中文题目：大连工业大学网络规划与设计

外文题目：NETWORK PLANNING AND DESIGN OF DALIAN INDUSTRIAL UNIVERSITY

毕业设计（论文）共 69 页（其中：外文文献及译文 14 页）图纸共 0 张

完成日期 2015 年 6 月　　答辩日期 2015 年 6 月

摘要

当今大连工业大学的学校规模和师生规模都有很大的提升，原先的网络设计与规划都有些落后，带宽需求和访问需求都不能满足现在的需求，所以要对学校的校园网络进行一个新的规划与设计。

本文就大连工业大学校园网的设计和建设首先进行需求分析，明确师生工作学习的需求以及要解决的问题，然后根据需求初步设计出网络规划方案，确定方案实施的可行性，然后使用核心层、汇聚层、接入层三层架构，提供 WEB、FTP、NAT、组播等服务，使用 OSPF、HSRP 来完成校园网络的架设。

本校园网络设计与规划的目的是使校园网实现互相通信、资源共享的基本功能，并且使校园网络具备良好的监控功能和易扩展的特性。

关键词：校园网；网络规划；网络设计

ABSTRACT

Today of Dalian Industrial University campus scale and the scale of teachers and students have greatly improved, network design and planning of the original are some behind, demand of bandwidth and access are unable to meet the demand now, so to on campus, campus network is a new planning and design.

In this paper, the design and construction of the campus network of Dalian industrial university first needs analysis, clearly the work of teachers and students learning needs and to solve problems and according to the needs of the preliminary design network planning, to determine the feasibility of the implementation of the program, and then use the core layer, convergence layer and access layer three layer architecture，provide services such as FTP, WEB, NAT, multicast, etc., using HSRP, OSPF load balancing to complete the erection of the campus network.

The purpose of this campus network design and program is to make the campus network realize the basic function of communication and resource sharing, and make the campus network have good monitoring function and easy to expand the characteristic.

Keywords: campus network；network planning；network design

目录

1 绪论

现如今，大连工业大学的办学规模，其中包括校园规模和在校师生的规模都有了一个大幅度提高，校园网络的负载越来越大，当今的校园网络规模已经限制了师生的发展，构建一个更加合理更加科学的校园网络显得格外重要。

校园网作为一种在学校教育中应用的局域网，其教育应用系统的建设应满足学校教学与管理工作的需要为目的，概括起来有以下四个方面的典型应用：首先，校园网能够为学生的学习提供网络服务，它拥有很多资源可以提供下载也可以让学生与外界联系。第二，校园网能够为教师提供科研和教学服务，它拥有海量的教学资源能够让老师下载并且还可以远程教学。第三，大学的校园网可以提供各种管理服务能够有效的管理各种教务。第四，大学的校园网既可以让校内的师生享受网络服务，也是对外展示学校的一个窗口。

2 需求分析

2.1 学校概况

大连工业大学校园网络是为全校教育和科研建立的计算机信息网络，利用各种网络设备和先进的网络技术将校园里的各类终端连接起来，实现资源信息的共享，通过中国教育网和科研计算机网(CERNET)与 Internet 互连。

大连工业大学校园网从 1999 年 9 月开始架设，在 2001 年 3 月 20 日建成运行，其网络中心在 2000 年 10 月建成，属于网络管理中心。2004 年 3 月与现代技术教学部网络工程专业、计算中心和计算机基础教研室一起，与校基础教学部、信息工程系共同组建了信息科学与工程学院。2005 年 9 月校园网进行了全网的二期建设升级， 2010 年 3 月网络中心划归现代教育技术部管辖。

2.2 需求调研

需求分析是所有工程生命周期的第一个阶段并贯穿于工程的整个生命周期。任何一个工程，实际都要经历需求分析、系统设计、建造实施、质量完善四个阶段。需求分析的目的是确定工程系统的目标。促使目标系统最大地满足用户需求。完整、准确、有效的需求分析结果是工程设计成功的基本依据之一。正确、有效的分析工作是一个工程能够顺利完成并取得预期结果的基本保证之一。

2.2.1 用户需求

大连工业大学现共有 14 栋教学楼、1 栋实训中心、1 栋行政楼。学校共有 8 个学院（部），现有在校全日制学生 18000 余人。各个学院须满足基本通讯需求和资源共享功能，且相互独立。1998 年学校建设了覆盖两个食堂和商业一条街的商务卡系统，2003 年成立了校一卡通服务中心归属校财务处管理，完成了一期改造和东山食堂的覆盖，2007 年 9 月并入校网络中心，2008 年 3 月完成了校园卡系统的扩充建设，2012 年 5 月校园卡系统进行了重建升级。

目前，校园网有无线接入点 107 个、有线接入点二万多个，线缆数十千米，几乎连接了学校的所有楼宇建筑；校园刷卡点 400 余个，覆盖了校内所有的餐饮、洗浴、机房、公寓和其它商务点；网络服务部 5 人，承担着校园卡结算管理、网络与校园卡窗口业务办理和报修、校园卡系统的运维和相关建设施工等工作，为学校近二万师生的日常生活、学习和工作提供着服务。另外，网络技术部现有人员 4 名，保障着学校约 880 台设备 365 天 24

小时的不间断运行，承担着校园网系统与应用平台的运维和建设工作，为全校教学、科研和管理的网络信息平台提供技术支持与运行安全保障。

学校行政机构分布如图 2-1 所示：

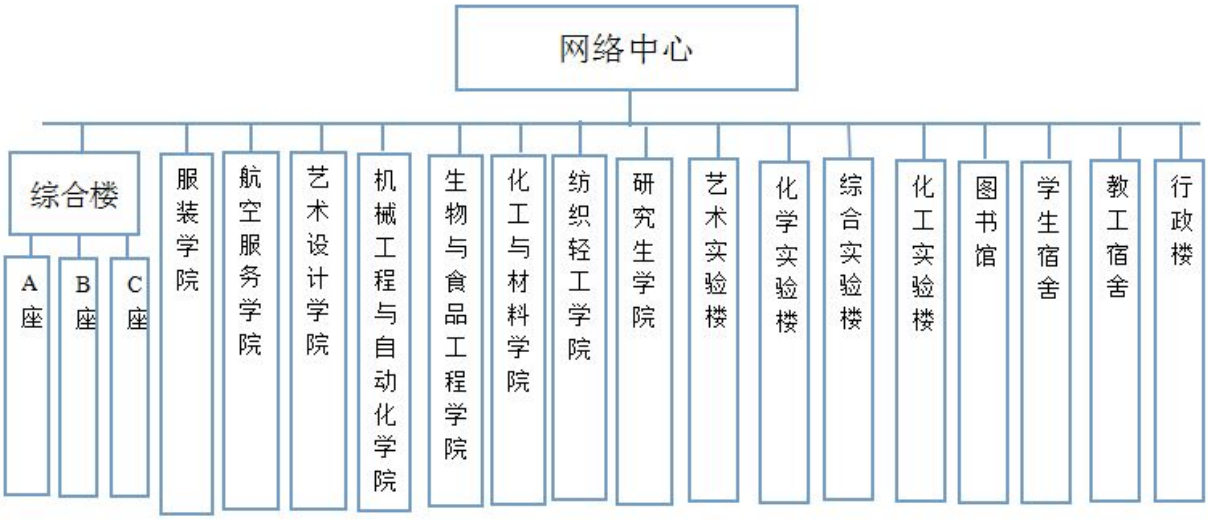

图 2-1 大连工业大学学院机构分布图

Fig. 2-1 Distribution chart of Institute of Dalian Industrial University

2.2.2 使用需求

学校的校园网建设就是让网络成功的接入到每个建筑中，学生宿舍与教师宿舍也要接入网络。所以校园网建设的重中之重就是让各个建筑接入成功的到外部网络。

校园网里的师生可以使用以下的几种服务，有远程教育、网上购物、各种娱乐活动、网上内容下载、网上工作等。所以，在校园里进行校园网建设，布设校园网络，是 21 世纪的大势所趋，校园网已经成为校园不可或缺的基础硬件设施。

大连工业大学校园网建设于 2000 年，满足了校园师生的基本网络需求，但随着社会科技的不断发展，当前的网络建设已经制约了学校师生的学习工作需要。

大连工业大学当前的学生老师人数 2 万左右。分布在同一个学校，师生多采用校园内部网络通讯，也使用 internet 连接外部网络内容，然而，网络流量大多产生于校园网的内部，所以网络要有很强的交换能力，校园网更会有传输和备份、多媒体应用、语音传输、OA 应用等多种带宽使用。

信息交互大体有两个方向的服务功能：Internet 通讯服务和园区通讯服务。Internet 通讯服务能够让任何一个办公场所的计算机实现网上搜索、寻找信息的能力，使老师能够开拓眼界，使用 internet 上的资料辅佐教学授课，改变教学手段，提高老师的教育教学、授课水平和研发能力。

同时可以使用 internet 资源来宣传学校，展现学校的教育本领与教育水平，展现老师的授课本领与科研水平，提升学校的办学形象。

园区通讯服务可以为教学授课和管理控制提供一些服务，为全校师生创造一个交流、学习的平台。

根据上面的需求完成以下方案：

（1）配置优秀的网络交换设备让每栋建筑间实现千兆光纤连接，使将来数据大规模传输不出问题。

（2）各个院系间不互相干扰，使其拥有相对独立的网络空间。

（3）具有高扩展性，使未来增加师生仍能够正常工作，技术可扩展性也是必须的。

（4）保证小量的增加师生数目以及技术升级等不会增加大量的投资成本二次投入。

2.2.3 布线研究

大连工业大学平面图 如图 2-2 所示：

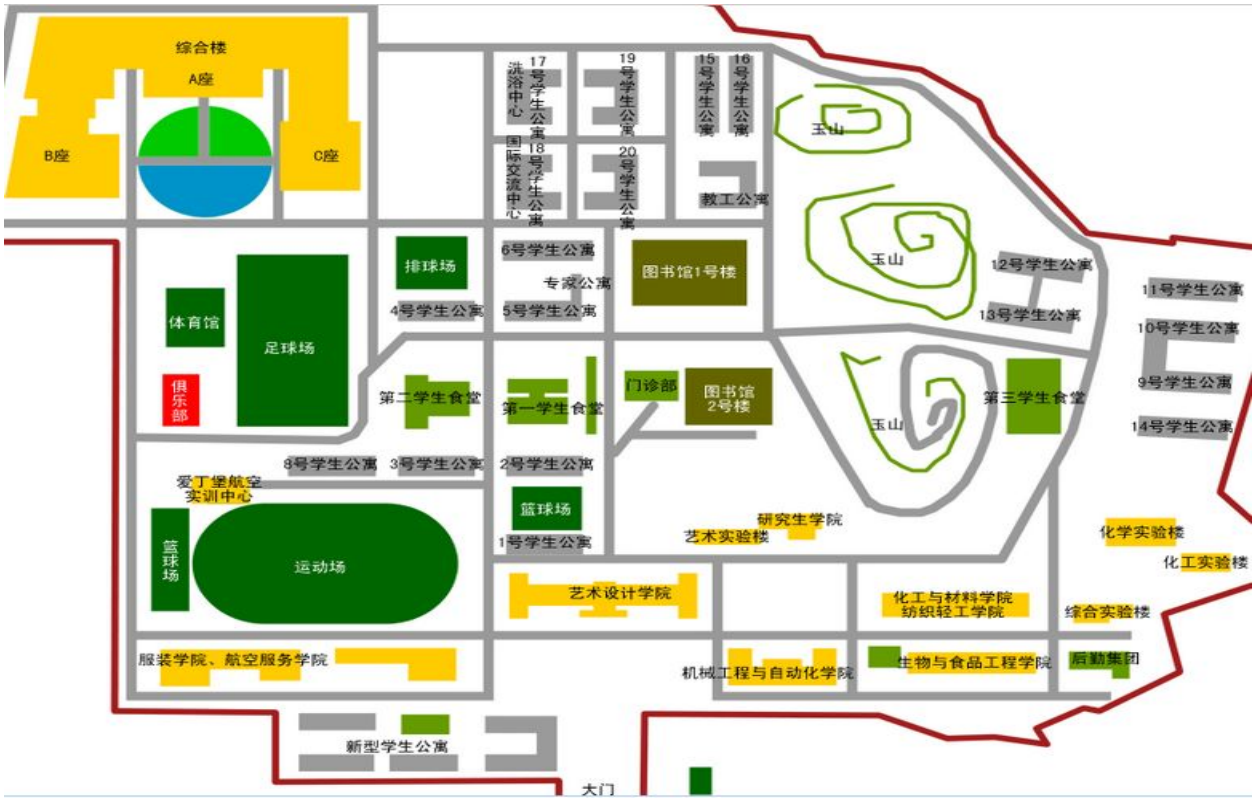

图 2-2 大连工业大学平面图

Fig. 2-2 Dalian Industrial University plan

大连工业大学大体上分为六个区域，因为各区域楼宇间距较远，不能采用双绞线布线，采用光纤布线效果更好。因为每个楼里房间都有网络接口，因此先不用考虑楼内的布线工

程。每个区域之间的距离在 100 米到 400 米不等因此使用多模光纤传输效果比较好。因为学校还有可能增加用户增加楼宇所以要使网络布线具有高可扩展性。

2.2.4 综合布线需求

因为大连工业大学具有很多建筑，规模很大，所以学校要采用一个高可靠性的布线系统，工作区和水平系统需要采用超五类原件，主干网络使用多模光纤，构成主干千兆以太网。能够满足如今对多媒体教学的基本需求，也为以后扩展整个网络更加方便。整个学校有一万个左右的信息点。针对以上要求，提出布线方案。校园里的布线建设要考虑到各个影响因素。想要将成一个科学的校园网络，就得在布线上面下狠功夫。

2.3 安全需求

2.3.1 可靠性需求

大连工业大学的校园网应该具有高可靠性，容易运行和可监控的特性。校园网的构建、选择、搭建和配置的每个环节都要确保没有差错，保证系统安全可靠。

并且，校园网还要具备更灵活的特点，具备更良好的可扩展性，不仅能在网络用户增加网络负载高时能够稳定运行，而且也要使校园网更容易升级扩展。

所以，校园网络的可靠性设计是重中之重，既让网络通信保持实时通畅，还要让整个网络不能因为一个小的故障而全网瘫痪。现在学校的很多管理工作已经转移到了互联网上，要为校园网络设置成一个没有中断的稳定网络。校园网的可靠性设计要考虑到：

（1）设备可靠性：不能因为一个小小的故障让整个网络瘫痪，核心设备需要有备份，做好适当的冗余。

（2）业务的可靠性设计：在更换网络设备时，不该影响大部分用户的网络使用。

（3）链路的可靠性设计：链路的安全由以太链路的选择决定，不同区域所使用的网络协议也有可能不同应当考虑到路由协议的重分发，从而使不同区域网络可以互相通信，提高链路的可靠性。

2.3.2 安全性需求

安全共享和网络资源分配是一对矛盾。网络用户需要开发安全政策和措施与应用的要求，通过通信网络和应用中实现的设计。对于不同的安全隐患需要相应的安全措施来解决，网络的安全到达一定的安全水平。

校园网络的安全性需求可以看成校园里的数据资料的安全性需求，来保证师生使用校

园网络可靠安全。本方案将从以下几个方面来保障校园网络的安全性需求：

1)大连工业大学校园网主干网内部安全控制

在大连工业大学校园网每个部门只能进入自己专属的虚拟网，对他们是用虚拟网络技术，让外界用户无法进入他们的专属网络。

虚拟网内部的访问使用如下方法来保障安全：

身份认证，用来分辨是非法用户还是合法用户，来阻止非法用户的访问；

权限控制，由系统给用户进行授权，决定了用户可以访问哪些资源；

审计跟踪，它将记录哪个用户在何时访问了哪些资源，用于收费记帐和非法事件发生时能够有效地追踪；

有一些机密的文件使用加密来进行存储，如果用户拥有权限后方可查阅。

2)主要网关的设计方法的安全性方面，只提供了安全控制，安全控制根据应用需要的具体程序要求。网络安全保障可以通过控制功能之间的网络访问，在各部门未经授权的网络访问之间。

2.3.3 稳定性需求

网络稳定性是非常重要的基本性能要求，稳定性目标作为一个关键，需要设备冗余和自身的性能;各级链路冗余;第二和第三层的冗余设计考虑。同时一个完整的网络安全解决方案还当经受各种攻击，以确保稳定的这一重要方面。在校园网的负载能力接近操作层面的设计稳定性要求提供不间断服务为主体的用户和主要的网络服务。

2.3.4 可扩展性需求

校园网络在建设完成后，网络拓扑结构和用户数量和结构不怎么改变然而，发展和变化的网络应用是肯定的，网络的性能要求，必须逐渐增加。因此要求网络完成后，通过几个处理模块或添加关键网络设备的性能，解决了本地性能的问题。

2.3.5 可管理性需求

建成校园网后使学校资源可以统一管理分配，如学生档案，教材，考试成绩，各种设备等的统一管理;并实现办公自动化，各部门加强协调，提高工作效率。

按照统一规划，多层次的网络管理系统基于统一的网络管理平台的建设和管理各级网管边境管理权限和管理界面的清晰描述的前提;

1）提供强大的网络管理平台，设备管理，链路管理。

2）使用专用的性能管理工具来监视网络性能，收集，分析网络性能问题。

3）完整的用户认证计费系统，用户管理整个网络。

4）自动化网络管理，制度化，规范化;

5）建立与网络架构的可扩展性好，适应调整网络的网络管理系统的二次开发或用户定制尺寸，支持。

学院校园网应该使用现代技术和多媒体教学手段完成教学的视觉形象后解释，以增强了解学生的兴趣和水平，从而提高教学和学生素质的素质，提高水平。

3 整体设计

3.1 总体设计

大连工业大学网络计划应该使用成熟的技术，并最大限度地利用先进的技术，;采用国际标准有广泛的支持厂商，最大限度地利用产品是同一厂家的;该方案应该是带宽的合理分配，使用户不受互联网上的影响“堵车”;并应充分考虑未来可能的应用，如桌面将承受大型应用和多媒体传输需求的压力;在网络高可扩展性。能量为用户数量的未来扩展已经调整扩张的手段和方法;

组网图如下所示：

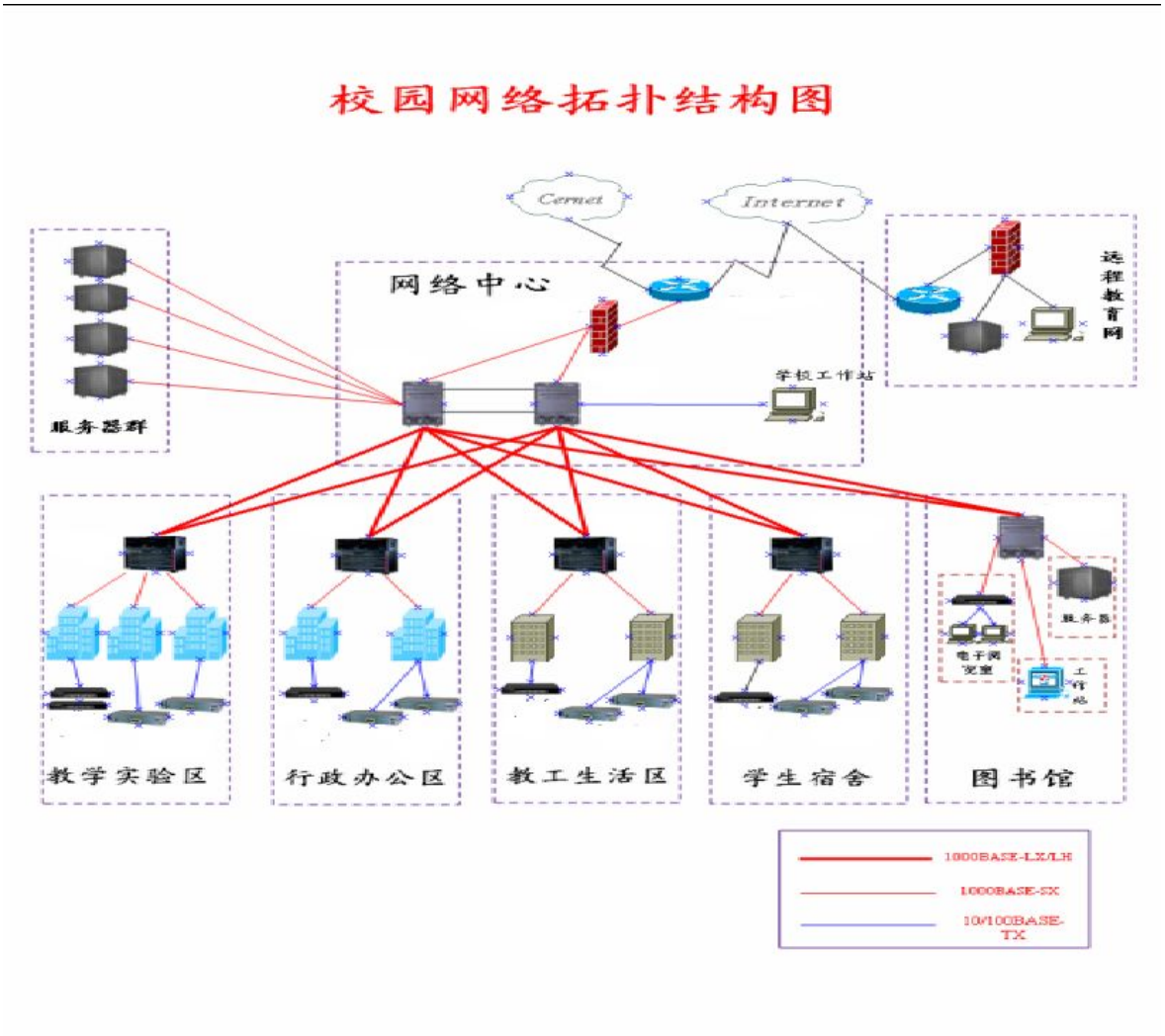

图 3-1　总体规划图

Fig.3-1 master plan

3.1.1 校园媒体服务中心

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,Cisco IP/TV 是 Cisco 公司推出的一套基于 TCP/IP 协议传递 MPEG-I 格式的高质量全动态的视频图象、语音及数据的客户服务器软件系统。该系统由内容管理服务器、内容服务器、客户端软件三大功能模块组成，拥有视频点播、定时广播、现场直播、多视频源广播等功能；包含了 Cisco AVVID（Architecture for Voice, Video and Integrated Data），即一个包含了音频、视频整合数据的通信框架,采用了先进的组内广播技术和磁盘优化读取技术，具有单机性能优异、网络传递高效、操作简明快捷、统计分析功能完备等特点，采用 RTP(实时传输协议)，RTCP(实时传输控制协议)，RSVP(资源预留协议)，MULTICAST(组播协议)，利用了经济实惠的 Windows 95, Windows 98, and Windows NT 平台，并充分利用了微软的 Windows Media 技术（WMT）。同时与苹果公司的 QuickTime 客户端，UNIX VIC and VAT Mbone tools,即 Netscape 插件结构兼容。且该方案可以在任何 IP 网络上工作，如 10BaseT 、100BaseT Ethernet 或千兆位以太网上工作，也可以在电缆、ADSL 调制解调器及局域网仿真的 ATM 网络上工作。，端到端完整的网络视频解决方案。整合了高性能的视频服务器-Cisco IP/TV 3400 系列服务器，IP/TV 3400 系列服务器预先配置了强壮的 IP/TV 3400 服务器软件，而客户端桌面 PC 配置 IP/TV 客户端软件。Cisco IP/TV 解决方案提供丰富的软件功能，可以提供高质量的视频流和具有良好的可管理性、扩展性、带宽有效利用等特性。对于视频播放，Cisco IP/TV StreamWatch 软件可以收集观众的信息，如观众人数、身份、及观看节目时间，对点播节目，日记文件能记录观众正在收看的节目. 可以轻松地满足校园网络上的电视会议、广播领导讲话、电视节目广播与点播、楼宇监控、网上教学、现场实况转播、校园课件点播和广播等多种高标准应用，并且完全可以满足学校提出的网络闭路电视系统的各项要求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 服务保证机制来实现，而 IP 组播技术是解决这些问题的关键技术。

3.1.2 无线应用方案

另外还需考虑的是校园网络对无线网络的需要, 在某些大型会议室、实验室等不宜布

线的地方,无线局域网采用标准无线局域网利用常规的局域网(如 10/100/1000M 以太网)及其互联设备(路由器、交换机)构成骨干支撑网。利用无线接入点(AP)来支持移动终端(MT)的移动和漫游。配有无线网卡的台式 PC 机、笔记本电脑或其他设备就可以与无线网络连接起来。一层是连接有线网络的无线 AP，另外一层是各大楼内分布的无线 AP。这两层的无线 AP 通过内部集成的桥接功能，实现它们的无线互连。连接有线网络的这个无线 AP 最好安置在离需要组建无线局域网的大楼附近，并且中间最好没有建筑物阻挡，相隔距离也不要超过 300 米，在信号比较弱的地方可以考虑安装增强天线,这样才能让无线 AP 性能得到发挥，最大限度节约成本投入。而需要组建无线局域网的大楼内我们每一层楼布置了一个无线 AP，无线网络覆盖全园,使全校师生以及来访客人能够随时随地方便高效地使用信息网络，促进学校的教学、科研和管理水平的提高。

3.2 服务器设计

3.2.1 DNS 服务

域名服务（或称域名解析服务）是网络的基本服务之一。它建立于主机名到 IP 地址的映射关系是 WWW，FTP，电子邮件等互联网服务的基础。大连工业大学校园网的 DNS 服务可以通过现有的 DNS 服务器中心来完成。如果我们考虑更多的领域的搜索流量，你可以设置 DNS 服务器 1-2 台，大连工业大学校园网格，完成大连工业大学校园网 DNS 服务。大连工业大学校园网的 DNS 服务器可以备份整个校园网络的 DNS 服务。

3.2.2 邮件服务

大连工业大学校园网的邮件服务利用校园网现有的邮件服务体系。动态主机配置 DHCP Service 大连工业大学校园网的 IP 地址分配策略以固定 IP 地址配置为主，在某些地区例如图书馆和综合楼处，师生需要动态地址的分配。因而，在这些地方和无线网络分配的地方需要配备校园 DHCP 服务器服务。

3.2.3 DHCP 服务

DHCP(Dynamic Host Configuration Protocol)是动态主机配置协议,一种简化主机 IP 地址配置管理的 TCP/IP 标准。DHCP 基于 C/S 模式,它允许 DHCP 服务器来动态向客户端分配 IP 地址和相关的配置信息。您可以指定子网掩码，DNS，网关和其他信息在 DHCP 服务器上的 IP 地址。当客户端启动时租约到期 DHCP 服务器会收回该 IP 地址来获取信息，和贷款

的使用。改变 IP 地址大面积的这种动态管理方法出现在网络中，DHCP 服务器只需要一个简单的修改。

3.2.4 NAT 服务

NAT(Network Address Translation)即网络地址转换。NAT 被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决 IP 地址短缺的问题，而且还可以有效避免网络外部的攻击，隐藏和保护内部网络的计算机。通过 NAT，当一个专用地址“内部”网络通过路由器发送数据包的装置，私有地址被转换成合法的 IP 地址，只用少量的公网 IP 地址的局部区域网络可以实现专用地址的网络的所有电脑和互联网的通信需求。

3.2.5 AAA 服务

其主要目的是管理哪些用户可以访问网络服务器，具有访问权的用户可以得到哪些服务。如何对正在使用网络资源的用户进行记账？具体为：

1、 验证(Authentication)：验证用户是否可以获得访问权限。

2、 授权(Authorization) ：授权用户可以使用哪些服务。

3、 记账(Accounting)：记录用户使用网络资源的情况。

AAA 服务器（AAA 服务器）是能够处理一个用户的访问请求的服务器程序。提供认证，授权和账户服务。 AAA 服务器通常与网络访问控制，网关服务器，数据库和用户目录和工作的其它信息相关联。在与 AAA 服务器的网络连接服务器接口的合作是“远程身份验证拨入用户服务
(RADIUS)”。

3.3 层次化设计

校园网络中层次化设计会使设计简单明了。

（1）接入层：

接入层是用户可控和可接入的设备与网络相连之处。接入层提供有线和无线连接，并包含能确保整个网络的安全性和永续性的特性及服务。接入层提供了用户可控和可接入的高速设备连接。过去曾是昂贵选择的千兆以太网和 802.11n 无线网络等高速接入技术，现在已是最终用户设备上的标准配置。在大多数情况下，最终用户设备不会长时间使用这些连接的全部容量，能够在执行日常任务时突发满足高速需求的能力，使网络成为最终用户

日常工作的一个重要组成部分。用户等待设备备份、发送电子邮件或打开内部网页中的文件所需等待的时间越长，网络就越难实现透明。通常，多种不同类型的设备会在接入层连接。个人电脑、IP 电话、无线接入点和 IP 视频监控摄像头都能连接到同一接入层交换机。因为从性能、管理和安全角度出发，将这些设备分区较好，所以接入层能在一个物理基础设施上支持多个逻辑网络。

永续性和安全服务一般来说，基础设施中永续性和安全性服务的目的是确保网络始终可用，且不会对任何需要使用它的人造成损害。作为网络和客户端设备间的连接点，接入层的作用是确保网络免遭人为错误和恶意攻击的影响。这种保护包括确保与网络相连的设备不会试图向超出其授权范围的任何最终用户提供服务，确保这些设备不会企图接管网络中其它设备的工作，并在可能的情况下，验证以确保该设备具有网络接入权限。

在接入层中实施这些服务，不仅有助于网络的整体安全，而且能够提高网络的永续性和可用性。支持先进技术最后，接入层提供了一系列支持先进技术的网络服务。语音和视频在当今校园中已经普及，网络必须提供支持这些技术的服务。这其中包括为这些设备提供特别的接入功能，确保这些设备的流量不会遭到破坏，并高效交付网络中许多设备需要的流量。

（2）分布层：

分布层为局域网提供许多重要服务。其主要功能是作为特定地点或园区中多个接入层交换机的汇聚点。在一个无论是不同接入层设备之间还是从接入层设备到广域网之间的连接都需要端到端穿越局域网的网络中，分布层支持这种连接性。可扩展性在多个接入层设备部署于一个地点，提供最终用户连接的网络中，当接入层不断扩展，超出两或三个交换机的规模时，就无法互联每个接入层交换机。分布层提供了一个逻辑点，以汇总编址，并为接入层运行所必要的协议和特性创建边界。

分布层边界的另一优势是，它创建了故障域，能将故障或网络变更限制在其直接影响的网络部分范围之内。对于校园来说，最终的结果是，分布层能够通过提高自身效率、减少所需内存，并处理面向网络其它位置的设备的资源，降低网络运营开支。此外，它还能将故障限制在较小的域中，从而提高网络可用性。降低复杂度，提高永续性本设计采用了一个简化的分布层设计，其中包含单一逻辑实体，能够通过一对作为单一设备运行的物理上相分离的交换机、一个作为单一设备运行的交换机堆叠，或是一个采用冗余组件的交换机来实施。校园能够受益于简化的分布层配置和运行，因为只需极少的协议，且几乎或完全不必进行调整，就能在发生故障或运行中断时在一秒钟或更短时间内实现收敛。电源、

管理引擎和模块等物理冗余组件，以及到冗余逻辑控制平面的状态化故障切换，提供了设计永续性。

简化、统一的设计降低了配置和维护网络的运营成本。灵活的设计分布层为网络服务、广域网和互联网边缘提供了连接性。网络服务包括但不限于广域应用服务(WAAS)和无线局域网控制器等。根据局域网的规模，这些服务和到广域网及互联网边缘的连接可能位于专用分布层，而非与接入层设备共享分布层。与接入层相同，分布层也为应用流提供 QoS，以保证关键应用和多媒体应用能达到设计性能。

（3）核心层：

在大型局域网环境中，通常需要多个分布层交换机。其原因之一是，当接入层交换机位于多个地理位置分散的建筑物中时，您可以在每个建筑物中部署一个分布层交换机，从而节省建筑物间昂贵的光纤布线。

当网络在单一地点扩展到超过三个分布层时，校园网就应该使用一个核心层来优化设计。使用多个分布层交换机的另一原因是，与单一分布层相连的接入层交换机数目有可能会超过网络设计者的设定目标。在模块化、可扩展设计中，您可以为数据中心、广域网连接或互联网边缘服务分别配置分布层。

局域网核心层是可扩展网络的重要组成部分，但从设计角度来看，它也是最简单的一个部分。分布层提供故障域和控制域，核心层则在它们之间提供 24x7x365 不间断连接。在本设计中，核心层采用两个物理和逻辑上都相互独立的交换机。进出核心层的连接仅为第三层连接，这提高了永续性和稳定性。因为核心层不必提供和分布层相同的服务和边界，所以双机箱设计不会显著增加配置复杂度。

4 方案设计

4.1 设计原则

大连工业大学的网络系统方案设计与规划将秉承一下几个原则。

1.实用性与先进性

根据实际情况和学校的特点，尤其是在设计强调实用性和先进性的结合，应使用是成熟的网络技术，保证校园网络效用;跟踪国际网络技术，网络设计和先进技术的新发展。在校园网络，以确保可靠，实用，先进的研究的基础上，可以提供先进的网络技术的研究环境为学校的研究和开发。

2.开放性与标准化

大连工业大学校园网的设计使用开放的网络架构，使网络的升级、扩展和互联变得更加容易。同时，在选择服务器、网络产品时应该看重产品所支持的网络协议的国际标准化。

3.可靠性与安全性

校园网的设计，主要考虑两个层面：第一，整个网络的可靠性和安全性，高可靠性，高安全性的网络架构，包括广域网接入控制和内部局域网接入控制，外部网络的合理设计的安全性进入到备份链路;二是可靠性网络设备，主要用于热插拔模块，双电源，冗余端口安全，网络设备设置用户表和密码限制手段。

4.经济性与可扩充性

在满足校园使用需求的前提下，应该选用性价比高的网络设备。采购的网络架构和设备，应充分考虑到可以轻易升级换代，而且在升级时能够最大限度地保护原有的硬件设备和软件投资。

4.2 设计方案

根据设计原则，我所设计的大连工业大学网络结构拓扑图如下图所示：

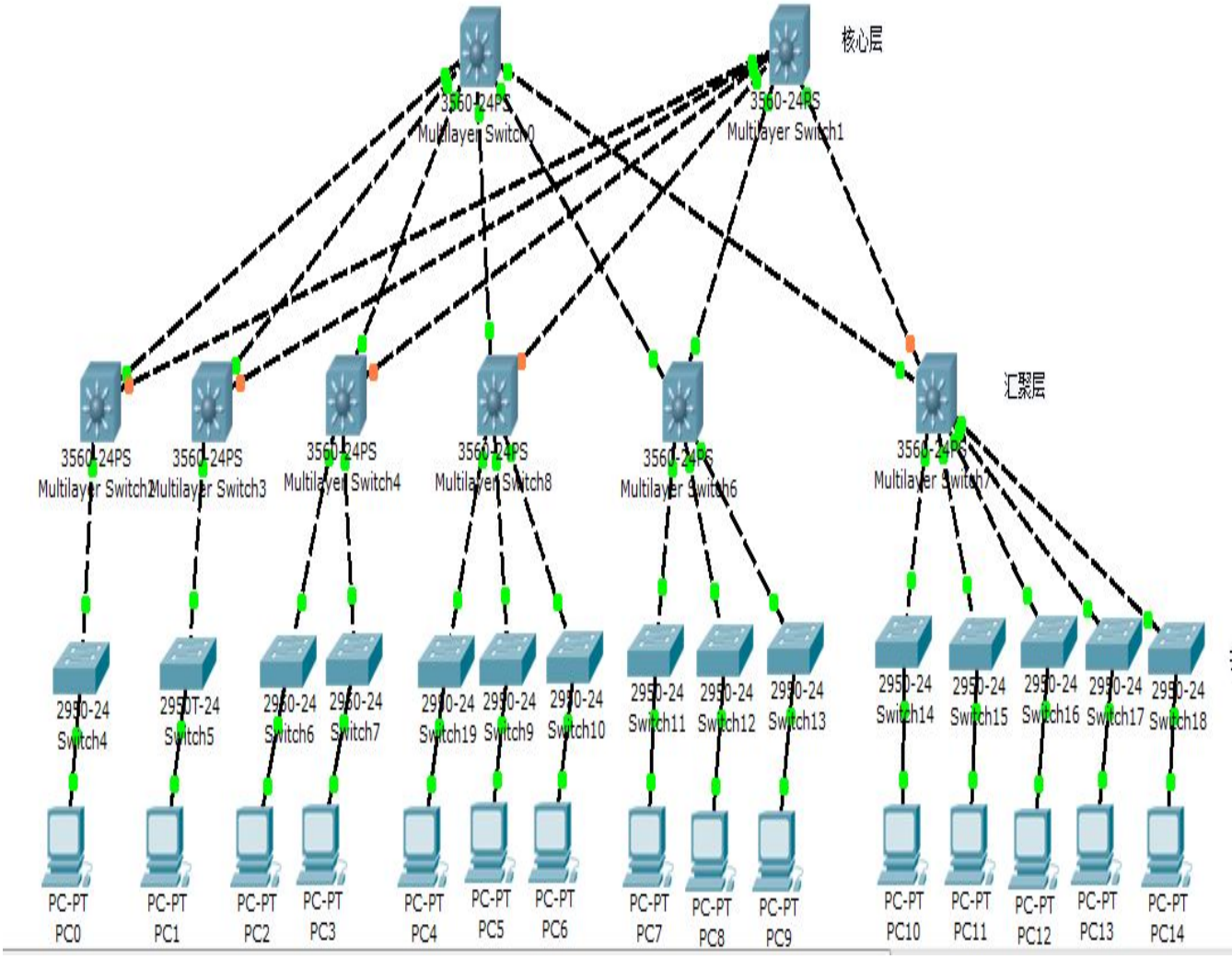

图 4-1　大连工业大学拓扑图

Fig.4-1 Huludao campus topology

在网络管理区域配置双核心交换机，在航空服务学院、化工与材料学院、九号学生公寓、五号学生公寓、二十号学生公寓和综合楼 A 座布置主交换机。这些主交换机连接两台核心交换机，两台核心交换机配置热备份路由 HSRP 协议。HSRP 作用于三层核心交换机上，该协议中含有多台路由器，对应一个 HSRP 组。该组中只有一个路由器承担转发用户流量的职责，这就是活动路由器。当活动路由器失效后，备份路由器将承担该职责，成为新的活动路由器。这就是热备份的原理。

实现 HSRP 的条件为系统中有多台路由器，其中它们组成一个“热备份组”，这个组形成一个虚拟路由器。在任何一个时间，一个组只有一个路由器是活动通过将其转发数据包，如果活动路由器出现故障，备份路由器将选择更换活动路由器，但网络视图中的主机，虚拟路由器没有改变。所以主机仍然保持连接，由故障没有影响，所以解决问题的路由器交换机。

4.2.1 结构设计

首先对大连工业大学的校园网络进行分析

校园网的规模远大于传统局域网能覆盖范围，应用到局域网互联技术，网络的层次较多。

学校的不同功能的部门分布在不同的位置上，要将他们进行子网划分，以方便管理。

学校校园网使用星型的拓扑结构。核心是主干网，分布在它周边的是各个子网，子网的下层连接工作组网，工作组网再向下再连接基层网段。

校园电脑终端根据功能和配置的不同，连接到不同的网络层。

学校的主干网络必需有很强的中心交换处理能力和很大的带宽。

校园子网相对独立，在主干汇接处搭建子网边界。学校校园网支持远程访问。

校园网完成后，该系统包括被跟踪的网络系统中，每个通信功能协议的功能的层级结构。体系结构的网络系统也被称为“集合级别并达成一致。”第一步是选择的网络系统的设计的网络结构，应使用决策的核心组协议。

4.2.2 IPv4 地址规划

在网络规划中，IP 地址方案的设计至关重要。好的 IP 地址方案不仅可以减少网络负荷，还能为以后的网络扩展打下良好的基础。分配地址之所以成为网络规划中最棘手的问题之一，其原因如下:

网络 IP 地址资源是有限的，尤其是资源贫乏的公网地址，如果地址段规划不合理，会浪费宝贵的资源地址。

规划申请，规划是基于对互联网用户分配 IP 地址。

地址分配通常被认为是一种管理方法，而忽视了其对网络稳定性的影响;而事实上，如何分配的 IP 地址将直接影响到网络的稳定性。

后分配地址，这是难以改变的，因为一台主机常常需要重新配置。

安全性和网络的接入计费信息资源管理，网络息息相关分配 IP 地址。

据互联网技术的发展趋势，结合学校网络的现实是真实的 IP 地址，我们推　　荐以下原则设计的 IP 地址规划：

使用私有 IP 地址，NAT 后，远程访问服务器区;

1. IP 地址，并使用真实 IP 地址的互联网连接设备;

2.局部互连采用私有 IP 地址;

3.通过为地址转换的统一出口边缘设备（路由器，防火墙）3.面向用户的私有 IP 地址。使用合法 Internet IP 地址是出口路由器（防火墙）；

这样的设计可以充分利用现有公网 IP 地址，解决 IP 地址空间不足，既可以方便地与每个互连通信，地址转换（NAT）由网络边缘设备共享这耗费资源的设备，完善的整体网络的数据传输的性能

4.2.3 IPv4 路由规划

决定在校园网络中采用 OSPF 协议，因为它有许多优点。

1、OSPF 算是是真正地 LOOP- FREE(无路由自环)路由协议。因为其算法本身的优点。(链路状态最短路径算法)

2、OSPF 收敛速度快:能够在最短的时间内将路由变化传递到整个自治系统。

3、提出按照区域(area)划分的概念,将自治系统划（AS）分为不同区域后,通过区域间的对路由信息的摘要,大大减少了要传递的路由信息量。同时也使路由的信息不会因为网络规模的扩大而急剧膨胀。

4、将协议自身的开销控制到最小。

1)用于发现和维护邻居关系的是定期发送的是不含路由信息的hello报文,非常短小。包含路由信息的报文时是触发更新的机制。(有路由变化时才会发送)。但为了增强协议的健壮性,每 1800 秒全部重发一次。

2)在广播网络中,使用组播地址(而非广播)发送报文,减少对其它不运行 ospf 的网络设备的干扰。

3)在各类可以多址访问的网络中(广播,NBMA),通过选举DR,使同网段的路由器之间的路由交换(同步)次数由 O(N*N)次减少为 0 (N)次。

4)提出 STUB 区域的概念,使得 STUB 区域内不再传播引入的 ASE 路由。

5)在 ABR(区域边界路由器)上支持路由聚合,进一步减少区域间的路由信息传递。

6)在点到点接口类型中,通过配置按需播号属性(OSPF over On Demand Circuits),使得 ospf 不再定时发送 hello 报文及定期更新路由信息。只在网络拓扑真正变化时才发送更新信息。

5、通过严格划分路由的级别(共分四极),提供更可信的路由选择。

6、良好的安全性,OSPF 支持基于接口的明文及 MD5 验证。

7、OSPF 适应各种规模的网络,最多可达数千台。

4.2.4 VLAN 划分

即虚拟局域网。为了便于管理，并提高网络的效率和安全性，除了上述网络的物理设计外，还需要对网络进行逻辑设计，即划分虚拟网,将不同部门不同节点上的办公应用服务器分别划成独立的虚拟子网，除了一些相应端口服务对校内开放外，其他对这个子网的访问的都受到限制，而不只依赖服务器本身的安全保护。

对于 Cisco 的产品划分，VLAN 主要是基于两种标准协议：ISL 和 802.1Q。在我们这里，因为所采用的均是 Cisco 的网络设备，故在进行 VLAN 间的互连时采用 ISL 的协议封装，该协议针对 Cisco 网络设备的硬件平台在信息流的处理、多媒体应用的优化进行了合理有效的优化。赋予 VLAN 不同对外访问权限，如只能访问校内，或只能访问中国教育科研网，或能访问整个互联网等，虚拟网虚拟工作组模式下共享同一个＂局域网＂。当部门内的某一个成员移动到另一个网络位置上时，他所使用工作站不需要作任何改动。实现合理分配网络资源，均衡网络负载，有效降低网上广播信息,方便对用户的分组管理。

在网络已成为现代信息处理不可缺少的工具，已经成为我们日常工作的重点，利用 VLAN 技术变得越来越重要。对于信息系统的 VLAN 意义体现在：

1.一个 VLAN 可以提高网络的通信效率;

由于流量限制为这一子网，它不会干扰其他子网。

2.VLAN 广播风暴是可以避免的;

在大型网络中，有大量的广播信息，很容易导致大幅度降低网络性能，甚至网络瘫痪。该 VLAN 只作一个子网广播，不会使扩散毫无意义，从而消除了发生广播风暴的条件。

3.VLAN 大大提升网络与信息安全;

由于子网不能免费参观，得到很好的控制信息流。

4.VLAN 使组织网络更加灵活。

网络中的网络用户的物理位置不会影响访问用户的逻辑，不会是完整的物理网络规划的限制。

有一个大的关系，规划师和 IP 子网 VLAN 的。在具体实施过程中，根据以下原则应是：

1，IP 地址的整个网络进行全面的规划，确定在每个子网主机的数量，并根据在 IP 子网掩码的数量来确定主机的长度;

2.确定 IP 子网的聚集点，下面的聚合点连续子网。聚合点到核心路由交换机路由至

少通知;

3，选择合适的路由协议的子网;

4，根据规划 IP 子网中，交换机 VLAN 的规划和分工，建立 VLAN 和 IP 子网之间的对应关系;

5，NMS 采用完全独立的 IP 子网和 VLAN，所有的网络设备，因此更安全的管理;

6，根据流量和的信息来确定的 VLAN 和 IP 子网服务器集群分布;

7，建立相应的 VLAN 和 IP 子网和绑定在三层路由交换机 VLAN 的网关;

在大连工业大学中，决定划分 16 个 VLAN，他分别以各学院以及行政中心为划分依据，

表 4-1 VLAN、IP 划分表

Table 4-1, table IP VLAN division

名称	VLAN 划分	IP 地址划分
研究生学院	VLAN10	192.168.10.1～192.168.10.254
轻工与化学工程学院	VLAN20	192.168.20.1～192.168.20.254
生物工程学院	VLAN30	192.168.30.1～192.168.30.254
食品学院	VLAN40	192.168.40.1～192.168.40.254
纺织与材料工程学院	VLAN50	192.168.50.1～192.168.50.254
机械工程与自动化学院	VLAN60	192.168.60.1～192.168.60.254
信息科学与工程学院	VLAN70	192.168.70.1～192.168.70.254
艺术设计学院	VLAN80	192.168.80.1～192.168.80.254
服装学院	VLAN90	192.168.90.1～192.168.90.254
管理学院	VLAN100	192.168.100.1～192.168.100.254
外国语学院	VLAN110	192.168.110.1～192.168.110.254
国际教育学院	VLAN120	192.168.120.1～192.168.120.254
继续教育学院	VLAN130	192.168.130.1～192.168.130.254
思想政治理论课教学科研部	VLAN140	192.168.140.1～192.168.140.254
体育教学部	VLAN150	192.168.150.1～192.168.150.254
行政部	VLAN160	192.168.160.1～192.168.160.254

4.2.5 组播业务

组播技术作为一项新的网络应用，在网络带宽、网络安全方面对校园网的管理者来说提出了更高更深的要求，因此在校园网内部署组播服务需要全面考虑、统筹安排。多播服务涉及网络的所有层：MAC 地址级，II）层，应用层，主机需要接入层交换机的三层交换的每个级别配置组播协议。组播业务必须在详细规划和论证的前提下，选择合适的网络设备和组播方案的拓扑结构。在操作过程中的每个阶段，要继续完善和提高组播能力的管理，最终提供一个稳定，可扩展，可管理的组播服务。它是一种有效的方式，以节省网络带宽。

的网络的音频/视频广播，当一个节点需要信号发送到所述多个节点中，无论是重复自组织通信，或广播应用，将是网络带宽的严重浪费，只有多播是最好的选择。多播，一个或多个组播源只发送到特定组播组的数据包，但只有加入组播组的主机可以接收数据包。

4.2.6 QOS 部署

网络的建设必须符合当前网络应用的需求，并能有效促进发展和使用的网络应用。随着因特网的不断发展，日新月异基于互联网的网络的应用程序，不仅意味着增加新应用程序的流量，并改变了流动特性，特别是，许多新的多媒体应用的网络带宽，延迟等的应用有不同的要求，网络系统需要有优先权，分配带宽用于各种应用的能力。

因此，网络解决方案和设备必须导向的应用，尤其是多媒体应用，如多媒体课件，视频点播，电视会议，协作学习，因此网络必须支持多个级别的 QoS 服务，多媒体服务，以确保数据流的可靠传输。同时，这些多媒体服务，交换和路由的执行将不影响整个网络的性能。

QoS 的目标是提供更好的，更可预测的网络服务，提供专用带宽，控制抖动和延迟，并提高损耗特性。 QoS 的方法来实现这些目标是提供一套工具来管理网络拥塞。塑造网络流量，更高效地利用昂贵的 WAN 链路，并在网络上设置的交通政策。

QoS 的工具有三个主要功能 - 拥塞管理（队列和调度），拥塞避免和流量整形和政策制定。这些工具的单个网元内使用。在一般情况下，这些工具可以在一个接口提供者开始提供正确的 QoS 特性，特定的网络应用程序。此外，该网络设备软件还提供三种功能和其他链路效率机制集成到协调不同的工具的工作能够提高 QoS 服务。

QoS 实施策略专用网络可以采取分步策略：

第一步：业务量不大的情况下，利用从最终整个网络的最终的 Diff-Serv 的技术，保证高优先级流量的服务质量。

第二步：在更复杂的网络的情况下，引入 VPN 技术，不同的服务需要不同的 VPN。

在 IP 端局（汇聚交换机）进行流分类，流量监管，流量的不同标记与在核心层率不同的优先级为临时使用的带宽，基于 TOS 或 COS 的核心路由器的每个端口配置服务不同的优先级域流分类，不同类别分成不同的队列。

为了保证高优先级流量不拥塞时为标有一个低优先级标记力包的优先级服务终端，确保获得上一级的网络流量很高的有效优先级。

因为区分服务是基于统计的服务质量保证机制，要求交通服务必须在网络带宽的不足

30%，在这种情况下，业务能够在网络中有保障的传输。随着网络规模的扩大，　　今后可以考虑融合 MPLS TE 和 VPN QoS 技术，以进一步确保最终用户的业务和 QoS。

完善的 QoS 机制，以满足未来 IPTN（IP 电话网络）的建设要求。能充分保证不同的延迟，抖动，带宽，丢包率，承诺要进行的 VoIP（IP 语音）等电信级的服务，满足多业务 IP 网络的发展要求。

流分类是指按照一定的规则对流量分类，并关联的同类型流量的一些动作，形成一个战略。之后实现这一政策是基于应用的流量监管，流量整形，拥塞避免功能。

无需 QoS 保证的时候还是不要的情况分类，分组或不匹配的流分类规则，尽一切努力来转发数据包 BE（尽力而为）的过程。

配置复杂流分类通常是核心路由器在对面的边界路由器上配置简单流分类。

通过监控网络流量负载塞避免技术，可预见和避免拥塞发生在公共网络瓶颈。这是当拥塞发生在不同的拥塞管理技术的其管理。的主要工具，以避免拥塞是加权随机测试（WRED），这将在下面描述。

1. WRED 拥塞避免

在拥挤随机早期检测（RED）算法可以发生在网络上，以避免拥塞。 RED 监视网络上的流量负载，如果拥塞开始增加，这将需要的点随机分组丢弃的措施。结果会被丢弃的信息源将发现有流量丢失，从而降低其传输速率。 RED 主要是常见的在互联网环境下，TCP IP 协议。

2. WRED QoS 信令技术和共享

WRED 结合 IP 优先级和 RED 算法的功能。这种组合提供了较高优先级业务处理优先级的数据包。当接口拥塞开始出现，它必须有选择地丢弃较低优先级的通信，并针对不同的服务级别提供不同的性能特征。

5 通信设备选型

5.1 选型原则

大连工业大学的校园网络建设的设备选型原则是一下几条：

选择交换机的基本原则:

⑴适用的组合和先进的原则。不同品牌产品的大量功能之间切换的价格差异不一样，不仅品牌或追求高价因此选择，也不能只看价格低，应根据应用的实际情况，选择超高的性价比，既满足当前的需要，而且也能适应未来几年的网络交换机的发展。

（2）选择的主流产品选择基于开关应在国内市场上可以选择具有相当大的份额，高性能，高可靠性，高安全性，高可扩展性，产品的高可维护性，如 CISCO 市场，中兴，3COM，华为更大的份额。

（3）一个安全可靠的原则

安全开关决定了防伪网络系统，交换机的选择，这是非常重要的，主要是在安全交换机的 VLAN 划分，过滤技术开关。

（4）产品和服务相结合的原则

当选择开关，我们必须着眼于品牌也以制造商和销售的商品如果有强大的技术支持和良好的售后服务，技术支持或买都不在交换机发生故障，没有的商品和服务，使学校遭受损失。

选择路由器的基本原则：

(1)实用性原则

采用成熟的、经实践证明其实用性的技术。这能满足现行业务的管理，又能适应 3~5 年的业务发展的要求；

(2)可靠性原则

设计详细的故障处理及紧急事故处理方案，保证系统运行的稳定性和可靠性；

(3)标准性和开放性原则

网络系统的设计符合国际标准和工业标准，采用开放式系统体系结构；

(4)先进性原则

应该使用支持 VLAN 划分技术设备，HSRP（热备份路由协议）技术，OSPF 等协议，以确保迅速变化和路由的网络融合，网络广播风暴抑制的传输性能，降低数据传输延迟;

(5)安全性原则

该系统具有多层次的安全保护措施，以满足用户身份认证，访问控制，数据完整性，可审计性和安全性的传播等方面的要求;

(6)扩展性原则

在业务不断发展的情况下，路由系统可以不断升级和扩充，并保证系统的稳定运行；

(7)性价比

不能盲目的追求高性能的产品，要采购适合校园网需求的产品。

选择防火墙的基本原则：

（1）价格的总成本：

防火墙产品作为安全屏障的网络系统，拥有的总成本应不超过最大程度的保护网络体系可能遭受的成本损失。最后的结果将是防火墙管理，决策，而不是工程的功能。

（2）明确系统要求：

这就是你需要网络监控，并控制冗余的水平。可以列出一个必须监测如何转移，则必须允许如何传输线的流动，以及哪些应被拒绝转移的清单。

（3）应符合校园的特殊要求：

校园安全政策的特殊需要，并非所有的防火墙可以提供，在选择防火墙，如这　　往往成为一个因素要考虑：加密控制标准，访问控制，特殊的防御功能。

（4）防火墙安全：

最难以评估的防火墙产品方面，防火墙的安全性能，普通用户一般无法判断。在防火墙产品的用户的选择，你应该尽量选择在同一时间较大的市场份额，通过产品的国家认证机构认证测试。

（5）防火墙产品的关键要求：

针对校园用户的防火墙产品的主要需求有：网络安全要求，细粒度的访问控制能力的要求，VPN 的需求，统计和核算的需要，带宽管理能力的需求，这些被认为是重点的防火墙上的选择。

（6）管理和培训：

管理和培训是防火墙的质量评价的一个重要方面。人员培训和日常维护费用通常占有相当大的比重。一个优秀的安全厂商必须提供良好的培训和售后服务为用户。

（7）可扩展性：

网络扩展和网络应用是可能的新技术和新增加的风险成本也出现大幅上涨的网络，因

此他们需要具有更高的安全性提高了防火墙产品。

选择服务器的基本原则：

（1）可靠的原则：

为了保证网络的正常运行，服务器首先由用户选择，以确保稳定性。服务器是特别重要的经营业务或存储用户信息的数据库服务器的核心。

(2)适当足够的准则：

对于用户来说，最重要的是，从目前的情况和未来的扩展出发，有针对性的选择，以满足当前的应用需求，并适当超前，没有太多的投资方案。避免购买服务器来追求性能，要求高的需求良好的误差。

（3）扩展的原则：

为了减少由升级服务器和对企业的影响的开销，服务器应具有高的可扩展性，可以调整配置以适应用户自己的发展。

（4）易于管理原则：

所谓易于操作和管理用于与适当的技术以简化管理，以减少成本和维护成本，通常由硬件和软件两者来实现这一目标。

（5）服务原则：

选择服务好的厂商的产品是一个明智的决定。在具体选购服务器时，用户应检查企业是否有一个完美的以客户为导向的服务体系，并在这一领域未来的计划。

（6）原则的特殊需要

不同的用户需要不同的信息资源，使服务器能够满足用户，用户选择的特殊需要，他们也需要特别注意。

5.2 核心交换机

大连工业大学小区规模庞大，师生人数众多，对网络需求较高，建议使用两台高性能核心交换机互为备份来保障校园网络。

基于 Supervisor2T 的 CiscoCatalyst6500 系列交换机是首要的局域网核心平台。它提供了可扩展的性能、智能和广泛特性，能够满足要求最为严格的大型校园部署对于构建模块化、永续、可扩展、安全的第 3 层骨干解决方案的需求。

使用新的 CiscoCatalyst6500SupervisorEngine2T,将每插槽交换容量提高至 80Gbps，并提供了更出色的可扩展性，以及增强的硬件支持特性。性能的提升使系统能够提供未来

40Gigabit 的以太网上行链路，以满足最为苛刻的分布层到核心层连接的要求。Cisco6500Supervisor2T 支持启用了 PolicyFeatureCard4（PFC4）的新线路卡（如 WS-X6816-10G 和 WS-X6908-10G），它们可提供增强的 QoS 和安全功能。基于 Supervisor2T 的交换机通过提供 MacSec 加密和基于角色的访问控制（RBAC）列表，加强了对 CiscoTrustSec（CTS）的支持，并提供了改进的控制平面监管（policing），以防御拒绝服务攻击。

利用铜质或光纤介质，支持千兆和万兆以太网高密度连接，提供满足任何网络核心层所需的规模和多功能性。核心层设计中使用的 Catalyst6500 能使用与分布层 Catalyst6500VSS4T 系统完全相同的管理引擎、机箱和电源，从而方便备件的准备，减少所需支持的平台。《紧缩数据中心和园区核心层部署指南》介绍了当局域网和数据中心核心层功能结合在一套设备上时，如何将 CiscoNexus7000 系列交换机用作核心层平台。

5.3 分布层交换机

分布层的主要功能就是汇聚校园中的接入层交换机。分布层位于接入层第二层域和连接至网络其余部分的第三层域之间。它为局域网提供了两个重要功能。在第二层端，分布层为生成树协议创建了一个边界，限制了第二层故障的传播。在第三层端，分布层在 IP 路由信息进入网络之前，提供了一个汇总该信息的逻辑点，减少了 IP 路由表，从而简化了故障排除，能够更快从故障中恢复。

CiscoCatalyst3750-X 堆叠

堆叠被配置为单一设备单元，但 StackWisePlus 堆叠中的每个交换机都有独立的负载共享电源和处理器。面向大型校园的 IBA 智能业务平台—无边界网络架构使用了一对堆叠的 3750X-12S-E 交换机，来提供第 2 层和第 3 层交换。交换机使用小型可插拔（SFP）收发器作为到接入间的铜缆或光纤千兆以太网 EtherChannel 上行链路的端口选项。

CiscoStackWisePlus 利用 64-Gbps 堆叠互联，最多能堆叠九个 CiscoCatalyst3750-X 交换机，故障恢复时间不到一秒。

CiscoStackPower 可以在 CiscoCatalyst3750-X 交换机堆叠中共享电力。因此，能够在堆叠中灵活地安排电源，实现不占空间的冗余电源部署和智能负载分流功能。

Cisco3750-X 系列拥有模块化上行链路，能够以千兆或万兆以太网的速度连接至核心层，并支持 IOS 特性集的升级以及 TrustSec 和 Medianet 等增强校园功能，确保交换机功能随着校园的发展而提高。

5.4 接入层交换机

接入层是用户可控和可访问设备与网络相连之处，也是每个局域网中必备的一个架构组件。因为接入点是网络服务和客户端设备间的连接点，它在保护其它用户、应用资源和网络本身免遭人为错误和恶意攻击影响方面具有重要作用。接入层中的网络永续性和安全性是通过使用 CiscoCatalyst 基础设施安全特性（CISF）实现的，这其中包括 DHCP 监听、IP 源防护、端口安全、动态 ARP 检测和网桥协议数据单元（BPDU）防护等。为提供一致的网络接入功能，简化网络部署和运行，本设计针对所有接入层设备都使用了相同的部署方法，无论这些设备是位于总部还是远程站点。为降低复杂度，接入层的设计使您能够为独立电脑、IP 电话、与电脑相连的 IP 电话或无线接入点使用单一接口配置。接入层接入层局域网接入层通过 10/100/1000 以太网端口为设备提供高速连接，提供千兆和万兆上行链路连接选项。万兆上行链路也支持千兆连接，提供了灵活性，并有助于在升级到万兆以太网过程中保持业务连续性。局域网接入层配置为一个第二层交换机，支持通过直连分布层或路由器提供的全部第三层服务。

CiscoCatalyst2960-S 系列是固定配置的可堆叠 10/100/1000 以太网交换机，提供 PoE+和无电源版本，适用于入门级大型校园、中端市场和远程站点网络。

通过向交换机添加一个堆叠模块，能够支持 CiscoFlexStack。由此，最多能将四个 Catalyst2960-S 系列交换机堆叠起来。

CiscoFlexStack 链路是全双工万兆以太网链路，恢复时间在 1-2 秒之间。

6 安全设计

6.1 可靠性

大连工业大学的校园网通过采用可靠的网络技术，计算机机房环境及网络运营商的可靠性，以确保严格的管理。网络技术，主要是考虑了以下三个问题：

链路的可靠性：通过多个连接到不同的路径，以避免单电路故障，提高校园网络路径冗余线的每个节点与其他节点之间的线路应尽可能使用不同的物理光纤链路；

设备的可靠性：采用性能稳定，可靠的设备。消除单点故障，采用设备的使用异地热备份技术，保证网络和业务的连续性；

路线可靠性：自动路由和迂回，因此，当在网络路径切换意想不到的一部分时，在上层的服务这些操作是透明的主机。

室内环境主要包括稳定的不间断电源，应变能力等。网络运营管理，包括合理的网络管理系统和相关的管理体系。

如图下图所示：

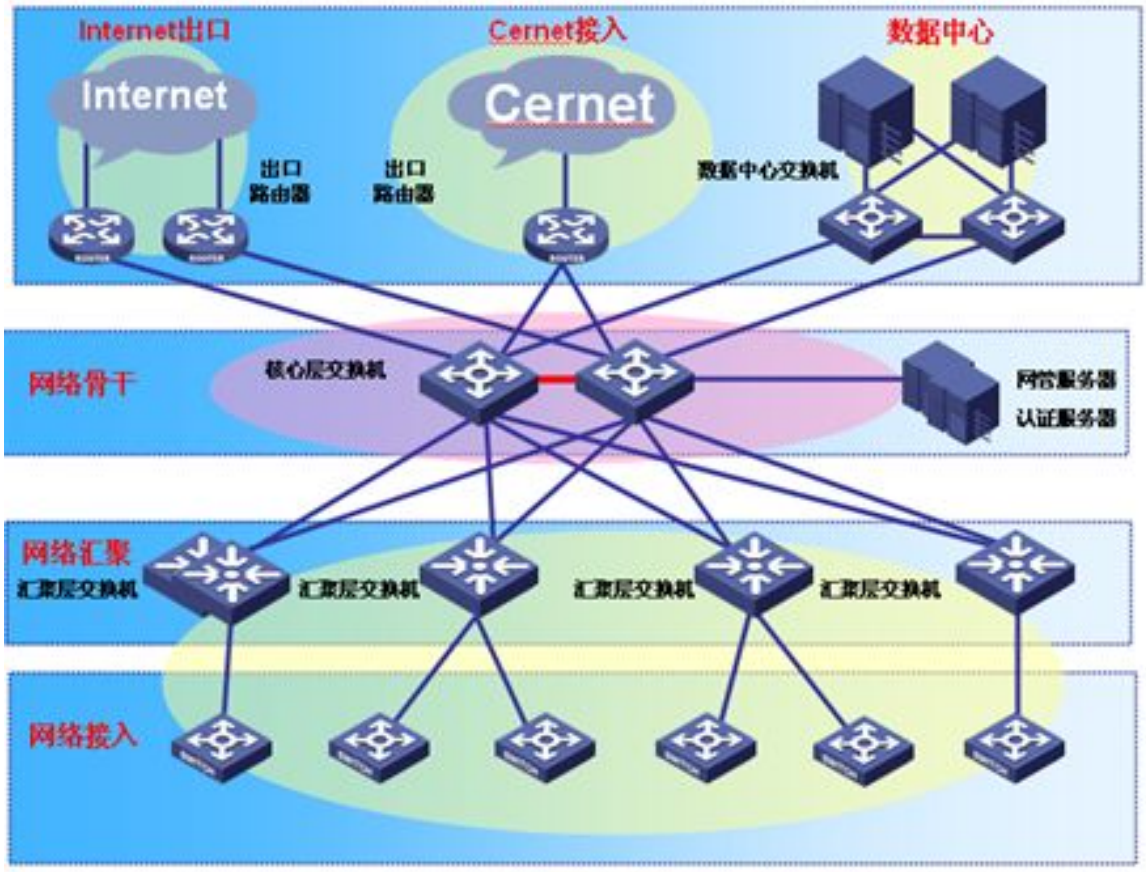

图 6-1 冗余拓扑图

Fig.6-1 Redundant topology

采用双核心交换机配置热备份路由协议 HSRP，互为备份，保证一台核心交换机发生故障时另一台能够保障校园网络依旧畅通。

高可靠性是大连工业大学校园网的设计目标之一。高可靠性设计通过多种层次的技术特性实现。设备的可靠性，具有多重冗余的关键部件（管理模块，交换矩阵，电源，风扇），线路卡在线插入和高冗余核心层设备。链路的可靠性，使用汇聚和核心实现之间的多个链接。链路层配置后路由的可靠性，冗余性，动态路由协议 OSPF，充分利用多链路的条件下，负载均衡或备份的执行情况，在适当的条件下。OSPF 协议可以在链路出现故障后，及时发现和路由收敛，探索了一条新路，来更新域间路由表项，以确保整个网络互联互通的可靠性。

6.2 管理 VLAN

管理 VLAN 用于管理接入交换机，每个交换机组成的 IP 子网的管理。管理 VLAN 和用户 VLAN 隔离，其主要目的是为了使用户能够与数据分离的管理交换数据，以提高网络设备可以控制和系统的安全性。用户 VLAN 是一样的，同样的管理 VLAN 终结设备的会聚装置上。

6.3 防火墙的选择

先进的思科 ASA5500 系列防火墙凭借其集成的防火墙和防-X 功能，Cisco ASA 5500 系列可以进入网络并影响威胁的业务运营，这是在网关处拦截它们在网络之外。这些服务也可扩展到远程访问用户，并提供一个威胁保护 VPN 连接。思科 ASA5500 系列解决方案提供：

1.可广泛部署的防火墙技术--Cisco ASA 5500 系列构建于 Cisco PIX 安全设备系列上面。其应用控制功能，以限制对等文件共享，即时传输消息和恶意流量的，因为它们可能导致安全漏洞，并且因此对网络的威胁。

2.市场领先的 Anti-X 功能 - 通过可选内容安全和控制安全服务模块（CSC-SSM）提供，思科 ASA 5510 自适应安全应用提供了全面的保护需要的重要的网络周边安全强大的 Anti-X 功能。

防病毒 - 屡获殊荣的防病毒技术是最有效的点在你的基础设施 - 互联网网关防御已知和未知病毒，保护您的内部网络资源。通过过滤电子邮件和 Web 流量在外围，而不需要开展资源密集型的恶意软件感染的清理，并帮助确保业务连续性。

防间谍软件 - 阻止通过互联网流量（HTTP 和 FTP）和进入您的网络电子邮件流量间谍软件，让 IT 支持人员不再需要昂贵的间谍软件清除过程，并提高员工的工作效率。

·防垃圾邮件 - 有效地阻止垃圾邮件，并且误报率极低，有助于保持电子邮件效率，不影响与客户，供应商和合作伙伴沟通。

解决方案给校园网带来优势：

思科 ASA5500 系列提供一个易于使用，并具有全面的安全解决方案，大规模的功能。它结合了优异的防火墙，VPN 和可选的 Anti-X 功能，让您的网络是一个很好的网络安全。与此同时，通过控制访问网络资源来保护业务数据，该解决方案也可以最大化网络的正常工作时间。通过控制文件共享和即时消息，垃圾邮件和过滤以除去可能出现其他威胁。 IT 资源免受病毒治疗，间谍软件清除和解放的系统清理任务。您也可以放心地，没有风险配置新的服务。

思科 ASA5500 系列解决方案提供的安全性和连接性，可以帮助你的网络：

满足不断变化的业务需求 – 通过为广泛的常见应用提供先进的应用层安全服务，以确保新应用的部署，包括那些基于应用程序，电子邮件，IP 语音（VoIP），视频和网络的多媒体应用。

用于访问控制的商业资源 – 提供了和 Microsoft Active Directory，轻型目录访问协议（LDAP）或 RSA 的 SecurID 服务紧密集成未经授权的访问基于身份的访问控制服务，以避免应用和信息。

降低清除成本 – 通过防止干扰发生，释放 IT 支持资源，减少了昂贵的去除间谍软件，病毒和其他恶意程序的软件。

提高运营效率 – 通过使用一个简单，易于安装和使用的解决方案，降低了部署和日常管理成本和监控安全解决方案。

这些优势使得思科 ASA5500 系列解决方案能够满足校园，校园网络的安全需求，帮助创造更多的价值。(具体产品介绍见附录 D)

6.4 防病毒软件

一般来说很多学校有很多的计算机，建立校园网各学校的教师与机器，机器室学生可以成功连接到网络，并通过转发服务器或路由器连接到外部网络。因此，更多的基于网络的病毒感染，一般文件类型，单一类型的病毒爆发的难以完全在学校网络，即使爆发只会影响一个的两台计算机，在多数情况下，直接回收系统网络管理员可以解决的。

因此，在普通学校病毒感染尤其是基于网络的蠕虫类病毒，主要是在一个非常大的传播力量，虽然根据教育部要求各公立学校购买了正版的杀毒软件，但理解网络安全和系统安全性的读者都知道，只有杀毒软件是不够的，怎么说没有什么杀毒软件杀毒能力，即使能够彻底查杀，如果你的系统漏洞没有及时安装适当的补救措施，那么，迟早会成为漏洞病毒的入侵。这是在学校的网络尤为明显，危害极大的感染都是大漏洞病毒。

综合两人在校园网漏洞型病毒存活属于一方面是最重要的蠕虫病毒的爆发，他会引起学校的整个网络完全瘫痪，而另一方面针对这种病毒的查杀是非常困难的。漏洞型病毒需要学校每台计算机安装系统补丁或软件更新，蠕虫，每台电脑都会有学校进行检测，发现病毒的原因，但在实践中往往多台电脑已成为毒品来源频繁影响其他数据包发送病毒的计算机。

7 网络管理设计

7.1 网络管理概述

如果网络能真正发挥效益取决于网络的管理。大学必须有一个网络管理员。网络管理和单一管理有重要的区别，其中包括大量的网络软件的维护，除了保证电子公告板，电子邮件执行情况的报告，论文，无纸化传输和网络等网络顺畅，更重要的是确保该网络的数据共享功能，对数据机密性的网络管理必须得到保证。和广泛的网络侧，涉及的人员，难免有瑕疵，犯错误，所以你必须设置网络管理，并结合一定的管理系统的发展，以确保网络的安全，可靠运行。

在大学校园网络，网络硬件，各端子的数量大时，有可能会被损坏。并与教师和学生使用学校计算机网络频率的增加，提高的幅度越大，网络的依赖，更大的影响是产生因网络故障，从而维护设备，以保证状态的正常运行网络管理员很重要的。

为了保证校园网的正常运行，学校必须制订网络公约，大家要尊重，个人的责任，以维护学校的计算机网络操作。每一个网络终端的奖罚制度，应设立负责落实，建立各种教学和科研管理制度，每个班级的管理体系，使一系列有效的制度，以保证网络的运行。

校园网络管理的主要目的是保证质量的网络操作，诸如维护网络的传输速率，以减少传输错误率，以保证网络的安全性。因此，校园网络系统管理技术人员对网络的管理工具或技术专长来实现自己的网络管理，内容可以分为以下几点：

系统管理及时了解网络的增加或　　减少在设备，管理组参数，所有网络设备的任何变化。当故障发生时，管理人员可重置或改变网络设备的参数，以保持网络的正常运行。

故障管理，确保网络系统的高稳定性，当网络出现问题时，你必须成为意识到了这个问题。它包含所有用于各种通信协议操作状态，通常的故障跟踪检查和测试记录的节点。

管理是评估网络系统的操作的效率，以及使用的通信协议，如网络资源的传输容量统计外，还提供未来网络升级或更新的基础的规划。

安全管理，防止未经授权的用户没有被授权使用网络资源和用户故意破坏安全的网络系统，我们应该始终做好安全措施，如法律和其他设备的访问控制和加密。

计费管理了解网络的使用时间，可以利用统计每个本地网。您可以使用网络作为基础进行充电，同时也为未来的网络升级或更新规划的参考。

信息转换成两部分的信息管理网络，第一个是，管理员设置信息，它们的质量是普遍较高;另一部分被置于由用户，可能存在一些问题，这部分的信息管理。

网络管理实施

1，网络管理员

网络管理员都是网络管理的骨干大型网络，派技术人员到全职网络管理网络的能力。除了网络管理员管理的网络，而且还负责培训用户等。

2，网络管理的实施

网络管理的实施，应抓住选用高品质的网络管理人员的以下关键环节，明确责任：

网络管理和操作流程的严格规则

选择合适的网管系统

认真训练

制定切实可行的网络管理规划和实施方案

建立和维护好各种证件

3，日常维护布线系统

布线系统做好日常维护工作，确保基础网络连接完好，正常的计算机网络，高效运行的基础。目前，除微波，卫星电视频道和其它无线连接城域网和广域网之间的互联，户外电缆敷设仍然是一个有线连接的唯一途径。布线系统的测试和维护通常依赖于双绞线测试仪和订单分析仪，测试仪通道，采用智能分析仪器，提高了布线的管理水平和效率可以更好的保证计算机正常运行的网络。

4，关键设备的管理

无论计算机网络的规模，关键设备的管理是一个非常重要的工作。这是因为关键设备在网络中的任何故障都可能导致网络瘫痪，给用户带来不可挽回的损失。校园网核心设备一般包括网络主干交换机，中心路由器和关键服务器。要通过除了自己以外的国家工作实时监控的网络管理软件管理这些关键的网络设备,,更多的是他们的备份。备份主干交换机，现在似乎比较几家公司能够提供系统的解决方案，因此只能由网络管理员加强以保持网络主干交换机的正常运行，在日常管理监控骨干交换机的性能和运行状况。

5，IP 地址管理

在 TCP / IP 协议今天成为事实上的行业标准，任何一台工作站的 TCP / IP 网络的主机都需要有一个有效的 IP 地址才能够正常工作。建设：规划计算机网络，组织内各部门应该准备为互联网服务调查和统计数据的需求来确定计算机网络的大小。 IP 地址管理是适当与否，是维持关键的计算机网络上运行效率的能力。如果 IP 地址管理手段完善，该网络很容易受到 IP 地址冲突，IP 地址将导致合法用户无法访问网络资源，影响网络的正常运行，

甚至有一些关键数据的损失。

6，其他管理

当然，对应于不同的网络环境，也有做了很多的管理。具有互连的内部网络和互联网，除了保持各种数据的可靠性，同时也保证机密数据的安全网络管理员。因此，计算机网络安全管理（例如防火墙设置）网络管理已成为一个非常重要的方面。

总结

规划校园网对每个学校来说都不是一件容易的事情，校园网不只是涉及技术方面的问题，而是包括网络设施、应用平台、信息资源、专业应用、人员素质等的综合化、信息化教学管理环境系统。因此，需要确立建设校园网的目标不仅要考虑技术方面，更要考虑环境、应用和管理等，必须与学校各方面改革、建设相结合，与学校长远相结合，论证和决策。根据这样的使用要求：建设一个技术先进、扩展性强、能覆盖全校主要楼宇的校园主干网络，将学校的各种 PC 机、工作站、终端设备和局域网连接起来，并与有关广域相连，形成结构合理、内外沟通的校园计算机网络系统。还有，学校的目的是通过教学过程来培养人才，因此对教学过程提供直接支持应是校园的基本功能；校园网必须能够支持学校的日常办公和管理；与 Internet 的联接也是校园网的基本功能之一。校园网要能很好地应用与发展，很大程度上取决于设计方案(包括组网技术、拓扑结构、IP 及路由规划、设备选型等)的设计实施成功与否。为了满足校园网的更先进和可扩展性，设计校园网的设计应尽量采用符合国际标准的、比较成熟的技术，兼顾网络技术的发展方向，选择结构化、可扩充、多用途的网络产品，保证网络在较长时间内不落后。同时网络设计应结构合理，在通信网络、资源配置、系统服务和网络管理上有良好的分层设计，使网络结构清晰，便于使用、管理和维护。另外网络应坚持高效实用的原则，着眼于教学、科研、管理的实际需要，用有限的资金优先解决工作急需的问题。最后，高的性价比是校园网设计的实际问题，对一个学校来说，经济的、实用的、适用的才是最好的。

在选型和画拓扑结构图时注意：路由器交换机的设备选型是针对现在国内网络的发展以及考虑校园网络将来的扩充作出的高性价比的选择方案，能够满足学校现在及将来十几年内对网络速率的要求。

使用 VLAN 对各个学院专业和行政部门的划分，可以实现使用逻辑拓扑解决物理上的连接问题，并且具有一定安全性。

通过该校园网的设计，本人完成了校园网的组网的规划工作。考虑到可行性因素，在写这篇论文中，在网络中搜索了大量的资料和阅读了大量的书籍资料，收获也甚多。最重要的一点是：对于这些设计需要的知识掌握的不够好，从而浪费了很多不必要的时间。因此，需要更多的学习和熟练。

致谢

本论文由曲长波老师对我进行指导，本人最初对整个设计流程不是很了解，对于内部的结构该如何架设也没有太多经验，有些知识概念自己掌握的还不是特别扎实，对很多关键性的知识有些模棱两可。正是由于曲老师对我孜孜不倦的指导与教授，让我对这些知识体系又有了更加深的认识，才完成这次毕业设计。原先只是学习书本上的知识，此次是运用已学过的知识去规划设计一个校园网络，使我对如何构建一个大型网络有了更多的经验。曲老师有着非常专业的知识，谨慎的指导理念，科学的教学方法，正是在曲老师无私的指导下我才能够完成此次设计。

此次设计我还参考了许多国内外的相关文献与资料，也为我完成此次设计提供了很大帮助，感谢他们。

最后感谢了我的同学尤其是我的室友，他们在我设计的时候提供给我许多建设性的意见，在此衷心感谢他们。

参考文献

[1] 谢希仁.计算机网络.电子工业出版社.2010
[2] 雷震甲.网络工程师教程.清华大学出版社.2011
[3] 校园网管理技术的体系架构及其实现.江宇.电子技术与软件工程.2015
[4] 数字化校园与信息化学习环境的研究.任晓霞.品牌.2015
[5] 高校校园网安全需求及安全方案设计.花丽.电子世界.2014
[6] 校园网的建设与实践.李图江.电子世界.2014
[7] 校园网网络安全体系模型设计研究.伍爱宝.东方企业文化.2013
[8] 高校无线校园网的设计.张旭.中国科技信息.2015
[9] 校园无线局域网的设计.董述杰.通信电源技术.2015
[10] 符水波.校园网系统维护与故障诊断.清华大学出版社.2013

附录 A 中文译文

校园范围内的无线网络分析

论文类别：计算机论文 - 互联网研究论文

发布时间:2005-11- 20 9 时 30 分 00 秒

摘要：了解使用模式，无线局域网（WLAN）的是为那些谁开发，部署和管理无线局域网技术，以及那些谁开发系统和应用软件，用于无线网络的关键。本文提出了从网络活动的规模最大，最全面的跟踪结果在一个大的，生产的无线局域网。十一个星期，我们追溯到近两千用户从一个普通的校园总体中抽取的活动，利用遍布达特茅斯学院 476 接入点的校园范围的网络。我们的研究扩展了那些由唐·贝克完成的，具有较大的显著和更广泛人群.我们发现，居住为主的交通所有其他流量，尤其是在住宅居住着新学员;学生越来越多地选择一个无线笔记本电脑作为他们的主计算机。虽然网络协议是交通量最大的单一组成部分，网络备份和文件共享贡献了意外大量的流量。虽然有一些内部的网络会话漫游，通过我们的情况，其中卡漫游过多，无法定居在一个接入点的数量感到惊讶。跨子网漫游是一个特殊的问题，因为他们打破 IP 连接，指示需要，以避免或容纳这样漫游方案。

关键词：无线网络，无线网络，802.11 无线局域网，工作负载特性

1.简介

无线局域网（WLAN）的日益普遍，特别是在大学校园和企业园区。例如，392 学术机构[5]现代的调查发现，几乎所有的计划，安装无线网络，大约有一半已经拥有有限的部署，以及少数（7%），有一个“全面”的部署。尽管技术如 IEEE 802.11b 的广泛部署和使用急剧增加，鲜为人知的是，如何将这些网络中使用。在实际的 WLAN 使用模式的清晰理解是为那些谁开发，部署和管理无线局域网技术的重要信息，和那些谁开发的系统和应用软件的无线网络这提出从一个庞大而全面的跟踪网络活动的结果大，生产的无线局域网。达特茅斯学院有 11 Mbps 的 802.11b 的覆盖整个从 2001 年秋季学期整个网络几乎每一幢建筑物的校园，包括所有行政，学术和住宅楼，以及最具运动可行性.我们广泛收集跟踪信息（此写在 2003 年 4 月，该网络包括超过 550 个接入点。）于波局域网研究唐与贝克[17]，其中 74 追溯到计算机科学的用户在一个大楼 12 周，我们的工作显著扩展。我们的研究跟

踪近两千用户从一个普通的校园人群得出，在整个 161 大楼一学期（11 周）。它也扩展了的 Metricom 研究唐与贝克[16,18]，其跟踪的城域网七周。虽然，微量涵盖广泛的地理区域和接近 25,000 的用户，我们的跟踪包括有关网络负载的量和性质的详细信息已使用 SNMP 来跟踪四个[2]，109 [9]和 117 [3 网络种群多样性和细节我们的数据采集]接入点，但从来没有在我们研究的规模，或者与我们的 syslogs.尺寸提供了详细的移动数据，提供了广泛深入的无线网络使用.尽管每个环境都是不同的，我们的研究有下一个描述我们的研究第 3 节环境，达特茅斯学院的校园里，然后我们详细追查的方法在第 4 节，我们提出和讨论的最有趣的特性常见的住宅和企业发展特点数据。第 5 节比较我们的结果与早期的研究，和第 6 节得出结论。

2.测试环境

达特茅斯学院的校园紧凑，有超过上 200 亩，包括行政，学术，住宅和建筑物的运动 161 建筑。每一个建筑是连接到校园骨干网。每一间办公室，宿舍，和报告厅，并在一些地方每个座位的报告厅，已有线以太网。在 2001 年达特茅斯安装 476 接入点从思科系统，每一个型号的 Aironet 350，提供 11 Mbps 的覆盖几乎整个校园。每个接入点（接入点）的范围为约 130-350 英尺的室内，所以有多个接入点，但在所有的建筑物最小。虽然没有具体的努力，涵盖室外空间，校园紧凑，内部的接入点往往覆盖大部分的户外 spaces.All 接入点共享相同的网络名称（SSID），无线使客户能够无缝漫游，从一个接入点到另一方面，在建筑物的接入点被通过交换机或集线器到建筑物的现有子网连接。在 161 覆盖建筑物跨越 81 子网，所以在许多情况下，无线客户端从一个建筑物漫游到另一个将被迫安排一个新的 IP 地址。 （达特茅斯选择不建立一个独立的校园范围的子网无线网络，无线安德鲁项目[4]。不同）达特茅斯学院拥有约 5500 名学生和 1,215 全时间教授。在 2001 年秋季大约 3,330 未毕业的学生住在校园里。拥有电脑的每个要求。每年，大约在研究生 1000 进入达特茅斯学院，并通过校园计算机店内大部分购买电脑。这些购买的电脑，笔记本电脑已经变得越来越占优势，近年来：在 1999 年的 27％，在 2000 年的 45％，在 2001 年 70％，88％in2002。假设学生获得计算机别的地方选择在同一个分数的笔记本电脑，并在 1998 年（对于没有数据可用），约 15％的笔记本电脑购买的，约 40％在 2001 年秋季的笔记本电脑拥有在我们研究的时间本科生。所有的笔记本电脑购买入夏以来 2001had 内置无线支持，以及超过 1000 802.11b 的卡是在 2000-2001 年出售给其他用户。企业的塔克商学院要求所有 480 名学生，以自己的笔记本.此外，大多数工程学校毕业的学生，自己的笔记本电脑。我们估计，大约一半的笔记本电脑是无线功能的 2001 年秋季。

3.跟踪收集

我们开始于 2001 年 4 月被安装在第一接入点时收集的数据。后的数据 2001 年 5 月初步研究[15]，我们开始全面的数据采集时的学生在 2001 年 9 月通过回到校园在本文中，我们重点关注的十周的秋季 2001 学期间收集的数据周二 9 月 25 日周一 12 月 10 日，包容性。虽然我们事先和大约一个月后，有数据为一个星期左右，有放假期间显著较少使用，所以我们限制了我们的分析到活动 period.At 跟踪周期的开始有 465 接入点（接入点）。十多个接入点分别安装在第一个月由 10 月 21 日正如我们下面讨论，使总数达到 476，则显得有些的“安装”接入点并没有完全正确或者在跟踪期内然而配置，这导致在我们的数据。我们代表更少的接入点使用三种技术来收集有关无线网络使用数据：syslog 事件，SNMP 轮询和 TCP 监听器转储。

3.1。系统日志

我们配置接入点发送的每一个客户端卡认证，相关的时间系统日志消息，重新关联的关联，或者 deauthenticated 与接入点（见下文定义）。系统日志消息通过 UDP 到达在我们的实验室，里面记录了所有的 3533352 人或更高版本分析.大多数接入点促成了系统日志跟踪，尽快为他们进行配置和安装的服务器。 476 接入点中，只有 430 人表示在我们的痕迹。虽然有些似乎从来就没有被使用，许多人错误地配置并没有派出 syslog 消息。此外，我们有不完整的数据时，校园经历了停电，或中央 syslog 进程显然挂了几个日期。最后，由于 Syslog 使用 UDP 有可能是某些消息丢失或乱序。由于这些时空孔犯罪所造成的痕迹，我们的一些统计数据将在数实际活动.我们系统日志记录的服务器增加了一个时代夯实，以每封邮件到达时。每个消息包含接入点名称，卡的 MAC 地址，和消息的类型认证。前一个卡片可使用网络时，它必须验证。我们忽略此消息关联。认证之后，卡选择的在范围内的接入点和关联到特定的接入点之一;所有流量从那张卡片通过接入点

.Reassociated。卡监视来自接入点的周期性信标和（基于信号强度或其他因素）可以选择重新关联另一个接入点。此功能支持漫游。不幸的是，有些卡显然从未使用重新关联协议，并始终使用准漫游。当卡重新关联一个新的接入点，新的接入点上广播以太网该事实;在收到的旧接入点发出的 syslog“漫游”的消息。我们忽略此消息;因为它依赖于 IP 层之下的接入点间协议，它只有当一个卡漫游到另一个接入点相同的子网内发生。

关联。当卡不再需要网络时，它断开与它的当前接入点。然而，我们发现，该系统日志中几乎不含这样的消息。

Deauthenticated。虽然可以为显卡要求解除认证，这几乎从来没有发生在我们 log.Normally，

相关接入点

deauthenticates 卡之后 30 闲置分钟。在我们的记录是很常见的看到几个解除认证消息广泛漫游卡，从访问会话中的每个子网一个消息;我们忽略所有但从最近接入点.我们网络的消息中不再接入点使用 MAC 层认证，或在 DHCP 服务器的 IP 层的认证。任何卡可以与任何接入点关联，并获得一个动态的 IP 地址。因此，我们不知道用户的身份，并提供给用户的 IP 地址，从时间变化到时间和建筑物的建筑。我们做近似的假设等同于用户卡，尽管一些用户可能有多个卡，或者有些卡可以由多个用户.在共享本文中，我们使用术语“牌”精密，虽然与意图卡用户大约。

3.2。 SNMP

我们使用简单网络管理协议（SNMP）来定期轮询受影响; 476 的接入点 回应我们的调查。我们选择轮询每隔 5 分钟，以获得信息合理频繁，计算和带宽可用的范围内对我们的两个轮询工作站.我们迹周期包括这些 SNMP 记录 193111734。不幸的是，我们有不完整的数据的日期如下：10 月 7 日，9，和 12（维护我们的服务器），11 月 19 日（不明原因），而 12 月 5 日（校园范围停电）。我们选择完全排除这些日期从我们的分析，因为我们大部分的基于 SNMP 的地块检查每天的流量，这个数字会由“短”天.每个民调返回最近有关客户站的 MAC 地址被污染，而目前两个计数器，一个用于入站字节，一出站字节值。轮询当接入点没有重置计数器，那么我们计算并且由一个轮询检索的值由下一个轮询检索到的值之间的差。该计数器是 32 位无符号整数，而我们计算妥善处理反翻车。我们忽略的结果，但是，在两种情况下：（1）当成功轮询之间的时间超过 12 分钟（两次轮询间隔加上少许松弛）;（b）在所得到的字节数大于所述无线接口可以发送或自上次民意测验时收到的。在前一种情况下，接入点是无法访问一个以上的民意调查中，我们都不清楚多少次计数器可能会在那些错过投票卷起。在后一种情况下，接入点（及其计数器）进行可能重置由于维护或失败.尽管每个 SNMP 记录包含与接入点关联卡的列表的功率，我们选择使用的系统日志数据进行跟踪卡，因为日志数据提供精确的系列每张卡的事件，而 SNMP 轮询的数据是不太精确。

3.3。监听器

系统日志和 SNMP 的痕迹让我们来计算有关交通，用户和移动性基本统计资料。为了获得更好的画面什么样的用户在做与网络，我们使用的 TCP 转储捕获所有的数据包报头在选择校园周围的接入点的。因为数据和隐私问题的容积的，我们只记录分组报头。因为数字和受影响的地理分布，我们的网络结构（许多子网和交换以太网），和交通量，这是不

可能的，以捕获所有的无线通信。在每一个四个位置我们连接有计算机和建筑物的接入点到一个公共集线器，并附着在校园网络上的轮毂的上行链路到交换机端口。在混杂模式这种“嗅探器”，我们使用的 TCP 转储记录每一个数据包经过的头;在我们后面的分析中，我们只专注于无线嗅探器包.Our 记录往往无关他们的枢纽无线接入点的数据包，所以我们需要一种方法不仅要研究无线数据包。以决定在给定的分组是否是无线，我们检查了源和目的地 MAC 地址在其以太网帧，并与出现在我们的系统日志微量的 MAC 地址的列表进行比较。不幸的是，tcpdump2 记录无效的 MAC 地址的所有结构 3 对于包含 IP 数据包，我们检查了源和目的 IP 地址的帧大约 8%;如果 IP 地址是与一个最近的 IP 分组中的有效的，无线的 MAC 地址相关联，那么，我们假定这个分组中使用的相同的 MAC，并把它作为一个无线数据包。我们固定的约三分之一坏互助这种方式。对于不包含 IP 数据包的帧，我们无法修复的 MAC 地址，因此假定该帧不是无线的。这样一来，我们在计数的非 IP 无线结构.我们统计选择了四个具有代表性的地方

我们在努力了解在网络.尽管我们的人口大和多样化的活动模式进行无线局域网用户的大型跟踪为基础的研究，它的上下文中理解我们的结果是很重要的。我们居住的大学校园人口可能无法反映周活动在企业园区，公共场所，或其他场所.活动和交通变化很大，从小时到一小时，一天又一天，和一周。虽然我们确实看到清晰的每日和每周的模式，他们反映住宅的校园和一个混合的学术工作，其中包括隔夜多比使用中可能企业 WLAN 是共同的。我们发现，许多无线网卡都是非常积极的与接入点关联时，导致了大量的短期“会话”，并在回话关于漫游漫游参与会议的 17%的高度，而这些“移动会话”约 40%涉及漫游到一个不同子网.从轶事证据，这些额外的子网漫游常时，当用户是静止的，从而导致 IP 拥塞.网络设计者失败应该注意高方差在建筑物，接入点的活动发生，和卡片，在这两个时间和空间。我们需要新的解决方案，以防止卡从漫游太频繁，不牺牲覆盖。我们需要网络层[13]和应用层的解决方案，以支持多子网漫游。最后，请注意，未拥塞明确出站入站或比拥塞每天都在变化显著为主，建设以建设，协议的协议。这一结论反驳了非对称带宽.在任何设计的无线项目的早期阶段，工作人员在达特茅斯学院辩论是否会重要的是提供无线覆盖的宿舍，这已经与有线居民每人至少一个端口。我们的数据表明，大部分无线活动的发生在住宅。此外，对于无线网络连接是有用的 TOA 移动用户，它需要普及，使用户能够抓住他们的笔记本电脑在路上出了门，相信将有网络接入的地方，他们可以走了。然而，我们看到，大多数用户很少访问接入点和建筑物在跟踪的生活，大多数用户是固定在一个会话中。

附录 B 英文原文

Analysis of a Campus-Wide Wireless Network

DAVID KOTZ * *

Department of Computer Science, Dartmouth College, Hanover, NH 03755, USA

KOBBY ESSIEN

Department of Bioengineering, University of Pennsylvania, 120 Hayden Hall, 3320 Smith Walk, Philadelphia, PA 19104, USA

Abstract. Understanding usage patterns in wireless local-area networks (WLANs) is critical for those who develop, deploy, and manage WLAN technology, as well as those who develop systems and application software for wireless networks. This paper presents results from the largest and most comprehensive trace of network activity in a large, production wireless LAN. For eleven weeks we traced the activity of nearly two thousand users drawn from a general campus population, using a campus-wide network of 476 access points spread over 161buildings at Dartmouth College. Our study expands on those done by Tang and Baker, with a significantly larger and broader population.We found that residential traffic dominated all other traffic, particularly in residences populated by newer students; students are increasingly choosing a wireless laptop as their primary computer. Although web protocols were the single largest component of traffic volume,network backup and file sharing contributed an unexpectedly large amount to the traffic. Although there was some roaming within a network session, we were surprised by the number of situations in which cards roamed excessively, unable to settle on one access point. Cross-subnet roams were an especial problem, because they broke IP connections, indicating the need for solutions that avoid or accommodate such roams.

Keywords: wireless network, Wi-Fi, 802.11, WLAN, workload characterization

1. Introduction

Wireless local-area networks (WLANs) are increasingly common,particularly on university and corporate campuses. For example, a contemporary survey of 392 academic institutions[5] found that nearly all plan to install a wireless network,about half already have a limited deployment, and a few(7%) have a “comprehensive” deployment. Although technology such as IEEE 802.11b is broadly deployed and usage is increasing dramatically, little is known about

how these networks are used. A clear understanding of usage patterns in real WLANs is critical information for those who develop, deploy,and manage WLAN technology, and those who develop systems and application software for wireless networks.This paper presents results from a large and comprehensive trace of network activity in a large, production wireless LAN. Dartmouth College has 11 Mbps 802.11b coverage for nearly every building on campus, including all administrative,academic, and residential buildings, and most athletic facilities.We collected extensive trace information from the entire network throughout the Fall term of 2001. (As of this writing in April 2003, the network includes over 550 access points.)Our work significantly expands upon the Wave LAN study by Tang and Baker [17], which traced 74 computer-science users in one building for 12 weeks. Our study traces nearly two thousand users drawn from a general campus population,across 161 buildings for one academic term (11 weeks).It also expands upon the Metricom study by Tang and Baker [16,18], which traced a metropolitan-area network for seven weeks. Although that trace covers a wide geographical area and almost 25,000 users, our trace includes detailed information about the amount and nature of the network traffic.Others have used SNMP to trace networks of four [2], 109 [9],and 117 [3] access points, but never on the scale of our study,or with the detailed movement data provided by our syslogs.The size, population diversity, and detail of our data collection offers extensive insight into wireless network usage.Although every environment is different, our study has characteristics common to both residential and enterprise deployments.We next describe the environment of our study, the campus of Dartmouth College, and then detail our tracing methodology in section 3. In section 4 we present and discuss the most interesting characteristics of the data. Section 5 compares our results with those of earlier studies, and section 6 draws conclusions.

2. The test environment

The Dartmouth College campus is compact, with over 161buildings on 200 acres, including administrative, academic,residential, and athletic buildings. Every building is wired to the campus backbone network. Every office, dorm room, and lecture hall, and in some places every seat in a lecture hall,has wired Ethernet. In 2001 Dartmouth installed 476 access points from Cisco Systems, each an Aironet model 350, to provide 11 Mbps coverage to nearly the entire

campus. Each access point (AP) has a range of about 130–350 feet indoors,so there are several APs in all but the smallest buildings. Although there was no specific effort to cover outdoor spaces,the campus is compact and the interior APs tend to cover most outdoor spaces.All APs share the same network name (SSID), allowing wireless clients to roam seamlessly from one AP to another.On the other hand, a building's APs are connected through a switch or hub to the building's existing subnet. The 161 covered buildings span 81 subnets, so in many cases a wireless client roaming from one building to another will be forced toobtain a new IP address. (Dartmouth chose not to construct a separate campus-wide subnet for the wireless network, unlike the Wireless Andrew project [4].)Dartmouth College has about 5,500 students and 1,215full-time professors. During Fall 2001 approximately 3,330undergraduate students lived on campus. Each is required to own a computer. Each year, approximately 1000 under graduate students enter Dartmouth College, and most purchase a computer through the campus computer store. Of those purchases,laptops have become increasingly dominant in recent years: 27% in 1999, 45% in 2000, 70% in 2001, and 88% in2002. Assuming that that students obtaining computers else where choose laptops in the same fraction, and that in 1998(for which no data is available) about 15% purchased laptops,about 40% of undergraduates owned laptops at the time of our study in Fall 2001. All laptops purchased since summer 2001had built-in wireless support, and over 1000 802.11b cards were sold over the 2000–2001 year to other users. The Tuck school of business requires all 480 students to own laptops.In addition, most engineering-school graduate students, own laptops. We estimate that about half of those laptops were wireless-enabled in Fall 2001.

3. Trace collection

We began collecting data in April 2001, when the first access points were installed. After preliminary study of the data in May 2001 [15], we began full-scale data collection when students returned to campus in September 2001. In this paper we focus on the data collected during the eleven-week Fall 2001term, Tuesday September 25 through Monday December 10,inclusive. Although we have data for about a week prior and about a month after, there was significantly less usage during vacation periods and so we limit our analysis to the active period.At the beginning of the trace period there were 465 access points (APs). Eleven more APs

were installed in the first month to bring the total to 476 by October 21. As we discuss below, it appears that some of the “installed” APs were not completely or correctly configured during the tracing period,however, which resulted in fewer APs represented in our data.We used three techniques to collect data about wireless network usage: syslog events, SNMP polling, and tcp dump sniffers.

3.1. Syslog

We configured the access points to transmit a syslog message every time a client card authenticated, associated, reassociated disassociated, or deauthenticated with the access point(see definitions below). The syslog messages arrived via UDP at a server in our lab, which recorded all 3,533,352 of them or later analysis.Most APs contributed to the syslog trace as soon as they were configured and installed. Of the 476 APs, only 430 were represented in our trace. Although some appear never to have been used, many were misconfigured and did not send syslog messages. Furthermore, we have incomplete data for a few dates when the campus experienced a power failure, or whena central syslog daemon apparently hung up. Finally, since syslog uses UDP it is possible that some messages were lost or misordered. As a result of these spatial and temporal hole sin the trace, some of our statistics will under count actual activity.Our syslog-recording server added a times tamp to each message as it arrives. Each message contained the AP name,the MAC address of the card, and the type of message

Authenticated. Before a card may use the network, it must authenticate. We ignore this message.

Associated. After authentication, a card chooses one of the in-range access points and associates with that AP; all traffic to and from the card goes through that AP

.**Reassociated.** The card monitors periodic beacons from the APs and (based on signal strength or other factors)may choose to reassociate with another AP. This feature supports roaming. Unfortunately, some cards apparently never use the Reassociate protocol, and always use Associate

Roamed. When a card reassociates with a new AP, the new AP broadcasts that fact on the Ethernet; upon receipt, the old AP emits a syslog “Roamed” message. We ignore this message; because it depends on an inter-AP protocol below the IP layer, it only occurs when a card roams to another AP within the same subnet.

Disassociated. When the card no longer needs the network,it disassociates with its current AP. We found, however,that the syslog contained almost no such messages.

Deauthenticated. While it is possible for the card to request deauthentication, this almost never happened in our log.Normally, the associated AP deauthenticates the card after30 minutes of inactivity. In our log it is common to see several deauthentication messages for a widely roaming card,one message from each subnet visited in the session; we ignore all but the message from the most recent AP.Our network does not use MAC-layer authentication in theAPs, or IP-layer authentication in the DHCP server. Any card may associate with any access point, and obtain a dynamic IP address. We thus do not know the identity of users, and the IP address given to a user varies from time to time and building to building. We make the approximating assumption to equate cards with users, although some users may have multiple cards, or some cards may be shared by multiple users.Throughout this paper we use the term “card” for precision,although with the intention that cards approximate users.

3.2. SNMP

We used the Simple Network Management Protocol (SNMP) to periodically poll the APs; 451 of the 476 APs responded to our polls. We chose to poll every 5 minutes to obtain information reasonably frequently, within the limits of the computation and bandwidth available on our two polling workstations.Our trace period includes 193,111,734 of these SNMP records. Unfortunately, we have incomplete data for the following dates: October 7, 9, and 12 (maintenance of our server), November 19 (unknown causes), and December 5 (a campus-wide power failure). We chose to entirely exclude those dates from our analysis, because most of our SNMP based plots examine traffic per day, a number that would be polluted by “short” days.Each poll returned the MAC addresses of recently associated client stations, and the current value of two counters,one for inbound bytes and one for outbound bytes. The AP does not reset the counters when polled, so we compute the difference between the values retrieved by one poll and the values retrieved by the next poll. The counters are 32-bit unsigned integers, and our computation properly handles counter roll-over. We ignore the result, however, in two instances:(a) when the time between successful polls is more than 12 minutes (twice the polling interval plus a little slack);(b) when the resulting number of bytes is more than the wireless

interface could have sent or received in the time since the last poll. In the former case, the AP was unreachable for more than one poll, and we were unsure how many times the counter may have rolled during those missed polls. In the latter case, the AP (and its counters) were likely reset due to maintenance or a power failure.Although each SNMP record contains a list of cards associated with the AP, we chose to use the syslog data for tracking cards because the syslog data provides the exact series of events for each card, whereas the SNMP polling data was less precise.

3.3. Sniffers

The syslog and SNMP traces allowed us to compute basic statistics about traffic, users, and mobility. To get a better picture of what the users were doing with the network, we used tcp dump to capture all of the packet headers on a selection of the APs around campus. Because of the volume of data,and privacy concerns, we recorded only packet headers. Because of the number and geographic distribution of APs, the structure of our network (many subnets, and switched Ethernet),and the volume of traffic, it was not possible to capture all of the wireless traffic. In each of four locations we attached a computer and the building's APs to a common hub,and attached the hub's up link to a switch port on the campus network. With this "sniffer" in promiscuous mode, we used tcp dump to record the header of every packet passing by; in our later analysis, we focus only on the wireless packets.Our sniffers often recorded packets unrelated to the wireless access points on their hub, so we needed a way to study only the wireless packets. To decide whether a given packet was wireless, we examined the source and destination MAC addresses in its Ethernet frame, and compared them with a list of MAC addresses appearing in our syslog trace. Unfortunately,tcpdump2 recorded invalid MAC addresses for about78% of all frames.3 For frames containing IP packets, we examined the source and destination IP address; if the IP address was associated with a valid, wireless MAC address in a recent IP packet, then we assumed this packet used the same MAC,and treated it as a wireless packet. We fixed about a third of bad MACs this way. For frames not containing an IP packet,we were unable to repair the MAC address and thus assumed the frame was not wireless. As a result, our statistics under count non-IP wireless frames.We chose four representative locations:

We conducted a large trace-based study of wireless LAN users in an effort to understand patterns of activity in the network.Although our population was large and diverse, it is important to interpret our results within its context. Our residential university campus population may not reflect activity on a corporate campus, a public space, or other venues.The activity and traffic varied widely from hour to hour,day to day, and week to week. While we do see clear daily and weekly patterns, they reflect a mixture of a residential campus and an academic workplace, including more overnight usage than might be common in enterprise WLANs. We found that many wireless cards are extremely aggressive when associating with access points, leading to a large number of short “sessions” and a high degree of roaming within sessions.About 17% of sessions involved roaming, and of these “mobile sessions” about 40% involved roaming to a different subnet.From anecdotal evidence, these extra-subnet roams often occur when when the user is stationary, leading to failures of IP traffic.Network designers should note the high variance in the activity of buildings, access points, and cards, over both timeand space. We need new solutions to prevent cards from roaming too frequently, without sacrificing coverage. We need network-layer [13] and application-layer solutions to support multi-subnet roaming. Finally, note that the trafficis not definitively dominated by outbound or inbound traffic.The ratio varied significantly from day to day, building to building, and protocol to protocol. This conclusion argues against any design with asymmetric bandwidth.In the early stages of the wireless project, the staff at Dartmouth College debated whether it would be important to provide wireless coverage in the dormitories, which were already wired with at least one port per resident. Our data shows that the bulk of wireless activity occurs in the residences. Furthermore,for wireless network connectivity to be useful toa mobile user, it needs to be pervasive, allowing the user to grab their laptop on the way out the door, confident that there will be network access wherever they may go. Nonetheless,we saw that most users visited few APs and buildings over the life of the trace, and most users were stationary within a session.

附录 C 部分配置命令

Router1

```
interface FastEthernet0/0
 ip address 2.2.2.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 2.2.2.3 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 2.2.2.4 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 network 2.0.0.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 2.2.2.2
```

Switch0（核心层交换机）

```
interface FastEthernet0/1
 no switchport
```

```
 ip address 2.2.3.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/2
 no switchport
 ip address 2.2.3.5 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/3
 no switchport
 ip address 2.2.3.9 255.255.255.252
 duplex auto
 speed auto

interface GigabitEthernet0/1
 no switchport
 ip address 2.2.2.6 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no switchport
 ip address 2.2.2.13 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
```

```
 shutdown
!
router eigrp 100
 network 2.2.0.0 0.0.255.255
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 2.2.2.5
ip route 0.0.0.0 0.0.0.0 2.2.2.14 10
```

Switch 1

```
interface FastEthernet0/1
 no switchport
 ip address 2.2.2.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/2
 no switchport
 ip address 2.2.2.5 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/3
 no switchport
 ip address 2.2.2.9 255.255.255.252
 duplex auto
 speed auto
```

```
interface GigabitEthernet0/1
 no switchport
 ip address 2.2.2.11 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no switchport
 ip address 2.2.2.14 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 network 2.2.0.0 0.0.255.255
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 2.2.2.9
ip route 0.0.0.0 0.0.0.0 2.2.2.13 10
```

Switch3（汇聚层交换机）

```
ip dhcp pool 10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.2
 dns-server 192.168.0.100
ip dhcp pool 20
```

```
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.2
 dns-server 192.168.0.100
ip dhcp pool 30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.2
 dns-server 192.168.0.100
ip dhcp pool 40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.2
 dns-server 192.168.0.100
ip routing

interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/1
 no switchport
 ip address 2.2.3.6 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no switchport
 ip address 2.2.2.6 255.255.255.252
```

```
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
!
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
!
router eigrp 100
 network 192.168.0.0 0.0.255.255
 network 1.1.0.0 0.0.255.255
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.3.5
ip route 0.0.0.0 0.0.0.0 1.1.2.5 10
```

接入层交换机：

```
interface FastEthernet0/1
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport access vlan 30
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport access vlan 40
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport access vlan 50
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 60
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan 70
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport access vlan 80
```

```
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport access vlan 90
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport access vlan 100
 spanning-tree portfast
!
interface GigabitEthernet1/1
 switchport mode trunk
!
interface GigabitEthernet1/2
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

附录 D 设备清单和设备简单介绍

设备名称	品牌	标配 参数	数量	单价	合计
服务器	戴尔 PowerEdge 12G R720(Xeon E5-2609/2GB/30	CPU 型号：Xeon E5-2609 标配 CPU 数量：1 颗 硬盘接口类型：SAS	5	12000	60000

	0GB)	标配硬盘容量：300GB 内存类型：ECC DDR3 内存容量：2GB			
磁带机	HP StorageWorks DAT 72e USB 72GB DAT(DW027A)	记录格式：ANSI/ISO/ECMA, DDS-3, DDS-4 和 D... 存储容量：36GB 压缩后存储容量：72GB 接口类型：Ultra-Wide SCSI LVD 持续传输率：3 MB/秒(10.8 GB/小时)本机、6 M... 脉冲传输率：6 MB/秒最大异步，40 MB/秒最大	2	4700	9400
交换机	CiscoCatalyst2960-S	传输速率：10/100/1000Mbps	15	15000	225000
	CISCO WS-C3750X-48P-S	传输速率 10/100/1000Mbps 闪存：64MB 交换方式存储-转发 背板带宽 160Gbps 包转发率 101.2Mpps MAC 地址表 4K 产品内存 DRAM:256MB	6	40000	240000
	CiscoCatalyst6500	Supervisor 1 MSFC：15Mpps Supervisor 2 MSFC：210Mpps Supervisor 720：400Mpps 32Gbps 共享总线 256Gbps 交换矩阵 720Gbps 交换矩阵	2	30000	60000
防火墙	ASA5500	千兆级 并发连接数 130000 网络吞吐量最高 300Mbps 安全过滤带宽 170Mbps	1	12000	12000

		用户数限制无用户数限制用户入侵检测 DoS			
机柜	跃图高档服务器机柜 ADT61042-C	类型：服务器机柜 容量：42U 标准：19 英寸国际标准 高度：2000mm 宽度：600mm 深度：1000mm	10	3600	36000
配线架	康普	100 对配线架	48	300	14400
光纤盒	康普	机柜式光纤收发器	6	850	5100
UPS	山特 K500	后备式 0.5kva 输出电压范围 220（1+10%）V 输出频率范围 50Hz ± 1Hz	20	300	6000
	山特 A UPS-24K	电源阵列 24kva 输出电压范围 215-224V 输出频率范围 50±0.25Hz	2	20000	40000
5 类线	康普	200 米/箱	500	200	100000
水晶头	TCL 电工	RJ-45 接口	2000	2	4000
总计	——	——	——	——	811900

项目 线路类别	一次性费用（元）					专线使用费（元）	
	初装	工程	设 备	调 测	小 计	基本流量(元/ 年)	线 路 租 金(元/ 月）
光纤接入	10000		81.19 万	3000		10 万	
布线施工	10000	10000					
_____类							
合 计	20000	10000	81.19 万	3000		10 万	

合计 94.49 万元