

主管: 中华人民共和国教育部
主办: 教育部科技发展中心
承办: 中国教育和科研计算机网CERNET网络中心

服务器新趋势

大连理工大学和中国人民大学都采用高配服务器和海量存储系统来实现数据中心的硬件配置,这两个项目可以说是国内大多数重点高校数字化校园建设的典型案例。其他高校也有类似的硬件结构,但是部分高校在硬件利用率、各种业务的支持、系统的后向扩展等方面都存在或多或少的问题。

那么,在高校投入有限的情况下,如何才能更好地使信息化建设持续发展?答案是实现服务器新时代的虚拟化技术、云技术和绿色节能技术。

首先,通过虚拟化技术可以提高硬件资源的利用率和管理效率。以前高校院系自行购买的设备在完成任任务之后,设备容易被闲置。而通过虚拟化将这些闲置的设备整合起来,可灵活分配资源。北京工业大学正是利用这一技术,把分散的资源集中起来做成高性能集群,通过虚拟化提供服务。除了分散机器的整合,虚拟技术也可以应用在高端服务器上。虚拟化能够有效地提高应用的部署密度,减少服务器的数量,降低IT系统复杂度。受益主要体现在两个方面:一是更好的业务保障,二是更低的成本。

其次,虚拟化的出发点是管理资源,而云技术的出发点是动态分配资源。建立校园云从本质上提升信息化的整体服务水平。通过云技术,用户能够方便、按需地从网络访问共享的可配置资源池,实现计算资源动态调配,进而更好地提升管理效率。校园云按照云模型建立资源池,对信息化建设的资源进行集中整合,可以保证校园信息化建设快速发展。

最后,服务器的产品研发需要更加注重能耗比。首先这符合国家倡导的政策,同时这也符合客户的切身利益,更低的功耗可以降低客户的总体运行的成本。新一代内存技术、CPU超频技术、插槽省电技术等都是从技术角度来降低能耗。同时,单机拒功耗存在上限,传统的风冷不能满足目前的需求,水冷技术逐渐被广泛应用。此外,机箱,电源的放置也是建设者需要用心思考的问题。

在数字校园的发展中,通过虚拟化、云和绿色节能技术,可以解决硬件利用率、各种业务的支持、系统的后向扩展等难题。

近年来,国内服务器行业也在激烈的竞争中逐渐成熟起来,通过系统化的解决方案和本地优势逐渐夺回市场。但是整体上看,国内服务器供应商还缺乏核心的技术竞争力来在同国外巨头的长期抗争中取得主动,这需国内供应商们仔细分析应对。

周晓娟

顾问委员会主任: 赵沁平
编委会主任: 李志民
编委会副主任: 吴建平
编委会委员: 马严 王兴伟 王陆 王珠珠
(按笔划排序) 张凌 张蓓 张德运 李卫
李未 李芝棠 李星 李晓明
杨健安 汪为农 汪文勇 陈禹
周全胜 金海 娄晶 祝智庭
赵宏 奚建清 袁成琛 康宁
黄荣怀 龚俭 雷维礼

总编: 吴建平
副总编: 曾艳 杨健安
终审: 袁成琛

主编: 傅宇凡
主编助理: 周晓娟
首席编辑: 王左利
编辑/记者: 周斌 谢晓丹 李茗
特约编辑: 杨望 郑先伟
美术编辑: 刘显中
市场副总监: 倪时敏
市场部: 程石 王悦
张永娟 赵玉梅 杨珊
发行主管: 李一夫

通信地址: 北京海淀区中关村东路1号院
清华科技园8号楼B座赛尔大厦8层
邮政编码: 100084
编辑电话: 010-62603857
发行电话: 010-62603896
传真: 010-62790637

电子邮箱: media@cemet.com
网站: <http://www.media.edu.cn>

开户行: 北京银行清华园支行
户名: 北京赛尔时代传媒文化有限公司
账号: 01090334600120105436980
国际标准刊号: ISSN 1672-9781
国内统一刊号: CN11-5287/TN
邮发代号: 80-354
国内发行: 北京报刊发行局
国外发行: 中国国际图书贸易总公司
国外发行代号: M02709
广告经营许可证: 京海工商广字第8067号
出版日期: 2010年10月5日
定价: 每册人民币15元
印刷: 北京画中画印刷有限公司

本刊已被CNKI中国期刊全文数据库、中国核心期刊遴选数据库收录。作者如不同意文章被收录,请向本刊声明。



政策与焦点

4 编读往来

[外媒速览]

5 IT技术导致中等收入层萎缩

[海外观察]

6 美投入 6250 万美元建设社区网

UCAN填补了一项关键空白,它将众机构连接成一个开放的社会支柱,而美国新一代网络的功能与透明度适合社会发展需要,并能完成高水平的运作与机构合作。

[高校资讯]

7 清华大学和IBM启动“清水计算”网格研究项目

[数字声音]

8 “相信学生就是中山大学善待学生的办学理念的最好体现。”

5D空间是一个以学生为主体并由学生自主管理、自主进行内容维护的大型综合门户网站。“5D空间”是“我的空间”的谐音,同时“5D”也代表着网站的5大板块,也有着“我的地盘我做主”的含义。

[产业]

9 IE9 来了!

[新思维]

10 移动“云”

[新闻速递]

11 我国互联网发展要从“大国”走向“强国”



[封面报道]

12 服务器: 突破壁垒

16 暨南大学: 服务器虚拟化解应用之困

服务器虚拟化不仅切合当前绿色低碳的环保理念,也是节约成本、提升效能的利器,更是构建高校“云计算”平台的基础。

19 清华大学图书馆: 服务器虚拟化提升服务质量

22 华北电力大学: 应用驱动发展

25 大连理工大学: 打造数据中心云基础

27 中国人民大学: 服务器成硬环境的脊梁

28 服务器加速发展的前奏

29 服务器技术的风向标

30 自主知识产权打造核心竞争力

研究与发展

[前沿技术]

32 识别 P2P 流媒体来龙去脉

35 HTML5 将带来什么

37 公共互联网网络安全问题利好



目录 CONTENTS



制程工艺的进步使得服务器变得越来越灵活,只要你愿意,可以在一个机柜里塞多台刀片服务器,但与此同时,你必须面对散热的难题。

建设与管理

[CERNET 之窗]

39 印度获较大 IPv6 地址

主干网进入暑假低谷

40 开学季:安全投诉事件增多

41 CNGI- CERNET2 主干网入 / 出流量回落

[IPv6]

42 中南大学下一代校园网升级步步为营

[无线网]

45 北京交通大学无线网顺势而为

[网络安全]

47 杀毒软件江湖:排斥与兼容的战争(上)

[校园网]

50 优化带宽之策

[案例展示]

52 数据中心:工艺与散热的博弈

54 惠普 VS 戴尔争夺 3PAR 幕后

57 南京大学 IPv6 “大提速”

58 西安理工大学:“五位一体”提升软实力

60 广西师范大学:SSL VPN 承载和谐的数图中心

61 确保下一代互联网平滑过渡

资源与应用

[开源社区]

62 Solr 学术索引应用显身手

华中科技大学图书馆累积的各种元数据总量接近 1 亿条。学校结合 Solr 开发了学术搜索系统,从而充分利用这些元数据。

65 插件助力网管软件运筹帷幄

管理员使用开源网管软件 Cacti 不仅可以方便地了解网络状态,并可以指定每一个用户都能查看树状结构、host 以及任何一张图,而且还能自己编写强大的插件来拓展 Cacti 的功能。

[网络教学]

68 网络教学缓解西部师资不足

[应用系统]

70 分布式用户认证为单点登录护航

LDAP 服务器直接暴露在其他应用系统和用户面前是具有一定的安全风险的,而以 Web Service 和 LDAP 相结合的分布式用户认证系统,则能让校园网用户进行安全的统一身份认证。



读者服务

[COST 论坛]

73 数字迎新:以人为本服务新生

[网管技巧]

74 STP 破校园网络环路难题

76 syslog 搭建服务器登录日志系统

78 使用 EMOS 搭建 Extmail 邮件服务器

79 高校数据中心:技术与管理并重

编读往来



随着“211三期”等项目的展开,校园网、数字图书馆等信息化建设项目的深入,迎来了教育行业服务器的应用高峰。如何解决服务器目前遇到的难题,使服务器有更好的发展,则需要我们共同的思考,需要各高校同仁们的智慧,希望大家能畅所欲言,贡献出自己的想法,提出好的建议。欢迎来信至 media@cernet.com。

每个月的杂志都看,尤其是网管技巧这块,经常能看到一些我需要的文章,虽然部分内容网上也有,但是很多细节的东西还需要咨询才能明白,通过杂志我能联系到作者,很多细节上的问题能做面对面的交流,解决了我工作中遇到的很多问题。

这样,杂志不仅仅让我可以处理工作上遇到的问题,还让我认识了很多高校的优秀管理人员。

十二五的专题,让我看到了其他学校在信息化建设的成果,使我校对下一步信息化建设有了更加明确的目标。虽然不能完全效仿兄弟学校的做法,但至少可以让我们明确建设目标。

在借鉴他人的同时,结合学校自身具体情况,一步一步扎扎实实地做好工作。

希望杂志能多做类似的专题,能让我们更多地了解相关信息,在建设校园网以及信息化的过程中少走弯路。

广西民族大学 吴骅

《中国教育网络》为各高校网络技术人员提高自己的专业知识结构和能力提供了一个交流的平台,在阅读杂志的过程中,不知不觉提升了自己的知识结构,更好地解决了在工作中遇到的各种问题。

由于各高校在工作之中存在共通性,我们在工作中遇到的问题,其他兄弟院校可能遇到过,各学校解决问题的方法不同,院校之间可以相互学习,共同建设好数字化校园。

211 等本科学校通过国家政策支持 and 自身雄厚的技术力量,在数字化校园建设建设

过程中积累了大量的经验,兄弟院校的数字化建设经验通过杂志、论坛等方式,为我们专科高职院校在建设数字化校园方面树立了标杆。

杂志的编辑们在各期杂志选题上,可以看出其浓厚的专业理论知识和技术的前瞻性,因为每期杂志上的内容,基本上都有各高校近期或者2-3年内所面临的问题。

建议是,在杂志和论坛中,能不能加强倡导211高校对高职高专院校开放更多的教育资源,特别是教学类的。

青岛黄海职业学院 李强

最近的“读者服务”栏目中的COST专题对我的帮助很大。看了安全意识培训这篇文章,我对如何加强用户安全有了一个较为系统的认识。文章深入浅出,使得读者能有一个从知道到了解、理解的过程。

这样的文章,希望日后能多一点。不仅仅让杂志作为我们的一个信息窗口,也成为我们的工具书。

COST论坛,让我和很多专家能够面对面的交流,解决了我不少问题,希望以后能多开展此类活动,让更多的专家能与我们交流。

我们通过《中国教育网络》杂志,看到了兄弟院校的建设成果和经验,看到了解决实际问题的方法,得到众多启发,使得我院在网络规划建设、网络管理等教育信息化建设中,将有限的建设经费用在了刀刃上,取得了较好的建设和应用效果。

湖南商学院 肖坚

屈指数来CERNET学术年会已经举行了16次,年会为高校的网络工作者提供了面对面的交流平台,每次参加都受益匪浅。为了更好地发挥年会的作用,建议:

1. 鼓励全国所有的高校参与进来。
2. 会议时间可适当延长,给予充足的交流和学习的时间。
3. 针对管理者与技术人员的会议分开举行,满足不同需求的人群。
4. 每年都找一所信息化建设出色的学校来深度分析,通过实地参观、交流来学习。

山东青年政治学院 张宏磊



Network World
2010. 8
电力行业需要更安全的 SCADA

电力行业毫无疑问是国家的重点行业，然而电力行业的数据采集与监视控制系统(Supervisory control and data acquisition)存在隐患,体现在以下几点

1. 任何电力输送的中断将造成大面积的基础设施的破坏;
2. SCADA 系统能够控制发电和输电系统并非事实;
3. 脆弱性分析项反复证明,电力公司没有意识到他们内部链接的脆弱性;
4. 商业间谍、恶意攻击对 SCADA 系统的影响案例存在;
5. 人们认为 SCADA 系统非常稳定而不需要更新补丁,结果这个系统在新老威胁面前都很脆弱;
6. 许多 SCADA 系统开发时没有考虑到安全或集成软件的质量保证。



Business Week
2010. 9. 9
大趋势——小型社交网站

Facebook 在社交网站中独占鳌头六年以后,社交网站出现了反趋势——即小型专业化。根据兴趣爱好、职业或者地区组成的社交网站数量在不断增加,而胡须男、母亲、科研人员、婴儿等等都可能成为社交网站的名称。这些网站虽然本身很小,但由于数量众多,总用户人数很庞大。

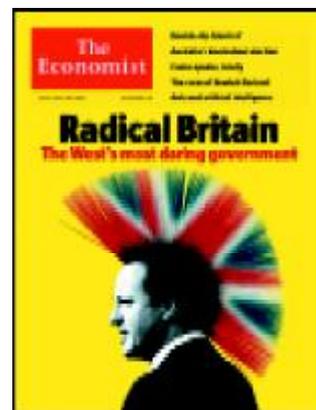
由于专业化专门化,广告商可以更有针对性地投放广告,因此这些小型网站的广告费率比一般的要高。



The Wall Street Journal
2010. 9. 9
消费电子获得风险资本关注

即使在经济衰退最严重的时候,经济危机见底的威胁都没有阻止风险投资者将大量资金投入消费电子产品的行动。例如数码产品制造商Livescribe公司获得了Crosslink资本3900万美元的投资,使近三年来公司总的资金投入达到1亿美元。

在华尔街日报的“寻找资金”(Money Hunt)专栏中,有很多大型的律师事务所都给一些处于初创阶段的消费电子公司很高评价,并将它们介绍给风险资本和天使投资人。



The Economists
2010. 9
IT 技术导致中等收入层萎缩

麻省理工学院的David Autor和马德里货币金融研究研究中心的David Dorn两个人,根据美国劳工部的职业数据,研究了美国不同收入阶层的数量变化情况。结果表明,在1980~2005年之间,美国就业市场呈两极化现象,即高收入和低收入层的工作都有所增加,但中等收入阶层人数却减少。

据此二人分析,原因在于IT技术普遍化。中等收入阶层,比如银行职员、工厂流水线旁的工人,所涉及的工作流程,容易标准化和数据化。而IT技术的发展,大大减少了日常事务性工作的时间,从而减少了对中等收入工作的需求。低技能工作,如餐厅的服务工作等,只要通过对普通人进行很短的训练就可胜任,然而,要编程让一个机器人来完成的话,编程的工作非常浩大。高技能的工作涉及决策,计算机只能辅助。

据悉,伦敦经济学院对9个欧洲国家、日本和美国的研究证实,对高等教育的工人的需求上升,而对中等技术工人的需求则萎缩。

美投入 6250 万美元建设社区网

UCAN 填补了一项关键空白，它将众机构连接成一个开放的社会支柱，而美国新一代网络的功能与透明度适合社会发展需要，并能完成高水平的运作与机构合作。

美国国家电信和信息管理局 (NTIA) 在 7 月将 6.25 亿美元联邦激励资金投放给国家教育科研网络组织群体，包括美国 Internet2、美国高速国家计算机网络 (National Lambda Rail, 简称 NLR)、印第安那大学和网络联盟，以支持发展一个覆盖全美、速度达 100Gbps 的崭新网络——美国联合社区网 (United States Unified Community Anchor Network, 简称 U.S. UCAN)，为超过 20 万家重要的社区机构提供服务。

该社区网由 Ciena 公司、思科、Infinera 公司和 Juniper 公司等合作建成，连接全国各地的区域网络，速度达 100G，这也是一项通过美国复苏与再投资法案资助的项目。除 NTIA 赠款之外，还将辅以额外拨款 3.43 亿美元，这些经费来自合作伙伴和供应商的捐款。

该社区网的基础设施将通过与区域和国家教育科研



网络的合作，连接包括如学校、图书馆、社区学院、健康中心及公共安全机构等社区机构，并实现传统互联网不能支持的应用。

该网络将加强复原能力及容量，以扩展 Internet2 的效能，整体网络会采用将近 12,000 公里的光纤网络，提供以 IPv6 及组播为基础的服务，如远程医疗及学习等需要极大容量和速度的多媒体应用，覆盖包括那些以前被认为太过偏僻的地区。

UCAN 填补了一项关键空白，它将众机构连接成一个开放的社会支柱，而美国新一代网络的功能与透明度适合社会发展需要，并能完成高水平的运作与机构合作。

美国 FCC 推动新 E 计划

“FCC 的高瞻远瞩不仅让这个国家最重要的教育机构迈上了一个新的台阶，也让整个美国的视野更开阔了。”



9 月 23 日，美国 EDUCAUSE、Internet2、美国高速国家计算机网络 (National Lambda Rail, 简称 NLR) 和 Quilt 机构赞成美国 FCC (美国联邦通信委员会) 发展 E 计划。

EDUCAUSE 的主席 Julius Genachowski 表示，他希望该机构放宽管理学校如何使用 22.5 亿美元互联网

接入联邦补助的规则，该补助旨在帮助学校获取更快互联网接入权以及为学生提供无线网络。

在新的 E-Rate 计划下，美国的网络机构都可以享用一个新的试点项目，学校可以利用融资来为学生提供无线互联网接入权。无线网这一技术可能将变得越来越重要，因为学生使用诸如平板电脑和智能手机等新设备来完成他们的功课。目前 E-Rate 计划已经实施补贴学校网络接入，要求学校使用零售住宅互联网接入服务提供商，这使得学校在能够寻求其他互联网接入的情况下，节约了开支，并从更快的互联网速度中获益。

“FCC 的高瞻远瞩不仅让这个国家最重要的教育机构迈上了新的台阶，也让整个美国的视野更开阔了。”德克萨斯州教育电讯网负责人 Carol Willis 称，“另外，我们也很高兴地看到，FCC 认识到了教育和科研网络在社区中扮演的批评者角色是有所用处的，不仅为教育机构带来了独一无二的资源，也让我们看到了一个可以预见的更好的未来。”

(沈浩浩)

清华大学和 IBM 启动“清水计算”网络研究项目

清华大学与 IBM 公司日前正式启动了全球网络大同盟“清水计算”研究项目。该项目旨在利用先进的物理水资源过滤处理技术，解决中国大规模城镇化的发展进程中存在着的诸多水资源污染管理问题。

根据世界卫生组织和联合国儿童基金会联合发布的报告，目前全球约有 8.84 亿人无法获得安全的饮用水。联合国环境规划署的数据显示，如按当前的水资源消耗模式继续下去，到 2025 年，全世界将有 35 亿人口缺水，涉及的国家 and 地区将超过 40 个。

IBM 全球网络大同盟 (WCG) 项目免费提供的计算能力，将有力地支持该项目中污水水处理过程的数字模拟，帮助研究人员洞悉如何提高海（污）水淡化效率，开发出更加节能高效的水过滤设备。

吉林大学打造高性能计算平台

吉林大学高性能计算中心日前揭牌。该中心已经超出了原有高校计算中心的概念，在作为校内重点学科的计算平台的同时，还将面向省内知名企业和科研院所开放资源。

“这一计算平台是吉林大学《服务吉林与东北振兴行动计划》的重要内容之一，希望它能够服务吉林科技和产业发展作出贡献。”吉林大学校长展涛在揭牌仪式上这样说。

吉林大学高性能计算中心是由吉林大学投资 1300 万元、吉林省工信厅出资 200 万元共同建立的，其计算能力达到 40 万亿次/秒，在国内大学高性能计算系统排名中暂居首位，同时这套高性能计算系统在 2010 年 6 月的全球高性能计算机 TOP500 排名中位居第 239 位。

上海电力学院首建智能电网研究机构

中国教育网讯 上海电力学院智能电网技术研究院近日正式挂牌，成为沪上高校首个智能电网专业研究机构。研究院下设 4 个研究所。

上海市智能电网推进办介绍，智能电网已成为本市高新技术产业化重点领域。

据了解，目前上海电力学院与上海电力、华电集团、通用电气所属电力企业签署一系列校企战略合作协议，签约内容包括与上海市电力公司联合建设一个工程技术研究中心。



CALIS 三期： 高校图书馆信息服务能力获提升

9 月 20 日，中国高等教育文献保障系统 (CALIS) 三期项目建设暨服务启动大会在北京大学 (CALIS 管理中心) 召开。

CALIS 致力于建设的“高等教育文献保障体系”是我国高等教育最重要的信息基础设施和公共服务平台之一。

经过“九五”“十五”两期的建设，已逐步建成以高校丰富的学术信息资源为基础、以先进的数字图书馆技术为手段、以中国教育和科研计算机网 CERNET 为依托的具有国际先进水平的开放式中国高等教育数字化图书馆的框架。

CALIS 三期项目的建设目标是全面挖掘、整合国内高校图书馆以及其他各级各类文献信息服务机构的资源和服务，有重点的整合国际相关机构的各类信息资源与服务，提高高校图书馆文献资源的总体保障率，提升高校图书馆现代化服务能力。

CALIS 三期将采用“预研一批、试点一批、推广一批”的思路，在充分挖掘大型图书馆的研究能力与服务能力的同时，引导中小型图书馆广泛参与。

本次启动大会上，CALIS 还开通了新的服务门户主页 eduChina，同时发布 CALIS 学术搜索引擎——e 读。

■ “相信学生就是中山大学善待学生的办学理念的最好体现。”

9月9日，中山大学学生自主网站5D空间暨中大手机网上线仪式正式启动。中山大学校长黄达人在启动仪式上如是说。

5D空间是一个以学生为主体并由学生自主管理、自主进行内容维护的大型综合门户网站。“5D空间”是“我的空间”的谐音，同时“5D”也代表着网站的5大板块，也有着“我的地盘我做主”的含义。

黄达人说，我们就是要办一个学生自己的网站，让学生发挥主观能动性来管理网站，因为相信学生就是中山大学善待学生的办学理念的最好体现。



中山大学学生自主网站5D空间暨中大手机网上线仪式

■ “物联网，雾里看花；云计算，人云亦云”

2010年9月“下一代互联网发展与应用论坛”上，工业和信息化部通信科技委委员侯自强研究员这样评议时下的物联网和云计算的普及程度。他认为要保持平和心态，切勿急功近利，关键是要应用驱动，重在效益。只要有应用效益就有需求，才能带动物联网的发展。而云计算为物联网提供了支撑平台。

■ “南开传播学科的发展以及南开人文素质和科学素质的普及教育在理论层面和实践层面为同互联网的合作提供了新的互动空间。”

9月18日，由南开大学文学院和互动百科网站联合主办的“2010中国维基行业峰会暨第三届互动百科用户大会”在南开大学田家炳音乐厅召开。南开大学常务副校长、文学院院长陈洪教授在会上如是说。本届峰会以“知识改变世界”为主题，吸引了包括业内专家学者、媒体以及来自全国各地的众多维基爱好者、百科网站站长、百科网站合作伙伴以及南开师生的参与。

10 倍

150 项

431 台

50%

3G 网络容量 4 年增 10 倍

国际电信联盟（简称ITU）日前表示，过去4年，3G移动网络增长近10倍，超过固定宽带连接。ITU预计，今年年底3G用户将超过9亿。

ITU在一份统计报告中称，2010年年初，全球3G移动网络容量由4年前的7300万增长至6.67亿，同期内全球固定宽带连接用户由2.16亿增长至4.79亿。3G在全部手机用户中的比例由2006年的3%提高至14%。

中国已主导制定
超过 150 项 电信国际标准

国家标准化管理委员会主任纪正昆透露，中国加入世界贸易组织之后，截至目前，提出或主导制定的国际标准草案已达210项。在国际电信联盟中，由中国提出和主导制定的国际标准已超过150项。

百万亿次超级计算机曙光
5000 已经售出 431 台

2008年推出的我国首个百万亿次超级计算机曙光5000目前已经售出431台。

曙光5000高性能计算机，其系统峰值运算速度达到每秒230万亿次浮点运算，Linpack运算速度超过每秒180万亿次浮点运算。

超过半数的学校
将增加预算

日前对313所高校的调研结果表明，约88.8%的学校在新学年中的总体IT预算不变或增加，其中159所学校预算将增加，占50.7%。



IE9 来了!

日前,微软发布了一套全新的IE的BETA版。正式版本要在几个月后推出,对于具体时间,微软表示无可奉告,但BETA版已让人眼前一亮。这个使用最频繁的浏览器现在有了全新的界面,更全面的HTML5和21世纪其他网络技术支持,浏览速度也得到了大幅提升。

这种转变对微软来说,实属不易,因为微软在浏览器方面的创新步伐一直以落后半拍而被人诟病。早在2009年3月IE8面世的时候,我们就发现它功能众多,却不支持新兴的标准,而这些恰恰是让互联网精彩的真正的技术支持。IE8虽然比之前几代浏览器更快、更安全,可是速度和易用性方面却相当差,无论Chrome,火狐还是Safari、Opera,IE8与它们比起来就像在打瞌睡。

微软IE浏览器部门总经理Dean Hachmouch在旧金山举办的新闻发布会上强调:“人们上网要找网站,而不是浏览器。如今网站已经很拥挤,浏览器的速度就很重要。”IE9支持30多种语言,流行网站如Facebook、亚马逊在线,CNN、ebay、twitter都在体验IE9的新功能。

随着人们更多地观看视频,登录Facebook, twitter等网站,IE9的面世可以让他们的新版本在处理图形时更加快捷好用。

微软希望IE9可以更快、界面更干净、安全,支持不断发展的网络技术,比如对HTML5标准技术的支持。它也和bing搜索引擎结合,这被微软寄予厚望,能够对Google造成威胁。

IE浏览器多年来一直主导市场,但自从Mozilla出品的Firefox和Google出品的Chrome浏览器问世后,IE已经失去原先的市场占有率。

谷歌:失控于安卓?

最近,谷歌长期的合作伙伴Verizon开始销售三星Galaxy智能手机,推广安卓操作系统。但这款很受欢迎的手机却出现一个重大不同:它内部并未使用谷歌的搜索引擎,取而代之的是微软的必应。

美国很多科技博客都为这戏剧性的变化感到惊讶。毕竟对安卓的用户而言,最大特色之一就是它使用谷歌的搜索引擎,而谷歌开发安卓也是基于占领通信移动领域的目的。几天后,一个后



续终端上的变化出现,谷歌搜索终于内置在手机里,然而必应还是默认选项。

还有一个与之前宣传相矛盾的地方是,开放和自由一直号称是安卓系统的基础,但这个自由越来越明显地不

再针对用户,而变成了运营商可以“自由地”在其销售的手机上做他们想做的事。这与苹果完全掌控iPhone完全不同。

然而,这些措施在大多数情况下都会损害消费者的使用体验,而谷歌也不能幸免。最糟糕的是如果谷歌希望Verizon继续销售和推广安卓手机,就注定对这个变化无能为力。谷歌最多只能希望自己的搜索引擎被保留,哪怕是身为搜索巨人的谷歌需要从自己开发的免费操作系统当中,去掉一些东西。

AT&T称2011年中将发布LTE网络

AT&T一直在宣讲,称他们不断地投资为了提高HSPA网络速度,并能最终过渡到LTE网络,最近,AT&T进一步透露了其开展工作的具体情况。

在日前,美洲银行一次会议发言中,CEO John Stankey宣布,AT&T将在2011年夏天发布第一个LTE网络。他们相信,到同年年底,LTE网络将覆盖大约7000~7500万的接入点。



在今年年内,AT&T会将HSPA网络升级到HSPA+,如此一来,无线下载速度可以达到7.2MB/秒。其实T-Mobile早就这么做了,还在最近挖补了HTC G2手机,这是第一个支持HSPA+的设备,秋天就会

上市。而Verizon无线的LTE到今年年底会在美国25~30个大城市市场覆盖1亿的接入量。



移动“云”

基于云的安全措施，如找到丢失的手机或者找回备份信息，已经成为移动设备安全的重要部分。

一家基于云的智能手机安全公司 Lookout 公司宣布在过去两个月它的用户增加了一倍，达到两百万注册用户。

这并不奇怪。随着世界从一般移动电话到智能手机的转变，越来越多的个人信息将被保存在我们随身携带的设备中。而这一切都是通过云才成为可能。虽然随时访问个人的信息能够极大地节省时间，也让我们更加自由，但这也加大了丢失手机的成本——手机里有我们宝贵的个人信息！

Lookout 宣称，在过去两个月平均每 15 秒钟就会找到一部丢失的手机。在最坏的情况下，Lookout 的用户也能够清除其手机上的信息。Lookout 的软件也能够提供关于恶意软件和病毒防护的服务。

Itsy: 让 twitter 回归简单

当前大多数 twitter 客户端都在尽可能向着花哨的方向发展。

比如最近发行的 Seesmic 桌面版，就可以添加 40 种不同的社交网络和服务。但有时候，你难免想要使用最基本和简单的 twitter，那么，试试 Itsy 吧，它是 Mac 平台上的 twitter 客户端，只提供最基本的功能。

Itsy 推出已有一段时间，但最近才为人所知，现在是时候尝试一下了。通常专业人士用的都是列表式的 twitter 客户端，比如 Tweetdesk 和 Seesmic，这是因为他们在工作中会大量用到 twitter，而且常常使用多个列表进行搜索。但是，对 twitter 普通的用户来说，大部分人很少有机会用到这些。

Itsy 是一种单列表式的客户端，不禁让人想起 Twiirl——twitter 早期最受欢迎的客户端之一。对于那些“超级用户”来说，Itsy 显然不是个好选择，它甚至没有功能列表，但它设计简约，并且与 Growl 集成，对于刚开始玩 twitter 的人来说，再完美不过——他们只关注非常有限的人，不会持续搜索，也用不着多重列表，或者与其他社交网站整合。

不过，Itsy 还是拥有所有必要的功能：用户可以查看推文中的图片，但不能上传图片，Itsy 也有答复链，还可以使用 twitter 的搜索。

漏洞测试：笔记本就是武器

漏洞测试技术有很多方法，以下是一些介绍。

战争拨号(war dialing): 使用电脑来拨通上千个电话号码以期访问某个系统。

战争游走(War driving): 带着笔记本在家旁边走动，来看可以使用哪个网络。

反追查(Sniffing): 通过数据包，把恶意代码用有效的 TCP/IP 网络地址来标记，恶意代码就会通过网络安全审查，发动攻击。

社会工程(Social engineering): 用欺骗的手段让用户点击一些他们不应该点击的链接。

深度挖掘: 通过对垃圾进行搜索以期找到敏感数据。

在最嘈杂的环境下通话

Orange 称其已引进技术来结束移动电话时的变音现象。该公司高清晰度的语音服务已经提供给法国电信。

做出这个技术创新是因为一项用户调查报告显示，75% 的移动用户认为通话质量是他们最看重的。Orange 称其新技术能够帮助移动手机用户在最嘈杂的环境下清晰通话。这个技术也意味着移动用户能够发现通话者声音中的细微差别。

与传统的移动电话相比，Orange 高清语音系统采用了不同的声音解码器，使用了更宽的宽带——从 70Hz 到 7000Hz（传统的只有 300Hz~3400Hz）。

目前，Orange 声音解码系统只能用于 Nokia E5 和 Anycall Omni a Pro 5230 两种型号的手机。



2010 下一代互联网发展与应用大会在北京大学召开，专家指出

我国互联网发展要 从“大国”走向“强国”

9月13日-14日，“2010下一代互联网发展和应用论坛”在北京大学英杰交流中心举办，总结了我国下一代互联网的建设与应用，交流了下一代互联网及其重大应用的基础技术和关键技术，为推动我国信息产业持续健康发展提供了宝贵意见。

会上，教育部科技司副司长陈盈晖指出，资源的问题是最重要而且紧迫的，目前IPv4地址短缺已经影响到互联网今后的发展，发展下一代互联网在拉动产业发展和提升国家竞争力等方面都具有重要的意义。其次，我国走新型工业化道路，通过寻找新的增长点实现跨越式发展，因此发展下一代互联网能为此提供契机，可以带动社会信息化投资，给网络制造业、信息服务业带来巨大的发展空间。第三，发展下一代互联网有利于高校增强下一代互联网自主创新能力。第四，高校IPv6实施推进了我国IPv6产业化进程，使下一代互联网拥有大规模的用户群体，有利于下一代互联网的试验和应用。

工业和信息化部信息化推进司副司长董宝青指出，目前我国已成为全球的互联网大国，但还不是互联网强国。推进下一代互联网发展还有很多工作要做。第一，进一步营造好有关政策环境。第二，着力推进技术研发，突破关键技术，摆脱核心关键技术受制于人的局面。第三，大力营造产业生态链。第四，大力推进下一代互联

网的应用。第五，促进国际关系，加强国际合作。

中国工程院院士汪懋华着重谈到了智慧农业发展与物联网农业领域的应用，他指出，IPv6应用发展指日可待，通过物联网、传感网建立起的网络体系会无处不在，将形成“人-机-物”互联的三元信息世界。

CERNET 国家网络中心副主任，CERNET 专家委员会委员李星教授做了《从CERNET到CNGI-CERNET2，再到Future Internet》的报告。他介绍和分析了目前国内外互联网发展的形势，出于战略目标的考虑，各国互联网在基础设施和资源获取上展开竞争，尤其2010年，美国政府加紧投入宽带网建设，决定继续支持学术网，以促进宽带网络的发展，并于今年七月投入6200万美元建设100G的社区网。此外，美国政府高度重视教育公益性网络，美国科研教育网资助的几个项目，包括基于内容网、移动互联网，以及B2B等三个层次架构。这给全球学术科研网的发展提出了新的机会和挑战。

面对下一代互联网的发展，李星教授提出三条“不变”的建议：第一，解决实际问题不变；第二，IPv6不要变；第三，过渡不要变。他指出，从现在和将来来看，与IPv4互联互通才是IPv6的杀手级应用。

同时，会议也得到了博科、AMD、浪潮、微软、神码等企业的支持，拓宽了下一代互联网“产学研”结合之路。



服务器：突破壁垒

伴随信息技术的进步，网络对信息系统数据处理能力、安全性等的要求越来越高。作为网络的关键部分，服务器承担了存储、处理网络80%以上数据和信息的任务，保证各种信息系统稳定运行，因此可以说服务器就是网络的灵魂。而CPU、虚拟化、集群、绿色等技术又是服务器向前发展的关键点，所以我们需要不断完善、增强这些技术，从而突破服务器的技术壁垒，加速服务器的发展。

■文 / 本刊记者 周斌 周晓娟

“到2020年，基本建成覆盖城乡各级各类学校的教育信息化体系，促进教育内容、教学手段和方法现代化。”《国家中长期教育改革和发展规划纲要（2010-2020年）》对教育信息化进程提出了明确的要求。服务器作为高校信息化的重要基础设施之一，其发展进程与各高校信息化建设密切相关。

目前，多数高校的IT基础设施因新增应用而日趋复杂，供需矛盾凸显。服务器的利用率低、能耗大乃至灵活性、可管理性、兼容性等方面的问题日益突出。如何攻破上述难题？业内专家认为，可以从CPU、虚拟化、集群技术、节能减排等方面寻求突破。

CPU需突围

作为整个系统中枢神经的CPU在机器整体性能

和硬件结构中占有重要的地位，服务器的分代可以以CPU类型和CPU技术为基础进行划分。可以说，服务器是网络的灵魂，而CPU是服务器的核心。

“CPU核心的发展应该朝着更低的电压、更低的功耗、更先进的制造工艺、集成更多的晶体管、更小的核心面积、更先进的流水线架构和更多的指令集、更高的前端总线频率、集成更多的功能以及双核心和多核心等方向努力。”北京邮电大学张欣教授表示。

对CPU的发展方向，中国科学院软件研究所姚继峰博士与曙光技术支持中心部门总经理曹振南的观点不谋而合，他们都认为，CPU集成GPU是未来CPU的发展趋势之一。

然而，CPU的发展并没有大家想象中的顺利。

美国国家科学院院士大卫科克(David Kirk)曾公开表示，CPU制造商所使用的多线程和多核心技术，看起来好像是使CPU的性能加倍，但从本质上说，并不能解决CPU主频提升以及制造工艺的瓶颈。

“多核 CPU 乃黔驴技穷之作”。大卫科克有了无奈的表情。

中国科学院计算所常务副所长孙凝晖与大卫科克有类似的想法。

“多核毫无疑问是一个趋势，但也是个不得已的选择”。

孙凝晖表示，多核在技术上没有革命性的进步，它实质上只是在模拟大型机在过去 30 年走过的并行道路而已，只不过现在做到了芯片内部。

“目前，CPU 还是服务器发展的一道坎，我们需要通过技术、工艺等方面的攻关来打破现在的僵局。”张欣表示。

“服务器的变化主要是跟着 CPU 走，从硬件来讲，CPU 变化最关键，而从业务来讲，虚拟化技术是关键。”姚继峰中肯地说。

虚拟化整合资源

众所周知，服务器虚拟化有助于 IT 机构从根本上提高数据中心的生产力。它能够整合基础设施，降低成本，在短时间内部署新应用并实现在不停机的情况下将正在运行的应用从一台物理服务器向另一台服务器的迁移，从而实现灵活的工作负载管理，获得经济高效的高可用性 & 灾难恢复能力。

“服务器虚拟化在服务器整合、业务永续、开发测试环境等应用场景发挥了重要作用，带来了诸如冗余高可用、在线迁移、灵活部署、集中管理等诸多好处。”暨南大学网络与教育技术中心网络工程部陈少涌老师在服务器虚拟化的益处层面做出了如上表述。

同样，图书馆作为高校信息化建设的重要部分，服务器的建设层面也有自己的思想。

服务器数量的增加可以提升图书馆的服务质量和水平，但随之而来的是设备成本、维护成本、运行成本

虚拟化

Illuminata 公司的 Jonathan Eunice 给出了这样的定义：“虚拟化是以某种用户和应用程序都可以很容易从中获益的方式来表示计算机资源的过程，而不是根据这些资源的实现、地理位置或物理包装的专有方式来表示它们。换句话说，它为数据、计算能力、存储资源以及其他资源提供了一个逻辑视图，而不是物理视图。”而 IBM 公司则给出了一个更加简洁的定义：“虚拟化是资源的逻辑表示，它不受物理限制的约束。”

和人员成本不断增加。

清华大学图书馆系统部副主任陈武给出的办法可以缓解上述问题，“虚拟化技术允许在一台物理服务器上运行多个平台，从而实现将不同服务整合到同一台物理服务器的目标。近年来随着 PC 服务器性能的大幅度提升，基于 PC 服务器的虚拟化技术得到了广泛应用，越来越多的图书馆采用这项技术来缩减服务器相关成本。”

不难看出，从软件、硬件到数据中心、云计算，都有服务器虚拟化技术的身影。然而，在虚拟化技术逐步普遍应用时，也出现了一些问题。

据了解，目前，多数高校的服务器都经历了更新换代，新旧服务器都在同时使用。而虚拟机无法在多代旧服务器之间迁移，虚拟池彼此隔离，这样大大限制了数据中心的灵活性。

针对上述问题，英特尔（中国）有限公司服务器平台产品经理张振宇表示，英特尔虚拟化技术可以加速基本虚拟化处理，减少延迟并避免潜在瓶颈。这种技术可减少对虚拟化软件的要求，可实现更多的服务器资源运行业务应用。同时，它支持基于英特尔处理器的多代服务器之间的实时虚拟机迁移，使添加新服务器同时保持整个数据中心的灵活性成为可能。

同样，虚拟化技术的安全问题也被越来越多的使用者所关注。

虚拟化技术带来的安全漏洞为恶意软件创造了可乘之机。IT 主管必须像保护物理机器那样来保护虚拟机，还要采取其他步骤来确保虚拟化环境得到保护，发现、配置、变革管理及其他方面的技术和制度对发现针对虚拟化环境的恶意软件尤为重要。

就虚拟基础设施而言，如果没有遵循和采纳最佳实践措施，那么虚拟化就存在危险。Hypervisor 必须像任何其他操作系统一样，定期修补安全漏洞，Rent-a-Center 租赁公司的高级信息安全经理 KC Condit 说：“VMware 今年以来已发布了 9 个重要安全公告，XenServer 也已发布了 6 个安全修复办法。”

“虽然服务器虚拟化技术本身有很多优势，但是它的发展仍需注意很多细节问题，遇到问题要积极解决，努力攻破，这样虚拟化技术才能更好地整合资源。”张欣表示。





当前中国服务器保有量在200余万台,如果能够较为普遍地采用云计算节能技术,则可以降低65%左右的能源损耗。以服务器平均能耗200瓦/小时计,全年可节约160亿千瓦时的电能,相当于葛洲坝电站2009年全年的发电量。而在夜间,数据中心整体负载降低情况下,则可将空闲资源转入休眠模式,从而在最大程度上实现数据中心绿色、低碳的节能运营。

集群提升计算性能

与虚拟化技术有异曲同工之妙,集群技术也能成为服务器的发展提供更大的空间,因为它能提升服务器的性能。

通过集群技术,可以在付出较低成本的情况下获得在性能、可靠性、灵活性方面相对较高的收益。目前,在世界各地正在运行的超级计算机中,有许多都是采用集群技术来实现的。

IBM系统与科技部System x中国区品牌经理徐行表示,服务器一个重要的技术就是提高计算能力,而集群可以把多数相对便宜,性能比较好的机器捆绑在一起做同一件事,这样可以提高计算的整体性能。

同时,他认为,在高性能集群中,机器之间的通讯很重要,保持数据的畅通是关键,这样能使高性能集群的效率有所提升。

集群技术相对来说是服务器的一种较新的技术,那么今后它究竟该如何发展?

曙光技术支持中心部门总经理曹振南向记者表示,集群的发展方向主要包括以下几个方面:首先是大型化,随着计算机的快速发展,集群系统的规模会越来越大;其次是小型化,蓝领化,随着应用的普及,高性能计算机离大家越来越远,数目将越来越多;再次是云计算使用模式,以前高性能计算中心提供的是机器和软件,而今后高性能计算中心提供的是服务,人人都可以通过浏览器申请服务,获

得服务;最后是计算加速单元,比如GPU计算,以及正在研发的众核处理器等等。

集群的应用使管理越来越复杂,如何让机器更好协同运行,用户不断增多的时候如何管理,这些都是需要思考的问题。

打造绿色服务器

自2008年1月1日起,由国家环保总局和财政部联合发布的《环境标志产品政府采购实施意见》和首批《环境标志产品政府采购清单》将在全国范围内全面实施。我国大力推广政府绿色采购制度,使得绿色环保再次成为各企业关注的焦点。

如何打造绿色竞争力已经成为影响我国服务器行业发展的重要因素之一。可见,绿色节能成为服务器发展的大势所趋。

据了解,目前服务器的产品研发更注重机器的能耗比,这不仅符合国家倡导的政策,也符合客户的切身利益,更低的功耗可以降低客户的总体运营成本。所以,服务器厂商在设计产品时就注重节能技术的创新。

徐行认为,服务器的节能应该从原件的选择、架构的设计,整个系统刀片中心的设计,整个机房的布局等方面来考虑,因为这些细节都会影响到整体的节能效果。

方正科技与IBM在原件选择上有类似的观点,方正科技服务器产品总监周良表示,新一代的DDR3内存比上一代的功耗就降低很多。CPU引进Turbo boost技术,使得超频更加节能。

对于现在发展迅速的刀片服务器,姚继锋认为,刀片服务器散热需求比原来大,对散热的要求更高,如果用刀片,制冷是关键,传统的风冷可能跟不上,而水冷直接冷却的是机柜,这样可以提高冷却效率,也是节能的一个体现。

同样,节能还可以从云计算出发。云计算数据中心,实现了资源的多租户应用。通过业务的历史统计信息,配合业务/资源调度管理,可以有效提高资源的利用率。在典型应用中,采用节能技术的云计算数据中心,可以将资源负载提高到80%,除去资源调度过程中的损耗,可以将资源的有效负载提高2倍。

对于今后服务器节能技术的发展方向,周良认为,后续的服务器在整机效率,以及关键部件的能耗和电源转换效率上会有更大的空间。■



INOC 互联网中心网络力量

掌控互联网世界的力量

INOC 互联网中心网络力量
INOC 互联网中心网络力量





暨南大学： 服务器虚拟化解应用之困

服务器虚拟化不只切合当前绿色低碳的环保理念，也是节约成本、提升效能的利器，更是构建高校“云计算”平台的基础。

■文 / 陈少涌 李哲夫 陈国良

信息技术发展日新月异，各种新技术的不断涌现，为人们提供了丰富的IT解决方案，其中云计算、虚拟化和IPv6已成为近年来最为热门的技术词汇，同时也是应对数据中心规模不断扩大的理想解决方案。

虚拟化技术应用与产品选择

暨南大学网络与教育技术中心面向全校提供网络和信息化的基础平台服务，除了提供网络接入，还通过数据中心提供服务器平台和各类应用，以满足学校以及下属各教学、科研和行政机构的信息化需求。

目前数据中心已拥有近200台服务器，类型包括PC机架式服务器和小型机。同时，还有近40TB的存储空间，形式有FC SAN、NAS和iSCSI SAN等。

在虚拟化产品的选择方面，主要考虑的因素包括：1) 费用，包括商业许可的费用等；2) 易用性，包括支持远程图形界面、管理维护便捷等；3) 性能，包括全虚拟化还是半虚拟化、硬件性能损失是否严重等；4) 高级特性的支持，包括资源动态调配、在线迁移、故障恢复、快速部署、高可用等；5) 支持操作系统种类。

近年来，暨南大学测试了多款虚拟化产品，通过综合分析比较，目前重点应用的产品包括集中在VMware的ESX和Citrix XenServer。

VMware ESX的应用实践

暨南大学数据中心测试的版本为VMware ESX 4.0。

1. VMware应用情况

本次测试方案为采用的虚拟化平台为ESX4.0，硬件为两台DELL2950服务器，存储系统为EMC的CX700；开启HA和DRS构建高可用分布式自动调度资源集群系统，在此集群系统中运行了8台虚拟机，如表1所示。

这些应用都有共同的特点，CPU使用率不高，内存需求较大，IO使用率不高。通过vCenter Server可对ESX主机及其虚拟机实现集中管理，并能对主机及虚拟机性能（CPU、内存、磁盘、网络接口使用情况）进行监控，图1显示了监控主机CPU性能的情况。

通过网管系统对虚拟机进行监测（如图2、3、4所示），可以看出该虚拟机性能良好，利用率显著提升。

2. ESX应用效果分析

通过分析监测数据，虚拟机的CPU峰值为75%，内存使用峰值亦是75%，虚拟机系统负载情况良好，完全

表1 VMware ESX虚拟机应用情况

序号	CPU个数	内存	操作系统	用途
1	8	2GB	FreeBSD	DNS
2	8	2 GB	FreeBSD	DNS
3	8	2 GB	FreeBSD	DHCP
4	8	2 GB	FreeBSD	DHCP
5	2	2 GB	Win2003	网管
6	2	2 GB	Win2003	网管
7	2	2 GB	Win2003	网管
8	2	2 GB	Win2003	网管

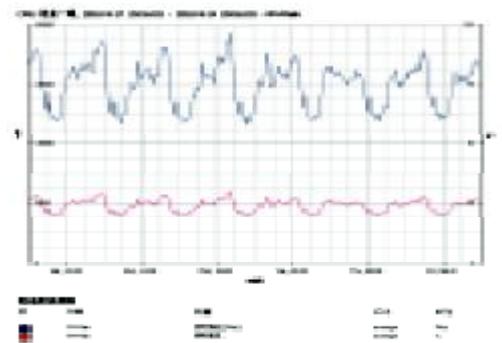


图1 VMware ESX主机CPU一周性能图



满足应用需求，充分利用硬件资源，节约投资，提高运营效益。

在虚拟机增多时，ESX 的 DRS 功能能很好地均衡虚拟机的负载，在多个虚拟机之间智能地分配可用资源。当虚拟机遇到负载增大时，DRS 将通过在资源池中的物理服务器之间重新分布虚拟机来自动为其分配更多资源。

ESX 使用虚拟机磁盘 (VMDK) 文件为虚拟机提供对自己专用数据存储区的访问，使管理员以功能完备、可驻留在共享存储设备上的独立文件形式灵活地创建、管理和迁移虚拟机存储。在出现硬件故障或灾难事故时可快速部署服务、快速迁移，减少服务中断时间。

在使用 EMC 的 CX700 作为存储系统之前，测试过使用 NFS 作为共享存储服务，由于 NFS 的传输及性能限制，使得虚拟机 I/O 读写性能低下，影响整体性能。所以当使用集群方案时必须进行存储系统投入，使得运营成本有所提高。

XenServer 应用实践

Citrix 于 2009 年 6 月发布了免费和不限制生产配置版本的企业级 XenServer 5.5 平台，其核心功能是将一台物理服务器虚拟为多台虚拟服务器。配合管理工具 XenCenter 和实时迁移功能 XenMotion，可实现多节点集中管理、嵌入式存储和完全实时迁移

等功能。目前此版本依靠完备的功能和稳定的特点，被广泛使用。

1. XenServer 部署

以 XenServer 5.5 为虚拟化平台，暨南大学网络与教育技术中心投入三台 Dell I 2950 进行虚拟化前期测试，其配置情况如表 2 所示。测试目的是结合高校应用的需求对 XenServer 5.5 的功能、性能及管理进行分析调研，并初步解决数据中心服务器数量不足的问题。

XenServer 服务器端的安装非常简便，服务器端主要功能为底层硬件和网络的配置，同时也支持以命令行方式对虚拟机的配置管理。

XenCenter 是 XenServer 配置的可视化管理工具，安装在 Windows 平台下，功能齐全，操作简便。利用 XenCenter，可以同时多个 XenServer 服务端进行管理，实现虚拟服务器的增加、管理、备份、删除和资源调整等操作，此外还可以实现远程操作、性能监控、日志查询等日常管理功能。

经过近 1 年的测试，目前已成功上线安装近 20 个虚拟机，其中一台内存和硬盘基本饱和，其虚拟机应用及资源分配情况如表 3 所示。

依据实践经验，虚拟机运行均相当稳定。实际

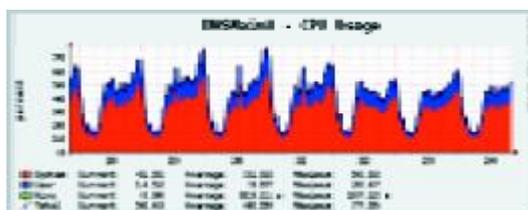


图2 虚拟机1 CPU一周监控图

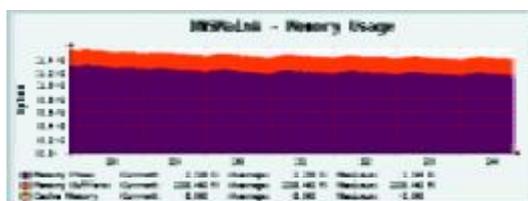


图3 虚拟机1内存一周监控图

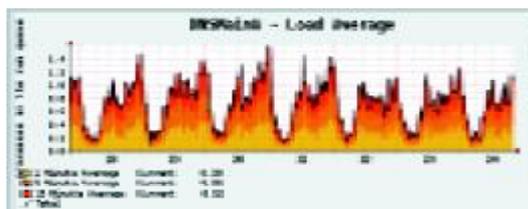


图4 虚拟机1负载一周监控图

表2 Dell 2950服务器硬件配置情况

项目	参数
CPU	Xeon E5410, 2.33Ghz, 2x4核, 支持VT技术
内存	16GB
硬盘	1TB
网络	双网卡, 分别连接教育网和联通网络

性能消耗如图5所示, 非高峰时期, CPU资源的利用率相当低, 只有4%。在某些虚拟机负载达到最高值时, 其利用率可达到15%左右。而内存的总体使用率较高达到55%, 在被监测的虚拟机中, 使用率均较高。两台运行了TOMCAT的虚拟机, 其负载均达到100%, 但从虚拟机内部检测可确定实际内存仍有50%的空闲。另外在实际管理中, 根据应用的负载情况, 需动态分配剩余的内存资源, 例如虚拟机8在新生入学阶段会较为繁忙, 就业平台在毕业阶段访问数则较多。

2. XenServer虚拟化技术应用效果分析

(1) 应用密度得到极大提高, 节约了空间和电力等成本; 如果数据中心新型服务器全部使用虚拟化, 在能耗基本不提高的情况下, 可将数据中心的应用密度提高一倍。

(2) 充分发挥了服务器性能, 节省机器购置成本; 利用虚拟化技术对校内提供可靠的云计算服务, 得到了各单位的高度认可和赞誉。解决了每个服务器运行一套系统, 资源严重浪费的问题。

(3) 在管理维护上, 安装系统方便, 利用预先做好的系统模板, 在20分钟内即可完成一个应用的部署; 在监控、迁移和备份上均相当方便, 可节省大量人力成本。通过定期备份, 并结合容灾备份系统, 可对生产系统提供数个版本的备份, 使数据更加安全。

(4) 资源调配较灵活。依据应用的需要, 提前分配好资源, 令计算能力达到最高值。如心理中心在进行心理测试的阶段, 可临时分配3G内存供其使用。

3. XenServer的局限

XenServer虚拟化技术带来了巨大的效益, 但在以下方面仍有局限:

(1) 虽然XenServer提供了免费的版本, 但需要反复申请有效期为1年的使用许可, 造成了业务上的不确定性, 大规模部署受到限制。

(2) 通过实践发现, 内存数量是各虚拟机的主要瓶颈, 而且XenServer客户端需损耗15%的内存, 因

表3 虚拟机资源分配与负载

名称	资源分配	应用说明	负载情况
VM1- VPN	1CPU, 1G内存 100G硬盘	VPN系统	低负载
VM2- CVS	1CPU, 1G内存 100G硬盘	CVS服务器	低负载
VM3- SAM	1CPU, 512M内存 50G硬盘	认证服务器	低负载
VM4- DB	1CPU, 1G内存 100G硬盘	数据库服务器	中等负载
VM5- TOMCAT1	1CPU, 2G内存 100G硬盘	Web服务器, 运行Tomcat	中等负载, 局部时段高负载
VM6- TOMCAT2	1CPU, 2G内存 100G硬盘	Web服务器, 运行Tomcat	中等负载, 局部时段高负载
VM7- JOB	1CPU, 2G内存 250G硬盘	暨南大学就业平台	中等负载, 局部时段高负载
VM8- XLZX	1CPU, 2G内存 100G硬盘	暨南大学心理中心网站、心理测验与管理系统	低负载, 局部时段高负载

此以每个虚拟机配备2G内存的方式较为妥当。目前发现, XenServer免费版限制虚拟CPU的个数为8个, 即每台物理服务器最多可虚拟8台的虚拟机, 结合CPU的实际使用效率, 在增加额外内存的情况下仍可容纳多一倍的虚拟机。

(3) 无法真正动态分配资源, 每次分配后需要重新启动相应的虚拟机系统。如果系统资源能实现共享, 则可以最大化利用硬件资源。

总结及展望

虚拟化技术在暨南大学测试取得一定成果, 学校还将在接下来的时间里重点针对开源版本的虚拟化技术进行深入测试, 并通过横向比较来选取最适合高校应用的解决方案, 从而推动“数据中心”虚拟化进程, 在不增加投资的情况下, 有效解决供需矛盾, 提高信息化建设水平。

同时, 服务器虚拟化不只切合当前绿色低碳的环保理念, 也是节约成本、提升效能的利器, 更是构建高校“云计算”平台的基础。相信随着虚拟化技术的深入发展, 虚拟化应用也将成为数据中心的标配和核心技术之一, 为校园信息化平台的心脏“数据中心”提供动力。

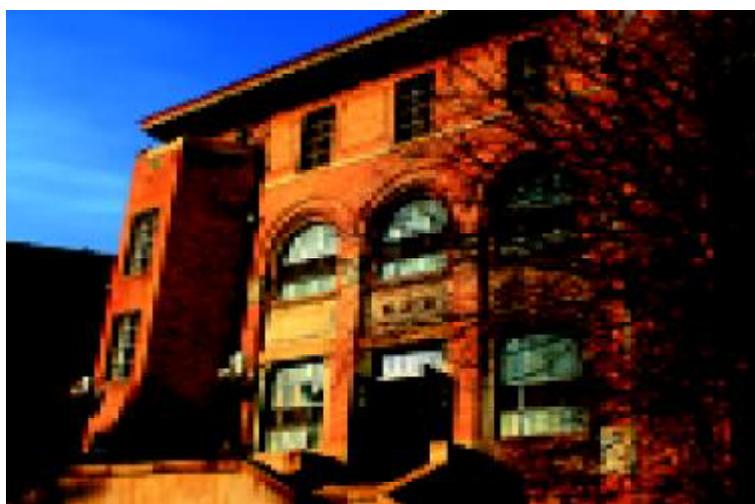
(作者单位为暨南大学网络与教育技术中心)



图5 通过XenCenter监测虚拟机状态



清华大学图书馆： 服务器虚拟化提升服务质量



■文 / 陈武

随着信息技术尤其是计算机技术的发展，图书馆的信息服务越来越依赖于计算机系统和网络。从最初利用计算机来进行纸本图书、期刊和资料的管理，到现在利用计算机直接提供电子书、电子期刊论文和资料的服务，图书馆用于支持自身运行和读者信息服务的服务器数量已经增长到较大规模，配套设施也得到了相应增加。以清华大学图书馆为例，服务器从1996年的几台发展到2008年正在使用的服务器数量达到110台，机房空间2次扩建，UPS和电源进行了3次改建和扩容，机房使用的空调也进行了3次扩容。

服务器数量的增加，虽然提升了图书馆的服务质量和水平，但是另一方面也带来了设备成本、维护成本、运行成本和人员成本地增加。为了应对这个问题，各个图书馆分别寻求不同的解决方法，例如服务外包、服务整合和虚拟化技术等。服务外包

是指将图书馆的信息服务外包给第三方公司，以减少图书馆自己的计算机设备数量和维护人员数量；但是目前来说还无法达到降低成本的目的，并且通常第三方无法提供图书馆所需要的服务质量。服务整合是指将图书馆的多项信息服务整合到同一台服务器上运行；考虑到目前图书馆的应用多为第三方应用，分别有不同的需求，整合时需要考虑太多因素，或者需要花费很长时间。虚拟化技术允许在一台物理服务器上运行多个平台，从而实现将不同服务整合到同一台物理服务器的目标。近年来随着PC服务器性能的大幅度提升，基于PC服务器的虚拟化技术得到了广泛应用，越来越多的图书馆采用这项技术来控制服务器总体成本。

虚拟化技术

关于虚拟化，Illumi nata公司的Jonathan Euni ce给出了这样的定义：“虚拟化是以某种用户和应用程序都可以很容易从中获益的方式来表示计算机资源的过程，而不是根据这些资源的实现、地理位置或物理包装的专有方式来表示它们。换句话说，它为数据、计算能力、存储资源以及其他资源提供了一个逻辑视图，而不是物理视图。”而IBM公司则给出了一个更加简洁的定义：“虚拟化是资源的逻辑表示，它不受物理限制的约束。”上面的定义都比较抽象，具体一些来说，服务器虚拟化就是允许在一台物理服务器上运行多个相互隔离的操作系统。

目前在PC服务器上应用较多的是完全虚拟化和超虚拟化。完全虚拟化的最大优点是操作系统无需任何修改就可以直接运行，但由于中间经过了hypervi sor 的协调过程，其性能要低于裸硬件，另一个缺点是操作系统必须要支持底层硬件。超虚拟化

提供了与未经虚拟化的系统相接近的性能，但是这种虚拟化技术需要为 hypervisor 修改客户操作系统。

随着虚拟化技术的不断流行，市场上出现了许多不同的虚拟化产品，包括免费产品和商业产品。常见的软件产品有VMware的vSphere，思杰公司的XenServer，微软公司的HyperV和Virtual PC，VI，KVM等。

通过实施服务器虚拟化，可以将多个服务整合到一台物理服务器上，具有如下一些优点：(1)提高服务器资源利用率，节省服务器购置成本；(2)减少服务器数量，从而减少配套设施成本及运行成本；(3)可以实现操作系统级别的隔离，使得各种应用互不干扰；(4)可以根据需要动态调整虚拟机的资源分配，实现快速、动态的业务调度；(5)可以实现零宕机时间的迁移、灾难备份和业务恢复，保证业务连续性；(6)将旧服务器系统迁移到虚拟机，从而维持老系统业务持续运行；(7)采用虚拟化平台，可以快速部署应用，有助于加快开发和测试进度；(8)采用虚拟化平台，可以简化或整合服务器的管理，降低服务器的管理成本。

虚拟化规划

为了通过实施服务器虚拟化达到降低运行成本的目的，需要进行良好的规划，包括现状调查、确定目标、费用估计、实施方法及周期等。

现状分析

在图书馆2008年开始实施服务器虚拟化之前，图书馆共有110台服务器。这些服务器的用途主要包括三大类：第一种是作为CALIS工程中心，与数据库厂商合作建立的镜像站点，用于为全国高校读者提供文献服务；第二种是本校所购买数据库产品的镜像服务器，用于为本校读者提供文献服务；第三种是业务支持服务器，包括主页、自动化管理系统、整合检索、开放链接、馆际互借、虚拟参考咨询等应用服务器。

这些服务器的购置成本接近500万元，每年的维护费用按照10%计算，也需要近50万元。

另外，为了支持这些服务器运行，图书馆多次对空调、电源和UPS进行了改造和扩容。这些配套设施的购置和运行成本对于图书馆来说都是不小的负担。

配合这些服务器的部署和运行，图

书馆系统部的工作人员数量也相应增加。

确定目标

考虑到图书馆服务器数量近年来不断增长，设备的购置成本、运行成本以及人员成本都相应增加，对于图书馆已经成为不小的负担。与此同时，图书馆技术人员也一直在跟踪服务器的相关技术，了解到服务器虚拟化技术已经发展成熟。

针对图书馆的现状，三种类型的应用中，后面二种应用都只对校内读者提供服务，用户数量是有限的，很多应用都不需要消耗太多的系统资源。根据图书馆多年来服务器的运行经验，90%以上服务器的平均CPU资源利用率都低于10%。因而从系统需求方面具备了进一步整合的客观条件。另一方面，由于这些系统大多由第三方开发，很多时候相互冲突，或者在发生问题相互推诿责任，所以这些服务又需要操作系统级别的隔离。

因此，图书馆确定了通过部署服务器虚拟化技术来达到缩减图书馆运行服务器数量，进而达到缩减相应购置成本、维护成本、运行成本和人员成本的目标。

预算估计

确定目标之后，需要进一步考虑实施虚拟化所需要的资金、人力等资源。首先需要考虑购买虚拟化软件的费用，以及为了实施虚拟化需要增加硬件的投资。除了软件和硬件资金投入之外，还需要考虑实施虚拟化额外需要的人员、培训等。

实施方法及周期

一般来说实施方法分为二种：一种方法是集中实施，迁移现有服务器。另一种方法是逐渐实现迁移。前一种方法的周期短，见效快，短期内需要投入较多人力和财力资源。后一种方法周期长，见效慢，但是过渡更加平滑。考虑到短时期内的人力投入有限，并且有些应用不能很快整合到虚拟化平台上，所以我们选择了逐步实施虚拟化的方案。另外，对于存储量需求很大或系统资源需求较大的系统，暂时不考虑迁移到虚拟化平台上。

平台选型

目前市场上服务器平台虚拟化厂商有很多，例如VMware，XenServer，微软，RedHat等厂商。

对于VMware，之前图书馆已经有一些基于Workstation版本的使用经验。它与服务器硬件具有良好的兼容性，但是它的成本较高，另外经过测

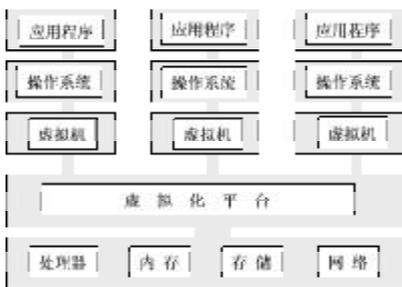


图1 服务器虚拟化架构

试表示它对于 I/O 密集型应用表现不够好。对于 XenServer 也进行了一些测试，结果表明它具有很好的兼容性，在虚拟机上的 I/O 性能具有更好的表现，而且它的成本更低；缺点是它的管理组件不如 VMWare 那样丰富，部署起来没有 VMWare 方便。

经过讨论，图书馆最后决定采用价格更加低廉的 XenServer。一方面图书馆的预算有限，短期内没有太多的 IT 预算来支持虚拟化迁移方案；另一方面前面已经决定选择逐步实施虚拟化的方案，采用 XenServer 可以更好地控制项目初期成本。

为了实施虚拟化，必须要增加一些硬件服务器。根据现有服务器的数量，考虑到每台服务器整合 8~10 个应用，初步估计需要 10 台左右的双插座、四核虚拟化主机。每台服务器配置双插座、四核 CPU，32GB 内存。因为计划逐步实施虚拟化，所以暂时不考虑集中的刀片方案。

在存储设备的选型方面，对于虚拟化平台，存储设备的选型也非常重要，因为在虚拟服务器上存储设备的 I/O 性能通常是瓶颈所在。对于比较重要的应用，我们选择使用 SAN 光纤存储设备，以保证虚拟服务器的存储性能。对于一些次要的应用系统，图书馆则选择了 IP-SAN 存储设备，通过专用 IP 网络来访问存储设备，更具灵活性。

部署及实施

准备好初始阶段所需要的虚拟化平台软件和服务器硬件之后，就可以开始着手进行虚拟化迁移了。

对于大部分系统，图书馆没有考虑直接进行物理服务器到虚拟服务器的迁移，而是在虚拟平台上构建新的服务器，重新部署该应用，然后再迁移数据。这种重新部署的方法要求准备好原来应用系统的部署和安装文档，并且在部署之后要进行仔细测试。其优点是原来的系统不受任何影响，并可以暂时保留，如果新部署平台发现任何问题，可以随时切换回原来的平台，待问题解决之后继续进行虚拟化迁移工作。

对于要迁移到虚拟化平台上的应用，应该考虑询问应用软件开发商，了解他们是否支持虚拟化架构。

在进行虚拟化迁移时，图书馆同时考虑了这个应用系统的灾难备份方案。有些应用系统在原来部署时受某些条件限制，没有考虑灾难备份，迁移到



在图书馆近三年的虚拟化迁移过程中，应用环境运行稳定，为读者提供了无差别的服务，基本上达到了平滑迁移的目标。同时通过迁移到虚拟化平台上，使得系统的灾难备份工作更加容易实现，提高了系统的可靠性。

虚拟化平台之后，可以很容易地实现灾难备份，从而提高原来系统的可用性。对于关键应用还可以考虑负载均衡或高可用解决方案。

图书馆还有开发任务，基于服务器虚拟化平台，可以快速部署一个新系统，用于开发或测试目的。通过将开发系统和测试系统快速部署到虚拟化平台上，不仅可以节省开发环境的硬件投资，还能加快应用系统的开发进度。

经验

图书馆从 2008 年初几台用于测试的虚拟服务器开始，到现在部署的虚拟服务器数量已经达到 30 多台。尽管这二年图书馆新部署了一些应用系统，但是有些系统直接部署到虚拟化平台上，所以现在物理服务器总数已经下降到了 90 台。后期图书馆还将可以考虑将更多应用迁移到虚拟化平台上。

根据对 UPS 电源的监测，服务器机房的能源消耗有一定下降，近期内不存在容量不足的问题；根据温度监测，机房内部的空调也运行良好，近期不需要考虑扩容。所以总体来说实施虚拟化达到了绿色节能的目标。

另外，在实施虚拟化时也需要注意一些问题。首先，虚拟化平台并不是免费的，有些厂商产品的授权甚至比物理服务器还要昂贵，在规划时需要考虑周全；其次，虚拟化平台将多个系统整合到一台服务器上运行，使得服务器硬件故障会导致多个系统停止运行；再次，虚拟化平台系统维护更加复杂，需要提高维护人员的技术水平；还有，虚拟化平台会产生额外的系统开销，硬件配置需要适度提高；最后，需要加强虚拟服务器的管理，避免虚拟服务器泛滥。

(作者单位为清华大学图书馆)



华北电力大学：应用驱动发展



■文 / 孙雅娟 付国 熊伟

“到2020年，基本建成覆盖城乡各级各类学校的教育信息化体系，促进教育内容、教学手段和方法现代化。”《国家中长期教育改革和发展规划纲要（2010-2020年）》对教育信息化进程提出了明确的要求。由于具有资源、人才、经费保障等优势，高校信息化发展不断加快。服务器作为高校信息化的重要基础设施之一，其发展进程与各高校信息化建设密切相关。在服务器选型、管理、规划、新技术应用等方面，各高校既有相同的发展历程，又各具特色。

服务器应用发展历程

华北电力大学1999年开始建设校园网。伴随着校园网的发展，学校的服务器应用数量和规模也不断扩大。推动服务器不断升级换代的原因主要有：Internet的广泛普及；学校规模的扩大；信息服务系统软件的升级；校园信息业务应用不断扩展；新技术的采用。从学校使用服务器的经验来看，校园信息业务范围的不断扩大，尤其是教学资源深入开发和应用，是驱动服务器规模增加和升级换代的最主要因素。

华北电力大学服务器应用发展分为以下三个阶段：

1 1999年~2004年，服务器主要用于提供基本服务，满足基本网络需求，实现部分校园业务自动化管理，采用分散管理模式。基本服务包括网站主页、邮件、DNS、网络计费等服务，系统分散而独立。校园业务包括教务管理、人事管理、财务管理等。其中邮件、DNS、计费系统等采用专用的操作系统（Solaris）和服务器（Sun）。业务管理系统仅限于管理者使用，并没有对师生提供广泛服务，因此对服务器的性能、处理能力、持续开机时间、操作系统等要求不高，对服务器也没有专门的要求，有的甚至用PC来代替。

2 2005年~2010年，伴随着校园信息化建设的深入开展，教务、教学、办公管理系统全面升级，数字图书馆、网络教学等大规模应用，服务器原来的应用管理模式已不适应发展。绿色节能的需要和校园网络带宽全面升级，推动了学校数据中心的建设。学校的两个校区（北京和保定）间建立1000M光纤通道，办公管理、信息交流打破了地域

限制,实现了统一管理。教学资源更是最大限度地应用网络手段,形成了互补和共享。备份机房的建设,集中托管的实施,解决了服务器数量的规模增长的管理问题,为信息化服务绿色可持续发展提供了保障。

3 2010年以后,学校下一阶段信息化建设目标为,数字化校园将全面应用,为两校区一体化办学提供帮助,实现基于学生社区化的教学和生活信息广泛服务。虚拟化、云计算等新技术,可能成为应对未来大规模服务器应用和管理的主要手段。

服务器应用现状

学校目前有各类服务器160台。各种业务所使用的服务器数量分布如图1所示。存储总容量为143T,主要用于各类教学资源建设,其应用分布如图2所示。

其中图1反映了各种信息业务应用现状,应用服务器数量最多的是主页、数字图书资源、网络管理及服务。图2反映了各种教学资源的应用状况,也说明了基于教学的资源建设仍然是校园信息应用的主要方向。

服务器数量分布统计,对服务器应用发展思路给出了指导方向,可以通过刀片服务器、虚拟技术,对业务量分散、占用服务器数量多的应用(如主页)进行整合和集中管理,实现高效、节能等建设目标。

服务器运行环境建设

高效、稳定、安全、可靠的服务器运行环境,是保障服务器硬件最大限度发挥功效,保持业务系统不间断、可持续运行的重要因素。学校在服务器运行环境的规划、建设、实施和管理方面投入了大量的人力、财力和精力,为服务器发挥其效能、应用系统高效稳定应用提供了保障。

1 高效能的数据中心

随着高效电子校务的建设和发展,业务系统不断增加并且复杂化,对于服务器的数量、配置、性能、稳定性都不断的提升要求,从而对于高校数据中心运行环境提出了挑战。经过近十年的发展,数据中心从空间、电力、散热、网络等各方面都存在改造和提升的要求。

学校2010年初正式启用新的数据中心,占地面积500m²,配置专业机柜84台,同时在UPS供电、恒温恒湿恒压以及高速网络方面均按照国家数据中心A级标准要求进行设计,充分考虑未来五至十年的发展和应用进行规划,致力于满足服务器持续增长以及业务系统的高稳定、高可靠的要求而对服务器运行环境的要求。

2 服务器统一管理

早期的业务系统是随着学校各个部门根据业务应用的需要不断建立起来的,因此造成业务系统和服务器需要独立管理,通常由业务系统管理员将服务器放置在办公室进行管理。这种各自为政的管理方式,无论从运行环境和能耗上,还是从数据整合方面,都存在着极大的弊端。

学校在具备了专业的数据中心以后,对学校的服务器进行了统一的规划和管理。学校的重要业务系统和应用服务器需要进行托管,统一购置刀片服务器,替代原有的各种PC服务器或PC机,采用专用技术,提升硬件指标,以保障专业的运行环境和业务系统的稳定运行。

同时,学校将进一步统一规划和统筹分配各种资源,包括存储系统、备份系统、安全系统以及硬件平台,保证业务系统持续稳定运行的同时,节约资源、节省能源、提高管理水平、提高服务效率。

3 服务器性能监测

采用专业的服务器监测系统,对在数据中心运行的服务器进行各项指标的监测,能够对服务器的运行状态、业务、进程、日志等多项指标进行实施监测,并且在出现异常时可以根据故障级别进行多种形式的报警。

例如,对于邮件系统,可以监测SMTP协议、POP3协议等特定应用,从而确保邮件系统的正常运行;对于业务系统,可以监测其WEB应用、数据库以及中间件的运行状态。

这种深度监测系统,

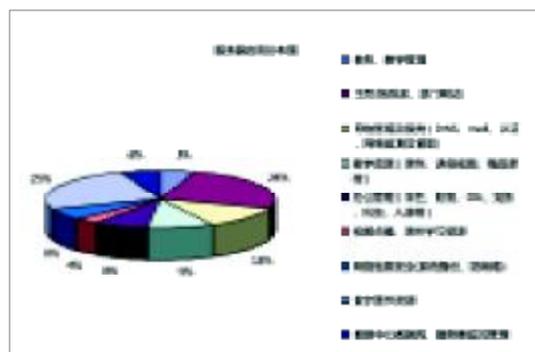


图1 华北电力大学服务器应用分布图

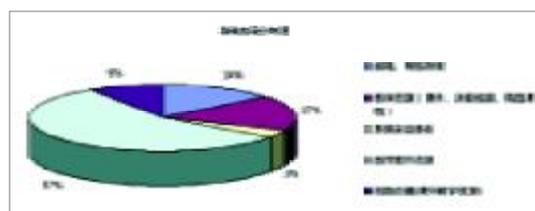


图2 华北电力大学存储应用分布图

服务器技术的发展与应用的发展是不断促进、相辅相成的关系，最终的目标是使应用的效果发挥到极致。随着芯片技术的发展、硬件价格的下降，为服务器的应用提供了广阔的空间。

比传统的服务器通断监测更为深化、细致，以最精细粒度确保服务器的稳定、正常运行。同时，服务器性能监测系统与机房的动力环境监测系统整合为一体，使数据中心的监测业务集中于一个平台上实现，有利于对服务器运行环境的保障，在业务系统出现故障时，能够快速、准确的定位和分析故障的原因，提升故障处理效率。

4 服务器远程管理

服务器一般集中在数据中心统一管理，随着数据中心的专业化，对机房内的恒温恒湿恒压，均有标准要求，因此，服务器的远程管理手段成为一个重要的指标要求。目前数据中心一般采用专用KVM系统进行服务器的远程管理。KVM系统对服务器管理主要有以下几方面优势：

①减少机房内人员出入，保持机房稳定的运行环境。

②提升服务器管理员管理效率，可以在办公室实现服务器远程管理。

③减少服务器外设的配备，节能环保。

学校采用Avocent KVM系统进行服务器远程管理，目前已实现对80余台服务器的远程管理，可以按照服务器的属性进行权限划分，既方便管理员的工作，同时也充分考虑安全性，有效地提升了服务器管理效率。

服务器发展规划

服务器是应用系统的重要硬件支撑环境，服务器的性能发挥效果直接影响到校务系统的运行效果。目前芯片技术飞速发展，服务器不断升级换代，以求能够满足业务及应用的需求。新一代数据中心投入运行，能全方位的为业务及应用提供保障，下一步的规划将是考虑充分发挥外部环境的价值，从而加快学校的信息化建设和发展的步伐，为建设高水

平大学提供助力。

1 统一规划、资源共享

学校在北京和保定分别设有校区，由于异地建设，因此一些业务系统、硬件资源、运行环境存在重复建设，不仅浪费投资，同时对于资源整合也存在着很大的难度。随着两地一体化办学的要求，通过两校区间的高速专线，实现两地资源统一整合和共享。

未来学校将统一规划和整合资源，统筹、合理分配数据中心的服务器、存储、备份等各项资源，做到充分发挥效能的基础上节约投入和开支。并且利用两地的优势建立重要应用系统的互相备份、异地灾备，不断提供业务系统的安全等级。

2 引入新技术，发展特色应用

随着应用的推进，服务器领域也不断发展各种新技术。未来学校将在原有运行环境和硬件平台的基础上，不断引入和应用新技术，促进应用系统、电子校务的发展。

①高性能计算：作为电力行业的高校，我校在能源、新能源领域具有较强的学科优势和多项重要科研成果，未来将利用信息化技术和平台，建立和整合学科数字资源，建设高性能计算平台和服务，从而与国内外高校和行业接轨，从而进行先进技术的学习和推广，推进国家能源行业的发展。

②虚拟化与云计算：由于业务系统和服务器硬件资源的一对一使用关系，造成一部分服务器资源空闲，一部分服务器资源紧张的情况，为更好的合理分配和利用硬件资源，虚拟化技术已经开始应用。未来将重点应用虚拟化技术进行服务器资源、存储资源的统一规划和分配，从而最大限度的节约投入，提高产出。在虚拟化发展到一定的基础上，将逐步转化为云计算，从更深更广的层面共享资源，从而推进应用的发展。

服务器技术的发展与应用的发展是不断促进、相辅相成的关系，最终的目标是使应用的效果发挥到极致。随着芯片技术的发展、硬件价格的下降，为服务器的应用提供了广阔的空间，而如何能够充分发挥其效用，需要更多的技术的产生和应用。目前高校的服务器建设都已具一定规模，未来的任务是如何整合现有资源，统筹规划，这是一项长期而艰巨的任务。

(作者单位为华北电力大学网络与信息中心)



大连理工大学： 打造数据中心云基础

■文 / 李先毅

服务器虚拟化以其高效、节能、高可用等诸多特点已经为人们所熟知，在高校校园网中服务器虚拟化的应用也越来越广泛，特别是在高校校园网数据中心（IDC）中服务器虚拟化的优势更为突出。

随着高校校园网的建设达到一定规模，校园信息化发展到一定水平，对数据中心的建设也提出了较高的要求，要能提供丰富、稳定、可靠的计算资源，满足教学、科研、行政管理等各方面不断快速增长的需求。当前高校数据中心普遍面临发展速度快、人手短缺的问题，服务器虚拟化是很好的解决方案之一。

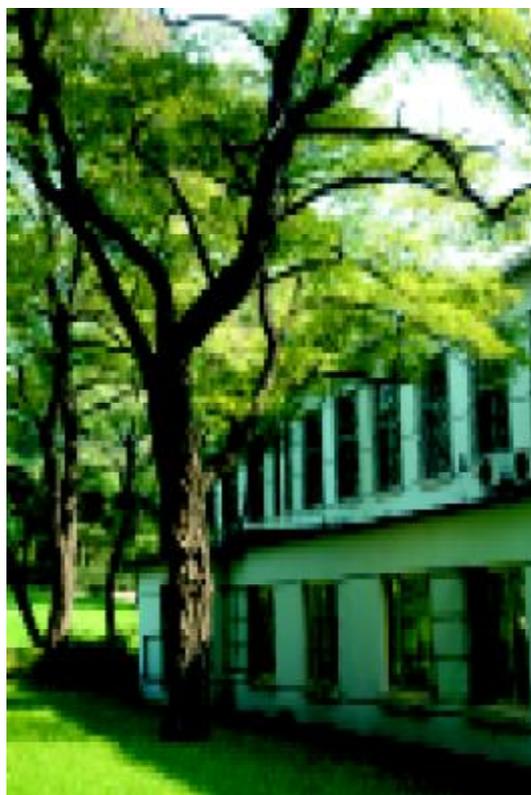
最初只是用虚拟服务器来简单代替实际的物理服务器，通过虚拟化提高硬件资源的利用率，节约能源，并利用虚拟化管理软件来提高管理效率。与传统的物理服务器比，这样的部署是有很大的提升，但从实际应用角度看并仍未做到最优。

虚拟机的配置基本还是由数据中心管理员定义，使用一些固定配置的模板，不能最大限度的接近用户的资源需求。相同的应用，内容不同对资源的需求也是有差异的，例如同样是部门网站人事处与统战部在内容、数据、访问量等方面差别是很大的，相对的资源需求肯定也是不同的，使用固定模板只能保证较高的需求，因此资源仍然存在一定程度的浪费。虚拟机的配置与生成还是由管理员手工完成，缺少与用户的交互，用户不能进行更灵活的资源配置，限制了数据中心的服务种类，每当有新应用出现，管理员就要进行新的资源分配。这种方式已经不太适应快速增长的校园信息化需

求，只是治标未能治本，而建立校园网数据中心云则可以从本质上提升数据中心的整体服务水平，服务器虚拟化则是建立校园网数据中心云的基础。

云计算同样是近几年迅速发展的重要网络应用之一。云计算是一种能够方便、按需从网络访问共享的可配置资源池的模式，且只需最少的管理或服务提供方交互即可快速供应和发布该模型，可配置的资源包括网络、服务器、存储、应用程序和服务。简单的说校园网数据中心云就是按照云模型建立资源池，向校内提供方便、灵活、快速的IDC服务。

云平台根据用户需求自动分配资源，不需要管理员过多的手工干预，减少重复性劳动，管理员可以更多把精力投入到云平台内部的管理。校内用户只需要通过数据中心云平台的用户界面提交需求申请就可以便捷的获得资源，并且当需求发生改变时可以方便的修改或注销资源配置。这样不仅提高了资源分配效率、管理效率，更提升了数据中心服务的多样性，基本可以忽略用户的应用类型，只要用户提出资源需求即可。可以说数据中心云提高了数





服务器虚拟化就是校园网数据中心云建立的基础，数据中心云中的资源配置等都需要靠服务器虚拟化来实现。



据中心的整体效率，对校园信息化建设的资源进行了集中整合，打造出可以保证校园信息化建设快速发展的基础平台。

服务器虚拟化就是校园网数据中心云建立的基础，数据中心云中的资源配置等都需要靠服务器虚拟化来实现。并且要求服务器虚拟化软件与虚拟机管理程序、WEB 方式的用户交互界面及校园网用户管理系统相配合，才能实现云平台。不同的虚拟化软件，其他方面的开发、设计也不同。某些商业化较好的虚拟化软件提供了一定的工具可以帮助云的建立，有些虚拟化软件没有相应的工具，相关的开发就会更加困难。由于校园网数据中心云是高校私有云，搭建比较灵活，要根据本校的实际情况选择相应的虚拟化软件，还可以制定一定的使用、管理规则来减少程序的开发，辅助云的实现。

大连理工大学网络与信息化中心基于虚拟化服务器正在建设校园网数据中心云。目前校园网数据中心配备了 16 台高配服务器及 2 套 FC 海量存储，构成了数据中心资源池。原机架式物理服务器构成的数据中心中基本都是学校二级网站，这些旧网站及新建的校内二级网站都已经构建到虚拟化服务器

中。在虚拟化服务器中还建立了很多新的应用服务，如网上信息中心、精品课平台、教学成果展示平台等教学系统、高清视频点播服务、信息化建设部分业务系统等等。甚至一些主机托管的需求也建立在虚拟化服务器中，不再单独购买服务器，即节约了机房空间降低了能耗，也为学校相关部门节省了开支。

目前校内主要的网络应用服务都可以建立在虚拟化的数据中心上，校园网数据中心利用服务器虚拟化基本上实现了 IaaS 层次的云。

另外，网信中心已经在校园网用户管理系统中部分实现了用户需求的提交，并制定了相应的使用管理规则，用户可以通过 WEB 界面在一定程度上实现与数据中心的交互。通过开发程序实现虚拟化服务器的自动配置后，将可以实现 PaaS 层次的云，也就是前面所说的校园网数据中心云。随着校园信息化的不断发展，未来实现 SaaS 层次的云不是没有可能，用户只需通过 WEB 方式提出应用需求，就可以由数据中心云实现，用户甚至无需关心所需的硬件资源，这就需要服务器虚拟化与应用服务更紧密的结合。

(作者单位为大连理工大学网络与信息化中心)



中国人民大学： 服务器成硬环境的脊梁

■文 / 葛泓 朱斌 王克平



中国人民大学自1996年10月用微波设备以126K带宽接入CERNET华北节点到2006年的十年时间中，校园网经过两次大规模建设升级，发展迅猛。建立了万兆核心、千兆到楼、百兆到桌面的校园网基础网络平台，并与CERNET2实现百兆IPv6连接，全校近三万个信息点，包括教学楼、办公楼和学生宿舍的53栋楼宇均接入校园网。同时，在校园

网基础平台之上建立了两百间多媒体教室，五百台多媒体互动教学公共计算机以及校园一卡通平台。

实现网络基础服务和网络辅助教学服务的硬件支撑环境包括：

1. 两台IBM服务器、一台富士通存储设备和两台梭子鱼防垃圾邮件网关，提供电子邮件服务；
2. 一台SUN490服务器和一台存储设备，构建BlackBoard校园网络辅助教学平台；
3. 八台嵌入式流媒体服务器，实现校园网络电视节目直播；
4. 两台HP服务器和一台华为3COM的存储设备，构成校园公共软件平台，为师生提供公共软件下载服务；
5. 两台学生上网计费服务器，实现学生上网按流量计费的功能；
6. 三台深信服VPN设备，实现校内资源远程安全访问和本校区与苏州校区的网络互连；
7. 一整套视频采编播设备和两台富士通服务器，构建校园网络电视台；
8. 一台移动通信设备，构建校园短信平台。

当前电子校务系统的硬件支撑环境包括SUN15k和SUN25k两台高端小型机、SUN L180磁带库、EMC CX700和COMPELLENT存储。

两台SUN小型机共包含48颗CPU，划分成十个域，作为电子校务系统的WEB服务器、应用服务器与数据库服务器。

EMC CX700和COMPELLENT磁盘阵列作为存储区域网，实现存储资源统一管理和使用。

SUN L180磁带库和Veritas存储备份软件作为存储备份系统，实现系统和数据的备份与恢复。

电子校务系统整个软硬件平台采用三层结构，分为WEB访问层、应用处理层和数据层，内外网分开，实现应用和数据的隔离和保护。

校园卡系统拥有10余公里的专网线路，近两千个信息点，一百二十台交换机，40台校园卡自助终端，两台SUN V880作为数据库服务器，5台SUN v680作为应用服务器，两台加密机，一台IBM服务器作为专网网关，一台监控服务器，多套照片采集和制卡设备，实现校园卡银行圈存、电子注册、餐饮、水控、门禁、医疗缴费、网络缴费等二十多项应用。

目前全校共有300间公共教室，全部为多媒体教室，公共教学用计算机一千多台，实现了基于485控制结构的多媒体网络集中管理和监控。大型多媒体交互式机房15间，由20台集群服务器和17台光纤交换机和一台存储设备实现对700台教学终端的集中管理和控制。

在“数字人大”硬件支撑环境的建设中，注重技术的先进性、硬件设备的高端品质、强大功能、卓越的处理能力以及一定的可发展性。在下一个五年计划中，学校对硬件支撑环境的建设思路也有些调整，在追求高品质和先进技术的同时，把低能耗、低成本、易维护、兼容性和可持续性作为重要的指标。同时整合应用项目，梳理流程，使软件和硬件更合理高效地配置，使系统更加安全高效地运行。

(作者单位为中国人民大学网络与教育技术中心)

理解需求和提升技术

服务器加速发展的前奏

■文 / 本刊记者 周斌

Q = 《中国教育网络》

A = IBM 系统与科技部 System x 中国区品牌经理徐行

高校发展需求决定技术升级

Q 服务器是网络发展的关键点，从服务器诞生到现在，服务器经历过多次更新换代，那么服务器在高校的发展经历了哪些阶段？

A 第一阶段，在 20 世纪 80 年代初期，计算机在高校比较少，多数学校只有一套或者两套主机，大家通过终端使用主机的服务。

第二阶段，在 20 世纪 80 年代中期，随着 PC 的发展，除了高校的计算机中心外，其他课题组也引进 PC 机，比如 APPLE、IBM PC/XT。PC 开始进入教研组，从开始的集中应用逐渐变成了分散。

第三阶段，在 20 世纪 90 年代，PC 逐渐应用变成专业应用，用来进行单机高性能的计算，比如 CAD、电子线路的设计、图形工作站等。

第四阶段，到了 21 世纪，随着图形服务器架构的变化，并行计算开始发展。当 PC 满足不了需求时，就可以购买大型机器或者集群系统来满足需求。随着 X86 的发展，集群的使用逐渐增加。

关键技术决定企业核心竞争力

Q 服务器的性能可以决定网络的性能，而服务器的精尖技术又能提高服务器的性

能，那么目前服务器有哪些关键技术？

A 首先，在计算能力方面，机器本身计算性能需要提高。单台机器的处理能力已经越来越强，CPU 的集成工艺也越做越精细，单个处理器的核数越来越多，主频也得到了改进，超线程技术发展迅速，这些都能使计算能力得到提高。

其次是网络技术地提高。当做高性能集群时，需要把很多机器集群在一起做同一件事，机器之间的通讯很重要，保持数据的畅通就更为重要，这样能使高性能集群的效率有所提升。

再次是存储技术，机器在做并行计算时，如何共同高速访问存储系统，并行存储的软件系统是很好的选择，IBM 的并行文件系统能够在高性能计算下动态地并发访问大量存储，把分布在不同地方的存储统一管理起来，然后并发地去使用。

最后是管理，随着集群的应用，管理的复杂性越来越大，如何让多数机器更好地协同运行，用户越来越多的时候如何管理，这些都是需要思考的问题。

技术优势

Q IBM 在技术方面的优势还有哪些，其中哪些特点是 IBM 独有的？

A 在高性能领域 IBM 有丰富的经验。搭建一个复杂的系统，需要设计一个均衡的系统，包括选择合适的计算能力，合适的存储和网络，合适的管理方式，然后合理地实施，IBM 都有明显优势。

在计算领域，IBM 是第一个用刀片技术做到千万亿次高性能集群的厂商。

在存储技术与大型的集群系统中，IBM 能均衡实施，合理管理。

在做一个整体系统时，实施、部署、管理都是 IBM 的强项。同时，系统的细节部分 IBM 做得也非常好。

在机房设计、节能、散热方面，IBM 的产品有长足发展。比如 IBM 为南京大学搭建的高性能计算集群，无论是从系统的设计、机房设计，还是安装部署、性能调优、管理系统等方面都做得很好，已经能够做到电费支出的平衡。

节能技术成新挑战

Q 服务器在节能减排方面目前有哪些好的技术，后续服务器在节能减排方面有哪些突破方向？

A 在节能方面，从原件的选择、架构的设计到整个系统刀片中心的设计，以及整个机房的布局，这些都会影响到节能的整体效果。

首先是对 CPU 本身的控制。从 CPU 本身是高负载还是低负载的状况分析，如是低负载就把闲置的核关掉，可以降低功耗，也可以通过在空闲状态把 CPU 的主频降下来，来降低 CPU 功耗。

其次，可以通过选用低功耗的内存、高效率的电源来实现节能。在整个设计系统中，散热问题非常关键，风路需要有完整的设计，尽量减少风扇的负荷，同时通过管理软件，监控每个部件用电的情况，从而制定出用电的规划。

最后是散热层面，机房的布局和架构应该设计合理。■

CPU 虚拟化 集群 绿色

服务器技术的风向标

■文 / 本刊记者 周斌

Q=《中国教育网络》

A=曙光技术支持中心部门总经理曹振南

Q CPU 是服务器技术的一个重点，您认为 CPU 的发展趋势是什么？

A CPU 的发展趋势是更多的核心、更高的性能、更先进的工艺、更低的功耗以及与 GPU 功能的整合。

CPU 集成 GPU 是未来 CPU 的发展趋势，明年 Intel 推出的下一代 CPU Sandy Bridge 以及 AMD 的“APU”都会集成 GPU。

Q 服务器虚拟技术的发展方向？

A 从技术角度看，从 CPU 到网卡，服务器硬件会越来越重视对虚拟化技术的支持和优化，当然，虚拟化软件也会越来越重视对各种具有虚拟化特征的部件的支持和融合。

从应用角度看，目前，利用虚拟化、云计算技术构建新型的数据中心成为业界的热点，而服务器虚拟化技术在这个过程中扮演着及其重要的角色。

因此，如何更好地与新型数据中心（比如动态数据中心、云计算中心）的建设需求相结合，是服务器虚拟化技术发展的重要方向。

Q 曙光与高校在集群系统方面有哪些合作？如何高效地实施集群系统管理？集群系统应用中遇到的问题以及如何解决？

A 曙光会积极地参与国内高校的高性能计算机集群地建设，这方面，我们已经取得了很大的成功，建成了很多高性能集群，比如有中南大学、中山大学、中国矿业大学、南京航空航天大学、湘潭大学等，曙光的高性能集群在国内高校中已经超过了上千套，目前正在积极参与的包括清华大学、复旦大学、大连理工大学、中山大学三期等等。

集群系统的建设其实是一个非常复杂的过程，除了最核心的

计算系统、网络系统和存储系统等 IT 核心硬件设备，还包括基础设施建设、管理调度软件与应用软件建设、运维及应用支持、管理员及用户培训等等，大部分集群系统在建设初期往往只重视硬件设备地建设，而忽视管理运维、高性能应用软件支持和培训等方面的内容，造成了项目建成后应用缺乏，应用支持能力差，系统用户满意度低，集群使用效率低等问题，所以高性能集群系统的建设不仅仅是一个硬件设备建设的过程，更重要的是一个服务与运维的综合系统。

例如我们于去年年底建成的中南大学高性能计算中心，就是一个非常好的典型案例，该系统在硬件系统合理可靠的基础上，非常重视应用软件的支持和整体的管理运维，培训等方面的工作，所以项目建成后效果非常好，校外用户众多，用户满意度高，集群使用效率长期保持在 90% 以上。

集群系统目前最大的问题是应用的支持和管理运维，解决方法就是通过专业应用支持，管理运维优化和培训来提高集群的使用率和用户满意度。

Q 服务器在节能减排方面目前有哪些好的技术？

A 服务器在节能减排方面一般采用两个方面的技术：

一是利用硬件技术，采用低功耗的处理器、内存、高效率的电源模块、线性预补偿的散热模块等部件来降低服务器系统的功耗，值得提出的是，具有较高计算密度、采用模块化设计的刀片服务器与普通的机架式服务器相比，也具有较低的功耗；

二是利用软件技术，通过节能软件降低服务器系统的功耗，如曙光公司的 Powerconf 节能软件系统，该系统根据服务器的应用负载自动调节服务器的工作状态，经过曙光公司的多方用户验证，节能效果在 20% 左右。

除此之外，有些厂商服务器产品的包装采用可回收降解材质包装，进行多次回收利用也是节能减排的一种手段。■

CPU 的发展趋势是更多的核心、更高的性能、更先进的工艺、更低的功耗以及与 GPU 功能的整合。

自主知识产权打造核心竞争力

自 2006 年以来，浪潮连续四年专利申请增长率超过 40%，2009 年完成 483 项专利申请，其中服务器、存储领域就申请了 215 项。

■文 / 本刊记者 周晓娟

Q=《中国教育网络》

A=浪潮服务器行业方案总监赵文慧

缩小技术差距

Q 服务器的关键技术有哪些？国内在这些领域的发展形势如何？目前跟国外比有哪些差距？哪些地方需要改进？

A 目前服务器涉及芯片组、操作系统和 CPU 三个主要技术领域。

第一，芯片组几乎决定着计算机的性能和功能，包括 CPU 的类型、主板的系统总线频率，内存类型、容量和性能以及扩展槽的种类与数量、扩展接口的类型和数量。如果说处理器是计算机的大脑，那么芯片组就是计算机的躯干。芯片组要求有良好的兼容性、互换性和扩展性，对稳定性和综合性能要求也最高。

第二，操作系统一方面管理着所有计算机系统资源，另一方面为用户提供了一个抽象概念上的计算机，一个交互的界面，避免了对计算机系统硬件的直接操作。更重要的是，操作系统决定了应用软件的开发标准，是软件产业的根基。

第三，服务器的 CPU 承担数据的处理能力，它是计算机产业的核心。通常处理器厂商对整个计算机产业都有极强的控制力，比如 Intel、AMD。

事实上，这三大技术中国都已经具备并取得了一定的成就，比如龙芯、红旗 Linux，都已经有了成熟的技术。但是 IT 产业，技术不是关键，关键是把技术产品化、产品产业化，而 IT 产业化恰是中国的软肋，我们与发达国家还存在着很大的差距。

Q 如何打造“绿色”服务器，服务器在节能减排方面的突破方向？

A 服务器能耗是一个十分重要的问题，降低服务器能耗的技术主要分为两类：

一是高效部件技术，现在已经成熟的服务器高效部件技

术有新处理器架构（比如 Intel 的 Nehalem 和 AMD 的 Bulldozer）、SSD 硬盘、智能感应风扇等；

二是能耗管理技术，如 Intel 的 Nodemanager 通过在业务低谷降低或者关闭处理器部分核心以降低功耗；浪潮硬盘管理技术，按照既定策略让非读写状态的硬盘进入休眠，需要操作时能够快速启动，这对于有大量服务器存储设备的 IDC 中心来讲意义重大，例如网易、网通等。

此外，在整体机房的供电、散热方面的技术进步也会带来极大的节能效果。一般数据中心每消耗 10 度电，仅有 4 度是设备发热，而有 6 度是散热设备消耗掉的。

当前最新的是水冷散热技术，水的散热效率是空气的 4000 倍，能够大幅度降低机房散热功耗。目前，浪潮基于水冷技术的高性能集群已经在山东大学超算中心成功应用。

后续服务器的节能降耗会在上述两个技术方向上不断发展，综合各种高效技术，为客户提供一体化的高能效整体解决方案，这种综合整体创新才能给客户带来价值。

浪潮作为整体解决方案供应商，提出绿色战略，着眼“器、管、用”三层，即从产品系统、应用部署和服务器管理三方面实现性能和功耗之间的平衡。

“器”，通过产品部件的技术创新，实现硬件的节能，这仅是一方面。电既是通过技术创新省出来的，也是通过“管和用”省出来的。“管”，通过对电源、芯片等系统部件的监控管理，浪潮创造了“向管理要效益”的 IT 节能新模式，系统功耗可以随负载变化而变化。“用”，就是大力推广虚拟化、云计算等技术的应用，通过高效整体方案提高系统资源利用率，降低服务器的数量，达到降低能耗的目的。

虚拟化解决方案降低成本

Q 目前服务器虚拟技术的特征？服务器虚拟技术应用的典型案例？服务器虚拟技术的发展方向？

A 虚拟化技术的本质是一种资源管理技术，本身不会创造任



何新的资源，只能是让资源更合理地利用，其最大的特征就是把一台物理服务器分拆成几个逻辑服务器，实现一台服务器当多台服务器用，并且应用之间相互隔离，互不影响。

浪潮虚拟化整合方案已经在全国多所高校成功应用。在齐齐哈尔师范大学，在单服务器单操作系统的传统应用模式下，资源占用率在10%以下，大量的服务器资源被闲置，并未得到充分有效的利用，而采用浪潮虚拟化解决方案，新平台的利用率提高到70%以上，服务器数量降低85%，总体成本降低70%。

虚拟化技术的发展方向主要有两个：首先，虚拟化技术从服务器向存储、网络、甚至于终端桌面不断延伸，比如存储虚拟化，网络虚拟化等，形成一个全虚拟化的技术环境；其次，服务器虚拟化相关增值技术的发展，例如大规模管理技术、资源动态分配技术等，最终能够把数据中心整合成一个透明可视的、资源自动流转的资源池，甚至实现跨数据中心的资源调度管理。

Q 高校的哪些应用适合虚拟化？对服务器的要求有哪些？

A 高校的信息化应用由于用户规模的限制普遍压力不大，因而除去极个别的应用，如高性能集群等，都可以进行虚拟化整合。

由于虚拟化大大提高了应用部署密度，一方面硬件平台各个单元网络、存储、计算等，需要承受较高的系统压力，处理器利用率一般保持在50%-80%；另一方面虚拟化整合以后通常一台服务器运行多个应用，虽然一般会通过虚拟机HA来提高系统可用

性，但是硬件平台宕机也会给业务带来很大的影响，因此虚拟化对平台的性能、可用性的要求都远超过一般的应用系统。

所以，虚拟化整合，尤其是大规模的虚拟化整合，通常会采用4路以上的大型服务器系统。

自主知识产权成亮点

Q 浪潮在服务器自主知识产权方面的基本情况？在高校市场分布情况？

A 浪潮以核心技术为关注焦点，创造性地提出“技术专利化、专利标准化、标准国际化”的知识产权战略。知识产权工作已经贯穿于浪潮技术创新和产品研发的全过程。自2006年以来，浪潮连续四年专利申请增长率超过40%，2009年完成483项专利申请，其中服务器、存储领域就申请了215项。浪潮集团牵头或参与的8项国家标准获得颁布实施，并正在参与其他9项国家标准的制定。

高教行业是市场增长的重要领域之一，尤其是高教HPC。同时，高教也是浪潮的主要行业市场，2009年浪潮高性能服务器在高教市场的带动下，业绩同比增长90%；在下一代互联网工程的建设中，浪潮服务器包括了清华、北大、南开、浙江大学等国内100余所高校的项目，市场占有率超过30%。

识别 P2P 流媒体来龙去脉

随着 P2P 技术应用的不断扩大,特别是流媒体业务的不断扩展, P2P 网络本身对网络带宽的滥用问题越来越严重,引起网络服务提供商的高度重视,因此,如何有效、快速的识别 P2P 流媒体流量并提取特征码亟待解决。基于覆盖率统计的特征码自动提取方法克服了人工提取的缺点,耗时短、效率高,通过采用 One-Way Hash 算法短时间内能实现实时提取,准确率也很高,能有效的识别 P2P 流媒体的流量。

■文 / 王世福¹ 李芝棠² 柳斌²

近年来,随着 Internet 的迅速发展,对等网络技术(peer-to-peer,简称 P2P)的应用越来越广泛。然而, P2P 技术在给人们带来娱乐和方便的同时,也带来了隐忧。P2P 应用的流量日益增大,它们占据了大量的互联网带宽,巨大的资源消耗引起企业及 ISP 瓶颈链路的阻塞。P2P 流量占用带宽接入的大量资源,许多 ISP 也纷纷报告他们的网络流量中有大约超过 50% 属于 P2P 流量。各大网络服务提供商迫切地需要识别已经限制某些 P2P 的流量,而对 P2P 流量识别最有效的办法之一就是特征码匹配识别,目前特征码的提取主要依赖专家提取,提取周期长、工作量大,往往不能及时满足服务商的要求。因此,针对 P2P 流媒体的特征码自动提取方法进行研究,有助于增强对 P2P 应用的监测和控制力度,阻止或减轻 P2P 造成的不利影响。

提取方法

现阶段特征码提取主要依赖人工提取。人工提取又名专家提取,是人工地去观察某一流媒体应用的连接建立信息(五元组信息)、监听端口信息、流量特征信息、以及数据包负载内出现的特殊字符串等信息。它主要关心的是某条何时建立,何时终止,以及在流连接建立的阶段出现了哪些特殊字段,而所有这些信息都要依靠专家们人工地去分析判断,得到的特征码虽然准确率比较高,但生成周期耗时

长、技术水平要求高,效率非常低。为了解决这个难题,迫切地需要一个流媒体特征码的自动提取算法。通过长期的观察实验, P2P 流媒体在资源共享的过程中,两两之间进行交互的控制信息非常频繁,并且这种行为有共同点存在,基于这个特性,设计出一种基于控制信息的特征码自动提取算法。在不失准确性的前提下,它缩短了特征码的提取周期,实现了程序的自动提取,克服了特征码提取技术水平要求高的问题,提高了特征码提取的效率。

特征码的提取过程

先做个假设,首先已经确定某台主机已经是在进行流媒体的行为,再对其进行特征码提取,特征码提取的流程如图 1 所示。

第一, P2P 流媒体流量捕获。捕获某一运行 P2P 流媒体应用主机的流量数据,从大量的数据实验可以发现, P2P 流媒体的数据传输通常采用的是 UDP 协议,而且流媒体的控制协议特征比较明显,这些包的字节大小范围大概在 65 字节到 300 字节以内。我们对数据进行了初步过滤,限定协议为 UDP 并且数据包长度范围为 65 字节到 300 字节范围内,将一段时间内的这些数据包信息进行捕获保存,以备下一步处理。

第二,监听端口识别。P2P 流媒体软件通常都会对某个或某几个特定的端口进行监听,如果能识别出此应用的监听端口的话,将会对特征码提取提供很大的帮助。根据 P2P 流媒体数据交互比较活跃的



图1 特征码提取流程

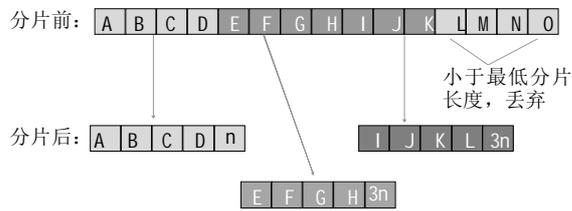


图2 数据包分片示意图

表1 特征串分片重组(十六进制)

重组前的特征码字符串	重组后的特征码字符串
1500 : 2	1500430000a1: 6
00a1 : 6	
0002 : 24	
0000 : 14	
0407 : 20	
4300 : 4	

特性，对每个端口收发的数据包数目进行统计，数据最多的往往都是流媒体应用。通过对端口的过滤提高数据的纯度，进而提高特征码的准确性。将第一步得到的数据进行端口统计，得到流媒体应用的监听端口号。

第三，数据分片。将第二步得到的端口号作为过滤条件，对数据进行再一次过滤，这样就得到了比较纯净的数据。然后将每一个数据包的负载部分按照固定长度进行分片，比如我们以 n 字节长度对数据包进行分片，如图2所示，每获取 n 个字节作为一个分片，然后在这个分片末尾增加一个字节去表示他的位置信息，这里取的是最后一个字节的位置，那么第一个 n 个字节分片的位置信息就是 n ，依次类推，第二个分片的位置信息就是 $2n$ ，第三个分片的位置信息就是 $3n$ ，数据包末尾部分如果小于分片长度将被丢弃。

分片以后我们将包含位置信息的分片进行 One-Way Hash，进而得到各个字符分片的覆盖率 O_t ，设定一个阈值 O 以表现某个特征码片段是否出现的很频繁，将覆盖率大于 O 的字符分片挑选出来供下一步处理。这里的覆盖率定义的某一字符分片在数据包中出现的频率。

$$O_t = \frac{n_t}{N}$$

其中 O_t 为字符串分片 t 的覆盖率， n_t 为包含字符串分片 t 的数据包个数， N 为总的数据包个数。

One-Way Hash 是这样一种针对字符串的 Hash 算法，它用字符串的 Hash 值作为这个字符串在 Hash 表中的下标，每一个 Hash 值进行取模运算 (mod) 对应到数组中的一个位置，这样只要比较这个字符串的哈希值对应的位置有没有被占用，就可以得到最后的结果了，这种方法的速度是最快的 $O(1)$ 。对两个字符串在哈希表中对应的位置相同的问题，One-Way

Hash 解决问题的基本原理就是：在哈希表中不是用一个哈希值而是用三个哈希值来校验字符串。假如说两个不同的字符串经过一个哈希算法得到的入口点一致有可能，但用三个不同的哈希算法算出的入口点都一致，那几乎可以肯定是不可能的事了，这个几率是 $1:18889465931478580854784$ ，大概是 10 的 22.3 次方分之一，对于普通程序来说已经远远足够了。

第四，字符串分片的重组。经过第三步的处理我们就可以得到若干覆盖率大于 O 的字符串分片，我们需要将这些零散的字符串按照位置信息进行重新组合，将位置连续的字符串合并到一起，考虑到过短的特征字符串没有实际应用意义，经过长期的观察实验，可以设定一个阈值，只有长度超过这个阈值的特征字符串才能被用作特征码，以表 1 为例，以 2 个字节长度进行分片，设置阈值为 4 个字节，那么合并后就只剩下一个符合条件的字符串，我们就将这个字符串作为一个特征码。

第五，特征码的验证以及去除冗余。这种提取特征码的方法虽然效率很高，速度很快，但作为交换牺牲了一些准确性，带来了一些冗余信息，这些冗余信息主要是跟时间或者当前流媒体播放的节目相关的一些内容，这些内容只会在这段时间内出现的比较频繁，而在之前或之后的时间内不会或很少出现，利用一个验证的过程就可以去除这些冗余，同时也对特征码进一步的提纯，并起到一个校验的效果。

我们将提取到的特征码字符串去检测匹配实际网络中的流媒体流量，对那些长期匹配量很少的特征字符串我们就可以认定为是冗余信息，进而将这些特征字符串从数据库中剔除。通过这样一个不断重复的过程，我们就可以得到比较实用、有效的特征码。

系统实现

系统实现分两大部分，后台部分及前台页面部分，这里着重介绍下前台部分。图3所示为系统的整体UI界面，分别显示全局流量统计、识别用户详情、特征码详情、端口统计分析、特征码管理、系统管理和登录管理等七大部分。全局流量统计又分历史流量、用户分类流量和分类应用流量三部分，提供历史流量信息、用户分类信息和分类应用信息的查询。特征提取详情部分中能分别显示新提取的流媒体应用的连接信息和流量信息、新提取特征码详情等内容，并提供新提取特征码所匹配的连接信息查询。

特征码管理部分则包括特征码详情、管理特征码和查看事务表三部分，特征码详情如图4所示，表

项分别显示特征码的编号、分类、名称、匹配流数、长度、偏移和内容，而且点击特定的项目还有链接出现，比如我们点击名称中第4条特征码则会出现如图5所示内容“4号特征码匹配连接详情”，从弹出的控件中我们可以看到此种特征码匹配到的具体连接情况，包括内外网地址、端口号，内外网物理地址、流量和持续时间等等。若点击匹配流量的某一条则会出现如图6和图7所示内容，分别显示相应特征码的匹配连接信息和匹配流量信息的饼状图。管理特征码部分可以对特征码进行添、删除和重命名操作，以便加入已知的特征码或删除过时的特征码以及对特征码进行重命名操作，如图8所示。

(作者单位 1华中科技大学计算机科学与技术学院 2华中科技大学网络与计算中心)

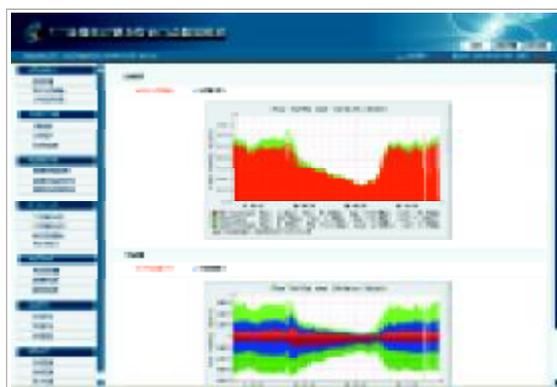


图3 特征码提取系统的UI界面

图4 特征码详细信息

图5 特征码匹配连接信息

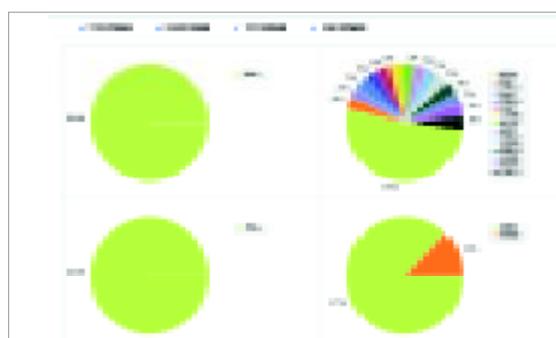


图6 特征码匹配连接信息



图7 特征码匹配流量信息



图8 特征码管理

HTML5 将带来什么



IE9可以独立查看网页中的所有动画元素

Web 开发者对 HTML 5 的参与度在不断上升升温。如今由 W3C (the Worldwide Web Consortium) 对 Web 置标语言进行彻底革新。很多人认为对 HTML 的修整早应完成,然而 HTML 却在近十年中没有得到适当提升。事实上,赢得 W3C 推荐席位的最后的置标语言是 2001 年的 XHTML 1.1, 这是

Web 标准过程中的最终阶段。

在这些年中, Web 开发者变得越发焦虑。很多人称 HTML 和 XHTML 的标准已过时了,并且仅聚焦以文档为中心并不能足够满足现代 Web 应用程序的需求。

HTML5 尝试改变这些。当它完成时,新标准将在改善的互动、多媒体和定位中提供多个 Tag 和 API。随着由实验支持的 HTML5 特征被加入到目前盛行的 Web 浏览器中,一些开发者已开始表示出对这新型现代的 HTML 的兴趣,而不再依赖于像 Flash, Quick Time 和 Silverlight 这类专有插件。

尽管一些著名的 Web 发行人,包括 Apple、Google、Mozilla Foundation、Vimeo 和 YouTube 已经开始胡乱修补新标准, W3C 内部人员称 HTML5 发展的道路仍然是艰辛的。虽然部分标准已经完成,但是有些具体事项还处于分歧中。也许完整的标准还会等多年时间才出现,网上冲浪的大众还会等更长的时间才使用 HTML5 兼容的浏览器。同时,开发者面临着一个巨大挑战:当人们正向明日的 HTML5 平稳过渡时,怎样用今日的技术来创建和丰富互联网应用

程序。

2004 年, Apple, Mozilla Foundation 和 Opera Software 公司的代表们创立了 Web 超文本应用技术工作组 (WHATWG) 的组织。此后, W3C HTML Working Group 于 2007 年成立并着手开发 HTML 5。目前,开发工作仍在进行中,并将于 2012 年向 W3C 提交初步意见,不过现在已经有不少浏览器部分支持 HTML 5。HTML 5 具有令人激动的新功能。

实现更丰富、基于标准的 Web

人们最迫切期待的 HTML 5 新增方面是那些新的元素和 API, 让内容创作者只要使用基于标准的 HTML, 就能制作丰富多媒体内容。现代网页越来越多地采用可扩展图形、动画和多媒体,但到目前为止,这些功能要求使用 Flash、Real Media 和 QuickTime 等专有插件。这类插件不但带来了新的安全风险,还限制了网页的受众面。

HTML 5 解决这个问题一个办法就是让浏览器原生地支持相关的标记语言。内容创作者可以把用 MathML (用于渲染公式) 和 SVG (用于渲染可扩展矢量图形) 编写的标记直接嵌入到 HTML 5 网页中。这种更强的灵活性让跨平台的 HTML 比设计当初就既要支持图形又要兼顾文本的 Flash 和 Silverlight 等更有竞争力。

不过, Web 开发人员对 HTML 5 新的音频和视频标签的呼声更高, 这些标签最终目的是要很容易地把多媒体内容嵌入到网页中。这些标签在 HTML 5 标准中要求与编解码器无关, 这意味着将由浏览器厂商负责提供能播放任何内容所需的编解码器, 只要符合一定标准就可以。其中, 视频标签尤其被寄予厚望, 因为对网上视频提供商来说, 它们希望自己的内

容未来可以在苹果的iPhone(手机上网)和发布的iPad上播放,同时这两款设备目前都不支持Flash。

画布(Canvas)标签让交互式Web图形向前迈进了一步,该标签可用来把浏览器窗口的某些区域定义为动态位图。Web开发人员可使用JavaScript来处理画布中的内容,针对用户操作实时渲染图形。从理论上来说,这项技术有望让开发者只需使用JavaScript和HTML,就能开发出完全交互的游戏。

除了这些显示技术外,HTML 5还引入了基于浏览器的应用缓存概念,应用缓存让Web应用可以把信息存储在客户端设备上。与谷歌Gears插件一样,这些缓存既提升了应用性能,又可以让用户即便无法连接互联网,也能继续使用Web应用。事实上,谷歌已经计划逐步停止支持Gears,改而支持HTML 5技术。

浏览器插件还未过时

尽管HTML 5有诸多新特性,但用户也不用期望插件会一夜之间消失。Web向来就有多种相互竞争的技术与媒体格式共存的传统,且很难克服这种传统的强大惯性。也许很多年以后,纯HTML 5浏览器的性能才赶得上如今各式各样的客户端的要求。

比如,尽管Vimeo和YouTube已经开放HTML 5视频,并且HTML 5版的YouTube支持变速视频播放,却不会像听上去那么顺利。W3C决定不在HTML 5标准中明确规定用哪种特定的媒体编解码器,这意味着开发人员无法保证任何一种媒体格式在每一种客户端设备上都能播放。比如,苹果、谷歌和微软都在力推H.264视频格式,但Firefox和Konqueror等开源

浏览器却无法(或者说不愿)把支持这种格式的相应专利权授给别人。除非解决这个问题,否则Web内容创作者要想覆盖最广泛的受众面,可能只好继续依赖Flash。

也并不是每个旧的Web应用都能针对HTML 5进行改写。比如,尽管谷歌低调对待自身的Gears技术,青睐基于标准的本地应用存储方法,但Gears API和HTML 5应用缓存API并不完全一样。谷歌自己承认目前还没有一种简单、全面的方法可以让具有Gears功能的应用(连同整个用户群)都改用基于标准的方法。除非真有这种方法,否则连使用完全兼容HTML的浏览器的用户也可能只好安装Gears以支持这些过去开发的Web应用。

最后,对钟情于HTML 5的开发者来说,浏览器市场份额也许是最大的障碍。尽管IE6存在渲染问题、在支持Web标准方面落后,却似乎仍是不可能马上消失的浏览器。旧版本的Firefox、Opera、Safari及其他浏览器也有庞大的用户群,而它们中没有一个支持HTML 5。除非这些浏览器换成新版,否则Web开发人员可能需要同时维护两个版本的网站:一个面向HTML 5用户的版本,另一个面向依赖过时渲染方法的面向旧浏览器的版本。

苹果的iPhone和iPad青睐HTML 5,不支持Flash,随着HTML 5日趋成熟,预计它们会支持这项标准。与之相似的是,谷歌的Chrome浏览器在支持HTML5方面一路领先,而基于该公司即将推出的Chrome OS的设备预计会亦步亦趋。不过,各大内容发布网站在标准支持方面一向很保守,就算拥有庞大的HTML 5用户群,财富500强公司可能也在多年以后才愿意冒险升级。 (翻译:袁殷)

微软发布支持HTML5的Bing

近日,在IE9 Beta发布会上,微软Bing团队带来了一段演示视频,展示了支持HTML5功能的Bing搜索。最新的升级的Bing搜索引擎能够使用HTML5 canvas标签来支持动态主页,而不需要借助任何插件或是视频。



模仿书法的HTML5演示



宝马3D模型展示网页

CNCERT发布8月网络安全监测数据

公共互联网网络安全问题利好

文 / 周勇林

根据 CNCERT 监测结果，除我国境内木马和僵尸网络控制服务器数量有所增长外，境内木马和僵尸网络受控主机数量、网页篡改数量等均有不同程度的下降。此外，根据通信行业报送的信息，8月公共互联网环境中各类事件数量较7月呈现小幅递减趋势，特别是恶意代码活动和网站安全方面，这与通信行业持续加强对木马和僵尸网络、网站安全事件的监测和处置有很大关系；部分地区运营企业报送的网内拒绝服务攻击次数也呈现下降趋势。总体上，8月公共互联网网络安全态势比7月份好，各单位应重点关注一些对本单位信息系统运行可能构成重大威胁或可能造成重大影响的事件信息和预警信息，如：桌面操作系统和应用软件漏洞。

8月，根据 CNCERT 的监测数据和通信行业报送数据，全国公共互联网网络安全状况的主要指标情况如下：

恶意代码活动情况方面，我国大陆地区约有 97 万个 IP 地址对应的主机被木马程序控制，同种类木马感染量较7月下降 16%；我国大陆地区约有 3.9 万个 IP 地址对应的主机被僵尸程序控制，同种类僵尸网络感染量较7月下降 52%；

网站安全方面，8月我国大陆地区被篡改网站数量为 2257 个，较7月下降 22%，其中被篡改政府网站数量为 267 个，较7月的 393 个下降 32%，占大陆被篡改网站比例也由 13.66% 下降到 11.83%；

事件受理方面，CNCERT 接收到网络

安全事件报告 617 件（不含扫描和垃圾邮件类事件报告），数量较7月下降 25%。

被控制主机数量减少

8月，CNCERT 监测发现我国大陆地区 970113 个 IP 地址对应的主机被木马程序控制，同种类木马感染量较7月下降 16%。数量最多的地区分别为湖南省 169457 个（占中国大陆 17.47%）、广东省 117623 个（占中国大陆 12.12%）和辽宁省 63198 个（占中国大陆 6.51%）。

2010年1月至8月，我国大陆地区被木马程序控制的主机 IP 数量月度统计如图 1 所示，同种类木马感染量较7月下降 16%，但新增监测的一种流量劫持类木马受控主机数量较大。

8月，CNCERT 监测发现我国大陆地区 17659 个 IP 地址对应的主机被利用作为木马控制服务器，同种类木马控制服务器数量环比增长 91%。数量最多的地区分别是广东省 2399 个（占中国大陆 13.59%）、浙江省 1973 个（占中国大陆 11.17%）和江苏省 1454 个（占中国大陆 8.23%）。

2010年1月至8月，我国大陆地区木马控制服务器 IP 数量月度统计如图 2 所示，8月木马控制服务器 IP 数量有所回升。

8月，参与控制我国大陆计算机的境外木马控制服务器 IP 有 9240 个，同种类木马控制服务器数量环比增长

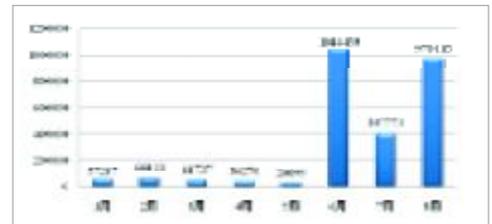


图1 中国大陆木马受控主机IP数量月度统计

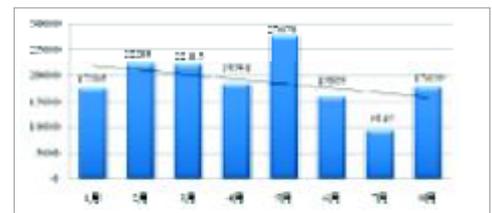


图2 中国大陆木马控制服务器IP数量月度统计

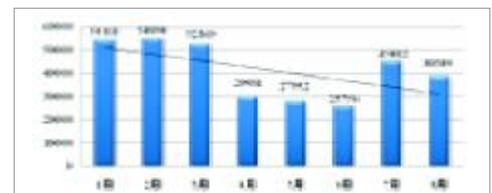


图3 中国大陆僵尸网络受控主机IP数量月度统计

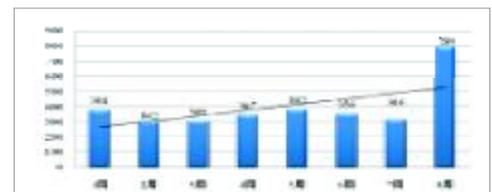


图4 中国大陆僵尸网络控制服务器IP数量月度统计

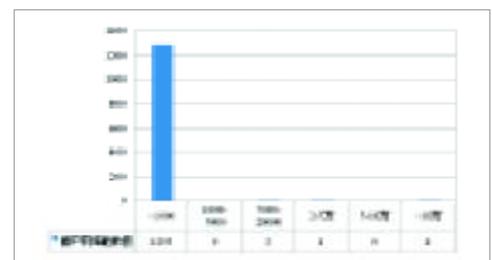


图5 僵尸网络的规模分布

29%，主要来自美国、我国台湾和韩国。

8月，CNCERT监测发现我国大陆38589个IP地址对应的主机被僵尸程序控制，同种类僵尸网络感染量较7月下降52%。其中，数量最多的地区分别是广东省5866个（占中国大陆15.20%）、江苏省2820个（占中国大陆7.31%）和浙江省2780个（占中国大陆7.20%）。

2010年1月至8月，我国大陆地区被僵尸程序控制的主机IP数量月度统计如图3所示，同种类僵尸网络感染量较7月下降52%。

8月，CNCERT监测发现我国大陆地区789个IP地址对应的主机被利用作为僵尸网络控制服务器，同种类僵尸网络控制服务器数量环比增长3%。数量最多的地区分别是北京市93个（占中国大陆11.79%）、江苏省80个（占中国大陆10.14%）和浙江省78个（占中国大陆9.89%）。

2010年1月至8月，位于我国大陆地区的僵尸网络控制服务器IP数量月度统计如图4所示，8月僵尸网络控制服务器IP数量处于较高水平。

8月，参与控制我国大陆计算机的境外僵尸网络控制服务器IP有508个，同种类僵尸网络控制服务器数量环比下降2%，主要来自美国和我国台湾。

在发现的僵尸网络中，规模大于5000的僵尸网络有4个，较7月减少4个，规模在1000以下的占99%以上。分布情况如图5所示。

网站篡改问题减轻

8月，我国大陆地区被篡改网站的数量为2257个，与7月的2877个相比下降22%，其中代号为“KhrYsa0R”、“HEXB00T3R”和“aGrEsiF”的攻击者对大陆政府网站进行了大量篡改。

在我国大陆被篡改网站数量按地区分布中，数量最多的地区分别是北京市428个（占中国大陆18.96%）、江苏省322个（占中国大陆14.27%）和广东省257个（占中国大陆11.39%）。

我国大陆被篡改网站数量按类型分布情况如图6所示。其中，被篡改数量最多的分别是.com和.com.cn，为1445个（占中国大陆64.02%），.gov.cn为267个（占中国大陆11.83%），.net和.net.cn为170个（占中国大陆7.53%）。

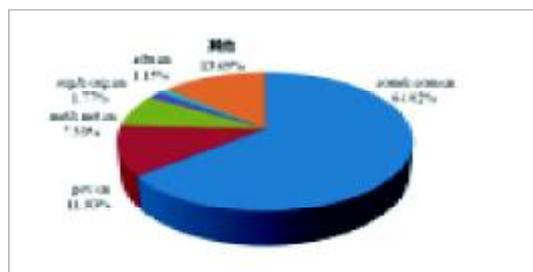


图6 中国大陆被篡改网站按类型分布

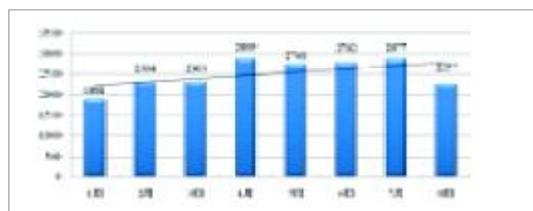


图7 中国大陆被篡改网站数量月度统计

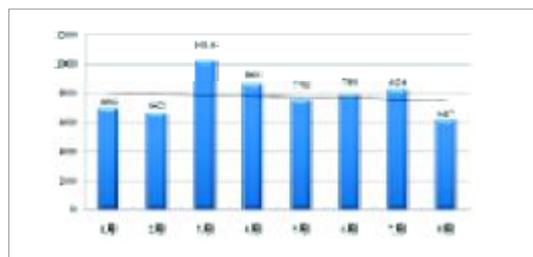


图8 网络安全事件报告数量月度统计

2010年1月至8月，我国大陆网站被篡改数量的月度情况统计如图7所示，8月我国大陆网站被篡改数量有所回落。

事件受理同比下降明显

8月，CNCERT收到国内外报告的网络安全事件617件，与7月的824件相比下降25%，其中来自国外的事件报告有601件。

在617件事件报告中，数量最多的分别是漏洞类事件259件，恶意代码类事件192件，网页仿冒类事件162件。8月，除“网页仿冒”事件报告数量略有增长外，其他网络安全事件报告数量均有不同程度的下降。

2010年1月至8月，CNCERT收到的网络安全事件报告数量月度统计如图8所示。8月收到的网络安全事件报告数量处于较低水平。

(作者单位为国家互联网应急中心运行部)



NIC2010 年 8 月

印度获较大 IPv6 地址

文 / 朱爽

8月全球IPv4地址分配数量为322B,其中获得最多的是韩国,103B,其次是越南,64B,中国48B列第三位。在过去的12个月,中国获得IPv4地址最多,共计741B。全球IPv4地址空间,预计在2011年上半年用完。

8月全球IPv6地址申请(/32以上),总计有114个,其中欧洲42个,亚太40个,北美28个,拉美4个,分别来自41个国家/地区。申请个数最多的是美国,24个。较大的申请,只有1个/31,来自印度。8月全球IPv6地址分配数量为115*/32,其中分配地址数量最多的是美国,24*/32。

8月CERNIC共批复IPv4地址申请5个,分配IPv4地址124C;EDU.CN域名注册4个。

IPV4	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
US	13	28	15	15	16	44	21	84	75	39	24	196					
UK	10	5	69	15	7	3	6	4	31	9	3	8					
JP	1	1	11	3	5	3	132	2	3	8	9	5					
NL	2	3	8	4	5	8	7	2	3	4	4	4					
DE	5	7	3	4	5	26	14	2	13	4	0	4					
FR	7	5	8	2	8	8	5	5	7	12	8	5					
BR	5	5	5	5	2	1	9	8	8	6	6	2					
RU	2	2	4	1	2	1	67	1	2	5	1	9					
CN	5	1	8	8	8	1	18	18	268	2	5	9					
IN	8	2	8	1	0	207	2	8	1	1	1	8					

图1 各国家/地区 IPv6 地址分配

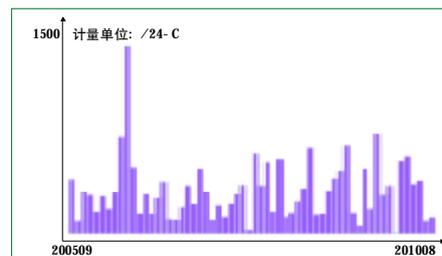


图2 CERNIC IPv4 地址分配

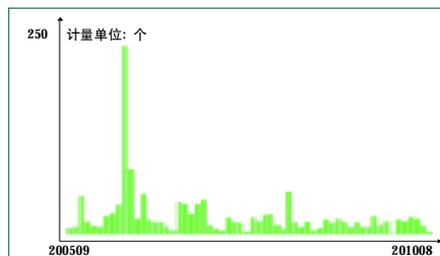


图3 CERNIC EDU.CN 域名注册

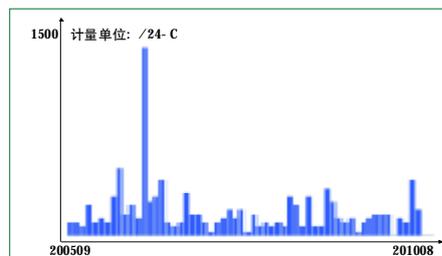


图4 CERNIC IPv6 地址分配

(本文作者系 CERNET 国家网络中心 CERNIC 负责人)



NOC2010 年 8 月

主干网进入暑假低谷

文 / 李鹏飞

八月份 CERNET 网络运行情况正常。由于 8 月还处于暑假期间,因此主干网及各地区流量仍然保持在较低的状态。8 月的最后一周,由于各地假期已陆续结束,主干网流量有上涨的趋势,这个趋势会在 9 月更加明显。8 月下旬国内互联和国际互联的入流量超过了出流量。

图 1, 2 表示了 2010 年 8 月 CERNET 全网运行情况。

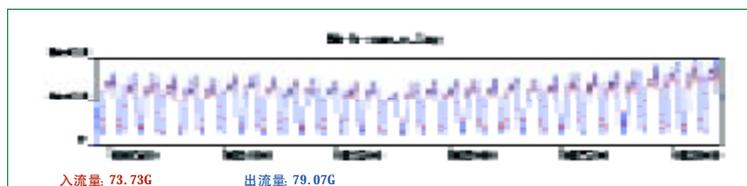


图1 8月CERNET流入/流出的主干流量

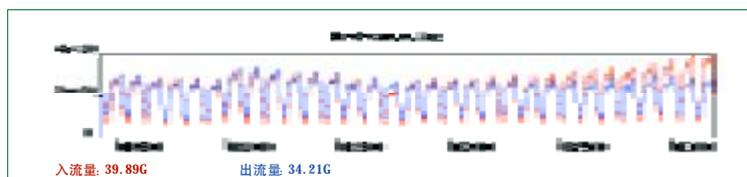


图2 8月国内互联流入/流出流量



开学季：安全投诉事件增多

■文 / 郑先伟

9月份,教育网网络运行平稳,无重大安全事件发生。

开学后,在线用户数量增加导致安全投诉事件的数量也有所增多。

病毒与木马

9月没有新增影响特别严重的木马病毒。微软在近期披露了一个关于Windows中第三方程序不安全加载DLL库文件的漏洞,导致利用此漏洞的木马数量有所增多。该漏洞实际上很早之前就开始被部分木马程序利用,但是由于漏洞的细节没被披露,所以利用的规模还不是很大,经本次公开披露后,利用的范围将有所增大。目前已知的很多常用的第三方软件都存在这个漏洞,木马可以通过将包含木马功能的DLL文件混在各类图片、音乐、文档等文件中引诱用户下载并打开,当用户点击打开这些图片、音乐或是文档时就可能相关的第三方程序调用该DLL文件,从而达到控制用户系统的目的。



2010年7月~2010年8月教育网安全投诉事件统计

近期新增严重漏洞评述

微软于8月23日发布了Windows下第三方软件使用不安全方式加载DLL文件的安全通报(2269637),通报中指出由于一些第三方的软件在编程中没有严格的指定自

身所加载的DLL文件的路径,导致程序运行时可能从当前运行目录调用DLL文件,这就使得攻击者可以在当前执行目录中放置与程序默认调用的DLL文件同名的具有木马功能的DLL文件来利用此漏洞(漏洞的具体原理请参见本期网管技巧中“Windows中不安全的DLL加载方式可能导致任意代码执行漏洞的原理分析”一文)。目前受此漏洞影响的第三方软件数量较多,微软给出了临时的解决办法,不过临时办法可能导致一些第三方软件无法正常运行。由于该漏洞并非是由Windows系统本身引起,所以微软在9月份例行发布的9个安全公告中并未包含此漏洞的补丁程序,这9个例行发布的安全公告中有4个属于严重级别,涉及的系统包括Windows系统、office软件、IIS软件等。用户应该尽快下载相应的补丁程序安装。除微软外一些第三方软件也发布了相应的安全公告,用户应该根据自己的使用情况,尽快升级相应的第三方软件,它们包括:

Realplay最新版本修补多处漏洞 http://service.real.com/realplayer/security/08262010_player/en/

Firefox发布3.6.10版,修补多个安全漏洞 <http://www.mozillaonline.com/>

MySQL 5.1.49更新修复多个拒绝服务漏洞

<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html>

以下是近期需要我们用户特别关注的漏洞:

Adobe Acrobat/Reader字体解析远程代码执行漏洞A

影响系统:

Adobe Systems Incorporated Reader 9.3.4

Adobe Systems Incorporated Acrobat Professional 9.3.4

漏洞信息:

Adobe Reader/Acrobat是我们常用的处理PDF文件的应用程序。Adobe Reader/Acrobat程序允许利用Cool Type.dll库文件调用外部字体,Adobe Reader的Cool Type.dll库在解析字体文件时存在栈溢出漏洞,攻击者构建一个包含畸形TTF字体的PDF文件引诱用户打开,可导致程序的内存被破坏,成功利用此漏洞可以以当前用户权限执行任意指令。

漏洞危害:

该漏洞的攻击代码已被在网络上公布,这个漏洞可以通过PDF文档进行利用,由于PDF文档可在浏览器中直接调用,因此该漏洞也可通过网页进行利用。这个漏洞目前正在利用来进行网页挂马攻击。

值得提醒注意的是类似的漏洞在之前的版本中出现过,Adobe Reader/Acrobat从9.3.3升级到9.3.4就是为了修补一个类似的漏洞,不过从目前的状况看,漏洞并没有被很好地修补。

解决办法:

目前厂商还未针对该漏洞发布补丁程序,建议随时关注厂商的动态:

<http://www.adobe.com/>

在没有补丁之前,建议用户谨慎打开来历不明的pdf文章。

打印后台程序服务中可能允许远程执行代码漏洞(MS10-061)

涉及系统:

Windows xp

Windows 2003

Windows vista



6NOC2010 年 8 月

CNGI - CERNET2 主干网入 / 出流量回落

■文 / 王继龙

CNGI - CERNET2 主干网路由无变化, 运行稳定。

CNGI - CERNET2 主干网入 / 出流量较 7 月有所下降, 其中入流量环比下降 21%, 同比增长 1.63 倍; 均值为 10915Mbps; 出流量环比下降 20.4%, 同比增长 1.68 倍, 均值为 10965Mbps。

8 月 CNGI - CERNET2 出口流量较 7 月有所下降, 入流量月峰值为 1.984Gbps; 出流量每日峰值略高于入流量, 月峰值为 2.014Gbps。

从 8 月的入流量分布图来看, 北邮节点仍居首位, 占到总入流量的 22%, 平均值为 2982.1Mbps, 其次是合肥、北大节点, 各占 9%, 第三位是北京节点, 占到总入流量的 7%。

8 月出流量分布图与 7 月基本一致, 北邮节点出流量比例略大于其它节点, 北邮节点出流量平均值为 1753.4Mbps, 占到总出流量的 16%; 北大节点平均值为 1161Mbps, 占到总出流量的 11%; 合肥节点平均值为 1075Mbps, 各占到总出流量的 10%; 排在前五位的节点还有西安节点第四; 北京节点第五, 它们占到总出流量的 52%。

(本文作者系 CERNET2 NOC 负责人)

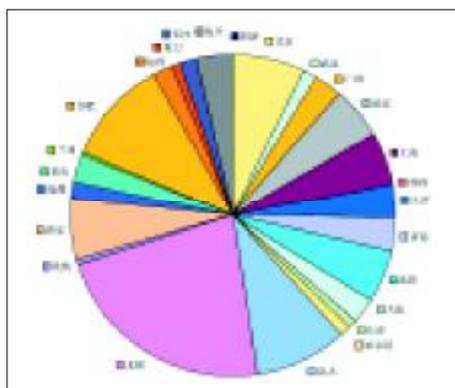


图1 主干网入流量分布

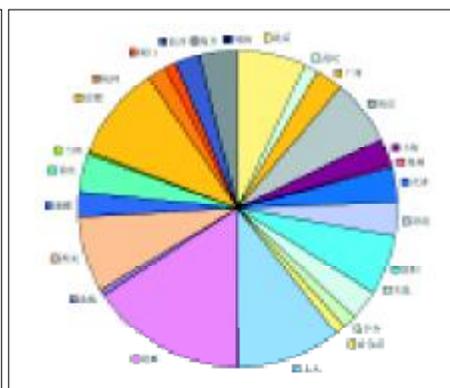


图2 主干网出流量分布

(数据来源: CERNET2 网络管理系统)

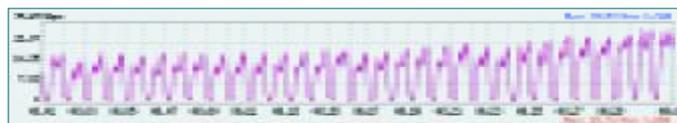


图3 主干网入 / 出流量汇总

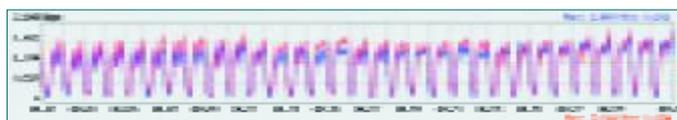


图4 CNGI - CERNET2出口流量汇总

Windows 2008

Windows 7

漏洞信息:

Windows 打印后台程序服务中存在远程执行代码漏洞, 可能允许未经身份验证的远程攻击者在受影响的 Windows XP 系统上执行任意代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。

攻击者可随后安装程序; 查看、更改或删除数据; 或者创建新帐户。除 Windows XP 外, 其他的 Windows 系统中, 这个漏洞可能引起权限提升。

漏洞危害:

该漏洞的利用条件是通过 Windows xp

共享打印机, 因此主要影响那些在局域网内利用 Windows 系统共享打印机的办公用户。这个漏洞可以直接通过网络利用, 微软提示目前网络上已经检测到利用该漏洞的攻击, 不过国内还没检测到明显的利用迹象。

解决办法:

厂商已经针对该漏洞发布了相应的安全公告和补丁程序, 建议用户及时下载安装相应的补丁程序:

<http://www.microsoft.com/china/technet/security/bulletin/ms10-061.mspx>

(作者单位为中国教育和科研计算机网应急响应组)

安全提示

针对近期的安全风险, 建议用户采取以下措施:

1. 及时更新系统补丁程序;
2. 安装正版的防病毒软件并及时升级病毒库;
3. 不要打开来历不明的 PDF 文件, (如邮件附件或是网页链接中的 PDF 文件);
4. 从网络上下载文件 (图片、文档、视频等) 压缩包解压后不要立即点击相应的文件, 应该查看同目录下是否有 dll 文件, 如果发现 dll 文件请不要点击任何文件, 直接关闭该目录, 并用防病毒软件扫描相应的文件夹目录。

中南大学 下一代校园网升级步步为营

文 / 刘海韬 黄家林 黄烟波

2008年8月,国家正式启动了CNGI二期的工程(下面简称CNGI2),随着作为《教育科研基础设施IPv6技术升级和应用示范项目》子项目之一的《中南大学校园网IPv6技术升级》项目的启动,中南大学的下一代校园网建设进入了一个崭新的阶段。

CNGI二期建设前校园网状况

中南大学校园网从1995年开始建设,经过十多年的建设与发展,校园网的规模与网络应用已达到较高水平。学校已建成连接分布在长沙市区的5个校区和3个附属医院的跨域域的千兆光纤网,校园网络以光纤、双绞线、无线等方式基本覆盖学校全部园区,信息资源得到了充分共享。校园网已成为学校的重要基础设施,信息资源丰富,网络应用齐全,为教学科研、学科建设、人才培养、管理后勤提供全面的服务。行政业务管理系统、教学科研支撑系统、网络教学系统、数字图书馆系统、“一卡通”系统等都已开发应用,提高了管理效率和教学科研水平。

校园网现有光纤线路1,200公里芯,IPv4用户数3万,IPv6用户数2000,网络覆盖信息点数4万,其中双栈信息点数1.5万。校园网IPv4出口总带宽1,700Mbps(其中到CERNET的出口带宽1000Mbps,到公众网的出口带宽700Mbps)。校内信息交换流量达到9,000Gbytes/日,校外信息交换流量达到10,000Gbytes/日。

校园网采用以环状主干网为核心向边缘星形扩展的拓扑结构,网络分为核心层、汇

聚层、接入层三层,校园网主干采用千兆光纤成网状拓扑,组网方案为IPv4采用L3控制到汇聚的方式。由于支持的设备较少,IPv6网络则采用简单的单层型结构进行扩展。

核心层设备共4台,其中1台Cisco 7609路由器、2台Cisco 6509路由交换机、1台BigIron8000路由交换机。汇聚层设备共9台,其中5台华为S3552G交换机、1台Cisco6509路由交换机,1台Cisco4006交换机、2台华为6506交换机。接入层设备共550台。无纯IPv6子网,IPv6覆盖率20%,建设有可访问的IPv6信息资源4个,分别是DNS、WEB、VIDEO、FTP服务。校园网主干拓扑结构如图1所示。

校园网以独立光纤(1Gbps)接入CERNET长沙节点,驻地网以独立光纤(1Gbps)接入CNGI-CERNET2长沙核心节点。

校园网主干网上IPv4路由协议采用OSPFv2,IPv6路由协议采用静态路由协议。在网络支撑技术系统建设上,配置了IPv4网管系统及IPv6网络管理系统、计费系统、集中身份认证系统(CAMS)、网络安全管理及日志系统、网络设备监控系统等。

IPv6升级建设方案

校园网整体以双栈方式实现IPv6技术升级,以IPv4方式接入CERNET,同时以纯IPv6方式接入CNGI-CERNET2。对于个别不能以双栈方式覆盖的区域,采用ISATAP隧道方式进行接入,待条件成熟后,再以双栈方式接入。同时建设一个小规模纯IPv6网络供科研和IPv6重大应用测试使用。

校园网原有的千兆核心设备全部

改为IPv4/IPv6双栈万兆核心路由交换机,包括3台H3C S9508和1台RG 8610。原有的核心设备Cisco7609由于支持双栈,并且配置有双FW模块,则作为升级后的出口路由器使用,Cisco7609和互联的H3C 9508之间以4个千兆端口组成port group连接,连接带宽达到4000M。以前的Cisco6509等设备则作为二层汇聚设备继续使用。各校区汇聚设备主要更换为H3C5500EI和H3C5500-28F等支持双栈的具有高速转发能力的3层交换机,这些设备具有丰富的千兆接口,并可以根据需要扩展到万兆。这次升级对不具有千兆上行端口的接入交换机全部进行了更换,累计更换接入交换机300余台。学校的校园网建于90年代中期,当时主要采用小对数多模光纤,远远不能满足目前网络高带宽的应用要求。为了提高整个网络的可靠性,学校进行了大部分楼宇的光缆改造和部分楼宇的综合布线改造,对不满足要求的楼宇的光缆重新铺设大对数单模光缆。

1. 校园网拓扑方案设计

中南大学下一代校园网是一个跨域域的包含6个校区网络及3个附属医院的较大规模的校园网络,各校区之间以光纤互联。考虑到冗余性、可靠性、稳定性及易扩展

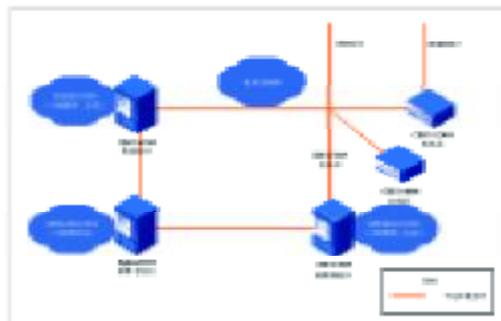


图1 CNGI二期建设前校园网主干拓扑图

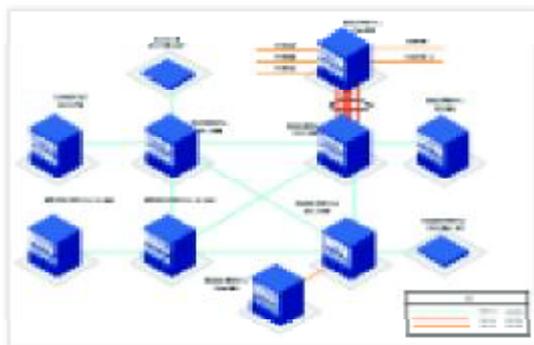


图2 CNGI升级后校园网主干拓扑简图

性，各主要校区之间的主干网设计为全连接网状拓扑结构；考虑到校园网未来的高带宽、高性能应用，校区之间以万兆或双万兆互联；考虑到校区内部分楼栋的高清晰大容量视频传输的需要，为各校区共配备万兆汇聚交换机30台。各校区内以星形拓扑进行拓展，根据通信量的大小选用不同档次的接入交换机，有需求有条件的楼栋，可以在汇聚层甚至接入层采用双归设计或双链路均衡设计以获得高可靠的网络服务。网络基本覆盖全部校园近200栋楼栋。拓扑结构简图如图2所示。

2. 地址规划方案

中南大学目前获得的IPv4地址有3段，分别为202.197.32.0~202.197.95.255, 218.196.64.0~218.196.127.255, 122.207.122.0~122.207.127.255，共计192个C类地址。校园网已经覆盖的楼栋数为142栋。IPv4地址的规划方案原则上以C类地址为基本粒度向各楼栋进行分配，部分楼栋因信息点多，规划了2个或多个C类地址，部分信息点较少的楼栋则根据就近原则被规划到同一个C类地址内。对于有数据隔离和保密要求的应用系统，还为之规划了跨越校区的应用系统VLAN，并分配私有的地址段。

IPv6的地址规划时考虑三大类地址：

第一，公共服务器地址，如DNS，WWW，Mail等；

网络设备互联地址和网络设备的LOOPBACK地址。根据IETF IPv6工作组的建议IPv6网络设备互联地址采用/64的地址块。IPv6网络设备的LOOPBACK地址采用/

128的地址。

第二，用户终端的业务地址；

第三，由于目前网络设备的IPv6 MIB信息的获取和OSPFv3中ROUTER ID等均要求为IPv4地址，所以即使是一个纯IPv6网络也必须要求每个网络设备拥有IPv4地址。

分配给学校的IPv6地址为：

2001:250:4400::0/48和2001:DA8:

D000::/48，共2段48位前缀的地址

段。部分区域的IPv6地址规划情况如表1所示。

3. 路由设计

中南大学校园网是一个跨城域的包含5个校区网络的较大规模的校园网络。校区之间的主干网为网状拓扑结构，校区内以星形拓扑进行拓展。基于此，我们选择的路由方案为：

(1) 校园网主干运行OSPF协议，针对IPv4，IPv6分别运行OSPFv2、OSPFv3，提高了网络路由的冗余度和通信的可靠性。

(2) 各校区网络内汇聚层和接入层配置静态路由协议，使校区内网络路由简单，运行稳定。

4. 主干接入

(1) 校园网以纯IPv6静态路由的方式接入CNGI-CERNET2主干网。

(2) 接入的核心节点为长沙核心节点，该节点拥有1台Juniper T640路由器、1台华为NE80路由器和1台Bitway12008路由器，具有较丰富的接入端口资源及带宽资源。

(3) 校园网核心与长沙核心节点之间距离近，接入线路可以按需供应。

(4) IPv4网络保持现有的千兆接入方式不变。

5. 应用系统建设与迁移

当下一代校园网建设达到一定程度的时候，面向下一代互联网的应用系统和资源建设就变得更为重要。因此学校也将加大应用系统和网络资源的建设力度。目前采用两种方式进行系统建设和迁移。对于支持双栈工作的系统，以双栈方式进行

系统部署；对于不能支持IPv6协议的系统，以反向代理的方式让应用系统也能面向IPv6网络进行服务。已完成的系统包括DNS系统，WEB系统、WEB邮件系统、网络管理系统、文件传输系统、视频服务系统、数字图书馆、招生服务系统、远程教育系统、教学管理系统、就业指导系统等。

另外学校还建立了一个IPv6主题网站，用于IPv6知识普及、用户培养和网络推广。

6. 纯IPv6网络建设

在现有的设备条件下，通过建立跨越整个校园网的二层VLAN，在此基础上连接接入交换机的纯IPv6节点而形成逻辑上独立的纯IPv6网络。该方式可根据需要增加网络规模和覆盖区域，利于纯IPv6网络的扩展。另外，学校的“下一代互联网技术研究中心”实验室通过OSPF v3将其大量的纯IPv6节点接入到现网中，进行基于纯IPv6网络的科研和实验。

升级实施五步走

下一代校园网整体建设工作非常繁杂，涉及到了几乎所有的网络通信设备、用户和部分光纤线路。为了让升级过程平滑过渡，对用户影响最小，我们制定了先核心再边缘、先主干后分支、先IPv4后IPv6、按校区分步实施、按时保质的总体原则。

第一步，将各校区内的核心路由由交换机用新的万兆路由由交换机替换，运行ospfv2

表1 IPv6地址规划表

序号	地址/前缀	用途
1	2001:250:4400::/52	网络中心内部使用
2	2001:250:4400:10::/60	校园网主干
3	2001:250:4400:20::/60	核心服务器群
4	2001:250:4400:30::/60	互联
5	2001:250:4400:40::/60	网络管理
6	2001:250:4400:50::/60	实验地址
7	2001:250:4400:1000::/52	纯IPv6网络
8	2001:250:4400:2000::/52	应用系统
10	2001:250:4400:2000::/64	应用系统1
11	2001:250:4400:3000::/52	校本部
13	2001:250:4400:3000::/56	教学区
14	2001:250:4400:4000::/52	宿舍区

协议。新核心设备先以千兆互联,全部更换完毕后再调整到万兆互联。

第二步,分校区将所有楼宇的汇聚设备逐一更换并连接至新核心,为使影响最小,校区内新核心设备与老的核心设备之间以Vlan Trunk的方式连接,便于将下行的线路转移到新的核心设备上。楼栋内的汇聚设备的更换也按照同样的方法进行,这样对单个Vlan用户的影响时间控制在数分钟以内。当所有的汇聚设备更换完毕之后,就自然形成了新的网络核心,原有的核心设备就可以下线或者降级使用。

第三步,分校区逐台更换接入交换机。

第四步,待v4全部切换完毕,运行稳定后,全网部署OSPFv3,实现用户的双栈接入。

第五步,将家属区等未由学校运维的网络以隧道方式接入到IPv6网络。

现代化机房已竣工

为了更好地满足学校发展的需要,借助中南大学新校区建设的契机,学校在新校区规划建设了新的网络中心机房,主机房面积约1000平方米,UPS、电池及配电室约220平方米。机房按照《GB-T 2887-2000 电子计算机场地通用规范》等国家标准和规范进行设计和施工。建设内容包括了供电系统、空调新风系统、防雷接地系统、综合布线系统、机房监控及门禁系统。

主机房内按照功能进行分区,共分为6大功能区,每功能区设置独立交换柜和电源回路。机房总体供电容量为1000kw,采

用双回路供电,并设计有移动发电机接口。机房设备采用双路UPS供电,UPS容量为200KVA×2。机房采用精密空调进行环境湿度控制,以静压下送风上回风方式工作。新风系统在保证室内空气洁净、维持室内空气的健康品质的同时可以维持机房的正压。机房综合布线系统以桥架系统为依托,采用上走线方式。机房监控系统实现了对机房供电系统、空调新风系统、机房环境湿度温度的检测及控制,同时实现了入侵报警、水浸报警、视频监控、门禁控制等功能。

主机房已于2009年10月竣工,机房搬迁也于2009年11月完成。近一年的运行表明,一个恒温、恒湿、可监控、无人值守的现代化电子信息系统机房能够很好地满足学校信息化工作发展的需要。

后续工作环环相扣

随着下一代校园网的深入建设,校园网用户的双栈接入已变得极为容易,目前的关键问题是如何管理和利用IPv6网络。由于时间上的原因,针对下一代互联网的安全技术和措施的研究还不够深入,安全产品也没有普及;从用户的角度来说,尽管很方便地接入到了下一代互联网,但是对下一代互联网的认识还比较肤浅。考虑到这些因素,我们将从以下几个方面开展工作。

1. 大力开展针对下一代互联网本身及基于下一代互联网的应用的研究工作。进一步加强IPv6安全防御体系的研究,为

IPv6网络的安全可靠运行提供保证。主要集中在两方面的研究:一方面是出口的安全,另一方面是接入安全。

2. 加强用户的培养工作。通过培养让用户对下一代互联网有正确的认识,即下一代互联网并不是现有互联网的补充,而必然是未来所依赖的必将完全替代现有网络的互联网。

3. 进一步加强和加快应用系统的迁移工作,使更多种类的应用系统为IPv6网络提供服务;已经迁移的系统,要改造得更好。要实现IPv6网络的优先访问。

4. 配合项目总体规划,部署IPv6应用示范项目并试用。

5. 加强基于下一代互联网的物联网的研究。要加快下一代互联网的发展步伐,研究并实施基于下一代互联网的关键应用是一个重要推力。从IPv6协议的特性和物联网的需求来看,下一代互联网将不可替代地为物联网提供基础网络。

随着国家2008年下一代互联网业务商用及设备产业化专项教育科研基础设施IPv6技术升级和应用示范项目的开展,我国的下一代互联网建设迎来了新的建设阶段。目前学校承担的CNGI2项目已基本完成,但相关的支撑系统的建设和广泛的应用系统的迁移才刚刚开始。同时,如何建设一个安全的下一代互联网是一个全新的课题。要想将下一代互联网发展成为目前IPv4网络的规模,还有比较长的一段路要走。但我们相信,未来是属于IPv6的。

(作者单位为中南大学网络中心)



卡片1

分配给我校的IPv6地址为: 2001:250:4400::0/48和2001:DA8:D000::/48,共2段48位前缀的地址段。

卡片2

校园网主干运行OSPF协议,各校区网络内汇聚层和接入层配置静态路由协议。

卡片3

中南大学下一代校园网是一个跨城域的包含6个校区网络及3个附属医院的较大规模的校园网络,各校区之间以光纤互联。

卡片4

接入的核心节点为长沙核心节点,该节点拥有1台Juniper T640路由器、1台华为NE80路由器和1台Bitway12008路由器,具有较丰富的接入端口资源及带宽资源。

采用 FIT AP 技术 北京交通大学无线网顺势而为

全校的无线热点数量达到 600 多个，形成覆盖 2 个校区教学区的，室内室外互补的校园无线网。

文 / 王宇杰 杨志军

校园无线网的规划建设

北京交通大学校园无线网络自 2002 年开始，历经 8 年的规划建设，经过 3 期的建设，优化，目前拥有 4 台控制器，600 个无线覆盖热点，已全面覆盖主校区教学区的所有教学楼及室外区域，并对东校区部分区域选择性覆盖，同时对学苑宿舍区的研究生报到区域加以覆盖。

学校最早的无线网应用始于 2002 年末，最初的应用局限于桥接。对于一些不方便有线接入的单位，我们选择合适的地点，通过无线 AP 做无线的桥接接入。当时采用的设备是 802.11b 标准的，速度是 11Mbps，设备价格比较贵。当时使用的设备是台湾的 Macromate 公司的无线 AP，同时使用外接的全向天线提高桥接的效果。利用这种技术，通过在 8 教学楼 7 层最西侧的北侧的房间放置 AP，将当时在家属区服务楼附近的校工会接入校园网（当时家属区没有网络，全校只有一部分教学楼接入校园网）。通过采用这种技术，网络中心的技术人员初步熟悉了无线应用和施工技术。

2004 年，利用和 Intel 合作建设无线校园计划的机会，学校正式进行了无线网的一期建设。当时采取 Fat AP 覆盖的技术，支持 802.11g 54M 标准，通过布放 20 多个胖 AP，建成了覆盖思源楼主会议室，思源西楼主要教室，图书馆主要自习室，天佑会堂，科学会堂和中心报告厅等主要室内区

域以及南门小树林室外区域的一期无线网，为每年的迎新工作和日常的会议通信服务，同时培养了一大批在思源西楼及图书馆等公共自习教室使用无线网的学生用户。

2006 年，借和中国银行合作建网的机会，学校投资兴建了 2 期校园无线网。这次建设前，网络中心测试了多家公司的设备，包括 Aruba，3Com，Trapeze，Cisco，最后 3Com 中标。此次建设采用了最新的 FIT AP 技术，通过 3 台控制器和近 300 个 AP 的布放，覆盖了学校教学区的绝大部分室内部分和室外公共区域。

2009 年，学校借和中国电信合作建网的机会，开始兴建 3 期无线网。3 期无线网采用 H3C 的 FIT AP 技术。经过 3 年的技术发展，目前的 FIT AP 技术无论在信号的强度方面还是系统的稳定性方面都有长足的进步。目前为止通过 2 次的施工，已经增加了近 300 个 AP 对逸夫楼和机械楼，电气楼，5 教，7 教，17 教，7/8/9 公寓和招分处等区域进行覆盖，同时对 2 期无线网中存在问题的部分区域如思源、思源西、思源东 3 个楼 100 多个 AP 进行替换。截止 2010 年 5 月份，仅三期建设的无线热点数量就已经达到 400 个。最近 3 期无线的第三次工程将开始，这次工程主要对二期的剩余部分设备予以升级以解决稳定性问题，同时对二

期覆盖不足的楼宇如东校区的教学区部分进行强化，3 期第三次工程结束后，全校的无线热点数量将达到 600 多个，形成覆盖 2 个校区教学区的，室内室外互补的校园无线网。

目前北京交通大学校园无线网络的逻辑拓扑见图 1：

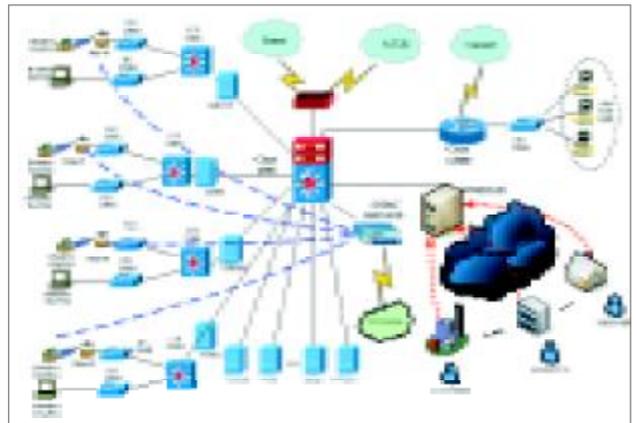


图1 北京交通大学校园无线网络逻辑拓扑

具体覆盖区域

室内部分：逸夫楼、机械楼、主校区体育馆、计算中心、思源楼、思源东楼、思源西楼、7 号教学楼、8 号教学楼、9 号教学楼、电气楼、综合实验楼、外事处办公楼、学科装备处办公楼、远程学院办公楼、科学会堂、图书馆、天佑会堂、中心报告厅

室外部分：主校区体育场、思源楼南北两侧、思源东楼南北两侧、计算中心楼南、东花园、主席像、小树林、天佑会堂南北两侧；

新采用的技术细节

目前采用瘦AP技术，所有覆盖热点零配置，统一由一台设备进行管理；同时支持IPv4和IPv6双栈技术。目前学校的无线改造没有完全完成，尚处于H3C和3com两套系统并行运行的阶段，但两套系统都使用FIT AP技术。下面为新的H3C的技术细节：

北京交通大学网络为三层结构(核心+汇聚)；汇聚层到核心层是三层路由；AC直接连接至核心层；各楼的POE直接接至汇聚。具体的设备型号是：AC为H3C WX6103，旁路在主核心H3C 7502E和Cisco6500上，采用二层方式，网关设置在7502E和6500上；FIT AP为，通过H3C POE交换机连接每个楼的汇聚交换机，FIT AP的管理地址由学校统一规划，地址池都在学校的DHCP服务器上，汇聚交换机上配置该楼AP的网关，采用DHCP Relay方式从DHCP服务器上拿地址分配给每个AP；每个POE交换机都配置有管理地址和登陆账号，方便管理维护；校内的内网无线用户，SSID为web1.wlan.bjtu，采用https方式认证，IP地址也是由学校DHCP服务器分配；

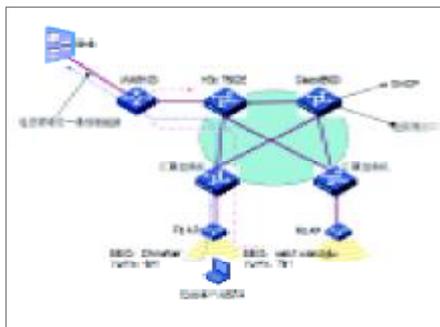


图2 北京交通大学Wi-Fi室内覆盖项目实施方案

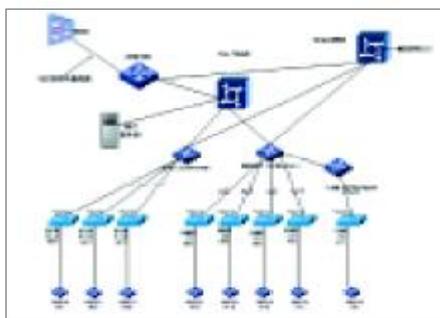


图3 北京交通大学Wi-Fi室内覆盖工程网络拓扑

另外增加一个SSID: ChinaNet, 供公众用户上电信3G网使用，IP地址及认证由AC上联的BAS设备统一处理，不加密；AC仅执行二层转发。

运行与维护

校园无线网的运行维护由学校信息中心负责。信息中心配备专人进行无线网设备运行状况的监控；目前学校的无线改造没有完全完成，尚处于H3C和3com两套系统并行运行的阶段，因此要同时监控2套系统：

H3C无线设备监控使用其网管平台IMC的无线管理组件，如图4。当AP出现故障时，监控图相应节点会变为红色。

H3C 6103自带的Web管理界面的页面如图5所示。

3Com无线设备使用其网管平台3WXM管理，监控界面如图6。

如何使用无线网

目前由校园无线网络统一提供的合法

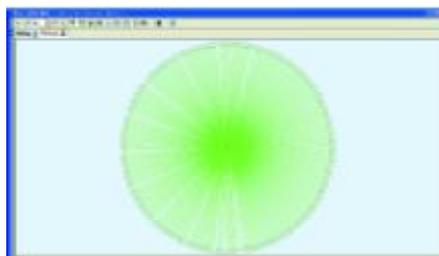


图4 当AP出现故障时，监控图相应节点会变为红色



图5 H3C 6103自带的Web管理界面的页面



图6 3Com无线设备使用其网管平台3WXM管理



图7 认证界面

接入SSID为web.wlan.bjtu和web1.wlan.bjtu，其他的SSID均不是校园无线网提供的；

用户需要通过Web方式认证才可以连接上校园无线网络，认证的用户名和密码为用户在北京交通大学校园网络计费系统上的有效账号和密码。

用户凭有效证件到信息中心服务台交开户费，开通上网账号。可使用校园内任意一台一卡通自助终端给上网账号里充值。开通上网账号后，将机器的IP地址配置为动态获得，然后扫描无线网，若扫到前面所述的两个SSID中任何一个，连接该接入点，用户就可以动态获得合法IP。此时用户在本机浏览器地址栏中敲入任何网址，将会自动拦截弹出无线网络接入认证界面，用开通的合法账号认证过后，用户就可以访问校内外资源。

用户通过校园无线网访问校园网内资源都是免费的，访问校外网站，资费同有线网络，按下行流量计费。

下一步建设计划

北京交通大学校园无线网下一步建设中，首先会考虑利用瘦AP技术可以广播多个ssid的优势，广播一个ssid ipv6.wlan.bjtu，通过这个ssid接入的用户将接入纯IPv6网络而不是接入双栈网络。这样可以建立一个跨越全校的纯IPv6的无线试验网，为CNGI的建设提供科研和试验环境。

另外，随着802.11n技术的迅猛发展，规划在条件成熟时建立802.11n的室内和室外实验点，为高速无线网络的研究提供环境。

(作者单位为北京交通大学信息中心)

杀毒软件江湖： 排斥与兼容的战争（上）



需要指出的是，绝大多数情况下，反病毒产品之间的兼容性冲突问题，都是技术与协调的问题，有其工作机理上的必然性，并往往具有一定的不可避免性。

■文 / 肖新光

反病毒产品兼容冲突问题

反病毒产品从最开始的行命令扫描工具发展至今，已经形成了带有文件、注册表、内存等多种本地监控机制；浏览器、邮件客户端等多种保护环节；以及整合了主机防火墙、入侵检测机制、主动防御机制的综合型产品。而其核心价值早在上世纪末，就已经从最开始的静态的文件扫描检测，变成实时化的主机防护。而实时化的防护推动了反病毒产品使用更多的服务、驱动等底层技术，运行于更接近系统内核的位置，这也为反病毒产品产生相互兼容性问题打下了伏笔。

随着操作系统的复杂化，威胁的不断离散化等影响，反病毒的监控保护点也日趋复杂，又加之反病毒厂商数量也在增加，而操作系统厂商并没提供比较标准的技术

规范，因此反病毒产品因互不兼容，发生共存冲突等问题越来越多，并间接影响了用户对反病毒产品的信任。

目前已经发现并被报道过的兼容性冲突问题包括：

造成系统崩溃和其他严重故障：从2000年以来，根据公开报道，已经出现多起因反病毒产品之间相互冲突，而导致系统蓝屏、死锁等事件。

资源占用：反病毒扫描、监控和其他防护机制，都会带来系统资源的占用。如病毒库的内存展开对内存的资源使用，文件监控、定时扫描可能导致更多的I/O开销、以及各种保护机制对CPU时间片的占用等等。这些对用户操作有一定影响，如系统延迟、文件复制操作时间变长等等。而由于消息传递等机制，有可能在多种反病毒产品共存时，其对资源和时间的影响不是简单的线性叠加，而是出现明显的性能恶化。

失效：由于监控机制之间的冲突，多种监控机制共存时，有可能造成其中之一失效，或者部分机制双双失效的风险。上述后果，可以在兼容性测试中被复现。

相互误报：由于厂商之间互信互通机制尚不够通畅，以及少数恶意的“误报构造”攻击的存在，厂商之间出现相互误报的情况，也时常发现。由于被报警为病毒而严重地影响了用户对产品的信心，因此，各厂商对被误报的问题也均比较敏感。

但需要指出的是，绝大多数情况下，反病毒产品之间的兼容性冲突问题，都是技术与协调的问题，有其工作机理上的必然性，并往往具有一定的不可避免性。相关问题多数并不是由商业竞争引发的，商业竞争也不是反病毒产品兼容冲突问题的本质。本文主要介绍当前反病毒产品冲突的主因，以澄清公众误解。

下文中涉及到安天实验室和兄弟厂商产品所使用的技术点，均用于说明反病毒

产品之间兼容性冲突的必然性，不是对实现水平进行评价。

主要冲突点详细解析

实时监控、主动防御等技术的发展是一柄双刃剑，一方面随着监控点的增加能应对新的安全威胁，另一方面也使反病毒产品的稳定性遇到挑战，测试难度普遍加大。反病毒产品自身的稳定性压力都在呈现几何级数增长，相互之间的兼容则变得更加困难。以下从文件监控、防火墙、浏览器防护、主动防御四个主要技术点，描述导致反病毒产品自身的稳定性下降、与操作系统之间和相互之间出现严重冲突问题的成因。

文件监控的潜在兼容性问题

文件监控是反病毒厂商普遍采用的技术手段，其主要机理是对文件的创建、读取、关闭等行为进行监控触发对文件病毒检测，以阻断病毒的执行和部分相关行为。

文件监控的实现方式主要有以下两大类：

1. API 挂钩。

根据钩挂 API 的层次不同我们又可以分为：

(a) Ring3 文件监控。

多采用 inline hook 的方式修改文件操作相关函数的前几个字节，跳转到自己的函数，然后对将要操作的文件和缓冲区进行检测。

由于实现跳转的方式有多种，所以不同软件的实现策略有所不同，很难保证多个软件共存时前一软件修改后不影响到后一个软件，而且很可能导致相关进程崩溃。

由于此类技术也多被恶意软件使用，一些安全软件不会在执行完自己的代码后执行修改前的自己，而是采用从原始文件中读取、分析、执行的方式，导致多个安全软件同时监控一个 API 时，只有一个生效。

出于性能考虑，不传递给原 API 处理而采用自己实现的代码完成该 API 的相应功能，那么也不会将相关信息传递给其他软件。

部分软件在执行完自己的函数后会把

修改后的字节还原，然后调用原系统 API 完成功能后再次修改、挂钩。两个使用此实现的软件同时工作则可能造成互相调用导致死锁，程序没有响应。

(b) Ring0 文件监控。与 ring3 的情况类似，但是后果更加严重。

由于 inline hook 不同实现造成的不兼容性很可能导致系统 API 无法正常工作，导致系统蓝屏。

例如：安天客户端产品 (Antiy Ghostbusters 4.0) 早期版本采用大量 inline hook，后因与其他产品严重冲突放弃；360 安全卫士中 inline hook 有几种不同实现方式共存的现象，并且与 360 安全浏览器有重合的监控点；

挂钩之间相互调用，会导致死锁，系统死机；

采用替换 SSDT 的方式，则只有自己的挂钩有效，其他软件的挂钩均无效。

例如：360 安全卫士等产品采用替换 SSDT 的方式，与其共存的安全软件通过标准方法获取的 SSDT 是无效的，导致其他安全软件功能出现缺失；

Vista 以后微软对内核进行保护，部分对内核函数的修改会导致系统蓝屏。

例如：多个产品在内测和对外版本都出现过对关键内核函数

进行修改，但是并没有仔细判断版本，导致兼容性出现问题而使系统蓝屏。

2. 文件过滤驱动

FileSystemFilterDrivers

FileSystemMiniFilterDrivers

过滤驱动的本质依然是挂钩，但微软为了方便厂商调用，对其进行了封装，属于官方的技术。此类技术本身已经力求稳定与兼容，多数都提供了一定的兼容性保障。微软自己的安全产品在驱动层面也多使用类似的方式。

但是在安全产品的实际应用中，多层监控逐层传递会造成效率的降低，一些厂商在实现时会绕过后续的过滤驱动，直接将

IRP 请求发给下一层驱动完成相关的功能，如表 1 和表 2。

防火墙的潜在兼容性问题

目前反病毒产品普遍使用单机防火墙技术来过滤出入数据，应对来自网络的威胁。

目前防火墙的实现方式包括：

T D I
N D I S
IP Filter
Windows Filtering Platform
Winsock Kernel

在以 Windows XP 为主的时期，多数防火墙选择前三者中的某一种或者某两种相结合的方式。在实际应用的过程中，同样存在多个共存无法同时生效的现象。其原因有：

1. 过滤时出于效率考虑，直接将允许通过的包交给下层驱动处理，而不是后续的防火墙驱动。

2. 由于 ND IS 和 IP Filter 比 TDI 更接近底层，前两者实现的防火墙会对 TDI 层造成影响。

3. XP 自带的 IP Filter 存在谁先设置谁先生效的问题。安天盾防火墙与金山防火墙某版本同时使用该方式，如果同时安装在用户的机器中，则出现谁先启动谁先生效的现象。

表 1

处置方式	交给后续过滤函数继续过滤	直接交给下层函数处理	拒绝访问
兼容问题现象	扫描次数多、系统变卡、变慢	后续过滤不生效，实际上只有一个安全软件在保护主机。	后续过滤不生效，只有一个安全软件报告病毒。

表 2

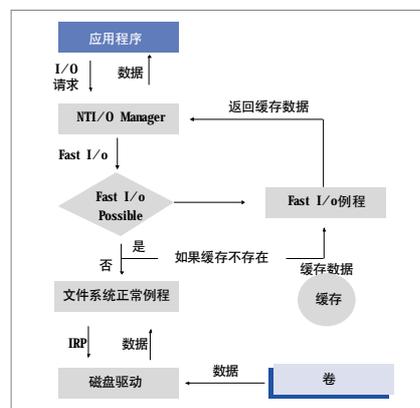


表3 主流安全防护软件监控点

进程名	金山网盾	360网盾	网马	作用
BinC	BinC/Navigate	BinC/Navigate	BinC/Navigate	拦截恶意URL
wsoc32	new	new	new	禁止网络
Win2_32	new	new	new	禁止网络
Wininet	WaaSend	send	send	拦截请求URL
	InternetOpenUrl			
	InternetQueryDataAvailable			
	InternetConnect		InternetConnect	拦截请求URL
	InternetOpenUrl		InternetOpenUrl	拦截请求URL
	InternetReadFile			拦截请求URL
	InternetQueryDataAvailable			拦截请求URL
	HttpOpenRequest		HttpOpenRequest	拦截请求URL
Vbscript.dll /script.dll	compile	ParseScriptText		对恶意脚本的拦截
Kernel32	CreateProcess(Internal)	CreateProcess(Internal)	CreateProcess(Internal)	文件格式输出检测
	CopyFile	CopyFile(Ex)MoveFile	CreateFile/Write/Read	
	LoadLibrary	LoadLibrary(Fa)	VirtualProtect	防止内存修改输出
	WinExec			
	NtCreateProcess(Ex)?			
NtLdr	ZwCreateProcess(Ex)			
oleaut32	SysAllocStringByteLen			
	CoRegisterClassObject			
	CoCreateInstance	CoCreateInstance	CoCreateInstance	阻止网络
	CoGetClassObject	CoGetClassObject	CoGetClassObject	阻止网络
Urlmon	UrlDownloadToFile	UrlDownloadToFile	UrlDownloadToFile	阻止网络
	UrlDownloadToFileCacheFile	UrlDownloadToFileCacheFile	UrlDownloadToFileCacheFile	
Advapi32	RegQueryValueEx			
Shell32		ShellExecuteExW	ShellExecute	
cmdcmd32		ShellExecuteExW	ShellExecuteEx	
WinTrust			WinVerifyTrust(Ex)	数字签名分析
浏览器行为分析	进程创建	进程创建	进程创建	数字签名分析
	模块加载	模块加载	模块加载	
	网络通信(嗅探)			
	文件下载	文件下载	文件下载	
	文件拷贝	文件拷贝	文件拷贝	
其他	内存溢出+保护	ActiveX对象创建	ActiveX对象创建	禁止网络
		内存溢出+保护	内存溢出+保护	禁止网络
		OnDocumentComplete	OnDocumentComplete	阻断

WFP和Winsock Kernel 是自Vista之后引入的方式，兼容性相对而言更好，只要实现得当，一般没有兼容性的问题。特别是WFP针对防火墙和IDS类软件做了设计上的考虑，兼容性问题得到了较好的解决。这也说明，操作系统提供相对规范的接口是解决安全产品冲突的较好方式。

浏览器防护的潜在兼容性问题

浏览器防护多使用ring3 API HOOK。下面结合网页防护类的主流产品分析其潜在的兼容性问题。

使用ring3 api hook实现的浏览器保护，不可避免的要遇到和文件监控一样的问题。在实际对抗中，网马不断发展升级，已经开始将浏览器中的ring3 hook摘除，为了对抗此类威胁，主流软件多会采取不断检测自己的hook是否存在，发现不存在则重新将函数挂钩。造成多款软件争抢一个API的现象，导致浏览器无响应或者响应缓慢。特别是与CreateProcess相关的。

在浏览器防护软件进行行为分析的时候，由于其他浏览器防护软件的参与会对浏览器的行为造成一定影响，这些影响可能是对堆栈的影响（由于多了一层Hook，实

际调用的堆栈可能会增加一层）。以某浏览器防护软件为例，其堆栈检测只会向上追溯5层，如果同时共存3个软件，那么其想要检测的那层调用，则会由原来的第5层变为第7层，原来的检测方式就失效了。

例如：360和金山网盾共存时，网马在创建进程时360进行检测。如果放行则会通过360的函数调用系统API，进而再次调用金山的进程创建检测，此时金山追溯堆栈会发现是360的模块调用，而不是JS脚本解释引擎调用，予以放行。

即使不考虑对堆栈的影响，由于不同浏览器防护软件都进行了拦截，对浏览器的行为也就产生了影响，造成相互的行为分析干扰，无法正确分析恶意行为，进而出现漏报或者误报的现象。

例如：金山网盾在脚本解释层根据特征检出了恶意脚本，构筑在其上层的其他防护的行为分析就无法发现该恶意脚本的行为。

再例如：360网盾会不断检测监控点是否存在，而检测的机制是基于二进制比较的，如果发现其他软件进行了HOOK，则用自己的进行替换，导致其他软件失效。

(本文作者系武汉大学客座教授)

云南大学实现高端路由器中兴通讯M6000规模商用

本刊讯 2010年的企业网市场可以说是中兴通讯数据产品高端年，一批大型行业承载网络项目接踵而至。云南大学新校区校园网项目实现了中兴通讯高端路由器M6000在企业网市场的规模商用，同时也是以BRAS设备为主导的新型校园扁平化解决方案的首次完整应用。

此外，国家税务总局过渡机房改造项目、包西铁路数据项目等多个行业承载网建设项目采用了中兴通讯高中低端路由交换产品，实现了2010年中兴通讯数据产品在企业网市场的全面突破。

OVUM最新统计数据显示，在大多数设备厂商出现不同程度市场份额下滑的情况下，中兴通讯以太网交换机产品依旧保持高速增长态势，排名跃居全球第3位。2010年是中兴通讯数据产品在企业网市场实现跨越性突破的一年，截止目前已经不少国家级项目和企业网重要市场都有所斩获，为后续企业网市场开拓打下坚实的基础。

来自中国电信节能减排技术应用蓝皮书的数据，芯片级每降低1W的功耗，由此而带来的功耗降低将会达到2.68~2.84W。中兴通讯易维系列交换机、M6000、T8000路由器等产品采用最先进的芯片生产工艺，主控芯片功耗降低20%。

中兴通讯及时响应市场需求，打造出满足当前和未来业务需求的ZXR10 T8000电信级路由器。中兴通讯拥有T8000完全的知识产权，最大支持16+64机架集群，具备最大集群200T的交换能力，线卡机框可提供每槽位100G的线速接口容量，并可平滑升级至400G。聚焦Internet核心节点、骨干网超级节点和大型城域网出口节点等需求，致力于构建扁平化网络，关注统一承载网的长期演进，是运营商和行业客户构筑精品网络的理想选择。



优化带宽之策

基于IPv6网络和无线网络的应用激增,以及结合测试实例证实的网络资源意外消耗所带来的额外损失,这些都给原有校园网络系统带宽添加了新的巨大压力。因此,这些高校有必要采取多种措施来应对。

文 / 邓峰

当前,基于IPv6和无线等网络技术上的应用激增,网络带宽需求出现巨大增长,网络资源相对紧张,给网络管理员带来了挑战和压力。

IPv6+WLAN下的带宽压力

在IPv6网络中,随着NAT门槛的消失,校际间的IPv6网络流量大增,一些IPv6站点,如葡萄站,六维空间站点等以BT方式下载的网站受到不少其他学校同学的欢迎,不少高校也开始开发自己的IPv6资源站点。

随着IPv6进一步地在高校推广,这种压力将会进一步体现出来。目前来看,流量有增长的趋势。2008年间CNGI-CERNET2的流量呈急剧上升的趋势,2009年2月的主干网入出流量均值是2008年1月的三倍强。2009年12月,CNGI-CERNET2主干网入出流量超过10G,2009年12月的主干网入出流量均值是2008年1月的十倍强。

而在无线网络中,由于采用802.11无线协议的WLAN使用了CSMA/CA机制,数据帧间的时间空隙要大于使用CSMA/CD机制的传统以太网。另外,由于采用了无线介质,WLAN的丢包率也要高于传统的以太网。这就造成了其传输效率明显低于以太网,一个无线AP拥有多名用户,相对有线网络更容易出现拥塞现象,无线网络总体



由于采用了无线介质,WLAN的丢包率也要高于传统的以太网。

网络应用增长及IPv6网络和无线网络的发展,带来了网络流量的大发展,也必然带来新的压力和瓶颈。

一方面,网络路由交换等设备的负载及出口带宽都可能会

也将占用大量网络资源。

目前来看,IPv6和IPv4必将有长时间的共存期,两者的分工配合将是主流。IPv4仍主要面向HTML,IPv6主要面向下载资源及未来可预见的物联网应用等。BT下载是当前IPv6技术的一个重要应用。

与此同时,无线网络也在不少高校得到了相当发展。无线网络的关键技术都基本成熟,而近年来802.11n的新技术的突破使得理论上无线网络终端可以承载巨大的吞吐量;无线网络的普及,给学生使用网络带来了很大的方便,而随着信息化的发展和网络应用的剧增,无线的日常需求也在激增。

承受更大的压力。

另一方面,各高校的网络在理论上也许具有较充足的带宽,但在实际应用中,总是有各种额外的消耗,使得最后的资源离理想最大值始终保持很大距离。

笔者曾为上海教科网做过跨区域网络的互联测试,其中有的测试点采用了主干网设备测试,而有的点则用的是下联设备。主干设备均为上海教科网分发的设备,具有相近的性能。结果双方均为主干设备的测试结果基本都能达到100M;而有一方用下联设备进行测试的结果则总有10M左右带宽的损失。表1中,S,J,H分别指代上

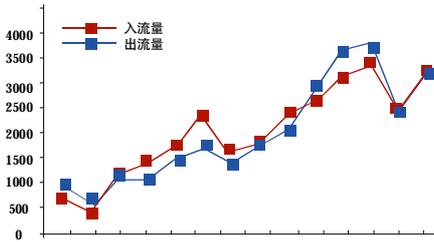


图1 2008年1月至2009年2月 CNGI-CERNET2 主干网入出流量走势图

表1 上海教科网跨区网络测试结果

测试条件	测试点	测试结果
S用边际路由器下联的交换机设备; J用主干网上边际路由设备	S- J	S和J之间为90M双向带宽; 平均延时为1.55毫秒
J用主干网上边际路由设备; H用主干网上边际路由设备	J- H	J到H之间链路带宽100M双向带宽; 平均延时为1.84毫秒
S用边际路由器下联的交换机设备; H用主干网上边际路由设备	S- H	S- H 90M双向带宽; 平均延时为1.49毫秒

海教科网上不同的测试点。该三测试点都具备非常相似的主干网条件,但有一家S是在下联设备中做的测试。

这组测试数据表明,尽管下联设备同主干网络设备一样,完全能支撑远大于100M带宽的能力,但在具体应用中,却带来意想不到的10M带宽损失。依此类推,校园网的带宽常被莫名消耗,计划可能赶不上变化。

因此,结合新增应用和需求来看,带宽资源有日益紧张的趋势,这可能构成一个新的巨大瓶颈,需要我们未雨绸缪地采取一些防范措施和对策。

三大措施应对带宽紧张

针对网络资源的相对紧张,可以有多种应对方法,一般可以采取数个方面的对策。

1. 开源节流的基本思路

校园网络扩容,增加出口带宽是各大高校争取网络资源的基本方法,当前教育网仍是不少高校重要出口,但教育网和公网之间不能完全互联互通也是瓶颈;同时,节制一些特殊的网络流量,则有可能起到四两拨千斤的特殊效果。这里所指的该重点节制的网络流量主要是迅雷的P2P流量。这是因为相当部分流量都来自于P2P的上传和下载,其中最大的又来自迅雷。

对于封迅雷及清理相关P2P流量的方法,可以结合封杀地址,端口,以及结合监控等方式来进行。

上海交大信息网络中心的姜开达等老

师通过对迅雷协议的分析,发现可以控制对 hub4u.sandai.net(教育网解析到58.254.134.201,其他地区可能有所区别)的访问来有效控制迅雷的流量。方法可以是针对这个IP做一条黑洞路由。例如 ip route 58.254.134.201/32 null 0,那么,UDP的流出量过上几小时就会显著下降,但是对TCP的流量没有明显影响。这种方式不会影响迅雷用户的正常使用,但是又可以明显降低这些用户对外上传流出的UDP流量。

2. 放开网络出口,改善网络结构的思路

一些高校的网络已构建多年,主体设备相对陈旧,网络层级划分未必清晰合理。在网络安全、多出口选择等新压力面前,又在总出口添加了防火墙或在出口路由器上进行各种ACL设置等。这样,如果操作不当,总出口及某些重要出口很可能成为问题多发点。

总出口相当于大门,若安装防火墙等设施在总出口,无疑于在总大门就进行了严格的检查。当流量激增时,很难避免总出口的排队拥塞。而如果对这个问题分而治之,将所有流量的检查分别安置在不同出口,将同一个地点同一个时间段发生的问题分别放在不同地方解决,可以缓解矛盾,各个解决。

同样的道理,各种路由规则设置和流量整形设备、负载均衡设备甚至QoS规则等也要慎重使用。虽然负载均衡设备和ACL等规则在流量控制方面表现得比较重要,但一些系统资源将在协调中意外消耗和损失。

尤其是设置在总出口的规则有时一旦出现例外,后果往往可能很严重。因此,在总出口之下采取措施再分而治之采用各种规则和规则,往往兼顾安全和性能。

笔者多次测试防火墙及路由器等设备的数据都表明,网络设备一旦打开多项功能,其测试性能必然下降。总出口如能限制开放过多的功能,对总出口性能及整体性能的提升都有很重要的意义。

在当前流量激增的压力面前,有的高校将总出口的万兆防火墙撤下,而分别在各分出口安置了千兆防火墙;有的高校则将总出口大门洞开,在相对后台的各个路由器或交换机上分别进行规则设置,加强安全防范等。

同时,“网络扁平化”虽然带来了较高的效率,但一旦出现安全等问题,可能仍会给整个网络带来较大的冲击。因此,具备合理规划的“核心、汇聚、接入”层次的网络架构及具备清晰结构的汇聚和接入层,仍是较合理的结构调整方向。

3. 为师生增添自助选择出口的方法及结合其他途径的综合思路

以上技术手段之外,我们还可以给校园师生增加选择余地。譬如,开设代理或VPN等方式可以适当避免或缓解单一出口紧张带来的问题。

此外,因为信息化建设本身并非单纯技术问题,结合学生的主动配合,一些复杂问题就会变得简单,一些难题应该也可能迎刃而解。

(作者单位为复旦大学信息化办公室)

数据中心：工艺与散热的博弈

制程工艺的进步使得服务器变得越来越灵活，只要你愿意，可以在一个机柜里塞多台刀片服务器，但与此同时，你必须面对散热的难题。



■文 / 本刊记者 王左利

维基百科的瘫痪

最近，百科全书网站维基百科瘫痪了两个来小时。全球的人都在猜测，出了什么问题？真实的原因是数据中心。据悉，散热问题导致维基百科两个数据中心中的一个（位于阿姆斯特丹）陷入瘫痪，而不断增加的访问流量最终让另外一个（位于佛罗里达）也陷入瘫痪。

“不过好消息是我们打算在美国再建一个数据中心了，如果你愿意的话，可以捐款为我们的服务器做点贡献。”危机解决后，维基百科的发言人说。

数据中心的散热可能是工程师最为头疼的问题。

随着技术的进步，服务器变得越来越小，直到现在刀片服务器将要垄断整个市场。与其说刀片服务器是服务器历史上革命性的改变，倒不如说，这仅是由于工艺设计的巨大进步。

工业设计的进步使得单位面积的模块上可以集成更多的核，更多的线缆，这使得服务器面积更小，计算速度更快。但与此同时，一个亘古不变的难题摆在了工程师的面前，那就是散热问题。

“现在是个多核的时代，一块板子里能容纳许多芯片，但这并不意味着你可以无限制地容纳，因为散热问题在那摆着呢。”这就好像一个大胖子，必须拥有一个强壮的心脏才能健康地生活。

而刀片式服务器成为主流使得这个问题更加紧迫。据IDC预测，仅在中国，2008~2013年，刀片服务器的采购量年度复合增长率为34.5%，其中值得一提的是，2012年，受服务器更新周期的影响，刀片服务器会达到相对较高的增长率，取代一批机架产品；预计2013年，刀片年出货量将接近25万台，是2008年的6倍。

因此，各公司一方面希望刀片服务器拥有更高的稳定性，更快的运算速度，更好地支持虚拟化技术，另一方面，他们必须分出一大批人来解决散热的问题。

Google的秘密计划

全球谁拥有最多的数据中心？这是一个商业机密。不过许多人认为一定是Google。根据现有信息，如果包括在建的，Google共有36个数据中心，因此也面临着最大的散热挑战。

在人才济济的Google，确实已经在秘密研发新的数据中心技术。这是一项与数据中心的冷却系统有关的技术专利，这种技术可以对服务器进行“精确制冷”，以达到降低能耗的目的。

另一个更令人吃惊的消息是——Google在服务器上早已自力更生，确切地说，他们所拥有的数十万台服务器都是自己设计打造的，Google认为这是

公司的核心技术之一。

参与过许多Google服务器设计的Ben Jai说,Google有自己的服务器计划,并且加入了很多创新的思想。他们每台服务器都内置12伏特电源,确保万一主电源断电时还可持续供电。这已经成为他们的一项专利。

大家不仅对于Google这种内建电池的作法感到新奇,而且,Google对此的保密性也让大家很佩服。据悉,Google从2005年就开始采用这种设计,已经有好几代了,而在2009年才初步透露出口风来。

据介绍,针对数据中心面对的庞大的散热量,Google设计了一种特殊形状的服务器机架冷却用空气管。这种空气管是一种可调节式的管道传输系统,管道将与冷气机的吹风管相连,并将为服务器系统输送散热用的冷风。

此外,Google还可以使用这种新的通风制冷技术在环境温度较低时直接抽取外界的冷空气来对服务器进行冷却,只有在环境温度较高时才需要开启空凋制冷设备。类似的冷却技术通常被称为“免费制冷”技术。

还有一种“精确制冷”技术,不必为整个服务器机房进行冷却,冷气机只通过这些通风管道对服务器的热区进行精确制冷。

值得一提的是,Google为服务器做了可移动的数据中心集装箱,这是他们的另外一项专利。每个集装箱中最多可容纳1160台服务器,耗电量可达250千瓦。

这透露出的一个信息是:对于服务器制冷最急迫的公司并不一定是服务器的生产商,那些拥有庞大数据中心的应用型企业对此也同样急切,包括Google,包括亚马逊,也包括软件大王微软等。不过谁知道Google会不会最终把自己的服务器制冷技术公布于众呢?如果是那样的话,相信很多人会对它的服务器感兴趣。

海量数据的力量

Google是否会进入服务器市场还只是句玩笑话,目前它还处于自给自足丰衣足食的“小农时代”。不过另一个以前与服务器不搭边的企业——思科已迈出了大胆的一步。2009年,思科推出“统一计算系统”(UCS)进入了服务器市场。

实质上,这两家公司对服务器的策略改变与现阶段IT数据中心的快速发展无法分开。Google的服

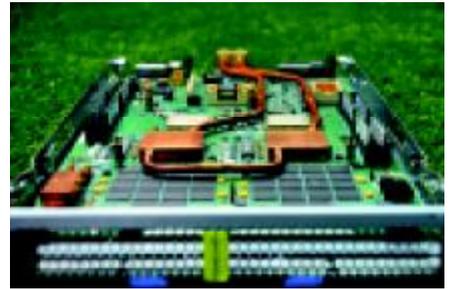
务器战略目前来看,显然是仅仅针对Google内部数据中心,而思科的服务器将面对整个市场。作为数据中心战略中重要的一环,服务器的出现使思科可以拥有全套的数据中心产品,思科还为了这个计划和它素日的合作伙伴HP差点闹翻脸。

尽管他们的战略步伐并不一样,但从前与服务器不沾边的两家公司却不约而同地拥有了自己的服务器战略。这似乎也可以看到一个苗头:随着海量数据的翻涌,数据中心的发展将极大地促进服务器技术新的发展。

那么,可以预见的是,未来几年服务器市场的一切技术改变都将以满足数据中心为核心。

而在节能的同时,有一件事情人们一定不会忽视,那就是服务器的吞吐量,随着对海量数据传输的效率要求,服务器的I/O瓶颈越来越得到新的重视。这将成为推动千兆以太网向万兆以太网过渡的动因。日前在一项针对服务器技术状况做的调研中,有超过10%的人员已经要求他们的服务器主板可以支持万兆以太网网络技术,有58%的受访者表示目前需要千兆以太网支持,将近一半的受访者表示他们正在考虑向万兆以太网过渡。

在刀片服务器之后,在多核之后,在虚拟化之后,在永远无法停止的节能技术之后,服务器的下一个增长点是什么?也许是高吞吐量。■



Google服务器设计

揭秘微软全球最大数据中心:集装箱放置服务器

微软在美国芝加哥新开设了数据中心,这被认为是全球最大的数据中心。这家数据中心的总面积为70万平方英尺(约合6.502万平方米),即使只启用半数服务器,能耗也将达到30兆瓦,是普通数据中心的数倍之多。



从外观上看,微软刚刚在芝加哥落成的大规模数据中心与工业园内的其他建筑类似。

然而,就在这些拖车里面,却存放着微软云计算产品的重要组件。在芝加哥数据中心的每个拖车的集装箱都存放了1800至2500台服务器,每台服务器都可以用来为微软即将发布的云计算操作系统Windows Azure收发电子邮件、管理即时通信或运行应用程序。

微软在楼上布置了4个传统的升降板服务器机房,平均每个机房约1.2万平方英尺(约合1114.8平方米),功率为3兆瓦特。

惠普 VS 戴尔争夺 3PAR 幕后



比起惠普，1984年成立的戴尔还是一个年轻的公司。与惠普相同，戴尔实施的是多元化战略，在IT领域发展的同时，也致力于商业相关，如金融服务的发展。

但其现在并不是资本交易的活跃时期，经济危机的影响还在，这让这笔交易更加特别。宏观方面，根据美国风险投资协会的数据，从2008年到今年6月初，只有44个风险投资支持的公司获得公开上市，这个数据仅是2007年的一半。同时，风险投资的金额较去年同期下降了56%，仅为19亿美元。联合国贸易和发展会议的数据显示，全球直接投资在2007年达到1.9万亿美元后，在2008年下降了14%，这个趋势在2009年更加恶化。《经济学人》做出的预测则表明，2010年全球的并购与2008、2009年相比虽然有所回升，但还是处于低位。

从公司数据来看，2009年，惠普和戴尔的营业额分别下降了3.2%和13%；惠普的净利润减少了6.69亿元；戴尔的净利润减少了10.45亿元。尽管如此，惠普和戴尔两家公司都有大量的现金及其等价物：在2009年10月31日，惠普有133亿美元现金；戴尔2010年1月29日有106亿美元的现金。正是这些现金，支持了并购的发生。惠普和戴尔拥有大量现金的原因是他们减少了短期投资、存货和应收账款管理水平的提高。

虽然惠普和戴尔手中握有巨资，但在自己营业额下滑、整体投资不活跃的情况下，他们选择投资会相当谨慎，那么他们为什么会掀起对3PAR的争夺战呢？

■文 / 本刊特约编辑 胡运霞

9月2日，惠普以每股33美元、总价23.5亿美元的价格正式收购3PAR。这无疑令3PAR股票持有者兴奋的时刻，仅门罗风险投资公司(Menlo Venture)一家就从中获利5.6亿美元；这也是让IT界金融界都兴奋的时刻，惠普六次出价，最终交易价格是戴尔初始出价11亿美元的两倍，让平素不受关注的存储行业屡上头条，也刷新并购交易历史。

首先, 3PAR 是一家存储公司。

3PAR 公司总部位于加利福尼亚州弗莱蒙, 是一家全球领先的公用存储厂商。它的主要产品是 Inserve 存储服务器, 包括 T 型和 F 型。主要客户包括中大型公司、金融服务公司、云计算服务提供商、客户导向的互联网和政府部门, 例如 Carphone Warehouse Group、NYSE Group、Cox Communications、Myspace.com、美国商务部等。中大型的公司主要是 IT 公司, 这些公司朝着共享、虚拟化的基础设施方向发展, 同时正在着手建立虚拟数据中心使基于云计算的内部服务传递成为可能。金融类基金是那些对存储系统设施有很高要求, 有大量交易需要处理的投资银行、证券交易所和对冲基金。云计算服务厂商是 SaaS 和 HaaS 等。总体来说, 3PAR 就是一家存储服务提供商。

在惠普和戴尔争夺 3PAR 战开始前, 3PAR 的市场表现一般。根据雅虎财经的公开信息, 从 2009 年 3 月到 2010 年 3 月, 3PAR 的收入仅增长了 5%; 自 2008 年上市以来, 一直处于亏损状态, 而行业的平均边际利润率为 0.09%, 行业领先者 EMC 公司的边际利润率为 10.6%。但 3PAR 非常重视技术, 研究投入占营业收入的比例一直在 24% 以上, 在 2009 年 3 月到 2010 年 3 月年达到 4,700 万美元。在过去五年, 3PAR 的营业收入平均增长率为 28.98%, 是行业平均水平的两倍。

其次, 存储行业发展和市场前景广阔。

云计算已经不是一个虚幻的爱丽丝梦境, 越来越多的公司的产品在朝云计算发展。思科推出云计算新平台 Quad; 一向对自己技术讳莫如深的微软在开放资源云计算方面也作出努力; 人们已经不满足于虚拟服务器, 推出了包括防火墙、路由、转化器的虚拟程序。存储对云计算至关重要。这些需求推动了存储行业的发展。存储行业过去五年的平均增长率为 14.75%。

此外, 在经济危机的大背景下, 更多的公司感到购买维护存储硬件设备的压力, 这为存储公司的发展提供了契机。在经济危机大爆发的 2009 年, 3PAR 总的营业收入从 2008 年的 1.2 亿美元上升到 1.8 亿, 增长了 57%。

最后也是最重要的, 3PAR 拥有惠普和戴尔需要的存储技术。

存储行业至关重要, 这是惠普和戴尔共同出发点。惠普作为一家历史悠久的多元化公司, 拥有雄厚的技术实力 (拥有 31,000 项专利), 但其近年来销售和技术的发展不尽如人意。在 2008 年 10 月~2009 年 10 月, 其营



在惠普和戴尔争夺 3PAR 战开始前, 3PAR 的市场表现一般。

业额相比上一个营业年度下降了 3%, 从 1184 亿美元下降到 1146 亿美元。惠普在研究上投入资金不断消减, 研究支出占营业额的比重不到 4% (见下表)。实际上, 有传言称, 惠普前任 CEO 赫德之所以离职, 是因为员工支持率过低。员工对赫德不满的原因正是他以放弃长期创新为代价来追求短期利润, 不仅取消了整个设计团队, 还削减了惠普的研发预算。而在公司存储和服务业务分部, 2007 年之后即出现了营业额下降。存储领域是惠普十分看重的领域, 惠普把“节约存储空间”作为其三大发展方向之一。在这种情况下, 通过并购在存储领域技术创新能力强的公司, 抢回因为研究投入

不足而耽误的时间, 尽快在存储业务上获得突破, 驱动惠普 6 次出价收购 3PAR。

比起惠普, 1984 年成立的戴尔还是一个年轻的公司。与惠普相同, 戴尔实施的是多元化战略, 在 IT 领域发展的同时, 也致力于商业相关如金融服务的发展。在 2010 年财政年度 (从 2009 年 1 月 10 日到 2010 年 1 月 10 日), 戴尔加大了存储领域的发展, 扩充了主要产品如 Dell PowerVault, Dell EqualLogic 和 Dell //EMC 的功能。戴尔在 10 年年报中写到, 将朝更多的戴尔品牌或者联合品

表 1 惠普 2007 年至 2009 年经营情况表

年报截止日	2009-10-31	2008-10-31	2007-10-31
营业额 (亿美元)	1145	1184	1043
营业收入增长率	-3.22%	13.50%	-
研究支出 (亿美元)	28.19	35.43	36.11
研究支出占营业额比重	2.46%	2.99%	3.46%
公司存储业务营业额 (亿美元)	153.59	194	166.39
公司存储业务营业收入增长率	-20.83%	16.59%	-

资料来源: 惠普 2009 年年报及其附注

表 2 戴尔 2007 年至 2009 年经营情况表

年报截止日	2010-1-29	2009-1-30	2008-2-1
营业额 (亿美元)	529.02	611.01	611.33
营业收入增长率	-13.42%	-0.05%	-
研究支出 (亿美元)	6.24	6.63	6.10
研究支出占营业额比重	1.18%	1.09%	1.00%
公司存储业务营业额 (亿美元) ¹	21.92	26.67	24.29
公司存储业务营业收入增长率	-17.81%	9.80%	-

表 3 3PAR 公司 2007 年至 2009 年经营情况表

年报截止日	2010-3-31	2009-3-31	2008-3-31
营业额 (亿美元)	1.94	1.84	1.18
营业收入增长率	5.43%	55.93%	-
研究支出 (亿美元)	0.48	0.46	0.34
研究支出占营业额比重	24.54%	25.16%	28.90%

资料来源: <http://finance.yahoo.com>

牌方向发展,这表明戴尔想改变目前代销EMC公司产品地位的愿望。从表中可以看出,戴尔与惠普的情况极为类似,即总的营业额下降,研发投入不足,存储业务发展不畅。戴尔研发投入不足比惠普还严重,研究支出占营业额的比重还不到2%。

相对于惠普和戴尔这样的产业巨头,3PAR非常小,但

其在存储方面的技术和研究实力还有市场前景让惠普和戴尔非常羡慕。3PAR既提供单片存储也提供模块化存储,行业内有这个能力的还有EMC, Hitachi, IBM公司;而惠普、戴尔、甲骨文等公司只能提供模块化存储。3PAR在研究上的投资有丰厚的回报,在美国拥有32项专利。根据2010年3月的数据,在其公司657名全职员工中,有208名是研究人员,占31%。这意味着,一旦惠普戴尔并购了3PAR,那么就拥有了存储行业全方位的技术,同时获得了存储方面的众多专家。3PAR没有实现盈利的主要原因是投入25%的



相对于惠普和戴尔这样的产业巨头,3PAR非常小,但其在存储方面的技术和研究实力还有市场前景让惠普和戴尔非常羡慕。

资金用于研发,2009年56%的增长,五年来平均25%营业额增长,正是惠普和戴尔需要的。

那么这场声势浩大的并购会对存储行业造成翻天覆地的影响吗?最终的赢家是惠普,而存储产品的销售只占惠普销售的0.01%;从2007年到2009年,3PAR公司的存储业务营业额连惠普存储销

售额的2%都不到。从行业竞争对手来看,行业老大EMC公司年营业额是155亿美元,其次是Seagate技术公司,为114亿美元。惠普收购存储公司,对其相关服务和技术发展是一个支撑,但短期内不会是惠普的主营业务。3PAR公司的良好技术与惠普良好的声誉、强大的资金实力、全球销售网络相结合,销售额可能扩大数倍,这会让EMC、Seagate、Hitachi等公司面临更激烈的竞争。但存储行业的格局,进而IT行业格局的变化,最终需要看惠普如何去管理操作3PAR公司。

2009年服务器存储市场并购风云

ORACLE

甲骨文以74亿美元收购Sun

2009年4月20日,美国数据软件巨头甲骨文公司宣布以74亿美元收购太阳微电子公司。当时甲骨文公司表示,这次收购将进一步巩固该公司在数据库市场的地位,并可能改变IT业的现有格局。

最新进展:2010年第二季度是Oracle收购Sun之后第一个完整的季度。Gartner统计数据显示,与去年同期相比,Sun的服务器收入下降了将近11%(10.9%)。除IBM之外(收入下降2.7%),其他竞争对手服务器销量均有所上涨。服务器行业巨头HP的收入上升了26.7%,Dell销量增长迅速,达到了39.5%。虽然Oracle擅长于购买和整合软件公司。但在其涉足Sun的收购之后,即便是其拥护者也表示Oracle对软硬件产业的区别还缺乏了解。

EMC
www.emc.com

EMC以21亿美元重磅出击赢得Data Domain

2009年7月,EMC以21亿美元的出价在与NetApp竞拍Data Domain中胜出。评论称,EMC需努力保持Data Domain的渠道和销售力,尽量加快发展业务。

最新进展:EMC公司继续保持在数据存储业务上的行业领先地位,2009年的营业额达到155亿美元。自正式签署协议以来,EMC在精简其整个产品组合方面做了大量工作,如将Data Domain的重复数据删除技术应用在EMC升级存储系统中、推出全局重复数据删除阵列、利用重复数据删除的数据存储系统提高其软件性能,在7月19日推出一个新的终端重复数据删除存储系统,在产品线性能提高的同时价格保持不变。

vmware

VMware以3.62亿美元收购SpringSource

2009年8月,VMware以3.62亿美元收购SpringSource,打算通过这项收购交易拓宽其虚拟机管理软件套装。VMware的首席执行官Paul Maritz在宣布这项收购交易的投资者关系会议上表示,VMware希望在其产品套装里增加“应用识别”功能。

最新进展:VMware行业领先地位稳定,2009年营业额仅次于赛门铁克。近日VMware公司宣布推出其云计算应用新平台,该平台充分利用了VMware并购来的部分资源并将Spring Java开发框架与VMware的最新vFabric应用服务进行了有效整合。随着VMware云计算应用新平台的推出,程序员将能够以一种熟悉的方式开发出更多的新应用程序。而与此同时,也使程序员对这些程序的运行环境有所选择。

南京大学 IPv6 “大提速”

南京大学是一所历史悠久、声誉卓著的百年名校。作为教育部直属的重点综合性大学，南京大学在教学、科研、国际交流合作、社会服务等各个领域都保持良好的发展态势，各项办学指标和综合实力均位居全国高校前列。

项目背景

为了发现和解决 IPv6 网络正式商用可能出现的各种问题，各学校网络中心的首要任务就是将原来在 IPv4 网络上运行的相应服务移植到 IPv6 网络上。

项目建设内容包括：

(1) 对 100 所学校的校园网实现下一代互联网技术升级改造，升级改造后的用户总数达到 100 万人以上；

(2) 研究完善面向校园网的试商用网络支撑技术和公共服务功能，为下一代互联网运营提供业务运营和网络管理平台；

(3) 实现 10 项现有教育科研资源和应用的技术升级改造，新开发和推广 10 项教育科研重大应用示范；

(4) 逐步扩充连接国际下一代互联网的线路带宽，增强国际出入口网络管理能力。

应用需求分析

南京大学现运行的 IPv4 资源情况如下：

(1) Web 应用：为学校各个院系提供 Web 应用服务，通过 Web 平台及时地发布各种信息，方便用户浏览各种网页信息，及时获得相应资源。

(2) 资源应用：包括 FTP 之类的资源共享类的下载应用，提供一个文件共享平台。

(3) E-Mail 应用：对内提供教工、学生之间的邮件沟通平台，对外提供一个统一学校形象的 E-Mail 后缀地址名称，方便与外部用户沟通。

(4) 流量控制应用：统计流量信息，控制某些大流量的连接（比如 BT，P2P 等），保证其他用户使用网络的合法权益。

(5) 认证计费应用：合法用户拥有相关帐号来使用网络资源，非授权用户则无法登陆到网络中，也方便统计用户上网时长等信息，合理收取相应网络运行费用。

此次南京大学 IPv6 升级项目，通过将原有服务的升级整合到 IPv6 网络，其目的不仅能够为用户提供更加充足的 IP 地址，还能优化和提升现有 IPv4 网络的相关服务。因此，南京大学 IPv6 项目对承担基础硬件平台的服务器提出了严苛的要求：不仅需要具备超强的性能，而且必须具备极高的稳定性和可靠性，需要服务器平台能够担负 7 × 24 小时不间断的服务。

方案设计

针对下一代互联网络 IPv6 平台的建设，联想推荐南京大学使用四路 R630 G7 服务器和双路 R525 服务器两款高品质的服务器作为基础应用平台，并设计方案如图 1。

相对 IPv4 网络，IPv6 网络的特点就是对用户提供稳定、可靠的服务。选择品质好、性能优的服务器来搭建基础平台对于 IPv6 网络至关重要。联想推荐的 R630 G7 服务器是 2008 年北京奥运会数据库服务器专

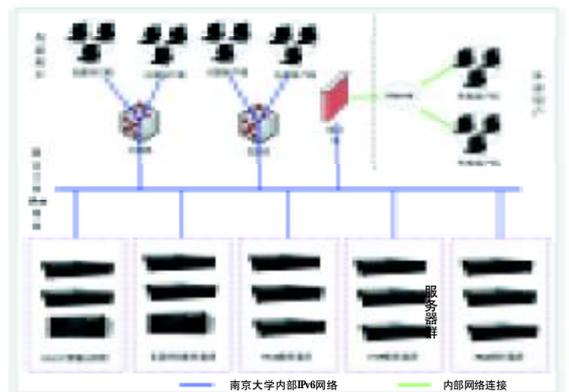


图 1 方案拓扑

用机，在整个奥运期间以零故障的表现支持北京奥运会。整机采用全冗余设计保证了整个服务器的最大化运行时间，包括电源、风扇、内存、硬盘等关键部件均提供相应的保护机制，在出现单部件损坏的情况下，均可以实现在线维护，保证了对外服务的不中断。

同样，联想 R525 服务器也是一款专为互联网中后端应用和大中型企业数据库应用设计的新一代高密度机架服务器精品，适合于对 I/O 性能、扩展能力、可用性要求高的应用环境。

用户收益

联想南京大学 IPv6 改造升级项目的顺利实施，有效地帮助用户搭建起了高效、稳定、安全的应用服务平台。随着南京大学校园网核心层骨干设备的升级、各种安全监控技术的建立与完善，一个安全、快速、稳定的校园网络环境和信息系统已逐步构建，并将为校内外 IPv6 用户提供更优质的互联网服务。■

西安理工大学: “五位一体”提升软实力

文 / 李瑞

十年建设校园网络管理日趋复杂

西安理工大学的校园信息化起步较早,早在1998年便开始建设校园网,至今已经走过十多个年头。“学校的信息化就是要提升学校的核心竞争力,提升学校的教学、科研和管理水平,高效稳定的网络环境是学校信息化的坚实基础!”网络信息管理中心李军怀主任如是说。

在这种理念的指导下,西安理工大学十多年来,不断升级、改造校园网,只为给学校师生提供更好的网络体验。经过多次改造后,现在学校各个区域的网络设备品牌五花八门、型号多种多样,这给整个网络的管理工作带来了巨大的挑战,管理员不得不熟悉各个厂商的命令体系和系统特点。由于每个厂家设备的管理方式都不相同,所以经常发生混淆的情况。各个厂家的协议兼容性有限,在一起工作经常会发生莫名其妙的未知问题。另外,很多型号设备都已停产,甚至有些厂家已经退出中国市场或被并购,售后服务无法得到有效的支撑和保障。

面向未来构建数字化整体校园

随着校园信息化的逐年深入,学校的各个业务系统逐步实现信息化,网络用户规模逐年增长,网络管理的难度越来越大。层出不穷的多媒体应用等问题时刻挑战着校园网的稳定和安全。十多年前规划、设计和建设的校园网络已经不能满足校园信息

化现有应用的需求,校园网变成了整个“数字校园”发展的瓶颈。

面对日渐复杂的网络管理和越来越急迫的业务需求,学校决定要重新规划、设计和建设校园网以适应新时代的发展。通过对网络环境的综合分析,网络的可靠、稳定和可扩展成为了此次校园网改造的重点。

校园网作为学校基础业务的保障,对可靠性有近乎苛刻的要求。网络采用全冗余骨干结构,确保全网无单点故障;利用万兆链路技术确保核心应用数据转发无拥塞、无延时;部署高性能出口引擎设备确保(PBR)策略路由和NAT(网络地址转换)的效率;通过高性能流控设备确保学校核心业务数据的服务质量得到保障。

在保证拓扑结构稳定的同时,还要保障网络设备和环境的稳定,随着各种网络攻击和病毒的泛滥,网络环境的稳定也直接影响着各项基本业务的稳定。把安全做到网络最边缘,从接入交换机的端口开始保证整个网络的安全。CPS技术绑定用户源IP地址、MAC地址和端口,使用户发出的每个报文都是真实可信的,从根本上杜绝了包括ARP欺骗病毒在内的所有源地址欺

骗类病毒和攻击。

面向未来,所有网络设备支持IPv6协议确保平滑升级到下一代互联网,现阶段校园网可运行双栈协议并接入CNGI-CERNET2,而且支持纯IPv6部署,在不久的将来全面进入下一代互联网协议的应用,将教学、科研和管理等数字化应用过渡到IPv6上来,在西部高校中起到示范性作用。

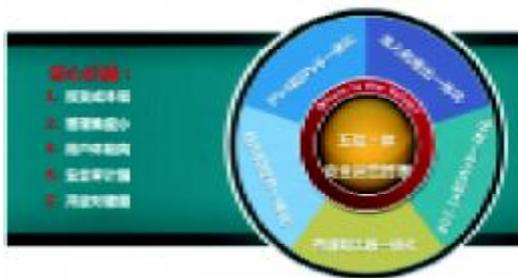
知行统一实施一体化管理

在校园网管理方面,此次设计的原则和目标是“知行统一”:通过智能感知技术对网络内部运行的数据实时统计分析,看到以前看不到的事情,分析清楚以前分析不清的事件,进而实现精细化、统一的管理。

1. 校园网一体化安全运营管理

校园网已经遍及全校的各个角落,随时随地为师生提供信息服务。如何能够为用户提供统一的操作界面、认证账号和服务密码等用户接口呢?如何处理准入和准出认证、802.1x和Web认证、校内和校外认证、有线和无线认证还有IPv4和IPv6认证呢?

统一的RG-SAM3系统提供的规范网络认证体系是一个不错的解决办法。RG-SAM3采用RADIUS协议与各个NAS(网络接入服务器)之间通讯,同时可以支持LDAP与各种目录服务器对接,实现数字校园统一身份的未来扩展。同时,它在网络层面统一了各种登录认证方式和账





号密码,实现了准入和准出认证的一体化;802.1x和Web认证的一体化;校内和校外认证的一体化;有线和无线认证的一体化;IPv4和IPv6认证的一体化,并能实现五个方面的整合。

准入和准出的一体化实现了校园内网的安全准入和运营保障的准出控制。学校采用实名注册的方式进一步强化网络安全审计,通过包月限流量的方式控制出口带宽的利用率,避免校园网有限的出口带宽拥塞。同时一体化的流控设备能保障了关键用户和关键应用的带宽,确保各类型用户都能得到良好的上网体验。

基于RG-S2600系列交换机的Web准入认证功能,能为全校教职工提供基于网页方式认证的服务,这种方式不需要安装客户端,避免了IEEE802.1x客户端程序的兼容性风险和安装使用问题的出现。同时Web准入认证提供了用户在通过认证后自动在交换机上绑定用户的IP+MAC+端口信息,做源地址报文检查,从而有效防范欺骗类攻击或病毒的出现。

RG-WALL V1600系列的VPN网关,能给全校用户提供在校外的校内资源访问服务。师生可通过校园网账号以SSL或IPsec的方式回拨到VPN网关上,访问经过授权的系统资源和科研数据库信息。

RG-WS和RG-AP220系列产品能实现有线和无线网络的有机融合,学生在有线网络上面采用包月限流量的计费策略,在无线网络上面可以沿用有线网络的计费策略,也可以根据特定区域的要求采用单独

计时长(1元/小时)的计费策略,二者使用同一套账号信息。

目前, RG-SAM3已经完全支持了纯IPv6和双栈状态下的网络认证,在严格、兼容、宽松等各种模式下均可满足过渡时所需要的认证需求。

2. 网络与应用的一体化管理

传统的网络管理只能管理网络设备,解决网络层面的故障和问题。但是网络信息管理中心作为学校整个信息化基础设施,它的管理者还负责很多业务应用以及它所依赖的计算、存储和环境等IT基础设施,这些设施和网络设备一起为数字校园的各种应用服务。因此,需要从业务应用的角度来看整个IT基础资源的健康程度和繁忙程度。这样,一套具有跨平台监控和管理能力的系统能满足管理所需,它能够以业务应用为视图来监控它所依赖IT基础资源。

RG-R11L对各种IT基础资源进行统一的抽象和提取,将各个运行指标和参数进行统一的监控和管理,向上提供基于SOA架构的开放管理服务,向下提供跨厂商的多协议管理能力。平台可以支持包括应用程序、操作系统、数据库、中间件、服务器、存储、交换机、安全设备等多平台的监控管理能力。

RG-R11L-BMC将一个业务所依赖的所有IT基础资源统一监控起来,把他们的各种运行状态指标进行综合加权而形成一个个业务卡片,分别用该卡片的繁忙度和健康度两个指标来衡量这个业务当前的工作状态,并综合评定该业务所依赖资源当前的工作状态。

整个监控页面一目了然,每个卡片的齿轮转速能够直接衡量它所关联的每个IT资源的繁忙程度,柱形图标则时刻反映每个IT资源的健康程度。当某一关键资源出现性能或功能的故障时,该业务卡片会直

接反映出问题的所在,并立刻定位导致该问题的是哪个IT资源出了什么样的问题。管理员可以直接定位问题的根本,无需漫长而又复杂的排查与检索故障的过程。在用户打电话报修故障之前就迅速定位并排除故障,先用户一步解决系统问题,提高用户满意度。

同时,该平台能客观准确地运行数据,并记录所有IT资源的运行数据,为整个IT流程的规划、整合、优化提供科学的判断依据,更为提高IT资源的利用率与效率提供客观的运行数据支撑。

育人为本助力学校发展

在部署了五位一体解决方案后,学校的信息化建设蓬勃开展起来,各部门的工作效率有了显著提高,网络管理成本大幅降低,工作人员能把有限的精力投入到更有价值的工作中。面对改造后的佳况,西安理工大学网络信息中心相关人员不禁感叹:“锐捷网络的五位一体解决方案着实让人兴奋,它使我们的经济的投资获得超额回报,管理效率大幅提升,我们不再为突如其来的问题而慌张;它是一个负责任的工作伙伴,我们的管理员很乐意和它一起工作,学校师生们的网络体验有了全新的开始。”

目前,西安理工大学的教务管理系统、学分制系统、精品课程系统、校院两级科研管理系统、数字化图书馆、办公自动化、实验室管理系统、财务管理系统、资产管理系统等十余个业务系和数十个业务部门的门户网站在可靠、稳定的网络中畅快运行,给学校师生带来全新的网络体验。同时,学校门户网站、电子邮件、文件传输等基础应用服务在网络中有了更为可靠的硬件依托,学校与外界的交流畅通无阻。各种各样的信息化应用手段在学校的教学、科研、管理活动等各个领域发挥着前所未有的积极影响,西安理工大学在奔向数字化校园的道路上急速前行。

广西师范大学： SSL VPN 承载和谐的数图中心

深信服SSL VPN是基于浏览器内置SSL协议建立的VPN接入方式，不需要用户安装任何客户端软件，免除了用户配置维护的麻烦，从而保证众多用户简单方便地使用SSL VPN网络。

文 / 申兴

广西师范大学近几年购置了大量的电子数据供广大师生开展教学研究。这些资源对于学校学科建设和科学研究工作有着很重要的意义，数字图书馆的建设和应用已经成为学校信息化建设和现代教育技术改革工作的一大重点。

然而，在建立和使用数字图书馆的过程中，电子资源商出于版权保护的需求，对其提供给高校的电子资源采取了一些保护措施，以防对数字产品非授权使用。高校图书馆所购买的电子资源多被限制了访问的IP地址范围，从而导致了电子资源仅能在校园网范围内访问。一旦离开校园，老师或学生将无法访问这些电子资源，而随着高校后勤社会化的深入发展，越来越多的教师和学生在校外居住，他们对各类电子资源的访问需求仍然是存在的，同时还有大量的校友、客座教授、外聘教师也需要随时随地地接入校园网共享丰富的校园网资源。因此，高校需要一套可管理、可认证、安全的远程访问电子图书馆的解决方案，将校园网当作校外用户的中转站，使校外用户通过相应的身份认证进入校园网后再通过校园网访问相应的电子资源数据库，从而满足更多师生访问馆藏资源、网上资源的需求。

由于电子资源的网外访问具有应用复杂（Web应用、C/S应用）、安全性要求高

（重要的科研教学数据）、访问量大（用户量大、流量大）、用户环境复杂（终端类型多、网络环境复杂、用户IT水平参差不齐）等特点，在选择相应技术和产品时应充分考虑所选择产品具有的易用性、扩展性、容量等多方面内容。

通过考察各高校数字图书馆目前普遍存在的问题，广西师范大学提出解决其在以下几个方面问题的需求：

网外用户访问校内图书馆资源的问题

图书馆的电子资源访问都是通过校园IP地址判断的，所以从校园网外接入的用户必须能够被分配校园网内指定IP地址。

移动用户接入安全问题

无论是学校电子资源的版权还是校园网内的科研教学数据都是无价的，远程访问资源的安全性必须得到很高的保证。其中，尤以用户的身份认证为关键，否则未授权访问将造成很严重的后果。

公网访问资源速度慢的问题

由于多数校外访问者使用的是当地运营商提供的网络（如电信/网通的ADSL），这些运营商网络与教育网之间的访问速度非常慢，该速度瓶颈必须解决。

大量用户访问问题

由于高校的资源多数都是购买授权的方式，上游的电子资源服务商除了限制发起的IP地址外，还会限制单一IP地址所产生的流量。另外校外大量用户的访问对系统的可靠性也提出较高要求。

根据以上需求，深信服科技为广西师范大学提供了完善的SSL VPN解决方案，得到了一致认可，最终成功中标广西师范大学SSL VPN远程访问系统。

深信服SSL VPN是基于浏览器内置SSL协议建立的VPN接入方式，不需要用户安装任何客户端软件，免除了用户配置维护的麻烦，从而保证众多用户简单方便的使用该SSLVPN网络。

在整套方案中，为需要进行远程接入访问的教师、学生开启SSL VPN登录帐号，并为其分配相应的教学资源访问权限，通过SSL VPN保证科研教学数据的安全授权、传输、访问。并采用SSL VPN用户流量控制，对每个用户的上下行流量做合理的限制，防止某一用户大流量长连接的过量占用资源。为了解决校外用户分配校内网地址问题，通过在SSL VPN设备中开启虚拟IP池，分配校内网一空IP段，并将该IP段地址与接入用户的帐号进行绑定。

广西师范大学是广西壮族自治区重点大学，是广西具有博士授权的三所高校之一。拥有1个博士后科研流动站、3个二级学科博士学位授权点、5个一级学科硕士学位授权点、88个二级学科硕士学位授权点、5个专业硕士学位授权点和49个全日制普通本科专业。学校各项事业蓬勃发展，取得了良好的社会声誉。建校78年来，学校为国家尤其是广西培养了近20万名教师和其他专业人才。

确保下一代互联网平滑过渡

文 / 祁玲

伴随着 CNGI - CERNET2 的蓬勃发展, 中国各高等院校正在积极主动地迎接 IPv6 的到来。在 IPv4 向 IPv6 的过渡阶段, 如何利用现有设备, 最大限度地节约投资? 又该采用何种策略, 更好地保证下一代互联网在应用上的平滑过渡?

目前的 Internet 以 IPv4 为主导, 不可能一次性将网络的所有设备升级为 IPv6, 必须分步骤分阶段地进行部署。为此, IPv6 商用需要提供多种过渡技术和解决方案, 保证与 IPv4 的互联互通。

从 2006 年起, 赛尔网络与清华大学等科研机构合作, 研发了一系列与 IPv6 建设相关的产品和解决方案, 力求支持各高校由 IPv4 向 IPv6 平滑过渡。

部分高校, 原有的 IPv4 网络建设完善、网络资源丰富, 鉴于预算、技术等方面的原因希望在进行 IPv6 部署时能够充分保护原有的设备投资。

面对这种情况, 学校可以在原有网络中采用隧道技术作为补充, 将纯 IPv6 终端接入 IPv6 广域网络, 原有网络拓扑和路由几乎无需调整, 只需要增加隧道终结的设备就能够使客户端访问广域的 IPv6 资源。

实践证明, 采用 ISATAP 自动隧道是理想的部署 (见图 1), 如果网络中有较

多的 IPv6 用户需要接入, 可以增加隧道终结路由器的数量, 以保证 IPv6 报文的转发能力。

还有一部分高校出于对未来发展的整体考虑, 更愿意直接建设一个全新的 IPv6 网络。这时, 可以使用双栈设备进行组网接入 IPv6 (见图 2), 组网按核心、汇聚、接入三层结构进行设计, 利用汇聚层及核心层网络进行高速转发。其中新建的核心层和汇聚层设备中全部设置了 IPv4 和 IPv6 两套协议栈, 针对的对象是通信端节点 (包括主机和路由器)。

这种方式对 IPv4 和 IPv6 提供了完整的兼容。使用 NAT-PT 进行协议转换, 根据协议不同对分组做相应的语义翻译, 从而使纯 IPv4 和 IPv6 站点之间能够透明通信。NAT-PT 技术可以较好地解决 IPv4 和 IPv6 的互通问题, 使得大部分应用层协议不需要修改就能够实现互通。

在 IPv6/IPv4 的网络中, 不仅要考虑针对 IPv4 的接入层、汇聚层的安全防御, 同样也要考虑在设备升级为双栈设备后, 针

对 IPv6 协议簇的攻击带来的安全问题。

赛尔网络的解决方案是采用三层防护:

首先, 在接入层设备上使用用户身份认证及接入层 ND 防攻击方案, 保证接入层的安全性;

其次, 在汇聚层设备上配置双栈防火墙业务板卡, 对园区内的 IPv6 访问进行策略控制;

最后, 对网络出口层、核心层、汇聚层、接入层的网络设备的安全策略均进行部署, 使用 SSH 访问, 关闭不使用的端口, 使用 SNMPv3 进行控制, 在路由协议中使用验证机制。

总之, 通过多方部署, 保护网络不受攻击, 控制异常行为影响网络高效数据转发, 以及保护日常园区网的正常使用。

伴随下一代互联网的建设与发展, 赛尔网络坚持自主创新, 积极开展 IPv6 运行保障和应用技术的研发工作, 协助高校全面向下一代互联网平滑过渡, 努力推动我国下一代互联网的产业化进程。

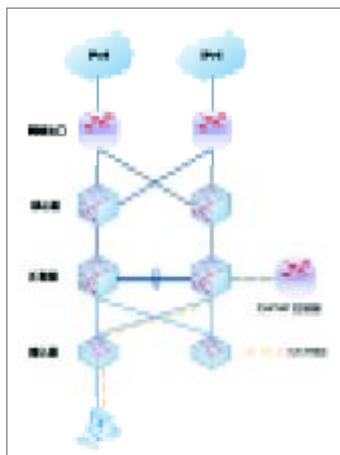


图1 使用隧道技术进行组网接入拓扑图

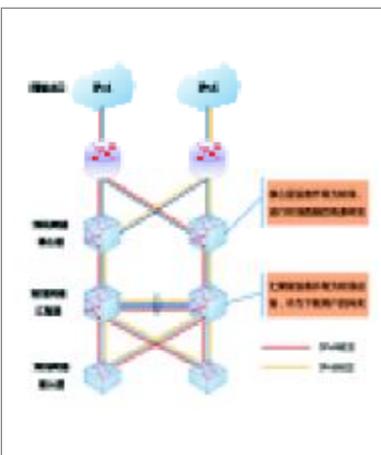


图2 使用双栈设备进行组网接入拓扑图

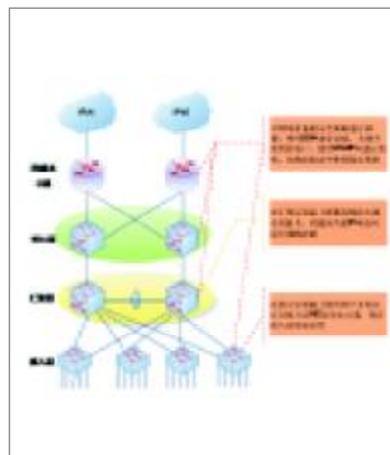


图3 IPv6/IPv4 网络安全拓扑图

| 华中科技大学 |

Solr学术索引应用显身手

华中科技大学图书馆累积的各种元数据总量接近1亿条。学校结合Solr开发了学术搜索系统，从而能够充分利用这些元数据。

■ 文 / 曾彪

华中科技大学图书馆在资源整合方面做了大量的元数据收集工作，累积的各种元数据总量接近1亿条，为了充分利用这些元数据，我们结合Solr开发了学术搜索系统（当前在<http://www.libsou.com>上运行）。

安装配置四步曲

Solr是一款非常优秀的全文搜索引擎组件，对千万级别的数据搜索速度能达到毫秒级别，Solr在2010年7月发布了1.41版。

Solr可以在Tomcat、Jetty、Resin等平台下运行，学术搜索的运行环境为：Windows 2008 R2 x64位、Solr 1.41版、Java 1.6 x64位、Tomcat 6.0.24 x64位（考虑到对32G内存的充分利用，在配置环境时选择了64位的运行环境）。

我们通过以下步骤配置Solr的运行环境

1. 安装配置Tomcat和Java运行环境，并调整了Tomcat的最大和最小的内存值。-Xmx30524M -Xms25524M，在Tomcat中配置solr.home，设置为Java的系统参数-Dsolr.solr.home=d:\solr。

2. 解压缩Solr，将Solr发布包中的example\solr目录复制到其他目录(d:\solr)，修改\$SOLR_HOME/conf\solrconfig.xml，找到dataDir设置，修改为索引存放的目录，默认为<dataDir>\${solr.data.dir:./solr}</dataDir>，修改为：

```
<dataDir>${solr.data.dir:d:\index}</dataDir>
```

3. 将apache-solr-1.4.1.war部署到Tomcat之下，并且可以将这个war复制到tomcat\webapps的目录下。

4. 修改Tomcat的server.xml文件(防止出现乱码)，设置URIEncoding为UTF-8：

```
<Connector port="8983" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" URIEncoding="UTF-8" />
```

增加tomcat\conf\Catalina\localhost\solr.xml文件，其内容为：

```
<Context docBase="${catalina.home}/webapps/solr.war"
debug="0" crossContext="true" >
<Environment name="solr/home" type="java.lang.String" value="${catalina.home}/solr" override="true" /></Context>
```

Solr主要是通过schema.xml和solrconfig.xml这两个XML文件来完成配置，solrconfig.xml文件包含了大部分的参数，用来配置Solr的缓存、索引路径、查询参数、查询相关的事件监听器、更新处理等，与Solr运行相关的参数都可以通过这个文件来配置。schema.xml相当于数据表配置文件，它定义了加入索引的数据的数据类型，主要包括types、fields和其他的一些缺省设置。该文件中配置的字段与索引字段的名称与属性一致，例：

```
<field name="id" type="string" indexed="true" stored="true"
required="true" />
<field name="kanming" type="string" indexed="true"
stored="true"/>
<field name="fenlei" type="string" indexed="false"
stored="true"/>
<field name="zhuaneye" type="string" indexed="false"
stored="true"/>
```

中文分词提高搜索准确性

在中文搜索中，中文分词的加入可以提高搜索的准确性。中文不同于西文，词汇之间没有明显的分界，但是计算机自然

语言处理是按词汇来进行分析的，因此中文分词的效果好坏直接影响中文检索和自然语言处理的准确性。当前开源的分词组件有：

1. ICTCLAS3.0分词速度单机是996KB/s，分词精度为98.45%，API不超过200KB，各种词典数据压缩后不到3M。ICTCLAS全部采用C/C++编写，支持Linux、FreeBSD及Windows系列操作系统，支持C/C++、C#、Delphi、Java等主流的开发语言。

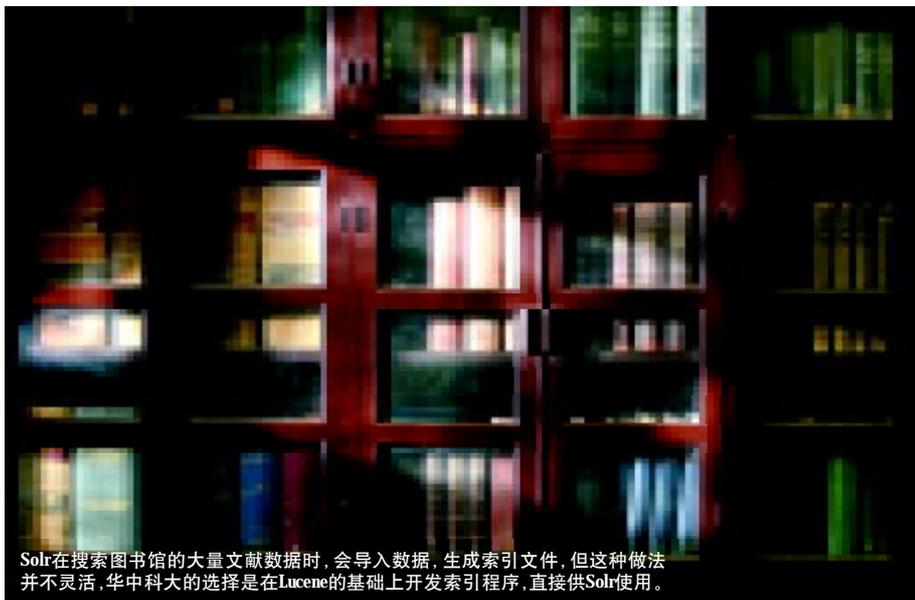
2. IKAnalyzer是一个开源的分词项目，它是基于Java语言开发的轻量级的中文分词工具包。结合词典分词和语法分析算法的中文分词组件。最新版本IKAnalyzer3.2.3，独立于Lucene项目，同时提供了对Lucene、Solr的默认优化实现。

3. Paoding提供Lucene和Solr接口，具有极高的效率和高扩展性，引入隐喻，采用完全的面向对象的设计。

4. MMSeg提供Lucene和Solr接口，MMSeg算法实现中文分词器，并实现Lucene的analyzer和Solr的TokenizerFactory。中文分词器可以在Lucene和Solr中使用。MMSeg算法有两种分词方法：Simple和Complex，它们都是基于正向最大匹配。Complex增加了4个规则过滤。

5. imdict-chinese-analyzer: 算法基于隐马尔科夫模型(Hidden Markov Model, HMM)，是中国科学院计算技术研究所的ictclas中文分词程序的重新实现（基于Java），可以直接为Lucene搜索引擎提供简体中文分词支持。

Solr在建立索引进行搜索时都用到了



Solr在搜索图书馆的大量文献数据时,会导入数据,生成索引文件,但这种做法并不灵活,华中科大的选择是在Lucene的基础上开发索引程序,直接供Solr使用。

中文分词组件,我们选择IKAnalyzer作为学术搜索的分词工具。

在设计好数据库和检索字段后,可以通过Solr提供的导入功能,将我们需要进行搜索的数据导入到Solr中,Solr会生成索引文件。这种方式虽然方便,但是不灵活。在学术搜索的排序中,要将最相关的、最值得阅读的、最新的、引用频次高的学术文献排到最前面,而Solr在建立索引的过程中对文献的评分不能有效地控制,我们选择了在Lucene的基础上开发索引程序,从而生成索引以供Solr使用。

调用 Solr 搜索

在完成上面的工作后,调用Solr搜索就很容易了,通过http发送指定的搜索参数,Solr就能返回XML或者json的结果。

搜索语法

Solr查询的格式如下:

```
http://localhost:8983/solr/select/?facet.limit=10&rows=10&start=0&facet=true&q=content:java&mlt.count=15&mlt=true&mlt.fl=title&mlt.mintf=1&hl.fl=title,content&facet.field=type,year&mlt.mindf=1&hl=true
```

以上参数表示:在content中查询关键词为java的记录,返回前面10条记录,并且按照type和year进行查询结果的分组。

Solr常用的查询参数如下:

q: 查询字符串;
fl: 指定返回哪些字段内容,用逗号或空格分隔多个内容;
start: 返回第一条记录在完整找到结果中的偏移位置,从0开始,一般用于分页;
rows: 指定返回记录条数的上限,配合start来实现分页;
sort: 对指定字段的排序,格式是year desc, year asc,默认是相关性降序;
fq(filter query): 过滤查询
qt(query type): 指定某个类型,用来处理查询请求,默认是standard;
indent: 返回的结果是否缩进,默认关闭,用indent=true|on 开启,一般调用json,php,phps,ruby输出才有必要用这个参数;
version: 查询语法的版本,建议不使用它,由服务器指定默认值。

分组

按照指定的字段分组检索是Solr的一项特性,目前有很多搜索引擎提供这项功能。在设计好分组字段后,建立索引时必须将需要分组的字段设置为Field.Index.NOT_ANALYZED。人们可以同时按照多个字段进行分组。在提交给Solr的参数中,facet.field用来确定需要分组的字段,facet.limit用来确定返回前分组数据的条数。

排序

学术搜索除了有海量的数据和高效的搜索引擎外,优秀的排序算法也非常重要,在互联网搜索引擎中,人们大多采用Pagerank来排序。Lucene中组合使用了信息检索的向量空间模型和布尔模型。下面是Lucene的评分公式:

$$\text{score}(q, d) = \text{coord} \cdot \text{queryNorm}(q) \cdots \sum (\text{tf}(\text{t in } d) \cdot \text{idf}(\text{t})^2 \cdot \text{getBoost}() \cdot \text{norm}(\text{t}, d) \cdot \text{ti} \cdot \text{q})$$

其中:

tf(t in d): 词条t在文档d中出现的词频

idf(t): 词条t在文档中的倒排词频

boost(t, field in d): 在索引过程中设置的字段参数;

lengthNorm(t, field in d): 字段的标准化值,表明在字段中存储了多少词条,这个数值是在索引过程中计算出来的,并且也存储在索引中;

coord(q, d): 协调因子,它的计算是基于文档d中所包含的所有可供查询的词条数量;

queryNorm(q): 在给出每个查询条目的方差和后,计算某查询的标准化值。

学术搜索在设计排序时结合了3个方面的内容:

1. Lucene本身的评分机制,学术搜索综合时间、类型、引用次数、是否核心期刊、是否基金项目等因素,通过doc.SetBoost(f)来给记录评分。
2. 在搜索时,对标题、关键词、文摘分别给不同的权重title^2 keyword^4 content。
3. 分析检索词的词性及分类属性,对应的分类文献给予较高的权重。

改进效率软硬兼施

我们有多种方式来提高Solr搜索效率与并发数,比如用更快的CPU、采取SSD硬盘或者SAS 15K raid 0的方式能大幅提高硬盘的读取效率、使用大内存虚拟硬盘来存放索引文件。

我们除了从硬件方面改善Solr性能之

外，还可以采用其他方式来改善其性能。

多级缓存策略

在建立索引完成之后，我们很难对索引结构作出较大改动，而缓存能大幅度提高搜索服务的性能，所以我们可以采用多级缓存的策略来提高 Solr 的并发性能和搜索性能。

Solr 中有如下几种类型的缓存：

1. SolrCache 缓存

Solr 提供了两种 SolrCache 接口实现类 `solr.search.LRUCache` (LRU = 最近最少使用内存中) 和 `solr.search.FastLRUCache` (FastLRUCache 在 1.4 版本中引入的)，后者速度在普遍意义上要比 `LRUCache` 更快。`LRUCache` 和 `FastLRUCache` 都使用了现成的 Map 来维护数据，不同点是如何来淘汰数据。

2. 过滤器缓存 (filterCache)

`filterCache` 存储了无序的文档编号列表 (Lucene `document id` 集合)。`filterCache` 主要用在查询过滤、查询结果分组、进行排序，在查询参数使用 `fq`、`facet` 的应用中，对 `filterCache` 的调优使得性能的改善效果明显。通过监控搜索服务器的缓存命中率来调整参数，从而获取更好的效果。

3. 查询结果缓存 (queryResultCache)

`queryResultCache` 是对查询结果的缓存 (Solr `IndexSearcher` 中的 `Cache` 缓存的都是 `document id set`)，这里的结果就是完全有序的结果。

4. 对象缓存 (documentCache)

在 Lucene 中，`Document` 是一个需要进行索引的“单元”，一个 `Document` 由多个字段组成，类似数据库中的一条记录。`documentCache` 用来保存 `<doc_id, document>`，要注意 `document` 中存储的字段多少，避免大量的内存消耗。

5. 自定义缓存 (User/Generi c Caches)

Solr 支持自定义 `Cache`，只需要实现自定义的 `regenerator` 即可，下面是配置示例：

```
<cache name="MyCache" class="solr.LRUCache" size="4096" initialSize="2048" autoWarmCount="4096" regenerator="myrRegenerator"/>
```

也可以使用 `memcached` 来替代 Solr 提供的缓存方式，这样能获得分布式缓存支持。

分布式搜索与索引

当索引越来越大，单台服务器无法满足搜索需求时，可以采取分布式搜索与索引来提高搜索效率：将原来大的索引文件，分隔为多个小索引文件，分发到多台 Solr 搜索服务器上面，客户端通过一次搜索多台服务器，Solr 将从多台服务器返回的结果合并，然后返回给客户端。分布式搜索可以大幅度提高 Solr 的并发处理能力。

需要注意的是要增大容器 `http` 处理线程数来防止阻塞，分布式搜索会加大 `http` 的请求数目，如果 `http` 容器没有多余的线程处理请求，`servlet` 容器就会阻塞刚来的请求，这种情况一直持续到正在处理的请求被处理完毕。

与分布式搜索相同，当需要索引的数据量非常大或者对数据的实时性要求比较高时，可以通过分布式索引来提供索引速度。在实施分布式索引中，索引的文档必须有一个唯一键，至于如何建立小索引，这点随用户的喜好而定。关于如何决定哪条记录放在哪个索引上，我们可以使用类似这样的公式：`uniqueId.hashCode() % numServers`。

监控性能

`LucidGaze for Solr` 是由 `Lucid` 开发的开源 Solr 监测工具，该工具提供了快照、存储、交互视图、比较各种 Solr 性能指标等功能，用 5 个不同的监视器来搜集统计数据，具体如下：

1. 分析统计数据: `Analyzer`、`TokenFilter`、`TokenStream` 和 `Tokenizer` 相关数据，以及哪一个 `Analyzer` 被用来为特定域产生 `TokenStream`。

2. 文档统计数据: 已建索引文档的总数，索引的各个域。

3. 索引统计数据: `IndexReader` 和 `IndexWriter` 的活动和行为，比如查看每个实例、跟踪每个相关方法的调用、查看缓存及内存使用情况和索引增加和提交的平均时间。

4. 搜索统计数据: 查询操作、搜索器性能和处理时间、方法调用统计以及对大多常用执行的查询。

5. 存储统计数据: Lucene 存储架构的目录实例 (`directory instance`)。☞

(作者单位为华中科技大学图书馆)

高效的企业级搜索引擎 Solr

作为 Apache 下基于 Java 的文本搜索引擎库 Lucene 的一个子项目，Solr 采用 Java5 开发，通过对 Lucene API 的扩展，形成了一个独立、高效率、高并发的企业级搜索应用服务器。Solr 提供了比 Lucene 更为丰富的查询语言和功能，同时实现了可配置、可扩展，并对查询性能进行了优化，有完善的功能管理界面，易于加入到 Web 应用程序中。Solr 支持多种输出格式 (包括 XML/XSLT 和 JSON 格式)，用户通过 `http` 方式与 Solr 交互，`Http Get` 操作提出查找请求，并得到 XML 格式的返回结果，提交 XML 格式的文档，而由 Solr 生成索引文件。

Solr 具备如下特点：

1. 基于标准的开放接口: Solr 搜索服务器支持通过 XML、JSON、HTTP 查询和获取结果。
2. 易管理与配置: Solr 可以通过 Web 页面管理，数据以 XML 输出，

Solr 配置通过 XML 完成。

3. 高效率分组 (facets): 高效率搜索结果自动分类，用户可以按照类型、时间等进行分组。

4. 高亮功能: 对匹配的字符自动在搜索结果中高亮显示。

5. 可伸缩性: 快速增量更新和快照分发/复制到其他服务器，支持多种方式的缓存。

6. 灵活的插件体系: 新功能能够以插件的形式方便地添加到 Solr 服务器上。

7. 分布式搜索: 支持单台或者多台服务器索引、搜索，大的索引可以分割成多个小部分，通过 Solr 一次搜索多台服务器，通过分布式搜索来提高效率。

8. 数据导入工具: 数据库和其他结构化数据源都可以导入、映射和转化为 Lucene 的索引格式。

插件助力网管软件运筹帷幄



管理员使用开源网管软件 **Cacti** 不仅可以方便地了解网络状态，并可以指定每一个用户都能查看树状结构、**host** 以及任何一张图，而且还能自己编写强大的插件来拓展 **Cacti** 的功能。

■文 / 王卫东

Cacti (<http://www.cacti.net/>)是一套基于PHP、MySQL、SNMP及RRDTool开发的网络流量监测图形分析工具。Cacti用PHP语言开发，通过SNMP服务获取数据，用RRDTool储存和更新数据并生成图表呈现给用户。Cacti软件功能强大、扩展插件丰富、用户界面友好，操作简洁方便。使用Cacti，管理员可以方便地了解网络状态，可以指定每一个用户都能查看树状结构、host以及任何一张图，还可以与LDAP结合进行用户验证，同时也能自己增加模板和插件。

利用Cacti，网管人员可以对校园网络进行很好的实时监控，从而做到运筹帷幄。

四大部分组成系统

Cacti系统由4个部分组成：

1. Cacti 页面(PHP)：它是用户控制的平台，用户在此进行所有的设置；
2. SNMP 采集工具：Unix下使用 Net-SNMP 软件包自带的“snmpget”和“snmpwalk”等程序，Windows下使用PHP的SNMP功能；
3. RRDTool 绘图引擎：性能数据的存储和绘画图像；
4. MySQL 数据库：储存RRDTool绘图所需的信息，如模板、rra、主机对应的信息等，要注意的是，MySQL数据库并不保存性能数据，性能数据保存在RRDTool自己的数据库格式rrd文件中。

安装软件

以在CentOS 5.4上安装Cacti为例，安装Cacti之前，需要先安装Apache、MySQL、PHP、Net-SNMP、RRDTool、Ruby等相关软件。

安装辅助软件

1. 安装Apache

```
[root@lab ~]# yum install httpd
检验是否安装成功：
[root@lab ~]# rpm -qa|grep httpd
httpd-2.2.3-43.el5.centos.3
```

2. 安装MySQL

```
[root@lab ~]# yum install mysql mysql-server
检测是否安装成功
[root@lab ~]# rpm -qa|grep mysql
mysql-server-5.0.77-4.el5_5.3
mysql-5.0.77-4.el5_5.3
```

3. 安装PHP相关

```
[root@lab ~]# yum install php php-mysql php-snmp
检验是否安装成功：
[root@lab ~]# rpm -qa|grep php
php-cli-5.1.6-27.el5
php-snmp-5.1.6-27.el5
php-common-5.1.6-27.el5
php-pdo-5.1.6-27.el5
php-5.1.6-27.el5
php-mysql-5.1.6-27.el5
```

4. 安装Net-SNMP相关

```
[root@lab ~]# yum install net-snmp net-snmp-utils
检验是否安装成功：
[root@lab ~]# rpm -qa|grep net-snmp
```



图1 Cacti的界面

```
net-snmp-5.3.2-2.9.el5_5.1
net-snmp-utils-5.3.2-2.9.el5_5.1
net-snmp-libs-5.3.2-2.9.el5_5.1
[root@lab-]#
```

5. 安装Ruby

```
[root@lab-]# yum install ruby
检验是否安装成功:
[root@lab-]# rpm -qa | grep ruby
ruby-1.8.5-5.el5_4.8
ruby-libs-1.8.5-5.el5_4.8
```

6. 安装RRDTool

当前版本为1.4.4, 根据系统的版本下载相关版本, 本例为CentOS 5, 所以下载el5的版本。下载地址: <http://oss.oetiker.ch/rrdtool/download.cad.en.html>

```
[root@lab-]#
rpm -ivh rrdtool-1.4.4-1.el5.wrl.i386.rpm rrdtool-perl-1.4.4-1.el5.wrl.i386.rpm
Preparing...
##### [100%]
```

1: rrdtool

```
##### [50%]
```

2: rrdtool-perl

```
##### [100%]
```

(1) 将Apache和MySQL设置成自启动

```
[root@lab-]# chkconfig httpd on
[root@lab-]# chkconfig --list|grep httpd
httpd
0:off 1:off 2:on 3:on 4:on 5:on 6:off
[root@lab-]# chkconfig mysqld on
[root@lab-]# chkconfig --list|grep mysqld
mysqld
0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

(2) 手动启动MySQL和httpd

```
[root@lab-]# /etc/init.d/mysqld start
[root@lab-]# /etc/init.d/httpd start
```

安装Cacti

1. 从Cacti网站<http://www.cacti.net>下载

Cacti for Linux/Unix, 当前版本为0.8.7g。

2. 安装

```
[root@lab-]# cp cacti-0.8.7g.tar.gz /var/www/html/
[root@lab-]# cd /var/www/html/
[root@lab html]# tar zxvf cacti-0.8.7g.tar.gz
[root@lab html]# mv cacti-0.8.7g cacti
[root@lab html]# cd cacti
```

3. 创建Cacti数据库, 并导入数据表

```
[root@lab cacti]# mysqladmin --user=root create cacti
[root@lab cacti]# mysql cacti < cacti.sql
```

4. 在MySQL里增加cactiuser用户, 密码为cacti

```
[root@lab cacti]# mysql --user=root mysql
mysql> GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY 'cacti';
mysql> flush privileges;
```

5. 设置配置文件

```
[root@lab cacti]# vim /var/www/html/cacti/include/config.php
Sdatabse_type = "mysql";
Sdatabse_default = "cacti";
Sdatabse_hostname = "localhost";
Sdatabse_username = "cactiuser";
Sdatabse_password = "cacti";
Sdatabse_port = "3306";
```

6. 增加Cacti用户, 通过该用户的crontab定时采集数据

```
[root@lab cacti]# useradd cacti
[root@lab cacti]# passwd cacti
Changing password for user cacti.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

将Cacti的采集脚本放入Cacti用户的crontab里, 每5分钟采集一次

```
[root@lab cacti]# crontab -u cacti -e
*/5 * * * * /usr/bin/php /var/www/html/cacti/poller.php >/dev/null 2>&1
```

7. 设置rra和log目录权限

```
[root@lab cacti]# chown -R cacti:cacti ma/ log/
```

页面设置

我们首先可以在浏览器地址栏内输入<http://IP/cacti>, 进入Cacti的初始设置页面, 然后输入一些基本信息, 如RRDTool、PHP、snmpwalk、snmpget的位置, 再输入原始的用户名和密码: admin/admin, 再更改admin用户的密码, 点击save, 最后安

装完成。

现在, 我们可以从浏览器进入Cacti的世界了(见图1)。

插件增强Cacti功能

Cacti插件是对Cacti的扩展, Cacti的强大在于有很多功能强大的插件支持。

如果我们使用Cacti插件, 就必须先安装Cacti的一个patch——Plugin Architecture, 这样才能支持插件。



图2 monitor插件

Plugin Architecture (简称PA)的下载路径为<http://cactiusers.org/>下载, PA当前版本为v2.8。

安装PA

```
[root@lab-]# tar zxvf cacti-plugin-0.8.7g-PA-v2.8.tar.gz
[root@lab-]# cp -R cacti-plugin-arch/* /var/www/html/cacti/
[root@lab-]# cd /var/www/html/cacti
[root@lab cacti]# mysql -ucactiuser -pcacti cacti < pa.sql
[root@lab cacti]# patch -p1 -N < cacti-plugin-0.8.7g-PA-v2.8.diff
```

Patch安装后, 首页显示会有些问题, 需要修改配置文件。

```
[root@lab cacti]# vim include/global.php
$config['url_path'] = '/cacti/';
```

安装成功后, 重新登录Cacti即可, 如果Configuration里没有Plugin Management, 在User Management里将Plugin Management选上。

Cacti的插件安装很简单, 下载相应的插件压缩包, 解压到Cacti的plugin文件夹, 修改include/global.php

```
$plugins[] = '插件所对应的目录名';
```

以安装monitor插件为例:

下载Monitor插件安装包, 网址是<http://cactiusers.org/download/cad/monitor.tar.gz>

```
[root@lab-]# tar zxvf monitor-0.8.2.tar.gz
[root@lab-]# mv monitor /var/www/html/cacti/plugins/
修改include/global.php
```

```
$plugins[] = 'monitor';
```

进入"Console" -> "User Management" -> "admin" -> Real Permissions把View Monitoring打勾

刷新页面, 就可以看到Cacti导航栏多

了一个monitor 标签,monitor插件安装成功,如图2所示。

Cacti 比较常用的插件有:

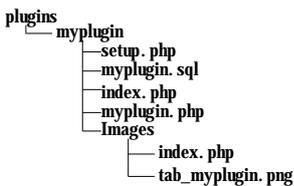
1. Settings插件,给不同的插件提供一些共用的信息,如邮件信息,DNS信息。
2. Monitor 插件,提供更简略、直观的设备状态图示。
3. Threshold插件,提供设备异常预警。

编写 Cacti 插件

文件结构

Cacti 的插件是以文件夹形式安装到plugins目录下,插件基本文件结构为:

Cacti 插件目录结构



其中:

1. myplugin 即插件的名称。
2. setup.php 插件由该文件与Cacti 做关联,由插件初始化函数plugin_init_myplugin()和自定义函数组成.plugin_init_myplugin函数是Cacti 初始化插件的入口,在plugin_init_myplugin函数中,初始化本插件各项参数,如在导航栏中显示的文本、图片,配置页面的显示。

初始化函数plugin_init_myplugin声明格式为:

```
$plugin_hooks['预定义函数名']['插件名'] = '自定义函数';
```

例如: \$plugin_hooks['draw_navigation_text']['myplugin'] = 'myplugin_draw_navigation_text';定义了导航栏显示myplugin插件时要调用的函数为myplugin_draw_navigation_text。

3. myplugin.sql: 插件所用到的数据表及数据。

4. index.php: 只是为了防止访问者直接浏览本目录,没有实际作用,一般为空或

者链接到首页。

5. myplugin.php: 插件的主文件,文件名必须和插件的名称一致。

6. Images: 保存图片的目录。

7. tab_myplugin.png: Cacti 导航栏插件标签所显示的图片,图片文件名可在setup.php中myplugin_show_tab函数修改。

制作过程

现在我们来制作一个Cacti 插件myplugin,插件功能很简单,输出“hello, world”,因为没有数据库操作,所以不需要编辑myplugin.sql。

自定义一张图片,保存为/var/www/html/cacti/plugins/myplugin/images/tab_myplugin.gif。具体代码如下:

```

[root@lab plugins]# mkdir myplugin
[root@lab plugins]# cd myplugin/

function plugin_init_myplugin() {
    Global $plugin_hooks;
    $plugin_hooks['top_header_tabs']['myplugin'] = 'myplugin_show_tab';
    $plugin_hooks['top_graph_header_tabs']['myplugin'] = 'myplugin_show_tab';
    $plugin_hooks['config_arrays']['myplugin'] = 'myplugin_config_arrays';
}

function myplugin_show_tab() {
    global $config, $user_auth_realms, $user_auth_realm_filenames;
    $realm_id2=0;
    if(isset($user_auth_realm_filenames[basename('myplugin.php')])){
        $realm_id2=$user_auth_realm_filenames[basename('myplugin.php')];
    }
    If((db_fetch_assoc("select user_auth_realm.realm_id from user_auth_realm where user_auth_realm.user_id=''.S_SESSID['sess_user_id'] and user_auth_realm.realm=id=' $realm_id2'"))){
        (empty($realm_id2)){
            print "<a href='". $config['url_path']. 'plugins/myplugin/myplugin. ugn.php' "><img src='". $config['url_path']. 'plugins/myplugin/images/tab_myplugin'
        }
    }

function myplugin_config_arrays() {
    global $user_auth_realms, $user_auth_realm_filenames;
    $user_auth_realms[36] = 'View myplugin';
    $user_auth_realm_filenames['myplugin.php'] = 36;
}
<?php
Chdir('.../');
Include("../include/auth.php");
Include("../include/top_graph_header.php");
Echo "hello, world";
?>

[root@lab myplugin]# vim setup.php
[root@lab myplugin]# vim myplugin.php
[root@lab myplugin]# vim ../include/config.php
    
```

```
$plugins[] = 'myplugin';
```

进入“Console”->“User Management”->“admin”->Realm Permissions把View myplugin 打勾

刷新后,myplugin出现在导航栏中,点击该插件后,myplugin成功运行。

Cacti 软件功能强大、扩展插件丰富、用户界面友好,操作简洁方便,用户甚至无需了解RRDTool 的众多参数就可以利用Cacti 软件绘制出理想的图形。Cacti 已经成为众多管理员进行网络监测的必备工具。

(作者单位为东北大学网络中心)

湖北省科技信息共享服务平台 理事会 2010 年度会议召开 拟完善服务功能系统

本刊讯 9月12日,湖北省科技信息共享服务平台(简称:平台)理事会召开年度会议,湖北省财政厅科教文处、湖北省科技厅条财处、湖北省科技信息研究院、武汉大学图书馆、国家科学图书馆武汉分馆、华中科技大学图书馆等平台共建单位理事出席。

在会上,理事会重点审议了《<湖北省科技信息共享服务平台运行管理办法(暂行)>实施细则(送审稿)》,通报了平台建设2009年度运行补贴经费分解办法。

据悉,经过五年的发展,平台通行条件得到了有效的改善,电信线路扩容至50M,同时优化网通20M和教育网用户的网络访问链路;局域网主干线升级为IPv6双栈网络;并构建了“六网联通、共建共享”的格局。平台现在可以实现的功能有:跨系统跨库统一检索、用户管理服务、共享服务和信息资源整合。

理事会制订了一系列运行管理办法,对平台的建设实行业主负责制,由业主(即建设单位)按照平台建设目标、任务和统一的技术标准、服务规范组织施工和建设。建成后,遵循“谁拥有、谁服务、谁收益”的原则运营。

理事会表示,2010年下半年要进一步完善平台服务功能系统,使其在用户和管理运行方面更加便捷、更加人性化、更有利于集成各方信息资源服务社会;运行管理机制既要鼓励社会资源的最大限度集成,又要适当考虑平台共建核心单位的地位和利益;并将在年底前对平台“十一五”建设任务完成情况进行整体验收,圆满结账。

网络教学缓解西部师资不足

文 / 曹雨 张小宾

石河子大学地处西部边疆,相对内地高校来说,师资力量薄弱,教学资源匮乏。尤其是近年来,学校办学规模不断扩大,规模发展与师资力量不足的矛盾日显突出。网络教学作为一种新型教学模式,以其学生自主化的学习环境,充分的交流互动,无限广泛的知识链接等特点,在学校人才培养过程有着传统教学模式无可比拟的作用,同时也成为西部边疆高校缓解师资与教学资源不足矛盾的一个重要途径。

网络教学的出现被认为是教育史上前所未有的变革,它是一种以网络为载体的全新的教育教学模式,因此传统的教育理念、教学观念无法完全适应并指导这一全新的教学实践。石河子大学从现代教育观念出发,深刻认识信息技术在高等教育教学中的地位与作用,在政策上制定激励导向措施,在经费上加大对信息技术软硬件建设的投入,在管理上有目的、有重点地开展教师现代教育技术培训工作。几年来,通过大力加强教学资源建设,开展教师网络教学培训,推动网络教学实践,使网络教学平台应用与教学资源建设进入良性发展轨道。

优化教学平台软硬件环境

为推进教育创新,促进现代信息技术在教学中的应用,2004年学校搭建了石河子大学网络教学平台。为适应网络教学向更深、更广层次发展的需要,2006年以来,在清华大学教育技术研究所支持下分两次对网络教学平台的软硬件进行升级改造,

逐步形成了以网络教学平台为中心的,包括教学资源库、视频课程库、精品课程网站在内的较为完善的网络教学综合平台体系。新的教学平台在充分汲取教育技术理论与方法的最新研究成果基础上,应用网络技术,根据不同教学模式、不同教育对象的特点,为开展网络教学提供灵活的,适合于多种层面、多种对象及多种网络环境的交互式教与学支撑平台。通过网络教学平台,教师和学生可以进行互动式的网上教学。平台中的教师空间为教师用户提供了强大的在线备课与施教环境,主要包括教学大纲、教学讲义、答疑讨论、教学博客、教学邮箱、教学日志、课程资源、在线测试、在线作业、主题探究教学等功能模块,充分互动的网络教学平台极大地拓宽了课程教学空间。尤其是其中的主题探究教学模块能够支持不同分组从问题定位、文献查阅、综合分析、沟通与协作到报告呈现、结果评价等探究教学环节,支持教师通过分组协作式教学活动,培养高层次的学习能力和沟通协作能力,充分体现了网络教学的魅力。

多形式开展教师培训工作

为使教师尽快适应网络教学的要求,掌握网络教学的特点与方法,2004年至今,以学院为单位开展了2次教师网络教学轮流培训;2004年、2006年、2008年三次聘请清华大学教育技术研究所专家来学校进行专题讲座和培训;截至目前接受过网络教学培训的教师达3000余人次。在此期间,三次设计印刷了《石河子大学网络教学平台教师手册》,共计4000册,发放到每位教师手中。使教师了解网络教学特点、网络教学中教师的

角色定位、如何开展网络教学以及网络教学平台应用等。帮助教师在网络教学中转变观念、进入角色。同时也印制了石河子大学网络教学宣传彩页6000份,发放到学生手中,以学生的应用促进教师的运用。

创设优质网络教学环境

2006年学校投入30万元建成大学流媒体工作室。通过录制、购买等方式引进视频资源,共收录各种视频教学片3000余部集,并通过视频课程库网站对外发布。4年来,支持完成了近2万名学生,724320人次的《科技发展史》的课程教学任务。同时该网站也受到广大师生的欢迎,成为教师课程教学、学生课程学习的重要工具和拓展知识空间的重要平台。依托全自动录播教室的建设,新的视频课程库网站将成为石河子大学视频教学资源中心。

大学网络课件立项是学校开展了七年,旨在调动广大教师开展CAI课件研究和应用的积极性,在教学一线普及、推广现代教育技术,更新教学手段,促进教学内容和方法改革,丰富本校教学资源,提高教师教学资源开发能力的一项重要措施。截至目前共有64部网络课件通过了结题验收,并在网上运行。与此同时,学校积极组织本校优秀课件参加全国课件大赛,增强与其他高校的交流,提高教师教学资源的研发能力。

总结几年来课件立项研发工作的得与失,2008年对《石河子大学网络课件立项管理办法》进行了修订,并出台了《石河子大学立项网络课件制作规范》,来规范开发行为、规范开发技术、提高开发质量,促进课件在网络教学中的应用。



引进名校教学资源是加快教学资源建设,改善教学资源来源结构的有效途径。清华大学教育技术研究所提供网络教学技术支持的同时,还为学校提供了丰富的教学资源。

激励导向措施推动网络教学

网络教学是一个新生事物。短时间内教师从教育理念和教学习惯等方面尚无法完全适应这样一种新型教学模式。由于高校教师的教学、科研较重,如果没有一定的激励导向措施,教师很难将有限的精力投入到网络教学中去。因此,开展网络教学就需要一个普及、推广、应用的过程。

首先探索适合本校网络教学发展途径。2007年,学校初步选定《机械设计基础》、《工程力学》、《大学物理》、《园林设计》等11门课程进行网络教学实践。

学校将网络教学实践工作分为平台初始化与教学实践两个阶段。经过近两个学期的网络教学实践,各课程组取得了丰富的网络教学实践经验与心得。截止目前共整理常见问题38个,在课程论坛中发表话题191个、学生浏览2566次、回复184次,布置作业32次、学生提交作业1839份、教师批改1401份。其中,《机械设计基础》、《大学物理》、《工程力学》、《园林艺术》、《遗传学》等5门课程成果最为突出,研究实践工作各有特色。

《机械设计基础》课题组重视网络教学

教学法的研究,对教师的角色定位,如何发挥网络教学的特点等有较深刻的认识和理解。认为网络本身只是信息的传输通道,是技术手段,是教学的局部因素。网络教学质量的高低关键在于教师融入其中的教学思想、教学策略、教学

方法,对教师运用和掌握知识有了更高的要求。

《工程力学》课题组注重课程常见问题库在网络教学中的作用,整理常见问题29个;课程论坛发表话题18个,被浏览508次,回复49次。课题组做好课题研究的同时,更多地了解学生们在项目实施过程中的实际情况进行统计分析,及时地调整研究策略和方法。不仅分析学生在“服务型”学习模式驱动下的学习,同时分析学生对学科的学习兴趣和办法。

《园林艺术》课题组发动全体同学来共同完善和丰富网站内容。其中答疑讨论中的课程论坛是老师和学生交流的一个最方便的通道,学生可以将自己觉得有价值的知识以及对课程的建议和意见通过课程论坛上传,这样学生和教师就有一个更好的交流,也为教师改革教学内容和教学方法提供了第一手的材料。

《大学物理》课题组运用课程论坛主要有两种形式,一是通过对教学中问题的提出,激发学生对问题的思考,引导学生参与讨论。二是让学生自己提出问题,让学生自行讨论,最后对学生的讨论进行总结,给出正确答案。

网络教学实践取得了初步成果,为学校网络教学的发展取得了宝贵的研究成果及实践经验。

其次研究制定网络课程评价标准。网络教学不同于现代教育技术所经历的语音教学、电视教学、多媒体教学,它不是教学

手段的更新,而是一种新型的教学模式,相对于教学过程来讲是教学结构的改革。网络教学不仅仅是课堂教学的延伸,更重要的是,这样一种新型教学模式在学生信息素养培养、自主化学习、知识体系自我完善等方面有着传统教学不可比拟的作用。因此,网络课程的质量是制约网络教学发展的关键因素。

在总结课程网络教学研究实践经验的基础上,学校制定了符合实际情况的《石河子大学网络课程评价标准》。通过制定网络课程评价指标,引导教师正确开展网络教学,避免盲目追求形式上的繁荣,避免课堂搬家现象的出现。充分发挥网络教学开放性、自主性、交互性、个性化和协作性的特点,弥补课堂教学的不足,使网络教学也能肩负起“传道、授业、解惑”的职责。

最后借助外力,大力推动网络教学精品课程建设教育部“质量工程”建设项目,受到各高校高度重视,以丰富多彩的网络教学促进精品课程的评审是精品课程建设过程中的普遍做法。此外,精品课程组师资力量相对雄厚;课程建设时间长,积累了丰富的教学资源,具备开展网络教学的充分和必要条件。

2009年4月学校在精品课程评审中做出规定,将精品、一类课程的建设、评审与课程网络教学开展情况相结合。使课程网站成为课程建设与评审的重要环节。

同时,石河子大学还注重通过学校各种与教学相关的课题或建设项目来推动网络教学。通过修订《石河子大学网络课件立项管理办法》,将网络课件立项研发与课件在网络课程中的应用挂钩。一方面促进课件的应用,另一方面推动网络教学的开展。

通过以上措施的实施,石河子大学网络教学平台总访问量达到190万次,近两年的日平均访问量达到3000次。两年来,扎实有效的网络教学研究、实践、普及、推广工作为学校积累了丰富的经验,为今后学校教学信息化向更深更高层次发展奠定了坚实的基础。

(作者单位为石河子大学现代教育技术中心)

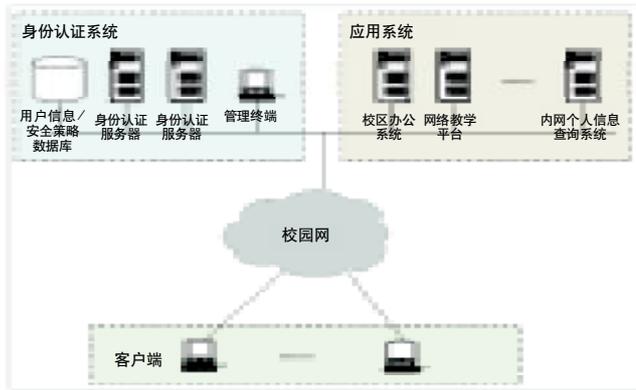


图2 身份认证系统网络结构

包括：认证方式、认证策略、资源和管理流程、管理策略。系统的设计必须能够有效识别这些变化，隔离这些变化，以策略或参数化的形式支持这些变化。

3. 现有应用系统最小改动的原则

系统设计时应充分考虑对现有应用系统的影响，保证现有应用系统改动最小，并在业务流程上保持现有应用模式。

4. 方便管理的原则

由于Web Service技术的松散耦合特点，它没有复杂的消息传递、对象引用和垃圾回收机制，因此非常适合于分布式处理。我们设计系统时需要考虑到校园网中用户身份和资源信息应具有简单方便的管理方式。

系统构成

身份认证系统由身份认证服务器、用户信息/安全策略数据库、客户端控件、Web服务代理、管理终端等构成。身份认证服务器由身份认证服务和安全策略配置服务两个模块组成。

身份认证系统采用B/S架构实现用户信息的管理和安全策略的配置，配置的信息通过安全策略配置服务程序写入到用户信息/安全策略数据库中，以供身份认证服务和管理终端查询使用。身份认证服务模块提供在线服务，实时接收来自Web安全代理的身份认证请求，并根据设定的策略对用户身份进行验证，为用户登录业务系统提供集中认证服务。

从图1可见，身份认证系统部署在用户层和资源层之间，对用户访问资源的登录行为进

行实时的控制：

1. 用户层

这一层包括校内所有教职工和学生。按照用户上网地点的不同，可以分为校内用户和校外用户；按用户接入方式的不同，可以划分为上网认证用户和不认证用户。

2. 资源层

这一层包括校内办公系统、精品课程、网络教学平台、内网个人信息查询、资源中心、学生选课及成绩查询、BBS等B/S架构的应用系统，而将来可以通过平滑升级的系统包括邮件系统和其它C/S架构的业务系统。

系统架构

Tomcat是JSP和Servlet的运行环境，AXIS框架来自Apache开放源代码组织，它是使用Java语言编写的基于最新的SOAP规范(SOAP 1.2)和SOAP with Attachments规范的开放源代码框架。使用AXIS实现Web Service非常简单，只需编写认证相关的Java类，然后将文件扩展名改为jws，无需编译，将文件拷贝到应用程序发布目录下即可。

网络构架与实现

综合考虑到性能和保护现有投资的要 求，校园网采用了网关认证和802.1x认证相结合的方式：学生宿舍全部部署支持802.1x的交换机，采用802.1x认证，办公区采用网关Web认证。两套认证系统使用统一的用户资料，用户资料存储在LDAP服务器中，通过Web Service实现用户身份的认证，Web Service通过Java技术实现，运行环境为Tomcat和AXIS框架。

在校园网内部署两台身份认证服务器，操作系统为Redhat Linux 9.0 安装Apache、登录认证服务器软件、资源访问审计服务器软件和安全策略配置服务器软件。其中，一台是数据库服务器，其操作系统为

Redhat Linux 9.0,安装的是Oracle数据库软件；另一台是管理终端，在应用系统服务器主机上安装Web服务代理。为了保证身份认证系统稳定可靠地运行，避免单点故障，使用两台身份认证服务器互相热备，以保证提供稳定可靠的服务。

校内用户访问校内应用系统时不需要通过该系统作验证，而是直接访问原有业务；校外用户访问校内应用系统时必须通过身份认证系统进行身份验证，认证方式为用户名/口令，身份验证通过后才能访问原有业务；用户通过身份验证时，只需输入一次口令，就可以访问校内应用系统。身份认证系统网络结构如图2所示。

目前，学校人事、教务、研究生、财务、校内信息服务等网络应用系统已实现基于Web Service的统一身份认证。根据校园网建设的需求，身份认证服务器采用双机备份，尽可能提高系统运行的可靠性，用户使用该系统访问业务系统时只需要输入一次口令，就可以连接多个应用系统，而其他应用系统不用作任何修改，就可以平滑升级支持单点登录、集中授权和集中审计。

(作者单位为华北电力大学网络与信息中心)

全面调整中国市场战略

Stonesoft亚太区总部迁至北京

本刊讯 近日，欧洲最大的网络安全公司Stonesoft在迎来20周年之际宣布，其亚太区总部将正式迁到北京，并将继续加大对中国市场的投入，深化与中国渠道商的合作伙伴关系。这是其首席执行官Ilkka Hidenheim在北京举办的“引领未来 安全共赢——Stonesoft中国市场新战略暨新产品发布会”上向在场的近200名渠道合作伙伴公布的关于未来在中国市场的战略。

在大会上，Stonesoft同时向中国市场发布了下一代StoneGate安全平台产品，包含了StoneGate Management Center、StoneGate Firewall / VPN、StoneGate IPS、StoneGate SSL VPN、StoneGate Virtual Firewall / VPN Appliance、StoneGate Virtual IPS Appliance、StoneGate SSL VPN Virtual Appliance。

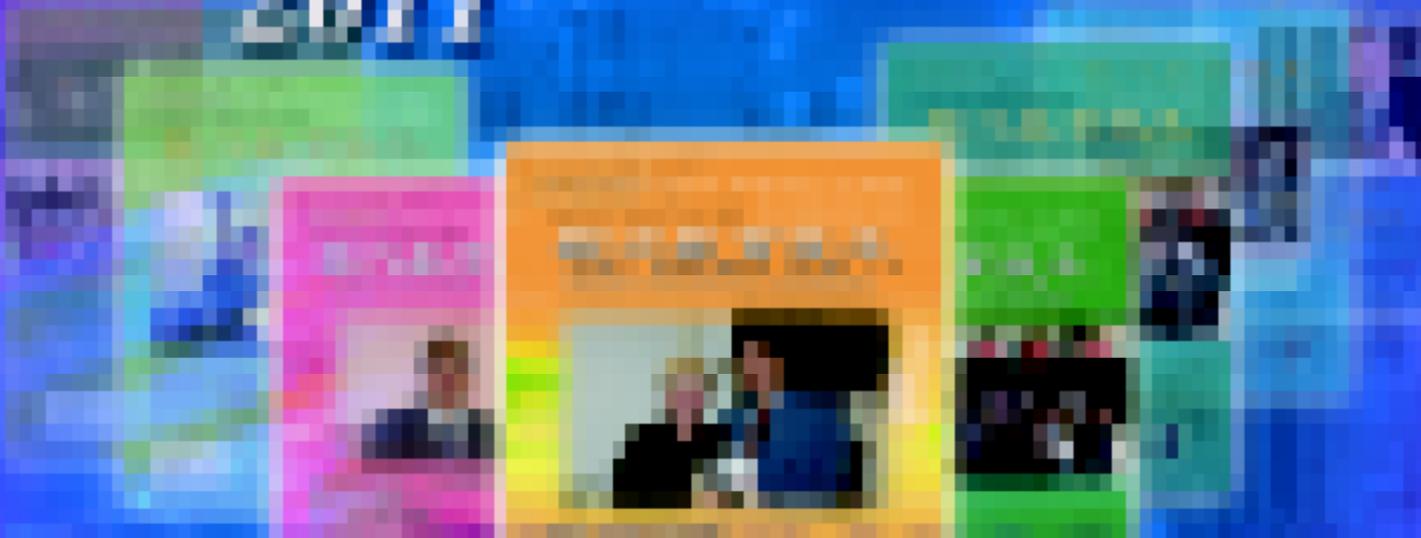


现代企业

MODERN ENTERPRISE



2011



现代企业 2011年12月 第12期

本期目录

封面故事 中国企业的社会责任
行业观察 中国企业的国际化之路
企业管理 中国企业的品牌建设
企业文化 中国企业的核心价值观
法律法规 中国企业的法律风险防范



COST论坛由CCERT、《中国教育网络》杂志于2008年共同发起,采取会员制,面向个人,完全免费,以开放、平等、自由的互联网精神运作。如需获取COST技术论坛视频、录音等资料,请登录:<http://www.cost.edu.cn/>。

数字迎新：以人为本服务新生

Q=COST论坛用户

A=中国人民大学网络与教育技术中心葛泓

Q 在数字迎新的流程整合方面有哪些经验?

A 我们在建设数字迎新过程中最重要的是心得是制定了“以人为本”的思路,以此为指导来设计业务流程。一开始,我们的建设还围绕着业务来进行的。我们将人事、科研、教学、管理等作为核心业务进行开发,比如新生住宿管理就被提到“数字人大”的第一期来建设,我们的初衷是在新生报到后,住宿分配就可以有序而高效地进行。然而在实践中,我们发现新生仍然无法迅速开展校园卡的使用、住宿登记等相关业务,原因并不在于数字迎新的单个系统的运行上(实际上它们运行良好),而在于各个系统之间的流程协调还不够平滑。因此,我们摒弃“以业务为中心”的建设思路,而以为师生服务为宗旨,首先做好迎新的准备工作,其次,通过红外线扫描,将学号和录取通知书号匹配起来,进行住宿和报到登记,其三,我们让新生在开学前通过网络上交照片,以便于我们提前制作好校园卡。这些细节的改进使得迎新压力减小了,同时得到了学校领导、家长和学生的肯定。

Q 统一身份认证平台建立以后,那些没有统一身份认证的临时人员如何管理,他们是否纳入数字迎新中?

A 我校的数字迎新并未将临时人员纳入体系中。对于院系和人事处联合管理的职工临时人员,由院系申请,人事处统一备案,我们的系统会给他们发放一个临时人员职工号。对于交流学生,学籍系统为他们建立交流学生信息表,其他系统就共享这些信息,这些交流学生就可以享受校园资源,比如图书资料查询、使用校园卡等。至于他们当中有哪些人可以使用哪些资源等具体的界定则由学籍管理处来操作。

Q 有些学校将校园卡和录取通知书一起寄给学生,让学生入校后就可以使用,请问您对此是如何看待的?

A 那种情况的确存在,究竟是入学前发校园卡还是入学后发放,可以根据本校的情况来选择。由于我校的

校园卡不仅仅用于消费,而且还具备身份认证的功能,因此,我们要等到校园卡附上照片之后才会发给学生。

Q 贵校在十二五规划中,是否有一些新的工作计划?

A 我校电子校务系统数字人大平台应用的建设开发工作已经进入运营阶段,现在要做的就是将原来围绕业务的各个模块的职能充分地利用起来,为更多的师生提供服务,让他们享受信息化成果。为此,我们专门成立了用户服务的办公室,从事服务管理的工作,如我校网络与教育技术中心内部流程管理的规范化、服务模式的统一化、服务质量的监督、服务工作的可计量化。工作侧重点是提供综合管理,如为学生提供全方位的网络服务、应用服务等信息化服务。

Q 贵校系统的开发和建设是否外包?若有外包,那么服务提供商做到什么程度?

A 我们与东软集团合作,由他们开发系统,现在开发已结束,我们主要负责运维服务,而东软集团则安排一、两个人为我们做支持。

Q 您认为手工干预对数字迎新工作能起到什么作用?

A 迎新实现数字化后,我们单纯依赖信息化的手段是不够的,我们需要手工介入一些需要灵活掌握的工作。比如,在电子注册中,如果学生不缴费,那么校园卡的功能就需要限制,不过不缴费的原因并不是单一的,需要区别对待,这就需要人工干预了。

Q 贵校由什么样的机构来领导、协调和支撑电子校务系统的建设?

A 我校信息化规划、建设、推广使用和服务都由网络和教育技术中心来承担,中心是学校处级机构,本质是教学辅助机构,而学校对其的定位是具有管理职能的机构。在中心之上是“数字人大”领导小组。我们还有专家小组,专门对我校信息化建设进行监督和把关。

STP破校园网络环路难题

文 / 李金方¹ 肖东² 吴滔¹

随着高校学生培养形式的变化,供教师使用的办公室逐渐演变成集教学、实验、科研为一体的工作室,从而使得校园网络接入的形式发生了一些变化,原先提供的物理信息点的数量远远不能满足师生入网的需求。通常的解决方法是师生自行购置一些普通交换机进行简单的互联,以满足上网的需要。由于用户对网络知识的了解和技术的缺乏,造成网络环路故障频出,对网络运行的影响较大。

网络环路的几种拓扑形式

网络环路是当前对校园网网络运行影响较突出的几种问题之一(如ARP攻击、DHCP欺骗等)。导致形成网络环路的几种行为如下:

(1)片面的理解端口聚合是交换机必需具备的功能和配置技术。校园网某些用户简单的认为在两交换机端口之间用两根以上的网线互联起来就可以增加物理带宽,从100M就可以达到200M以上的带宽,如图1所示,导致网络环路的产生。

(2)校园网某些用户缺乏对网络技术知识的认识。为了网络通信的可靠性,使用两台交换机首先互联起来,然后再分别用网线连接到校园网对室内提供的信息点上,如图2所示,导致网络环路的产生。



图1 同一交换机两端口之间形成的环路

图2 同VLAN不同交换机两端口之间形成的环路

(3)校园网某些用户在工作室内布置网线,受室内环境的影响经常会将同一根网线插在同一个VLAN里的交换机两端口上,如图3所示,形成网络环路。

由于上述原因,网络环路的产生总是存

在的,如何防止和消除网络环路对网络运行的影响,借助IEEE 802.1D生成树协议(Spanning Tree Protocol),可以取得一个较满意的效果。

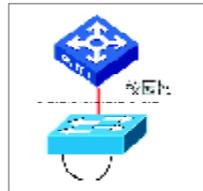


图3 下层交换机两端口之间形成的环路

生成树协议工作机制

生成树协议原理

冗余链路作为网络备份路径发挥着非常重要的作用,是网络运行可靠性的保障。而网络环路对网络运行来说又是致命的打击。STP的有效运作对网络是非常重要的,因为如果两节点之间存在多条路径,就会产生环路,导致信息的重复,从而使网络不通。而IEEE 802.1D生成树协议(STP)允许网络上存在环路时,自动断开环路连接。当检测到交换机间存在多条连接时,将只启动最主要的一条连接,而将其他连接都阻塞掉,将这些连接变为备用连接。确保同一时刻网络两节点之间只有一条路径是主动激活的,可以通讯的。当主连接出现问题时,生成树协议将自动起用备用连接接替主连接的工作,不需要任何人工干预。

可见STP提供了网络的动态冗余切换机制。因此使用STP,可以在网络设计中部署备份线路,并且得到下述保障:

在主线路正常工作时,备份线路是关闭的

当主线路出现故障时,自动激活备份线路,将数据流切换到备份线路,从而保证网络设备正常运行。

因此使用STP这种网络自动重构的功能,不仅可以保证在网络结构上存在冗余路径的情况时,阻止网络环路状态的发生,还能使得网络上的用户能够最大限度地与网络保持正常的连接。

生成树协议STP在交换机间进行通信时使用的是BPDU(Bridge Protocol Data Units)。交换机通过发送BPDU来进行通信并构建生成树拓扑,连接到LAN的所有交换机都将接收BPDU。交换机并不直接转发BPDU,但是接收BPDU的交换机会计算BPDU,如果网络拓扑发生改变,就会发出一个BPDU。

利用BPDU进行的交换机间的通信将导致如下结果:

一台交换机被选为根交换机。

为每台交换机计算到根交换机最短的距离(shortest distance);

选出指定交换机(TPESigned switch),该交换机是最靠近根交换机的交换机,数据包将通过该交换机转发给根交换机。

选出每台交换机上的一个端口,该端口是该交换机到根交换机的最佳路径。

选出生成树内的所有端口。

如果所有启动生成树协议的交换机都使用缺省的设置值,那么,具有最小MAC地址的交换机将成为根交换机(root switch)。通过提高交换机的优先级(数值越小),生成树协议可以将其强制选定为根交换机。

当生成树协议使用缺省参数值时,源站点和目的站点之间的路径未必是最理想的。例如,一个到某个端口的高速率的连接可能使得根端口发生改变,因其数值优于当前的根端口。因为生成树追求的目标就是根端口应具有最快的连接。

生成树工作举例

在一个环路中有三个桥(或三台交换

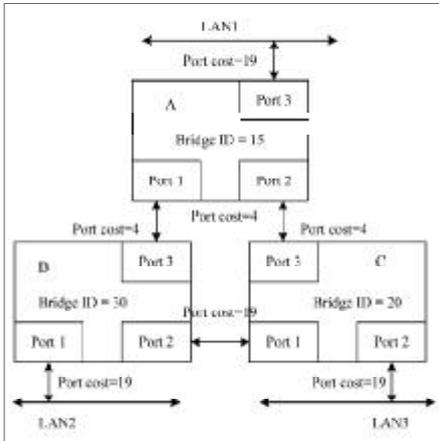


图4 应用STP之前

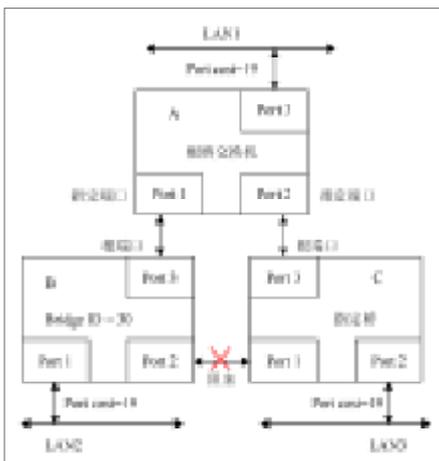


图5 应用STP之后

如图4所示。在此例中，如果不使用生成树技术，可以预见到可能发生的一些网络故障。例如，如果桥A向桥B发出一个广播包，那么，桥B将把此数据包广播给桥C，而桥C又会将此数据包广播回给桥A。随后会一直将如此反复，广播包将会在这个环路中被循环往复地传递，从而导致严重的网络故障。

为了避免网络环路的发生，可以如图5所示采用STP来解决。生成树将阻断桥B与桥C之间的连接，以打破环路的形成。STP算法将根据计算出来的各桥和端口之间的数值，来决定断开哪一条连接。现在，如果桥A向桥C发出一个广播包，那么，桥C将在端口1处将此数据包丢弃，那么此广播将结束。

但是，生成树的算法较复杂，所以在交换机上尽量不要改动其出厂默认设置值，(最

好在充分研究理解其之后，再去更改交换机上的生成树的设置)。生成树将自动任命根桥/根端口，并避免环路的形成。

由此可见启用STP的主要目的是在网络设计中部署备份线路，从而增加网络运行的可靠性。同理在网络设计中合理部署使用STP，可以有效的防止网络环路的产生，从而大大降低环路对网络运行的致命打击。

防止网络环路的技术实现

实现环境在一幢学生宿舍楼构成，楼内有520个信息点和1个3.3m×3.3m×3m的网络交换设备机房，机房内安置4个2m高的标准机柜，共有24端口的交换机23台(其中一台为神州数码网络公司生产的DCRS-5950-28T万兆汇聚交换机，其余22台为神州数码生产的DCS-3950-26C接入层交换机)。DCS-3950-26C接入层交换机分别通过千兆端口与DCRS-5950-28T万兆汇聚交换机的千兆端口级联，充分保证了负载均衡的能力需求。为了有效防止网络环路的产生，只在接入层交换机上启用STP协议，即使得每台接入层交换机均配置成根桥交换机，其100M的端口均设置成指定端口。其中任意一台DCS-3950-26C交换机配置的相关内容显示如下：

```
switch# show run
no service password-encryption
hostname switch
enable password admin
username admin privilege 15 password 7
21232297a57a5a743894a0e4a801fc3
```

spanning-tree (全局启动生成树协议，默认的生成树的类型为MSTP，防止交换机自身或交换机之间的环路)

loopback-detection interval-time 240 30 (全局开启环路检测功能，设置环路检测的时间间隔。防止交换机下接的HUB上的环路)

loopback-detection control-recovery timeout 240 (全局开启环路恢复时间)

```
!
ip dhcp snooping enable
(全局启动Dhcp snooping功能)
ip dhcp snooping binding enable
(全局启动DHCP Snooping绑定功能)
```

```
vlan 1
vlan 2
name management
!
```

```
vlan 20
Interface Ethernet0/0/1
spanning-tree portfast (将端口设置为生成树指定端口，使其快速成为转发端口)
```

```
switchport access vlan 20
loopback-detection specified-vlan 20
(将端口设置为在vlan20中检测环路)
```

```
loopback-detection control shutdown (当端口检测到环路后将端口关闭，并在240秒后恢复)
```

```
ip dhcp snooping binding user-control (设置端口的DHCP绑定模式，防止私自接DHCP服务器和私自固定IP地址)
```

```
!
!
!
Interface Ethernet0/0/24
spanning-tree portfast
switchport access vlan 20
loopback-detection specified-vlan 20
loopback-detection control shutdown
ip dhcp snooping binding user-control
!
```

```
Interface Ethernet0/0/25
switchport mode trunk
```

```
ip dhcp snooping trust (设置端口为DHCP snooping安全端口，即容许接受DHCP请求，也就是允许接DHCP服务器)
```

```
interface Vlan2
ip address 192.168.2.3 255.255.255.0
ip default-gateway 192.168.2.1
no login
end
```

交换机经配置重新启动后，经过检测1-24个端口均可正常上网使用。然后再用一根网线连接到DCS-3950-26C交换机任意两端口上，或者用一根网线连接到普通交换机的两端口上，再用一根网线上联到DCS-3950-26C交换机某端口上(如图3所示)构建产生网络环路的环境。登入DCS-3950-26C交换机查看可见形成环路的端口已发生阻塞(Blocking)，同时检测交换机其他端口均可正常上网。实验表明STP协议发挥了作用，有效地防止网络环路的发生，保障了网络的正常运行。

河海大学校园网络在接入层交换机未启用STP协议之前，网络环路故障频出，不仅花费大量的人力查找和排除故障，还严重地耽误了其他用户对网络的使用。而在启用STP协议之后，再未出现过环路故障导致的网络瘫痪问题。实验表明STP协议的启用，不仅保障了网络的安全和可靠的运行，还极大地减少了网络运维的工作量。

(作者单位：1河海大学信息中心；2河海大学图书馆)

syslog 搭建服务器登录日志系统

文 / 马庆忠

网络安全，一直是重点且热门的话题，特别在信息化发达的年代。一个合格的系统管理员，不仅要提供客户满意的服务，也要经常防范来自校内校外的安全攻击。

由于现在安全攻击防不胜防，管理人员经常在服务器遭到破坏之后才去清查服务器。首先都会检查服务器的登录日志，但是一般黑客都不会留下明显的痕迹。可以用 Red Hat Enterprise 5.4 自带的 syslog 服务搭建一个记录 Linux 和 Windows 登录日志集中的服务器，并且对日志进行简单地处理，以达到报警的功能。这不仅可以第一时间知道可疑的登录情况，也可以集中查看服务器的登录情况，更加了解服务器的使用情况。

syslog 服务器配置

首先，配置 Red Hat 上自带的 syslog 服务，使它能够记录来自其他服务器的 log 信息。

1、编辑 /etc/sysconfig/syslog 文件，修改 SYSLOGD_OPTIONS 选项，如下：

```
# Options to syslog
# -m 0 disables 'MARK' messages.
# -r enables logging from remote machines
# -x disables DNS lookups on messages recieved with -r
# See syslogd(8) for more details
SYSLOGD_OPTIONS="-r -x -m 0"
```

2、修改后重启 syslog 服务，使配置生效，如下：

```
[root@localhost ~]# service syslog restart
```

3、如果启用了 iptables 防火墙，确保 udp 514 端口可以被访问。可以在 etc/rc.local 中增加如下脚本，开放 udp 514 端口

```
iptables -I RH-Firewall-1-INPUT -s 192.168.1.0/24 -p udp --dport 514 -j ACCEPT
```

其中，RH-Firewall-1-INPUT 是 Red Hat 自带的 chain，192.168.1.0/24 网段是需要监控的服务器所在的网段。

4、/etc/syslog.conf 是 syslog 的默认配置文件，它允许指定好的每种类型的系统日志存放到指定的存放点，由于只记录登录日志，只需指定 authpriv.* 项的存放点即可。

```
# The authpriv file has restricted access.
```

```
authpriv.*
/var/log/syslog.pipe
```

/var/log/syslog.pipe 是一个命名管道，使服务器接受的信息可以传给脚本处理。

配置 Linux 客户端

配置好服务器后，需配置客户端，使客户端的 log 信息可以发到服务器上。用户只需指定 authpriv.* 项的信息传到服务器，具体如下：

```
# The authpriv file has restricted access.
authpriv.*@192.168.1.1
```

这里的 192.168.1.1 就是 log 服务器的 IP，“@”符号表示发送到远程主机。重启客户端的 syslog 服务使配置生效。

用 logger 测试一下配置是否成功

```
[root@metalib ~]# logger -p authpriv.notice "Hello, this is a test"
```

在服务器端监听管道

```
[root@localhost ~]# cat /var/log/syslog.pipe
Sep9 18:35:21 202.192.155.20 root: Hello, this is a test
```

如上所示，则表示已成功。

配置 Windows 客户端

对于 unix 类主机之间的记录日志，由于

协议、软件和日志信息格式都大同小异，因此实现比较简单，但是 Windows 系统则不同。因此，我们需要第三方软件来转换 Windows 的日志——evtsys（全称是 evntlog to syslog）。

下载地址为：<https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys/> 根据系统的版本下载 32 位和 64 位的程序。

解压后是 evtsys.dll 和 evtsys.exe。

把这两个文件拷贝到 c:\windows\system32 目录下。

打开 Windows 命令提示符

```
C:\>evtsys -i -h 192.168.1.1
```

-i 表示安装成系统服务

-h 指定 log 服务器的 IP 地址 启动该服务

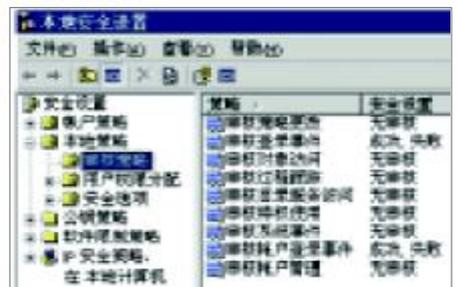
```
C:\>net start evtsys
```

如要卸载，则

```
C:\>net stop evtsys
```

```
C:\>evtsys u
```

打开 Windows 本地安全策略，修改本地策略中的审核策略，如下图所示：



用户只审核登录事件，所以只审核“审核登录事件”和“审核账户登录事件”即可。

Windows 的配置完成，还需再配置一下服务器的 syslog 配置文件，因为 evtsys 是以 daemon 设备发送到服务器上的。因此，在 /etc/

syslog.conf中需加入以下配置:

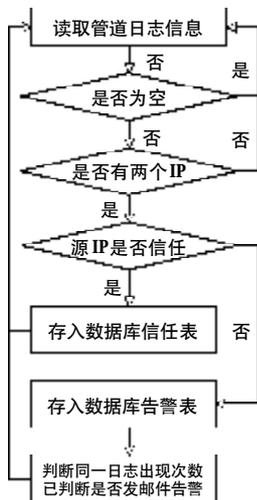
```
# for windows syslog
daemon.notice /var/log/syslog.pipe
```

关于syslog记录设备可以参考syslog文档。

分析处理接受的日志信息

现在,服务器和客户端的配置都已完成,所有客户端的登录日志都会发送到日志服务器上。但是Windows此时也会发送很多非登录日志,而且目前日志只是发送到命名管道上,所以还需再由一个脚本在后台不断分析管道中接收的日志。

下面是一个分析日志的流程图,当然读者可以根据自己的需求进行修改。



是否有两个IP: 因为Windows会发送很多非登录日志,可以根据日志中是否含有两个不同的IP地址来筛选。此判断比较简单,可以根据登录日志的格式再做进一步筛选。

源IP是否信任: 一般用户都有属于自己的工作网段,那么非工作网段都列为不信任网段,这样可以使用户在查询时比较方便。

是否发邮件告警: 如果非信息网段出现不断尝试登录的日志信息(可以设为5次),则发邮件告警。

具体的脚本如下:

```
[root@localhost ~]# cat /var/log/filter_log.sh
#!/bin/sh
if [ ! -p /var/log/syslog.pipe ]
then
mkfifo /var/log/syslog.pipe
fi
ip_temp="1.1.1.1"
ip_count=0
today=`date +%Y-%m-%d`
while read msg < /var/log/syslog.pipe
```

```
do
if [ ! "$msg" ]
then
continue
else
ips=`echo $msg | awk -v RS="[:=]" '/[0-9]+\.[0-9]+\.[0-9]+\.[0-9]/&&! a[$0]++`
ip_d=`echo $ips | awk '{print $1}'`
ip_s=`echo $ips | awk '{print $2}'`
if [ ! "$ip_s" ]
then
continue
else
time=`echo $msg | awk '{print $3}'`
date=$today "$time"
log_event=`echo $msg | cut -d ' ' -f5`
temp=`echo $ip_s | cut -d '.' -f1-3`
if [ "$temp" = "10.10.1" ] || [ "$temp" = "192.168.1" ]
then
`mysql -uroot -proot -D syslog -e "insert into syslog (log_time,log_ip,log_event) values('$date','$ip_d','$log_event')"`
else
if [ $ip_s = $ip_temp ]
then
ip_count=`expr $ip_count + 1`
else
ip_count=0
ip_temp=$ip_s
fi
if [ "$ip_count" -lt "5" ]
then
`mysql -uroot -proot -D syslog -e "insert into syslog_warn (log_time,log_ip,log_event) values('$date','$ip_d','$log_event')"`
elif [ "$ip_count" -eq "5" ]
then
`echo -e "From: Warning <test@test.com>\nTo: test@stu.edu.cn\nSubject: $ip_d warning\nMsg" | sendmail -t`
fi
fi
fi
done
```

在数据库中,必须建立两个表,即上述所提的信任表和怀疑表。

```
mysql> create database syslog;
mysql> create table syslog( id int unsigned not null auto_increment primary key, log_time datetime, log_ip varchar(30), log_event varchar(512) );
mysql> create table syslog_warn( id int unsigned not null auto_increment primary key, log_time datetime, log_ip varchar(30), log_event varchar(512) );
```

然后执行脚本测试,如果登录受监控的服务器后,在数据库中可以看到新插入的日志记录,则表示已成功。

必须让脚本在服务器开机时执行,需修改/etc/rc.local脚本,增加如下指令即可:

```
./var/log/filter_log.sh &
```

后续处理及扩展

1. 有了数据库的记录,可以写一个简单的网页来查询记录,方便监控和发现可以登录情况。

2. 可以记录更多更全面的日志,并且利用脚本分析日志信息再插入相应的表,以达到监控服务器全部日志的目的,可以使管理人员更加了解服务器使用情况。

3. syslog也可以记录交换机设备的日志,如下所示是记录cisco交换机日志的配置:

```
logging trap warnings
logging source-interface Vlan1
logging 10.10.202.247
```

(作者单位为汕头大学图书馆)

下一代互联网论坛开幕 赛尔网络体验中心精彩呈现

本刊讯 2010年9月13日-14日,“2010

下一代互联网发展和应用论坛”在北京大学英杰交流中心举办,吸引了来自互联网业界的400多名专家和学者,以及高校一线技术人员地参与。

赛尔网络积极参会,了解各高校对下一代互联网的业务需求、技术需求以及学校网络现状,力求为高校的科研提供更高质量的信息保障。会议同期,赛尔网络现场搭建了下一代互联网体验中心,得到与会代表高度关注与好评。

大会现场“赛尔网络下一代互联网体验中心”提供IPv4/IPv6双栈网络环境。通过IPv6高速网络,与会者能够登录到接入CNGI-CERNET2的百余所高校的对应主页,查阅各高校提供的丰富的软件资源,在线观看高清视频,还可以快速连接到欧洲GEANT2、美国Internet2、亚太APAN等国外的IPv6网站,畅享下一代互联网。

惠普“教师全程关怀”计划再掀热潮

本刊讯 9月8日,以“惠恩师、普服务”为主题的惠普“教师全程关怀”计划再掀热潮,惠普服务工程师走进校园,在国家教育行政学院为教师们提供了电脑免费清洗、维护以及使用技巧介绍等众多专属服务。

与此同时,从9月10日~9月17日,覆盖全国的惠普“教育金秋服务周”活动也将同步展开,教师们还可以到全国各区域惠普“金牌服务中心”体验多种教师专享服务:免费清洁保养服务,免排队优先服务,电话预约可免费取机服务,以及当场无法完成维修的机器可免费送机服务等。

使用 EMOS 搭建 Extmail 邮件服务器

文 / 周素林¹ 王宇²

使用 EMOS 搭建 Extmail 邮件服务器是目前搭建 Extmail 服务器最方便的方法。首先, 安装 EMOS 操作系统, 安装完成之后, 需要用户对邮件服务器进行简单地设置, 例如, 邮件服务器的域名, 数据库类型等。设置完毕后, 邮件服务器就能正常工作。但是, 为了更加贴近用户自身的要求, 用户需要对邮件服务器软件进行版本升级以及个性化的设置。

升级 Extmail 的版本

1. 下载最新的 Extmail 源码

目前最新的是 1.2 版本, 并上传到服务器上。

2. 备份原 Extmail 目录

命令: `mv -f extmail extmailbk`

3. 解压缩下载的 Extmail. tar. gz 文件到 /var/www/extsuite/ 并改名 Extmail

命令: `tar xzvf /extmail. tar. gz /var/www/extsuite/`

命令: `mv extmail- 1.2 extmail`

4. 复制生成一份 webmail. cf 文件

命令: `cd /var/www/extsuite/extmail`

命令: `cp -f webmail. cf. default webmail. cf`

5. 更改 webmail. cf 文件

主要修改数据用户名和密码, 如 mysql 用户名密码 免费注册 语言 网络磁盘等。

6. 修改权限 cgi 文件夹的权限

命令: `chown -R vuser. vgroup /var/www/extsuite/extmail/cgi/`

`chown -R vuser. vgroup /var/www/extsuite/extmail/tmp/`

新的 Extmail 下没有 TMP 文件 需要自己建立 同时在修改权限。

7. 升级成功

对 Extmail 进行个性化的设置

1. 页面 Title

修改文件: `/var/www/extsuite/extmail/lang/zh_CN`

修改位置: `%lang_login = (meta_title => 欢迎使用 'xtMail',`

2. 更改 Logo

修改文件: `/var/www/extsuite/extmail/html/default/images/logo. gif`

修改内容: 替换成需要的 Logo 图片文件

3. 鼠标指向 Logo 的显示

修改文件: `/var/www/extsuite/extmail/html/default/index. html`

修改位置: `<DIV class=lg><MG alt=ExtMail>`

4. 技术支持和自愿捐助连接

修改文件: `/var/www/extsuite/extmail/html/default/index. html`

修改位置:

```
<div class=donate> <a href= "http://www. extmail. org/support/<%LANG%>/index. html " target= " - blank " > <b><%support_link%></b></a> | <img style= " vertical- align: middle " src= " /extmail/images/donate. png " > <a href= " http://www. extmail. org/donate/" target= " - blank " ><b style= " color: # 5678A6 " ><%donate%></b></a></div>
```

5. 欢迎词

修改文件: `/var/www/extsuite/extmail/lang/zh_CN`

修改位置: `%lang_login = (wsplash => 快速可靠高性能 I/O 开源 MAIL 开足马力迈进中... "`

6. 页面底部信息

修改文件: `/var/www/extsuite/extmail/html/default/index. html`

修改位置: `<div class=pb>Powered by <%VERSION%> ? 2004- 2006 ExtMail. Org Runtime: <%TIME%></div>`

7. 设定默认域名

修改文件: `/var/www/extsuite/extmail/`

`html/default/index. html`

修改位置: `<TD><INPUT TYPE= " text " class= " input_n " NAME= " domain " ></TD>`

修改结果: `<TD><INPUTTYPE=>text " class= " input_n " NAME= " domain " value= " example. com " </TD>`

8. 修改 IP security 为默认不选择

修改文件: `/var/www/extsuite/extmail/lang/zh_CN`

修改位置: `<td><input type=checkbox checked name=nosameip><%ip_security%>`

修改结果: `<td><input type=checkbox name=nosameip><%ip_security%>`

9. 欢迎使用

修改文件: `/var/www/extsuite/extmail/lang/zh_CN`

修改位置: `%lang_login = (welcome_index => 日队 褂肱 xtMail!`

10. POP3 和 SMTP 设置信息提示

修改文件: `/var/www/extsuite/extmail/html/default/index. html`

修改位置:

`POP3 :& nbsp; & nbsp; pop3. yourdomain. com
`

`SMTP :& nbsp; & nbsp; smtp. yourdomain. com
`

11. 特点介绍

修改文件: `/var/www/extsuite/extmail/lang/zh_CN`

修改位置:

`%lang_login = (intro2 => ' 快速而可靠
引入索引缓存 (Cache) 技术和高效核心, WebMail 操作疾步如飞', intro5 => ' 高性能 I/O
轻松应付>1GB 邮箱/200M 附件, 远强于流行的各式 php webmail',`

12. 关闭注册

修改文件: `/var/www/extsuite/extmail/webmail. cf`

修改位置: `SYS_SHOW_SIGNUP = 1`

修改结果: `SYS_SHOW_SIGNUP = 0`

(作者单位: 1泰州机电高等职业技术学校 2泰州师范高等专科学校教育系)

高校数据中心：技术与管理并重

文/荆雪蕾 韩味华 杨玉杰

校园网和数据中心

聊城大学校园网经过十多年快速发展,校园网覆盖了两个校区的100多座楼宇,保证校园监控系统、一卡通系统、办公自动化系统、教务系统、邮件系统、档案系统、招生就业系统和学校主网站地畅通运行。

网络信息中心构建了自己的数据中心,配置了各自独立的IT基础保障环境,包括机房、空调、UPS、网络、服务器、存储等。

构建高校数据中心是教育行业信息化平台建设的一个里程碑。那么,数据中心建设的目的是什么?从表面上理解,是为了数据集中。而数据的存在是为了应用,所以建设数据中心的长远目标可以看成是为应用集中做基础。

校园网作为整个信息化建设的重要基础设施,其目标就是要为高校教学、科研工作搭建一个高速、开放、智能的信息网络平台。而随着高校信息应用系统不断增加,对资源和信息整合的需求极为迫切,高校数据中心软硬件资源整合逐渐成为关注的重点。

数据中心建设探索

聊城大学网络信息中心的数据中心拥有单独机房,成立后进行了不懈的探索。实践经验总结如下:

(1) 网络信息中心很重要的一项工作是用电安全。学校购置了60KW和30KW的两个UPS设备,60KW的UPS可以在出现问题时及时的发手机短信报警给网络信息中心相关负责人员。同时,每天均有人员负责检查和巡视。

(2) 为了使数据中心的服务器等各种设备在适宜的温度和湿度环境下运行,可以购置空调设备。尤其是购置精密机房空调,使机房中的温度和湿度较为恒定。同时,相关负责人员每天都对机房的情况进行认真检查

和巡视。

(3) 以“保安全、保运行、保畅通”为目标,努力保障校园网络安全、可靠和畅通地运行。在数据中心设置了高端防火墙,以增强服务器等的安全性。每个机柜上都放置千兆可网管交换机,每个交换机均是光纤接入上联交换机,服务器用双绞线连接到各自机柜上的交换机端口。

(4) 校园监控系统、一卡通系统、办公自动化系统、教务系统、邮件系统、档案系统、招生就业系统和学校主网站等重要应用都拥有自己单独的服务器。网络信息中心负责服务器托管,各个负责单位有专职人员进行管理。

(5) 聊城大学网络信息中心购置了高端存储设备用于重要数据和应用的备份。在某台重要服务器出现问题后,能及时地妥善处理后续工作。如:邮件系统的备份就直接实时存储在存储设备中,当邮件系统出现问题时,由存储设备中的备份做基础就很快恢复了邮件系统的运行。

(6) 在服务器上应用虚拟化技术,节省了物理设备和存放空间,减轻了用电等资

源消耗。

(7) 流程规范文档化,积累的与数据中心相关的流程和规范都应该文档化,不能记在个人的脑海中。同时,需要提供文档共享的机制,以确保大家都能看到并理解各个流程规范,这样才能在日常工作使流程和规范得到落实。

(8) 日常操作程序化,对于经常性的操作,要进行详细分析,制定出合理的流程。一个清晰的流程可以确保日常操作的服务质量,不因人而异。例如:关于一卡通系统的数据备份就有清晰的流程文档,每个值班的人员均可以按照说明恰当操作。

(9) “三分技术、七分管理”能更好的来形容此项工作。网络信息中心制定了详细的规则制度,并努力施行。技术与管理相辅相成,技术不断提高使管理更便捷,管理不断优化使技术能更好的被应用。数据中心的理想目标是:面向学校的各个应用提供IT基础保障和运行维护服务,将技术、产品、服务和解决方案完善结合起来提供和支持一个持续可用的环境,以确保应用面临变化时能够保持稳定和高效。

聊城大学网络信息中心数据中心的建设仍在探索中,无论数据中心建设到什么阶段,都需要有相应的运行维护管理体系和人员投入,都需要不断地提高技术与管理手段。

随着虚拟化、云计算以及绿色概念的盛行,新一代数据中心这个概念也随之出现。新一代数据中心与以往的数据中心有着截然不同的特点,以往的数据中心建设往往是一种工程建设,而新一代数据中心则要考虑自动化、节能等因素。数据中心的各个部分不再是独立工作的,而是可以互相联动。那么对于新一代数据中心的建设、运行、管理来说,只专精某一方面是不够的,必须要站在更高的层面上来发现与解决问题。

聊城大学网络信息中心数据中心会继续不断地前进,现在已经开始对高性能计算和虚拟化技术进行深入研究和学习以及应用尝试,相信会为新一代数据中心的建设应用奠定重要基础。

(作者单位为聊城大学网络信息中心)

SECRET

www.Liveworks.com

大型 集团 企业 集团 企业

集团 企业 集团 企业

