

应用层的显示服务提供图形化的报告输出。

总之,面向资源的管理模型充分利用Web 服务架构的特性,以资源为基础构建整个管理功能框架,灵活地实现功能服务间的相互交互,并通过标准化的机制实现资源的监视和管理的统一。

## 管理系统的实现架构

为了验证本文提出的管理体系和功能模型的有效性和可能性,本文采用了REST和RIA 技术开发了管理系统原型,如图5所示:

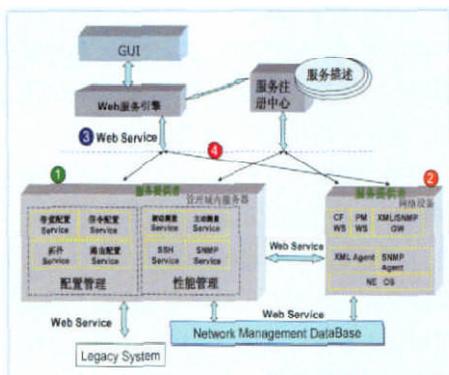


图5 基于Web Service的分布式管理系统实现架构

在原型系统中实现了网络管理中配置和性能两大方面的管理功能,其中服务注册中心将借助Internet中原有的DNS服务来实现。

整个系统与外部系统、管理域对等管理者之间、系统内部不同功能模块之间均采用统一的Web Service接口,系统的扩展性和灵活性高。

此外,系统的服务提供者主要包括平台和网元,管理应用通过服务引擎可以动态绑定服务并调用服务,也可以通过静态映射方式调用服务。

与其他基于Web服务的网络管理架构相比,该管理架构的优点在于:1.充分利用互联网及其服务的特性,提高了服务使用的效率,解决了注册中心带来的性能瓶颈;2.采用面向资源的功能模型,灵活地实现了网络管理服务间的信息交互,因此基于Web服务的分布式体系架构具有良好的应用前景。CEN

(作者单位为东南大学计算机学院)

## 上海交大图书信息楼启用

# “数字大学”资源服务进入新阶段

本刊讯 9月24日,上海交通大学(简称:上海交大)在闵行校区汇聚了来自教育部、上海市教委、中国教育科研和计算机网CERNET、中国高等教育学会教育信息化分会以及全国70余所高校近200位代表,共同庆祝上海交大“数字大学”建设十周年,见证上海交大网络信息中心新楼(已正式

命名为:图书信息楼)启用揭牌,并举行了“2009高校信息化实践者精英论坛”开幕仪式。

在本次大会上,上海交大校党委副书记苏明教授表示,新建成的图书信息楼为学校进一步的发展创造了有力的条件,为“数字大学”的深化建设翻开了崭新的一页。

他表示,十年来,“数字大学”的建设取得了明显成效。学校通过加强校园基础网络设施建设,完善管理信息系统,提供丰富的信息资源,极大地推动了教学方法的改革,提高了行



政办公的效率,促进资源的整合、采集、服务和有效的利用,为校园文化的发展和师生的生活提供丰富多彩的平台和良好的环境。这些对于提高学校信息化水平,构建大学管理现代化发挥了重要的作用。

据悉,图书信息楼占地总面积为5.7万平方米,一共分为两个部分:图书馆和信息

服务楼。图书馆共有4层,建筑面积达3.5万平方米,定位为“理工生医农科综合馆”,涵盖9大阅览室。而信息服务楼共有9层,作为学校“数字大学”建设管理、运行服务、技术开发和研究试验的基地。楼内汇集了校园网、数据中心、托管、高性能计算等设备机房,设置了功能完备的运行监控中心和舒适的用户服务环境。

上海交大校党委书记马德秀、原校长谢绳武、上海交大副校长印杰和教育部科技司信息化处付恒升处长共同为图书信息楼启用揭牌。

## “网络战”暗地打响

“种种信息表明,网络安全已经被越来越多的国家提升到非常重要的地位;网络战——作为未来战争形态之一,备受重视。”

中国科学院研究员许榕生在接受媒体采访时表示,作为一个可能的、全新的战争形式,网络战似乎模糊了战与非战、军事战争和商战、个人违法活动和国家行为的界限,且网络战的规模、影响力、震撼力、破坏力可能都会很大,如何避免网络战争以求得和平与发展,成为信息时代政治家、军事家、战略家以及专家学者们所关注的新的历史课题。

那么,什么是网络战?网络战具有哪些特点?

许榕生研究员分析指出网络战大体上分为三个等级:

第一个等级是通过通信干扰、破坏甚至控制对方的电子系统。这种破坏通信系统的信息轰炸方式,美国在伊拉克战争初期采用过,包括对伊军用系统进行电子干扰并使用网络攻击破坏伊地面部队的通信。美军的EC-130H干扰机在干扰伊军通信网络的同时,向部分频段的

通信网络散布假消息和指令,几乎“接管”了伊军地面部队。去年以色列战斗机在空袭叙利亚目标时,也使用了这种网络攻击技术,控制叙利亚雷达转向。

第二个等级是通过发动小规模的互联网攻击。策应、支援常规战争行动,或者进行警告。科索沃战争时期,大量南联盟黑客对美国重要网站发动进攻,就属于这种层次的网络进攻。

第三个等级是全面的网络战争。目前的网络系统存在安全上的弱点,很容易被敌方利用,从而攻入关键的系统,例如控制电厂、精炼厂、民用通信的网络以及金融机构和其他基础设施的控制网络。

他表示,研究网络里面可能要发生的情况是非常复杂的,有很多方面需要预先研究,同时采取技术与非技术的必要措施。关心网络战的一些问题,可以了解国外网络战的发展现状,同时思考我们自己面对的威胁在哪里?网络战与反恐斗争密切相关,保障网络安全应是人人有责。(来自《信息安全与通信保密》)