



稳固便捷的网络化知识库

思科高校数字图书馆解决方案



前言

随着计算机技术、现代通讯技术、网络技术在文献出版和信息传播领域内的广泛应用，传统的信息存储方式发生了质的变化。根据加州大学伯克利分校所做的年度研究报告，2002年全球新增数据信息量中，92%的数据信息是以磁介质作为存储方式的，包括个人电脑硬盘，计算机服务器和磁带机，而以纸张为存储介质的只占到不足0.01%。这也使传统的图书馆建设发生了翻天覆地的变化，这种变化虽然悄无声息，但却来势迅猛，触手可及。这种变化源于一种技术的发展和成熟，那就是数字化技术在图书馆的广泛应用，从而产生的数字图书馆。90年代以来，西方发达国家的图书馆正朝着网络化、电子化和数字化的方向发展。借助于网络通信和高新技术的发展，数字化图书馆的发展取得了巨大的进步，电子化信息的检索与提供，已成为越来越普遍的服务方式，以至出现了“数字图书馆”、“虚拟图书馆”等概念，并正在逐步成为现实。

数字化图书馆概述

图书馆数字化的发展

从国外发达国家图书馆数字化的历史来看，其经历了三个基本阶段。第一阶段可称为图书馆自动化发展的初级阶段，大约从60年代末、70年代初开始，以美国国会图书馆正式发行MARC II的机读目录为标志。第二阶段为图书馆在网上进行全球性、整体化的电子文献信息服务的阶段。这一阶段于1985年左右，以CD-ROM光盘和局域网开始在图书馆得到应用为主要标志，使人们开始可以在图书馆、办公室、实验室甚至家中访问图书馆的机读目录、光盘数据库和检索系统。第三阶段是图书馆自动化的高级发展阶段，也称为数字化图书馆阶段，90年代因特网的迅猛发展，将图书馆网上的电子文献信息服务推向了全球性服务的新阶段。

数字图书馆的优势

相对于传统的图书馆，数字图书馆具有以下几点显著优势：

- 信息储存空间小、不易损坏
- 信息查阅检索方便
- 图书资源网络化共享可以大大扩大馆藏
- 远程迅速传递信息
- 同一信息可多人同时使用

数字图书馆的建设模式

数字化图书馆是一个开放式的硬件和软件的集成平台，通过对技术和产品的集成，把当前大量的各种文献载体数字化，组织起来在网上服务。从理论上而言，数字图书馆是一种引入管理和应用数字化的物理信息对象的方法。它的功能有以下五项：

- 各种载体数字化
- 数据的存储和管理
- 组织对数据的有效访问和查询
- 数字化资料在网上发布和传送
- 系统管理和版权保护

以上五项，既是数字图书馆的基本功能，又是要使数字图书馆进入实用化的五项关键技术。而所有这些功能的基础，是一个高速安全可靠的数字图书馆网络架构。

高校数字图书馆建设的四个阶段和发展趋势

第一阶段——图书自动化管理：多数已实现

第二阶段——网络共享化

- 电子阅览室建设
- 网络的建设：常指与校园网的联通，实现校一级的统一管理、数据及资源的共享
- 信息资源库及设备的建设、电子文献资源的建设
- 网站的建设

第三阶段——统一管理平台

- 统一网络数字图书馆管理平台软件
- 全面开展数字化信息资源加工

思科高校数字图书馆解决方案

第四阶段——网络使用成熟标准化

- 实现网络用户上网使用的交互化, 提供使用的记录、提示和交流通道, 提供个性化使用的平台和空间
- 图书馆利用网络进行馆内工作的管理: 日常考勤考评、内部管理、OA 办公自动化等
- 图书馆利用自身在信息与资源的优势条件和组织能力, 开展为师生用户进行教学与科研的咨询服务和内容服务, 促进教学与科研的快速发展和成果实现

发展趋势

- 服务方式: 从传统图书馆以藏书借阅等读者上门服务为重点 -> 转向以电子文献信息资源的库存比例大幅上升、文献信息资源的网络化服务的大量增加、信息咨询服务的提供为重点
- 技术发展程度: 从图书自动化 -> 网络共享化 -> 加工数字化 -> 使用个性化、管理信息化、信息服务化

效益分析

建设一个现代化的网络数字化图书馆不仅是适应新形势的需要, 也是本馆数字化建设的重要组成部分。网络化数字图书馆建成后, 可为图书馆带来至少以下方面的效益:

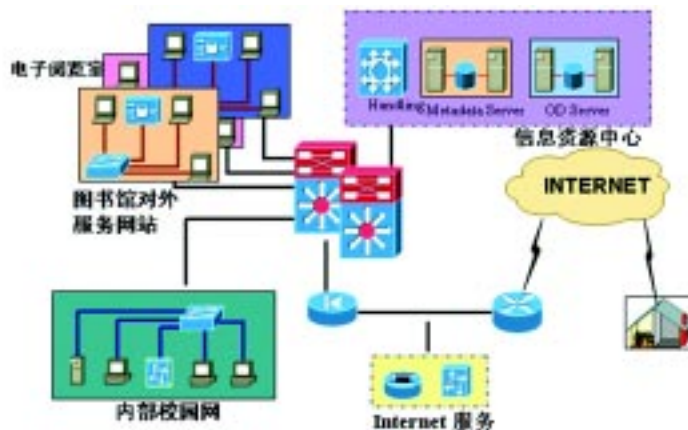
- 轻松地各种电子出版物、数据库存储管理起来, 组成一个强大的数字化图书馆
- 读者足不出户便可进行阅读和检索, 大大提高贵馆的自动化能力
- 80—500 个网络用户可在校园网上进行视频点播, 观看流畅生动的视频声像节目
- 可通过自制光盘系统制作适合校情内容的 CAI 教学辅助课件光盘让学生进行网上自学和教育, 提高师生上网学习兴趣, 从而提高学校整体素质
- 同时, 还可对外进行资源开放, 从而扩大学校的影响力, 创造经济及社会效益

高校数字图书馆网络架构

数字图书馆网络应用需求

底层网络基础架构是数字图书馆应用成功实施的关键成功因素。不能正确选择合适的网络基础架构将带来以下几个方面的问题: 系统传输延迟, 系统性能降低及高故障率, 过高的系统故障时间系统性能降低, 高故障率, 较长的系统故障时间, 对于管理者或用户的关键应用是不可接受的。此外, 如果没有正确的网络设计, 网络基础架构将很难满足高速发展的图书资源信息数字化存储和传输应用带来的网络扩张和升级能力。通过认真计划设计端到端的网络以提供校园范围内的连接, 可靠和扩展能力, 网络将能够满足数字图书馆系统初期实施和不断更新拓展。

图 1
典型图书馆局域网结构



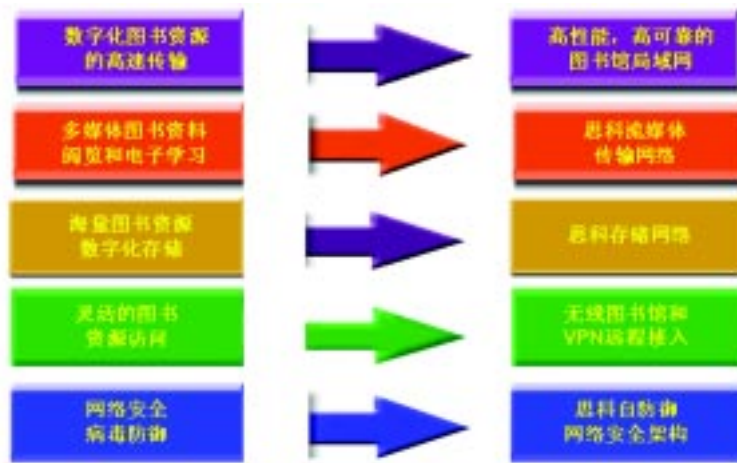
思科高校数字图书馆解决方案

一个典型的高校数字图书馆网络架构如上图所示,而在此架构之上运行的应用系统主要有以下几个:

- 校园网范围内的高速图书资源访问
- 多媒体阅览室和电子教室
- 图书馆对外服务门户网站
- 海量图书资源存储中心
- 通过 Internet 的图书资源共享和读者接入服务

而所有这些服务对于网络架构又都有其特殊的要求,这些要求引出了思科公司高校数字化图书馆解决方案中的具体部分。从图 2 我们可以看出思科产品和解决方案是如何对应于数字化图书馆建设的应用需求的。

图 2
数字图书馆应用需求与思科网络解决方案



高性能、好可靠的图书馆局域网

网络拓扑结构

图书馆网络主干是数据信息流动的动脉,同时还担负着信息流动的总调度任务。主干网从功能上来看包括几个方面:

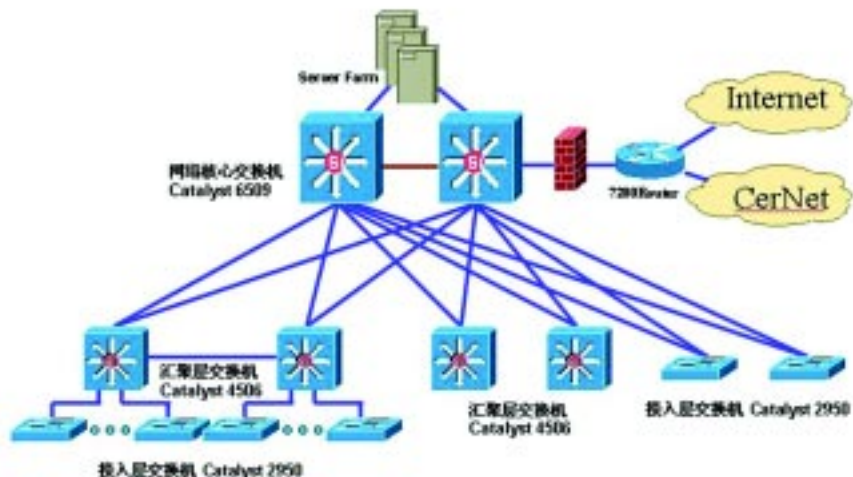
- 为图书馆内各个 vlan 子网间互联提供高速路由,实现核心数据高速交换。
- 为电子阅览室及电子学习教室提供基于流媒体的高速视频应用传输服务。
- 连接图书馆网络共享的高性能数字化信息资源服务器。
- 实现全网的系统管理和安全管理。
- 实现与外网的高速连接,实现网络教学资源共享。



思科高校数字图书馆解决方案

因而在网络的整体结构上，我们认为采用星形的网络拓扑是目前最好的选择，网络拓扑图如下：

图 3
星形网络拓扑图



如图 3 所示：网络的中心交换机应该选用背板速率足够满足大网络数据流和多业务流的需求的多层交换机，使网络的中心不会成为网络的拥塞点，同时还要保证网络的冗余性、灵活性以及出现网络故障时的快速收敛。因此我们选择了 2 台主交换机 6509 构成网络双中心，每台 6509 提供多达 9 个扩展插槽，背板速率可以根据扩充到 720G，同时多层交换能力也可以扩展到 400Mpps。同时每台 6500 上都选用了 4 端口 10Gb 以太网模块，它可以很好的支持 Cisco Catalyst 6500 上包括 10Gb 以太通道、流量分类和标记、流量策略、内容交换、入侵检测和大型帧在内的所有第二层、第三层和第四到第七层功能。

汇聚层的交换机选用 4500 交换机，可以提供 64G 的背板带宽和 40 兆的多层交换能力。汇聚层交换机通过多条千兆捆绑线路分别于两个中心交换机互联，同时通过千兆光纤线路连接接入层交换机。

对于大量的楼层接入交换机，我们选用 2950 系列交换机产品，在提供大量 10/100M 到桌面的连接同时，通过千兆线路上连汇聚层交换机或与核心交换机直接连接。

校园网通过 7206 路由器实现与教育网及 Internet 的互联。

网络主干技术选择

在图书馆网络建设中，网络主干技术的选择十分重要，它直接影响整个网络的性能。千兆主干，百兆到桌面的网络架构已经作为主流技术多年，也是最为常见的网络设计方案。但随着网络应用的不断发展，现在的网络应用早已从最初的点对点数据传输发展到今天的集中式数据访问，越来越多的多媒体视频流也开始大量应用于多媒体教室和电子学习系统，视频会议，视频监控等关键应用中，对网络的主干带来越来越大的宽带压力。随着网络技术的飞速发展，网络设备成本不断降低，千兆光纤网络成本已经与百兆网络相同，而作为全球网络设备的主要供应商 Cisco 公司，在其推出的下一代网络主干技术-万兆网络设备中，更将万兆网络的建设成本降到与千兆网络相当的程度，从而将今天的网络主干速度提升到了一个新的高度。因此，无论是作为现有网络的升级还是作为新建网络的设计，万兆网络主干技术都将是最好的选择。

思科高校数字图书馆解决方案



思科交换机 Catalyst 6509

拥有万兆骨干网络自然需要万兆的核心设备。在思科数字图书馆方案中，我们推荐在主要汇聚节点选用思科公司核心交换机产品 Catalyst 6509，主要的考虑因素如下：

系统高可靠性

当学校将内部教学应用及远程教育服务应用运行于网络平台上的时候，就要求网络系统能提供 7×24 小时的稳定可靠服务。网络还必须能满足数字图书馆网络不断增长的需要，可以伴随学校一同成长。本网络作为整个数字图书馆的核心平台，对安全可靠运行具有更高的要求。因此我们在考虑设备选型的因素时，高可靠性是第一位的。

Catalyst 6500 是思科公司为企业网络核心和高性能配线间环境设计的高可靠性网络平台。Catalyst 6509 利用系统平台、电源、控制引擎、交换矩阵和集成网络服务冗余性提供业界最先进的 1~3 秒的状态故障切换，从而减少关键业务数据和服务的中断。并可利用 Cisco EtherChannel® 技术、IEEE 802.3ad 链路汇聚、IEEE 802.1s/w 和热备份路由协议 / 虚拟路由器冗余协议 (HSRP/VRRP) 达到高可用性。

可扩展的性能

利用分布式 Cisco Express Forwarding (dCEF)，Catalyst 6509 交换机平台提供业界最高的交换机性能——720G 交换背板，400Mpps 包处理能力。Catalyst 6509 交换机支持多种 Cisco Express Forwarding (CEF) 实现方式和交换矩阵速率。在布线室、核心、数据中心、广域网边缘部署均可提供最优配置。

Catalyst 6500 系列中的所有型号都使用了统一的模块和操作系统软件，形成了能够适应未来发展的体系结构，由于能提供操作一致性，因而能提高 IT 基础设施的利用率，并增加投资回报。从 48 端口到 576 端口的 10/100/1000 以太网布线室到能够支持 192 个 1Gbps 或 32 个 10Gbps 骨干端口，提供每秒数亿个数据包处理能力的网络核心，Cisco Catalyst 6500 系列能够借助冗余路由与转发引擎之间的故障切换功能提高网络正常运行时间。

对新一代校园网络技术 IPv6 的支持

如今 IP 地址资源已经十分紧张。为了解决这一问题，下一代的地址分配技术 IPv6 将会很快得到应用。我国全部采用思科设备的第二代中国教育和科研计算机网 (CERNET2) 试验网已经开始投入建设。因此学校今天选择的网络设备能否很好的支持 IPv6 技术，是我们今天选型时必须考虑的因素。思科公司 6500 交换机目前就可以百分之百的支持 IPv6 技术，无论是硬件上还是软件上，因此可以使校园网在需要时很平滑的向下一代网络技术升级。

对万兆网络技术支持

2002 年 12 月思科公司开始在全球范围第一个正式发售符合国际标准的万兆以太网网络模块，目前在全球已拥有大量客户群，包括电信，金融和制造企业。国内也已经有许多装机用户，如：北京清华大学，北京师范大学，北京电信本地网小灵通工程等，经过一年多的市场运行考验，充分证明产品的稳定和技术可靠。思科公司于 2003 年 3 月 31 日向全球发布了端口密度最高的四端口万兆以太网网络模块，并与 2003 年 7 月中旬开始在国外领先开始销售。到目前为止已安装实施的用户有：

- Australia Woodside Petroleum Co., Ltd
目前部署了 5 块四口万兆卡，将来会再部署 5 块。
- Korea Telecommunication Corporation
目前部署了 4 块四口万兆卡，将来会再部署 200 块。
- 北京师范大学
目前部署了三块四口万兆卡，升级校园网。

思科高校数字图书馆解决方案



目前我们在数字图书馆项目中建议的6509交换机目前就可以支持万兆以太网模块,因此可以随时在需要时通过购置万兆以太网模块来实现校园网络骨干的平滑升级。

高速千兆桌面接入技术

大量的校园网用户正在开始使用新的PC和工作站,它们通常安装了10/100/1000网络接口卡(NIC),而不是过去常见的10/100卡。另外,具有速度更快的I/O系统和磁盘的、价格低廉的多处理系统也即将面世,这将会再次使网络的利用率接近或者超过它所能接收的极限。

此外,接近DVD画质的多媒体视频应用,三维产品设计软件,交互式视频会议系统等都要求桌面PC具有高带宽的网络接入能力。今天,Cisco高性能接入交换机已经可以为图书馆高速桌面应用系统提供通过双绞线的千兆连接,可以为高性能PC提供更好的连接服务。

大量百兆接入与少量千兆接入的组合,将是当今网络发展的必然。

链路备份

在网络的核心部分,我们设计了ETHERNET CHANNEL和千兆以太与万兆以太并行的环境,保证网络中存在可用的备份链路。一方面,在出现故障的时候,最大限度保证了网络的正常使用和最优化的网络性能。另一方面,在网络正常运行时,可以实现良好的负载均衡和流量规划。在出现故障时整个核心网路可以实现迅速自愈,以及网内节点或光纤设备发生故障时的网络传输及时恢复。当网络节点或链路发生故障时,可以在几秒钟的时间内恢复正常教学办公业务,这样的好处在于:

- 不需要人工干预,第3层路由协议自动重新收敛;
- 网络自愈非常快,几秒钟之内网络通讯便恢复正常,不中断IP业务;
- 故障排除以后,网络结构会自动恢复成最佳状态。

多媒体应用传输系统

视频点播系统

视频点播系统包括媒体播放服务器(Media Server),视频网络协议(Media Transport Protocol)及视频网络软件。视频网络协议对于整个点播系统至关重要,它必须与已有的网络协议(如TCP/IP、IPX)兼容,它要能控制、测量网络上视频数据的流量,保证平滑回放,不能出现任何停滞或间断,保证网络带宽利用率。

基于现在的网络的带宽、技术的成熟性等情况,我们建议在多媒体教室或局部VLAN中实现VOD。点播的方式可以采取服务器定期广播的方式发布视频信息,这种方式节约带宽;同时也可以采用终端点播的方式,这种方式比较耗费带宽,如果点数不多,在20~40个数据流时可以采用,对于MPEG-II的图像格式大约60MB的带宽。以上的两种方式根据学校的具体应用采用相应的实现方式。

基于网络的电子学习(E-Learning)

Cisco IP/TV解决方案是Cisco内容联网系列方案的成员之一,它能够为企业带来一个全面的网络视频系统。它能为台式PC、办公室和会议室提供电视质量的实时视频节目——包括管理广播,培训教学,企业电视,卫星节目等等。因为它采用了高效率的网络多播技术,所以企业可以通过它以最佳的网络性能,提供高质量的视频内容。

图 4
Cisco IPTV 网络学习系统应用实例

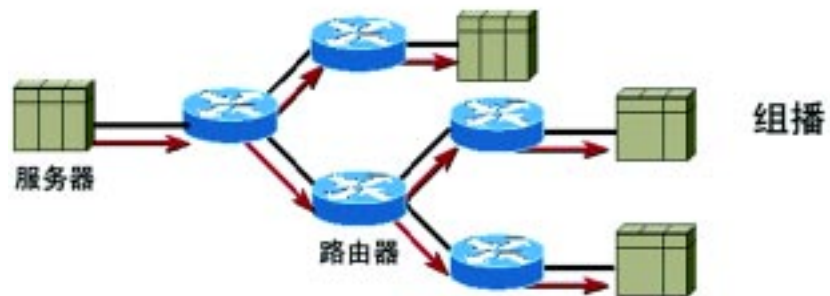


组播技术

校园网上实现的视频点播 (VOD)、可视电话、视频会议等视音频应用和一般应用相比,有着数据量大、时延敏感性强、持续时间长等特点。因此采用最少时间、最小空间来传输和解决视音频业务所要求的网络利用率高、传输速度快、实时性强的问题,就要采用不同于传统单播、广播机制的转发技术及 QoS 服务保障机制来实现,而 IP 组播技术是解决这些问题的关键技术。

IP 组播 (也称多址广播或多播) 技术,是一种允许一台或多台主机 (组播源) 发送单一数据包到多台主机 (一次的, 同时的) 的 TCP/IP 网络技术。组播作为一点对多点的通信,是节省网络带宽的有效方法之一。在网络音频 / 视频广播的应用中,当需要将一个节点的信号传送到多个节点时,无论是采用重复点对点通信方式,还是采用广播方式,都会严重浪费网络带宽,只有组播才是最好的选择。组播能使一个或多个组播源只把数据包发送给特定的组播组,而只有加入该组播组的主机才能接收到数据包。如图 5 所示:

图 5
IP 组播示意图



思科高校数字图书馆解决方案

目前，IP组播技术被广泛应用在网络音频/视频广播、AOD/VOD、网络视频会议、多媒体远程教育、“push”技术（如股票行情等）和虚拟现实游戏等方面。

无线图书馆

对于校园网络的用户来说，移动性强是一大特点。因此我们可以在校园网内部署无线接入网络，实现教师和同学们的随时随地网络资源访问。如图6。

图6
(左图) 建筑物内部无线网络
(右图) 建筑物间无线网络



Cisco Aironet 1100/1200 系列为大楼内和大楼到大楼间的无线局域网 (WLAN) 应用提供了基于标准、经过实践的高速无线网络解决方案。

图7
思科无线网络产品



Cisco Aironet 1100/1200 系列产品易于管理，可为那些要求移动性、灵活性和自由性的 WLAN 用户提供完整的解决方案。对于校园园区网络来说，思科无线网解决方案在为用户提供先进的性能和认证机制同时保证了无线网络的灵活和可靠性，提供给校内师生充分的便利：

- 方便老师、学生在学校的任何地方随时随地访问电子图书馆等网络资源，方便师生的工作和学习，不受场所的限制。
- 由于工作需要，学校管理人员需要在不同地点办公，方便的网络接入能够大大提高工作效率。

- 因为建筑物的限制，例如因为教师办公室座位布局，临时性地点等原因，有些不能或不方便立即实施传统的布线方式联网。采用无线网络，类似问题迎刃而解。
- 无线网络技术支持视距内的大楼到大楼间远程网络连接，能够避免铺设光纤所需的昂贵费用，同时不会产生挖掘、线路租用、道路使用权等问题，从而节约了网络建设投资和运营成本。

存储网络

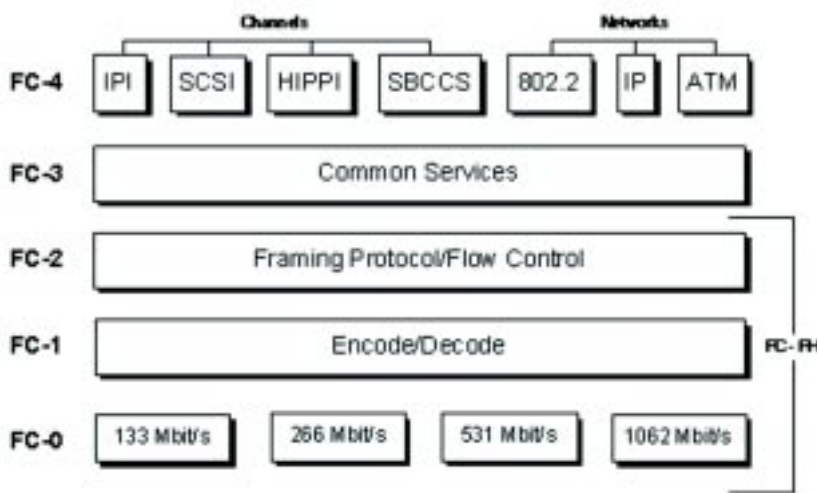
基于 Fibre Channel 的存储区域网（SAN）技术

在传统的基于 SCSI 技术的存储方式中，磁盘上的数据是服务器的专有资源，存储任务依赖于服务器及其所挂接的 LAN。由于这种技术本身的局限性以及存储任务对网络带宽的消耗越来越多，并行 SCSI 技术已渐渐不能够满足客户存储的需求。而 SAN 的推出首先使服务器同存储阵列之间的连接方式发生了根本性的变革，基于 Fibre Channel（同时具备网络和通道特性，能够以千兆位速度进行数据传输的技术）的 SAN 改变了传统服务器与磁盘阵列的主从关系。位于 SAN 上所有设备均处于平等的地位，任何一台服务器均可存取网络上任何一台存储设备，通过 Fibre Channel 高带宽和强大的 I/O 处理能力，SAN 技术在可连接性、可扩展性以及性能方面解决了 SCSI 技术无法解决的问题，成为存储领域具有强大生命力的新技术。

Fibre Channel 的结构

FC（光纤通道）结构定义为多层功能级，但是所分的层不能直接映射到 OSI 模型的层上。FC（光纤）通道的五层定义为：物理媒介和传输速率、编码方式、帧协议和流控制、公共服务以及上级协议（ULP）接口。

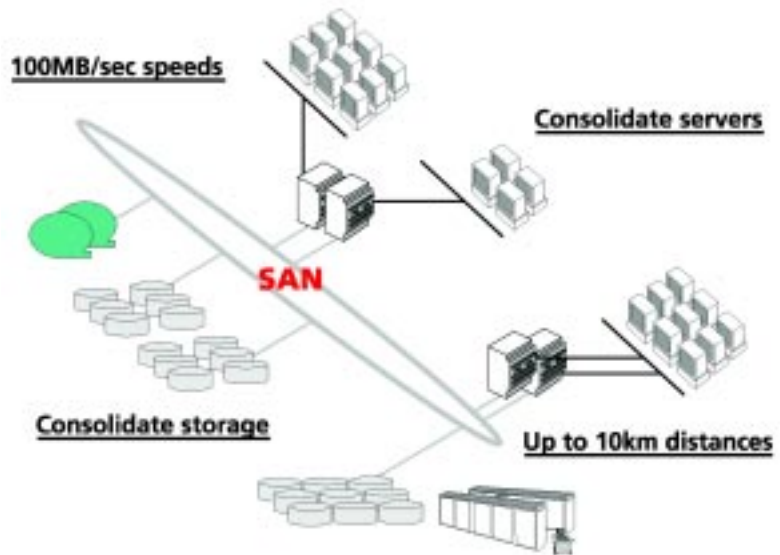
图 8



SAN 网络

存储区域网络（Storage area network-SAN）是建立在存储协议基础之上的可使服务器与存储设备之间进行“any to any”连接通信的存储网络系统。采用 SAN 可以实现在公司信息系统中的任何服务器、任何阵列子系统、任何磁带系统之间的互连。采用 SAN 可以建造一个存储池，实现多服务器共享一个阵列子系统、共享一个自动带库，实现数据的共享和集中的管理。

图 9



利用光纤通道技术实现的 SAN 的优势包括

- 方便连接和更远距离的传输：由于 SAN 方案是基于光纤通道技术，在使用光纤扩展连接设备时可达 30 公里，这就为企业级计算系统的异地存储系统规划提供了很大的便利条件。
- 更高速的数据传输：SAN 具有的 100MB/s 的环路带宽，提升了主机系统的存储带宽。
- 提供了更大的灵活性：多台服务器可共享 SAN 上的存储设备，可以根据需要扩展磁盘空间和改变存储类型。
- 减少了网络的复杂性：SAN 的更大的好处是减少了网络的复杂性。它可以腾出服务器的扩展插槽，允许用户不断地向其添加存储设备。

思科存储网络解决方案

Cisco MDS 9100 系列通过将思科智能化网络带入中小型 SAN 和数据中心边缘应用等领域，提升了光纤通道交换机的标准。Cisco MDS 9100 系列可以通过一个小巧的 1RU 机型，在成本、性能和企业级功能之间实现完美的平衡。Cisco MDS 9100 系列提供了 20 端口和 40 端口两种配置，因而可以提供多种存储环境所需要的端口密度。通过提供业界领先的可扩展性、可用性和管理功能，Cisco MDS 9100 系列让您能够以很低的 TCO 部署高性能的 SAN。通过在一个经济有效、外型小巧的交换平台上添加一组范围广泛的智能化功能，Cisco MDS 9100 系列可以满足中小型存储环境对于成本、性能、便于管理性和连通性的要求，并提供与 Cisco MDS 9500 多层控制器和 Cisco MDS 9216 多层光纤通道交换机的全面兼容，从而可以在大型数据中心核心-边缘部署中实现透明、端到端的存储服务供应。

Cisco MDS 9509 多层控制器所特有的交换架构让它可以无缝地集成新的传输协议，以获得最大限度的灵活性。支持 FC、iSCSI 和 FCIP。用户可以通过部署 2Gbps 光纤通道使用高性能的应用，利用基于以太网的 iSCSI 以低廉的成本连接到共享的存储空间，以及用 FCIP 在数据中心之间建立连接。CISCO 的 MDS9500 产品得到 HP, IBM, EMC, HDS 的认证，为用户提供可靠、可用的存储交换。

网络安全

对于校园网来说，建立了网络，必然会有人对它进行攻击，目前校园网的安全主要受到两方面的威胁，一个是来自黑客的诸如DDoS之类的攻击和黑客入侵，另外一个是有可能会被病毒感染，例如2003年造成很多高校校园网中心路由器瘫痪的sql蠕虫病毒等。对于前者，最有效的解决方法是设置内外网间防火墙（firewall）和入侵检测系统。而保证网络不受各种病毒的侵害，保证网络的正常运行，后者则应该配置网络防病毒软件。

基于 802.1x 的用户接入认证

对于网络用户的动态接入认证，本方案选用基于 802.1x 国际标准的网络接入层用户认证协议，并在此基础上进一步利用思科公司的扩展功能对用户的 VLAN 划分，带宽资源分配和访问限制等进行动态设置。从而实现用户可以在园区网内的任何位置用自己的用户名和密码登陆网络，并获得相应的网络访问权限和工作组划分。

图 10
标准的 802.1x 协议的流程图



当用户的电脑通过网线连入接入交换机时，交换机会向用户的电脑发送认证请求。用户的用户名和密码等认证信息由交换机传送到网络中的思科认证服务器 ACS 进行用户认证，当用户的信息通过认证后，交换机才会开放用户所连接的网络设备端口，从而用户才可以获得对网络的访问许可。

思科基于 802.1x 的扩展功能（IBNS）

思科支持 IEEE 802.1x 标准，并且可以提供下述扩展功能以进一步增强基于 802.1x 的用户认证服务：

- 基于 802.1x 的用户 VLAN 动态划分：
Cisco IBNS 能使基于用户的身份动态地将 VLAN 分配给相应端口。
- 带端口安全性的 802.1x
这种特性可以在 802.1x 端口上配置端口安全性。如果端口上只有一个介质接入控制（MAC）地址能够实现端口安全性，那么只有该 MAC 地址才能够通过 RADIUS 服务器认证。
- 802.1x 访客 VLAN
这种特性有助于让学校提供“访客”级网络接入。在启用这种特性之后，那些没有支持 802.1

思科高校数字图书馆解决方案



X 兼容主机的网络用户将被置于访客 VLAN 中，他们可以获得 Internet 的访问权限或只可以访问校园网主页信息等。需要访问敏感资源的用户可以通过 VPN 连接来进行数据安全访问。

- 带 ACL 分配的 802.1 X

无需损害用户的移动性或者造成管理损耗，就能够实现专门基于身份的安全性：严格限制用户对网络中某些网段的访问，限制对敏感服务器的访问，甚至限制可能使用到的协议和应用

防火墙

今天的防火墙不仅需要保护企业网络免受未经授权的外部接入的攻击，还必须防止未经授权的用户接入企业网络的子网、工作组和 LAN。FBI 的统计数据显示，70% 的安全问题都来自于企业内部。对于校园网络这个用户众多且行为随意性很大的环境，加强内部安全管理更为重要

集成模块

FWSM 安装在 Cisco Catalyst 6500 系列交换机或者 Cisco 7600 互联网路由器的内部，让这些设备的任何端口都可以充当防火墙端口，并且在网络基础设施中集成了状态防火墙安全。对于那些机架空间非常有限的系统来说，这种功能非常重要。Cisco Catalyst 6500 真正成为了那些需要各种智能化服务（例如防火墙接入、入侵检测、虚拟专用网（VPN））和多层 LAN、WAN 和 MAN 交换功能的客户的首选 IP 服务交换机。

适应未来需要

FWSM 可以支持 5Gb 的吞吐量，因而可以提供无与伦比的性能，让用户无需对系统进行彻底的升级，就可以满足未来的要求。在 Catalyst 6500 中最多可以添加三个 FWSM，以满足用户不断发展的需求。

可靠性

FWSM 建立在 Cisco PIX 技术的基础之上，并使用了同一个经过时间检验的 Cisco PIX 操作系统——一个安全的、实时的操作系统。FWSM 可以利用行之有效的 Cisco PIX 技术检测分组，从而可以在同一个平台上提供性能和安全的独特组合。

低廉的整体运营成本

FWSM 是基于 Cisco PIX 防火墙的，而且由于它是集成在设备内部的，大大减少了需要管理的设备数量，培训和管理成本都很低，可以提供所有防火墙中最佳的性能价格比。

易用性

Cisco PIX 设备管理器的直观的图形化用户界面（GUI）可以用于管理和配置 FWSM。在配置和监控方面，FWSM 可以获得思科管理框架和 Cisco AVVID（集成化语音、视频和数据体系结构）合作伙伴的支持。

FWSM 部署

FWSM 可以部署在企业园区的数据中心的网络拓扑中。FWSM 可以通过让用户和管理员以不同的策略在企业中设立安全域，提供一种灵活、经济、基于性能解决方案。

网络入侵检测

思科的集成化网络安全解决方案让机构可以防止他们的联网业务资产受到威胁，提高入侵防范的效率。这些解决方案中包括第二代思科入侵检测系统（IDS）模块，即 IDSM-2，它可以用在广泛部署的 Cisco Catalyst 6500 系列设备上。

主机和服务器网络安全保护

新一代思科安全代理网络安全软件可以为服务器和台式机计算系统（也被称为“终端”）提供威胁

思科高校数字图书馆解决方案

防范功能。思科安全代理与传统的终端安全解决方案的不同之处在于，它可以在恶意行为发生之前发现和阻止它们，进而消除潜在的已知和未知安全风险，防止其威胁到企业网络和应用的安全。因为思科安全代理采用的是分析行为而不是特征匹配的方法，因而这个解决方案能够以较低运营成本提供强大的保护。

思科安全代理位于应用和内核之间，它可以在最大限度地减少对底层操作系统的稳定性和性能的影响的情况下，最大限度地提高应用的可见性。这种代理的独特架构可以拦截操作系统对文件、网络、注册表资源和动态运行时间资源（例如内存页、共享库模块和 COM 对象）的所有调用。思科安全代理能够利用独特的智能，根据某个特定应用或者所有应用的不当或者不可接受行为的规则，关联这些系统调用的行为。正是这种关联和在此基础上对应用行为的理解使得软件——按照安全管理人员的指示——可以防止新型的入侵。

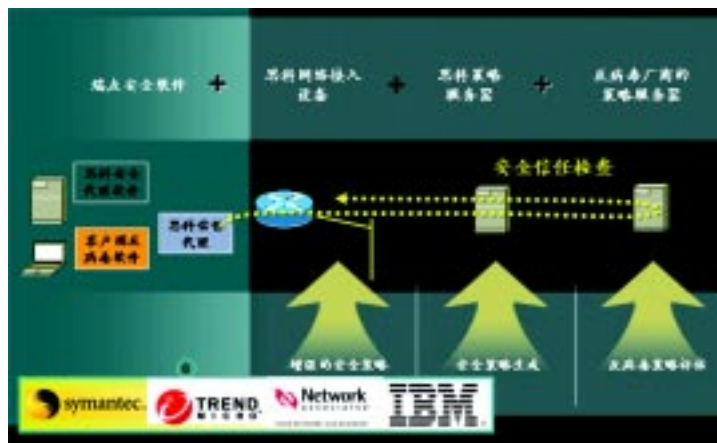
当某个应用试图执行某项操作时，思科安全代理将根据应用的安全策略检查操作，实时地做出是否允许或者拒绝这项操作的决策，并判断是否需要记录该请求。安全策略是 IT 和 / 或安全管理人员针对受保护的服务器和台式机或者对整个企业制定的一组规则。这些规则提供了对必要资源的安全应用访问。通过在缺省的服务器和台式机策略中集成采用了分布式防火墙、操作系统锁定、完整性保障、恶意移动代码防范和审核实践关联功能的安全策略，思科安全代理可以为存在对外连接的企业系统提供深层保护。

因为保护建立在阻止恶意行为的基础上，所以缺省策略无需升级就可以防止已知的和未知的攻击。关联是在代理和管理中心控制台上的。基于代理的关联可以大幅度提高准确性，在不影响正常活动的情况下发现实际的攻击或者网络滥用行为，在管理中心进行的关联可以发现全局式攻击，例如网络蠕虫或者分布式扫描。

网络准入服务

思科网络准入控制 (NAC) 是一项由思科发起、多家厂商参加的计划，其宗旨是防止病毒和蠕虫等新兴黑客技术对企业安全造成危害。借助 NAC，客户可以只允许合法的、值得信任的端点设备（例如 PC、服务器、PDA）接入网络，而不允许其它设备接入。在初始阶段，当端点设备进入网络时，NAC 能够帮助思科路由器实施访问权限。此项决策可以根据端点设备的信息制定，例如设备的当前防病毒状况以及操作系统补丁等。网络将按照客户制定的策略实行相应的准入控制决策：允许、拒绝、隔离或限制。一开始，NAC 将支持运行 Microsoft® Windows NT、XP 和 2000 操作系统的端点设备。

图 11
思科网络准入控制是如何运作的



思科高校数字图书馆解决方案



思科网络准入控制解决方案包括以下部件：

- 端点安全软件 (AV, Cisco Security Agen) 与 Cisco Trust Agent —— Cisco Trust Agent 从多个安全软件客户端收集安全状态信息，例如防病毒客户机软件，然后将这些信息传送到相连的思科网络，在那里实施准入控制决策。应用和操作系统状态信息，例如防病毒软件和操作系统补丁等级或委托书，都可以用于制定相应的网络接入决策。思科和 NAC 合作商将把 Cisco Trust Agent 与自己的安全软件客户端集成在一起。
- 网络接入设备——实施准入控制的网络设备包括路由器、交换机、无线接入点和安全设施。这些设备接受主机委托，然后将信息传送到策略服务器，在那里实施网络准入控制决策。网络将按照客户制定的策略实施相应的准入控制决策：允许、拒绝、隔离或限制。
- 策略服务器——策略服务器负责评估来自网络设备的端点安全信息，并决定应该使用哪种接入策略。Cisco Secure ACS 服务器是一种认证、授权和计费 RADIUS 服务器，它构成了策略服务器系统的基础。它可以与 NAC 合作商的应用服务器配合使用，提供更强的委托审核功能，例如防病毒策略服务器。
- 管理服务器——思科管理解决方案将提供相应的思科 NAC 组件，以及监控和报告操作工具。CiscoWorks VPN/ 安全管理解决方案 (CiscoWorks VMS) 和 CiscoWorks 安全信息管理解决方案 (CiscoWorks SIMS) 形成了此功能的基础。思科的 NAC 合作商将为其端点安全软件提供管理解决方案。

网络整体安全设计

要想构建起来一个强大、安全的网络，一方面我们需要有强大的硬件平台做支撑，此外更重要的是我们要有严密合理的整体安全体系。

首先我们要严格定义和分类校园网的各种信息资源有哪些，其重要程度如何，需要访问这些资源有哪些用户，不同的用户所拥有哪个等级的权限，同时将这些规则严格落实到最后防火墙 vlan 访问控制列表，arp 绑定等相应的规则的配置中去得以实现。对于从 Internet 过来的流量我们在 6509 上制定严密的限制性的安全策略采用特殊的许可与特殊的限制相结合，保证正常合法的流量的进入以及拒绝非法入侵。其次我们在本次校园网改造中所采用的网络设备，都支持 TACACS 的认证，应用这项技术可以使得对网络设备的访问控制可以集中设置、管理、授权。最后基于网络安全管理的重要性和防火墙保护范围的限制，这要求我们各个学校的管理部门进一步加强管理，制定相应的制度，加强防范，和防火墙一起配合，做到高度的安全。

这样我们可以很好地应用性能最为强大的防火墙设备，结合防火墙的应用策略，网络设备的安全性配置，安全管理等各个方面，构筑起一道强大的安全屏障来有效地保障校园网的安全。

总结

思科公司提供创建一个端到端应用网络所必需的所有产品——从 Internet 的核心设备到 WAN 边缘设备，从城域网到局域网，以及宽带接入设备。思科公司的产品战略是不仅为您提供一整套可以稳定协作的网络产品系列，还确保每个思科公司产品都保持领先——成为同类产品中的最佳产品。

思科在国内教育行业网络应用中具有领先优势，从 Cernet 的建设到全国大部分重点院校的校园网建设，思科均在其中扮演了重要的角色，并得到广大用户的充分认可。思科万兆网络正成为大量校园网络升级改造的首选。

思科愿以自己的先进产品和服务帮助学校建立适合自己系统应用的数字图书馆网络，从而使学校的信息化建设迈上新的台阶，在全球网络化教育大潮中立足于不败之地，并借助网络的力量在竞争中脱颖而出！



思科系统（中国）网络技术有限公司

北京

北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19~21层
邮编: 100738
电话: (8610)85155000
传真: (8610)85181881

上海

上海市淮海中路222号
力宝广场32~33层
邮编: 200021
电话: (8621)33104777
传真: (8621)53966750

广州

广州市天河北路233号
中信广场43楼
邮编: 510620
电话: (8620)85193000
传真: (8620)38770077

成都

成都市顺城大街308号
冠城广场23层
邮编: 610017
电话: (8628)86961000
传真: (8628)86528999

如需了解思科公司的更多信息, 请浏览<http://www.cisco.com/cn>

思科系统（中国）网络技术有限公司版权所有。

2005 ©思科系统公司版权所有。该版权和/或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS标识, Cisco Systems, Cisco Systems标识, Cisco Systems Cisco Press标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌, 名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。