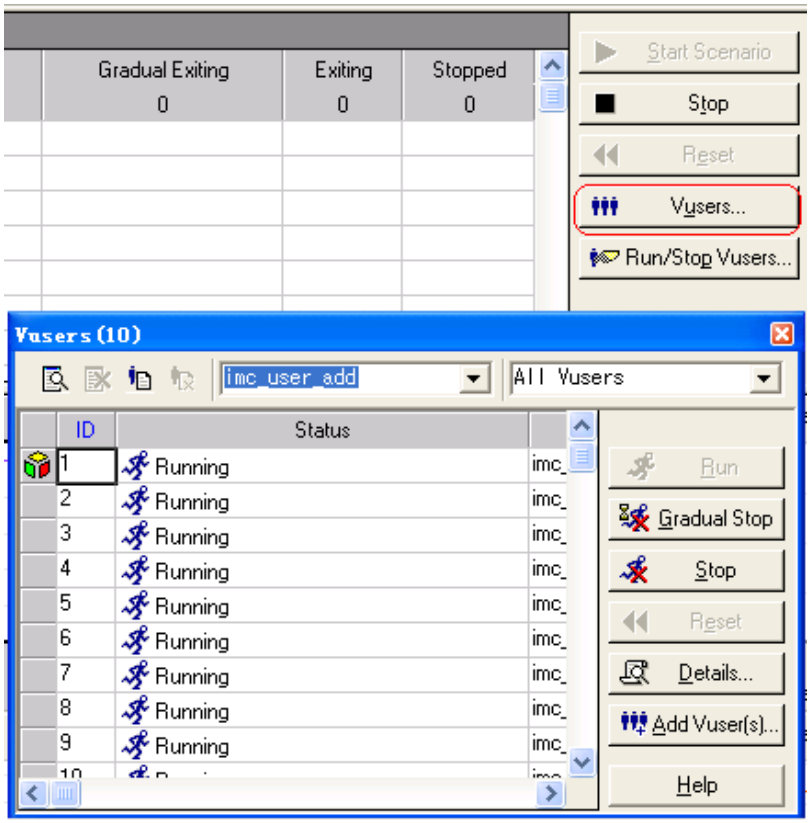


图29 Vusers状态

从该窗口中可以看到所有的用户从初始化状态再到running状态再到运行结束状态的全过程。上图中所有的Vuser都处于running状态，说明这些虚拟用户都在执行Action脚本。

对窗口中的任意Vuser点击鼠标右键，从右键菜单中选择“Show Vuser”，如下图所示，可以打开LoadRunner自带的浏览器，通过浏览器看到Vuser每一步的操作。这样可以更准确观察到Vuser是否成功执行了我们录制的操作。

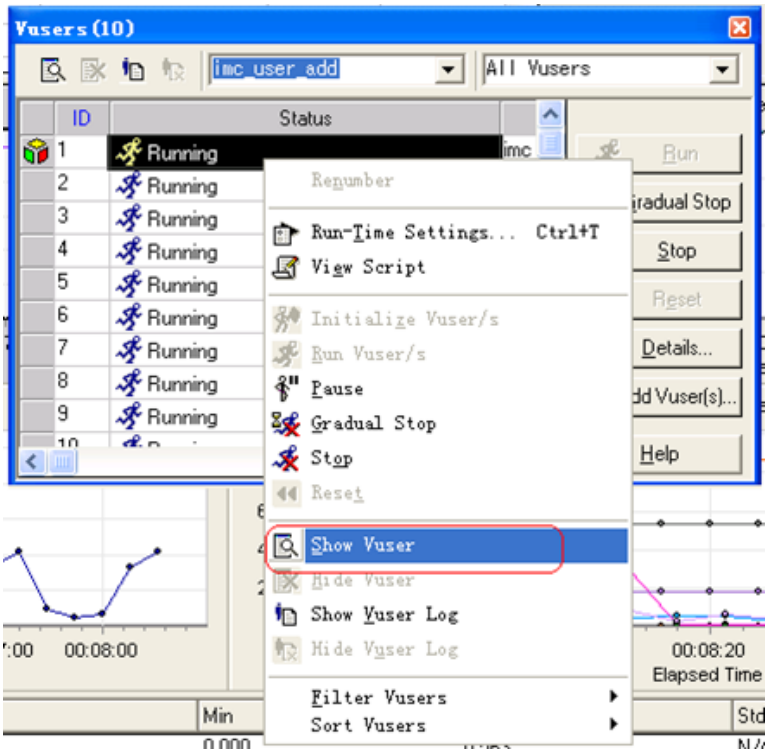


图30 Show Vuser菜单

运行结束后，在status窗口会显示所有Vuser运行的结果。如图31所示。如果failed transactions数量不为0，则可以点击展开更多信息，进一步定位执行错误。

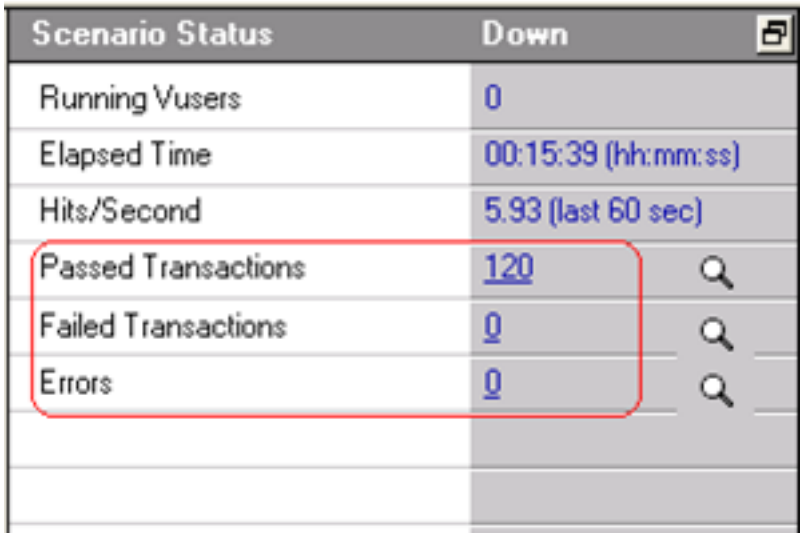


图31 场景状态

通过更改Vuser数量，Vuser登录时间间隔，脚本迭代次数等参数，可以产生不同负载情况。持续加大负载直到出现较多failed transactions计数，则可判断出现性能瓶颈。

总结

在上文中，我们通过执行测试例介绍了使用LoadRunner实现iMC压力测试的一般步骤。iMC包含众多模块，不同模块的实现大相径庭，对不同模块需要施加不同的压力以测试其性能和稳定性，因此需要有针对性的录制脚本，针对需要施压的步骤调整Vuser数量及脚本执行频度，以达到较好的测试效果。限于篇幅，本文只简单介绍了一些基本的测试步骤和测试方法，盼望能起到抛砖引玉的作用，帮助大家开发出更多、更好的脚本，对iMC的功能、性能进行更充分测试，为提高我司产品质量做出更大的贡献。

业务软件的自动化测试实践

文/赵晓丹

前言

软件自动化测试是通过计算机逐步执行预先设计的测试脚本，把得到的结果和预期结果进行比较的过程。好的自动化测试过程可以大大节省人力、时间、硬件资源等，从而提高测试效率。GUI软件指的是拥有图形用户界面的软件，GUI软件自动化测试是使用自动化工具模拟计算机鼠标、键盘事件对软件用户界面进行操作，从而替代手工执行测试用例的一个过程。GUI软件的自动化测试常用在基本功能的配置测试、软件的回归测试等。

业务软件产品iMC(Intelligent Management Center，以下简称iMC)是基于B/S架构的应用软件，客户端是使用浏览器进行操作的GUI界面，存在大量的配置操作。现有的迭代开发模式注定了版本转测试的间隔不断缩短，每个版本进行手工遍历测试在时间上是不允许的。所以，对于成熟模块采用自动化脚本进行遍历，可以解决人力投入不足无法保证原有功能模块覆盖测试的问题，从而保证软件产品的质量。

GUI自动化测试工具选择

业界常用的GUI自动化测试工具有以下几种：

◆ Rational Functional Tester (简称RFT)：RFT是基于Java语言的自动化测试工具，主要用于Web、Java App以及Win32 GUI应用程序。

◆ QuickTest Professional (简称QTP)：QTP是一款侧重于功能的企业级自动化测试工具，主要是VBScript脚本语言，支持Web、ActiveX等应用程序的测试。

◆ WinRunner：主要用于Windows环境下的各种GUI应用程序，使用类C的脚本语言TSL，不支持Java App的GUI应用程序。

◆ Auto IT：来源于开源社区的轻量级GUI自动化测试工具，但是对Web支持不太好。

◆ WatiN：开源的.Net类库，仅用于测试Web应用，脚本开发和调试基于.Net开发环境。

结合iMC产品的三个特点：1)B/S结构；2)Java语言开发；3)GUI界面应用，RFT非常满足业务软件自动化测试的需求。

GUI自动化测试简介

对于GUI软件自动化测试来讲，最常见最简单的莫过于记录–回放模式。一般的GUI自动化测试软件都支持记录回放功能。这种模式下测试脚本通过录制获取，在回放过程中执行录制的脚本。其优点是简单、方便、上手快。但是也存在明显的缺点，脚本孤立不能复用，寿命短；代码自动生成，可读性差，维护成本高。为克服简单记录回放模式的缺点，自动化脚本不断的抽象和封装，逐渐发展到系统化、层次化的自动化测试框架。

iMC的自动化测试，从开始选择使用RFT（Rational Functional Tester）工具到目前，实际上经历了三个阶段。

◆ 起步阶段：该阶段是工具选型后，自动化测试工作刚起步。此时纯粹采用录制回放技术，自动生成脚本。主要在测试执行开始时，作为测试工作的辅助手段，替代部分重复的手工操作。这个阶段的脚本基本上不具备复用性，脚本执行的功能也很简单。

◆ 发展阶段：通过脚本开发规范的逐步更新完善，在录制的脚本基础上修改生成的代码，增加注释，提高了脚本的可读性。同时，对于重复步骤的提取和封装，增加了部分脚本的复用性。这个阶段，自动化环境逐步固化，脚本复用程度提高，但是不足之处仍是采用录制，测试对象是静态对象，在产品界面变动频繁的情况下，脚本维护成本过高。

◆ 成熟阶段：经过几年的发展，目前iMC自动化测试工作进入成熟阶段。固定的测试组网环境，完善的脚本编写规范，成熟的测试流程步骤构成了一个系统的自动化测试框架。 目前的自动化测试框架下，脚本开发模块化，脚本架构层次化，同时采用动态的测试对象，更利于脚本代码的复用和维护。

目前业务软件产品iMC的自动化测试逐步规模化和系统化，主要步骤包括以下几个活动要素（如图1所示），形成了一个闭环持续改进的过程。

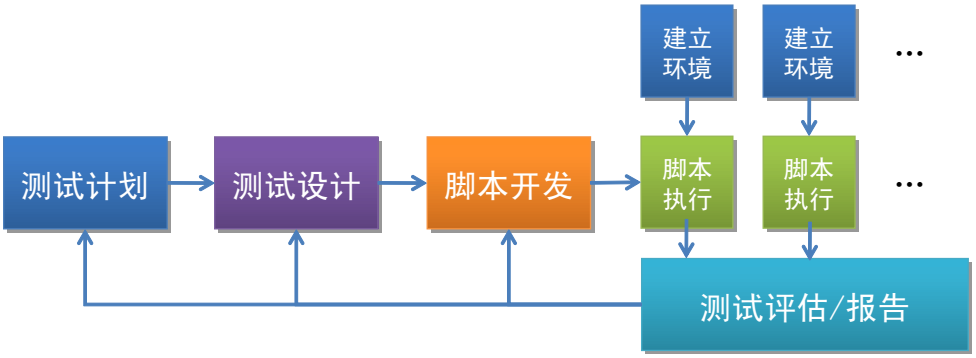


图1 自动化测试的步骤

以上的几个步骤是相辅相成的，测试计划明确测试设计和脚本开发的任务分配，测试设计为脚本开发提供测试用例，脚本的执行通过分析和评估，最终的结果又为优化计划和设计提供依据。各个步骤都有明确的责任人跟踪。自动化组网环境固化，由专人负责维护；脚本开发采用三层架构，使用VSS配置管理；每个版本测试责任人负责脚本运行和报告；自动化测试接口人负责脚本维护任务分配和测试点更新。从而确保自动化工作的持续改进。

业务软件自动化脚本架构

iMC自动化测试脚本包括公共类库和按照特性划分的测试脚本集组成。公共类库包路径为com.h3c.common ，如下图2所示，主要包含脚本日志记录、异常处理、表格操作、对象操作以及字符串操作等公共方法，不涉及具体的被测软件。 测试脚本和测试用例是一一对应的。测试用例设计是按照产品、组件、特性进行划分的，所以一个测试脚本集实际上是一个特性的所有自动化脚本集合。以iMC PLAT组件的告警特性为例，其脚本的包路径为com.h3c.imc.plat.alarm ，如下图3所示。

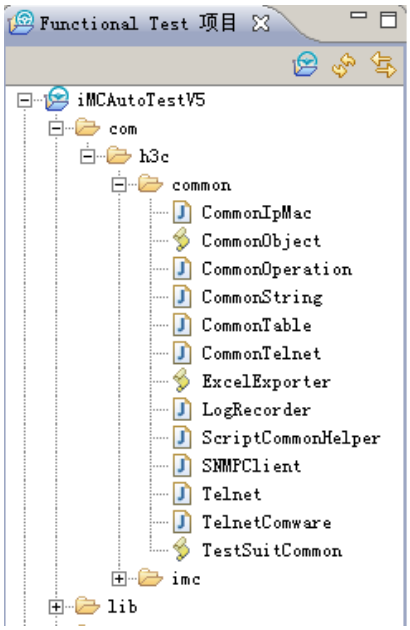


图2 公共类库结构示意图

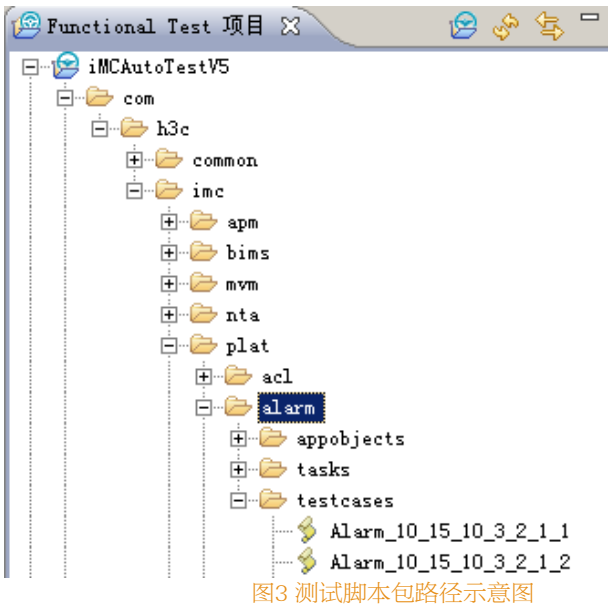


图3 测试脚本包路径示意图

特性的脚本开发采用三层架构，从下到上分别是对象层、任务层、脚本层 。三层结构使脚本可读性更强，复用率更高，易于维护和移植。

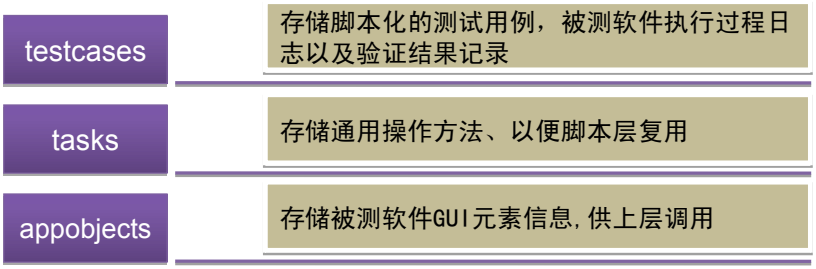


图4 自动化测试脚本的三层架构

测试对象层

测试对象层主要存储的是被测软件GUI元素，在RFT脚本中称之为测试对象。以下图5中的登录界面为例，其中操作员、密码输入框和登录按钮就是测试对象。

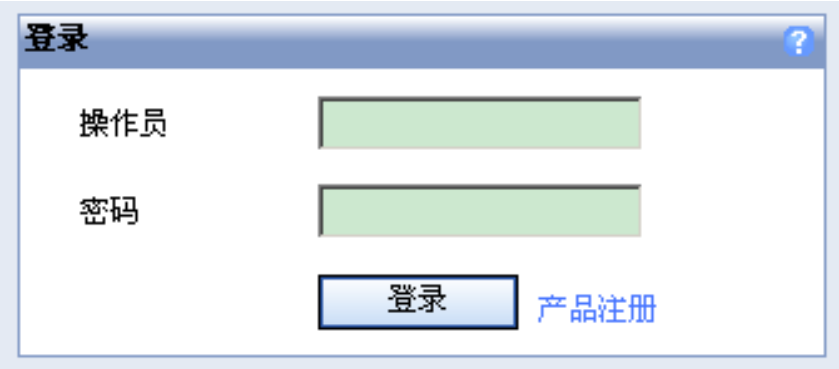


图5 登录页面GUI元素

在RFT自动化脚本中可以使用测试对象图保存测试对象和界面GUI元素的映射，也可以使用RFT提供的API中的find()方法获取测试对象。测试对象图使用xml文件保存识别GUI界面元素的关键信息，在脚本运行过程中通过这些信息映射到界面相关元素然后调用鼠标键盘事件进行操作，达到自动运行的效果。

使用测试对象图映射获取测试对象，包括以下几个步骤：

1、在对象层脚本的“脚本资源管理器”中，双击<专用测试对象映射>打开对应脚本的测试对象映射图；

图6 脚本资源管理器

2、在测试对象映射图中，点击 ，弹出对象查找器。如下图所示：

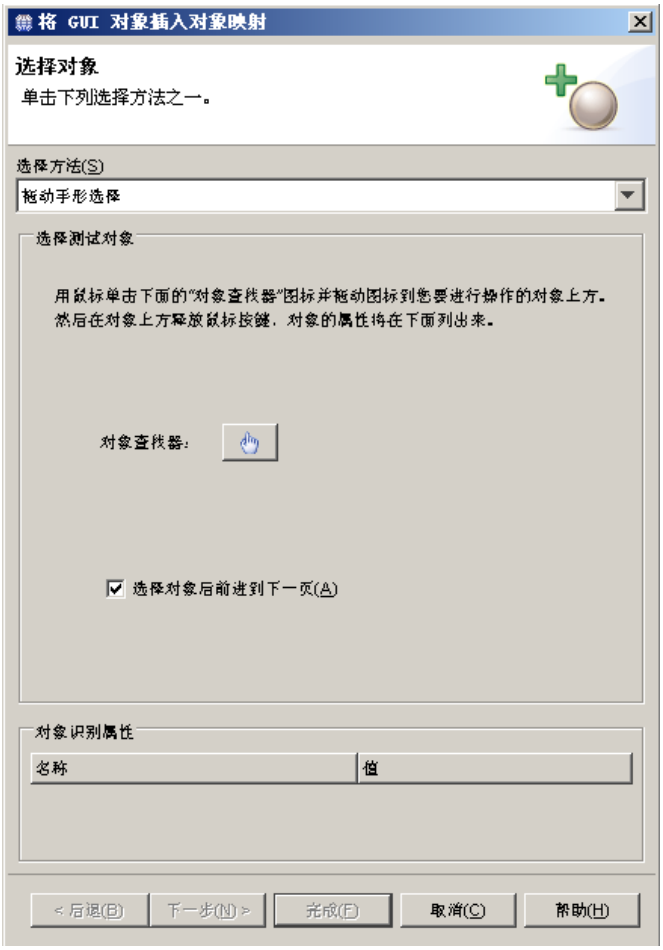


图7 对象查找器

3、通过点击手型按钮，拖动到登录页面相关控件上选取相应的测试对象。

图8 拖动并选取对象

4、然后完成抓取，测试对象被保存在对象映射图中，如下图所示。

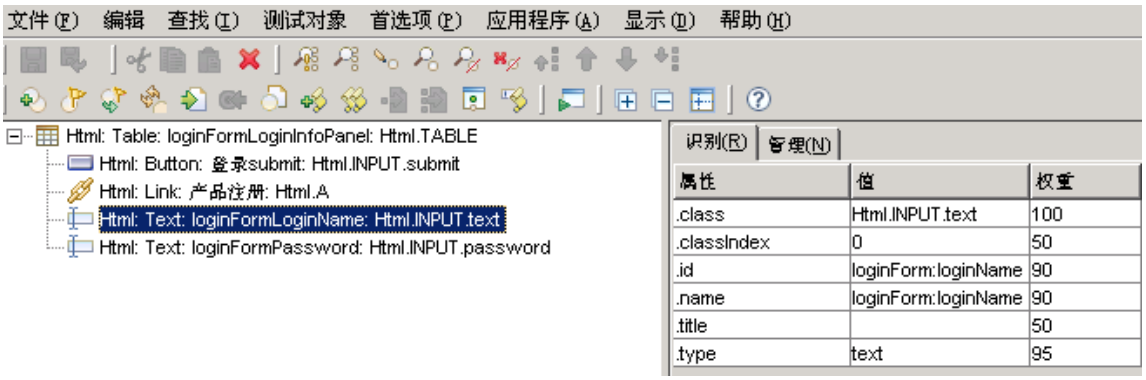


图9 登录页面测试对象映射图

一般对于表格等数据动态变化的界面元素使用测试对象映射，对于输入框、按钮等不涉及数据更新的界面元素建议使用find方法()。举例如下：

```
/**
 * 在登录表格中使用find方法查找登录按钮
 *
 * @param nInterval 两次find时间间隔
 * @param nTotal 累计find时间
 * @return 返回查询到的登录按钮测试对象
 * @throws Exception 识别对象不唯一和测试对象不存在两个异常
 */
public GuiTestObject btnLogin(int nInterval, int nTotal) throws Exception {
  // 使用RFT提供的find方法，根据控件的类型和id属性查找相应的测试对象
        TestObject[] objects = tblLoginInfo().find(
              atDescendant(".class", "Html.INPUT.submit", ".id", "loginForm:loginCmd"));
        int nRetry = nTotal / nInterval;

        // 尝试多次查找
        while (objects.length == 0 && nRetry > 0) {
              sleep(nInterval);
              objects = tblLoginInfo().find(atDescendant(".class", "Html.INPUT.submit",
".id", "loginForm:loginCmd"));
```

```
                nRetry--;
            }
            // 根据查找结果判断测试对象是否存在或多余
            if (objects.length > 0) {
                if (objects.length > 1) {
                  throw new Exception("识别对象不唯一：界面存在多个登录按钮");
                }
              return (GuiTestObject) objects[0];
            } else
              throw new Exception("测试对象不存在：当前界面不存在登录按钮");
        }
```

任务层

任务层主要存储针对界面操作封装的方法类。每一个方法都是一段界面操作，将具体的测试数据抽象为方法的参数，使任务层的方法可以在脚本中重复使用。登录操作的方法代码如下：

```
        /**
         * 登录iMC方法
         *
         * @param sUrl iMC地址
         * @param sUsrName 操作员名称
         * @param sPwd 密码
         * @return 登录成功返回true
         */
        public boolean Login(String sUrl, String sUsrName, String sPwd) {
            Info("登录iMC页面");

            // 打开IE浏览器并输入iMC地址
            com.h3c.common.CommonOperation.StartApp(Config.s_sIE_Path);
            sleep(3);

            if (!ToPage(sUrl))
                continue;

            Debug("输入用户名:" + sUsrName);
            objLoginPage.txtLoginName().setText(sUsrName);

            Debug("输入密码:" + sPwd);
            objLoginPage.txtLoginPassword().setText(sPwd);
            sleep(1);
```

```
        Debug("点击登录按钮");
        objLoginPage.btnLoginSubmit().click();

        // 3秒钟检查一次是否登录成功，半分钟后不成功认为登录失败
    // 登录成功会出现注销链接
        for (int i = 0; i < 10; i++) {
            sleep(3);
            if (objLoginPage.lnkLogout().exists()) {
                Info("登录成功。");
                return true;
            }
        }
        Error("登录失败。");
        return false;
    }
```

测试脚本层

测试脚本层存储测试用例对应的测试脚本。通过记录操作过程日志，调用tasks层的方法，打印DEBUG信息，判断脚本执行结果等构成一个完整的脚本。测试脚本包括以下几个重要内容：

◆ 测试数据声明：包括实例化tasks层类，用于脚本执行调用相关方法；声明测试输入和预期结果数据。

◆ 过程日志打印：脚本执行结果需要通过运行日志进行分析，从而判断是否是软件存在BUG，详细的过程日志（包括DEBUG信息）将大大提高定位分析问题的效率；

◆ testMain函数：RFT自动化脚本每个脚本中都有一个testMain函数，所有该函数中的步骤都会被顺序执行，测试步骤需要顺序在该函数中调用。预置条件、测试步骤、结果验证、后置条件等都需要在该函数中顺序调用。

◆ 验证点：每一个测试步骤建议设置验证点（也称检查点Checkpoint），判断该步骤运行是否和预期结果一致。

```
package com.h3c.imc.plat.system.testcases;

import com.h3c.imc.plat.common.Config;
import com.h3c.imc.plat.common.tasks.CommonOperation;
import com.h3c.imc.plat.system.tasks.LogOut;
import resources.com.h3c.imc.plat.system.testcases.System_10_15_10_1_2_1_4Helper;

/**
 * Description : 10.15.10.1.2.1.2.4 验证登录和注销操作
 * <p>
```

```
 * 步骤1：使用操作员admin登录成功<br>
 * 步骤2：注销操作员登录成功
 */
public class System_10_15_10_1_2_1_4 extends System_10_15_10_1_2_1_4Helper {

    // 注销操作封装
    private LogOut m_Logout = new LogOut();

    // PLAT公共方法封装
    private CommonOperation m_PlatCom = new CommonOperation();

    // 参数初始化
    // 验证的操作员登录名
    public String m_sLoginUser = “admin”;
    // 验证的操作员登录密码
    public String m_sLoginPwd = “admin”;

    public void testMain(Object[] args) throws Exception {
        if (m_sTestPoint.length() < 1)
            m_sTestPoint = "10.15.10.1.2.1.2.4 用户注销";
        ScriptStart();

        Step("检查操作员登录iMC");
        if (false == m_PlatCom.Relogin(Config.s_sImcWebUrl, m_sLoginUser, m_
sLoginPwd))
            ScriptNg("操作员" + m_sLoginUser + "登录iMC失败");

        Step("检查操作员是否能够正确注销");
        if (false == m_Logout.CheckLogOut()) {
            ScriptNg("操作员注销操作验证失败");
        }

        m_PlatCom.ClearUp();
        ClearUp();
    }
}
```

测试集是单次运行测试脚本的汇总，运行日志是按照测试集生成的。多个自动化测试脚本可以组成一个测试集，一般一个特性一个测试集。测试集运行完成后，根据运行日志汇总可以知道脚本运行通过情况，比如NG个数，通过率等。

GUI自动化的难点和改进方法

GUI自动化测试的特点决定了其主要难点在于界面变化。由于GUI自动化必须先有界面，然后才能开发脚本。对于脚本开发人员来讲，很难知道界面变化的具体内容，只有在脚本运行失败后才能知道界面变化了。当然GUI软件不可能界面一成不变，怎样尽量减少界面变化对脚本的冲击，是解决该问题的根本途径。

首先看一下RFT自动化测试脚本的特点，其实质是通过测试对象的识别，然后调用鼠标键盘事件对识别出来的测试对象进行操作以替代手工执行。归根到底最关键的是测试对象的识别。测试对象的识别有两种方式，一种是通过保存在测试对象图的抓取的页面元素，一种是通过find()方法获取的。这两种是根据页面元素的html属性来识别的，主要有“.class”“.id”“.name”“.value”等。只要这些属性固定不变，界面的布局变化也好、位置变化也好都不再影响测试对象的识别。通过制定界面修改的操作规范，明确规定开发人员界面变化时对GUI元素属性的处理。同时，在对象层采用动态测试对象和find()按照id属性获取对象，从而大大减少了界面变化对脚本的影响。

结束语

任何测试活动必须有完善的流程支撑才能顺利开展。通过GUI自动化脚本开发规范的制定，明确定义了脚本的三层架构、代码组织、脚本命名、脚本验收、归档入库等各项活动细则。在全员参与下，脚本库逐步丰富，自动化覆盖度逐渐增加。目前已经逐步覆盖业务软件iMC产品PLAT、NTA、APM、WSM、BIMS、MVM组件的21个特性730多个脚本，作为手工测试的补充，自动化测试正在不断发挥作用。

测试中心
TESTCENTER

网络之路

主办单位：H3C测试中心

策　　划：刘　宇 陈旭盛 杜祥宇

主　　编：陈　翀

本期编委：徐庆伟 符　斌 伊莉娜 袁亚屏 王白辉 史计达 袁　江 袁亚屏

徐泽新 其其格 王守唐 曾　劼 李　丹 刘宇征 赵晓丹