南京信息工程大学

滨江学院

《计算机网络安全》期末课程设计

（2020 -- 2021 年度第 2 学期）

课程名称：　计算机网络安全
题　　目：　校园计算机网络安全设计与实现
院　　系：　计算机学院
班　　级：　软工18级2班
学　　号：　20182344050
姓　　名：　毛济洲
指导教师：　王玉祥

日期：2021 年 05月 28日

目录

一、课程设计要求

通过学习计算机网络安全，设计校园计算机网络。

(1) 利用计算机网络安全技术进一步扩展校园网的覆盖范围，使全校师生能够随时随地、方便高效地使用校园网络；

(2) 提高校园网络安全，提升管理水平和效率，推动学校信息化建设；

(3) 要覆盖部分原来没有有线网的空间，诸如：食堂、礼堂、教室；

(4) 本工程是在校园有线网的基础上加以无线扩充（主要对网络安全方案设计）；

(5) 保证网络访问的安全性；采用非独立型的无线网络结构选型（即：有线无线结合）。

二、 引言:

教育信息化是我国信息化的重要组成部分，校园网建设是我国教育信息化的基础。随着计算机网络技术的发展，校园网建设已取得了可喜的进展。校园网的建设改变了传统的教学模式、教学方法和教学手段，促进了教育观念、教学思想的转变，大大拓展了教师和学生的视野。校园网网络系统是一个非常庞大而复杂的系统，它不仅为现代化教学、综合信息管理和办公自动化等一系列应用提供基本操作平台，而且能提供多种应用服务，使信息能及时、准确地传送给各个系统。而校园网工程建设中主要应用了网络技术中的重要分支局域网技术来建设与管理的，因此本毕业设计课题将主要学校园局域网络建设过程可能用到的各种技术及实施方案为设计方向，为校园网的建设提供理论依据和实践指导。

三、需求分析:

3.1环境需求

根据南京信息工程大学滨江学院实际情况粗略计算出各个大楼节点数以及与校园网信息中心的距离如下表所示:

部门名称	节点数	建筑层数	与信息中心的距离
行政楼	1000	6	50–100
金融院楼	1000	6	280
物联网学院楼	1000	6	360
气象学院楼	1000	6	300

部门名称	节点数	建筑层数	与信息中心的距离
图书馆	200	9	400
实验楼	2000	6	500
宿舍楼	20000	6	（多值）

3.2功能需求

（1）连接校内所有教学楼、实验室、办公楼中的PC。

（2）支持大量同时用户浏览Internet。

（3）对于多媒体形式的数据如语音、图象、动画演示、视频点播等，网络应该及时、高效地完成数据传输，确保电子教学的正常运做。满足学生上机要求。

（4）提供丰富的网络服务，实现广泛的软件，硬件资源共享。

3.3 性能需求

（1）校园网应能促进教师和学生尽快提高应用信息技术的水平。

（2）校园网为教师提供了一种先进的辅助教学工具、提供了丰富的资源库，所以校园网是学校进行教学改革、推行素质教育的一种必不可少的工具。

（3）校园网是学校现代化管理的基础，深入、全面的学校信息管理系统必须建立在校园网上。

（4）校园网提供了学校与外界交流的窗口，学校应将校园网与互联网联接，这也是学校信息化的要求，做到了这一步，通过校园网去了解世界、在互联网上树立学校的形象都是很容易的。

3.4 网络规模需求

网络应该支持大规模的数据库应用。随着我国基础教育水平的提高，通过网络运行基于服务器/客户机的数据库查询检索是日常教学中教师和学生经常要进行的活动。如何确保数据库查询迅速及时地得到反馈是网络应该注意的问题。

3.5 网络拓扑结构需求

随着校园网对因特网接入需求的增加，应该考虑校园网能够顺利实现与外部网络和Internet的连接。校园网应该具备使用灵活，管理简单的特性。由于校园网不可能投入太多的专业人员从事系统维护，因此在设计时就应该考虑网络使用和维护应该尽量简单。考虑到未来校园的扩建，教学发展的需要，校园网应该具备很好的扩展能力，能够保证在需要时校园网能够实现向未来网络的平滑升级。另外校园网应该能够保证新的应用形顺利开发实现。

3.6 网络管理需求

网络系统应该能够支持 SNMP，这样便于计算机管理人员通过网管软件随时监视网络的运行状况，一旦出现故障，可以自动报告出错位置和出错原因，管理人员可以迅速发现故障并即时维护，同时SNMP V2版本的协议还支持很多更高级的网络安全管理功能。

3.7 网络安全需求

配备的防火墙。防火墙的配备，极大的提高了我校校园网与外网之间的安全性，从根本上消除了多年以来存在的网络安全隐患。

四、设计原则

4.1 校园网对主机系统的主要要求原则

- 主机系统应具有良好的向后扩展能力，能为用户未来数目的扩展具有调整、扩充的手段和方法；
- 主机系统应具有较高的可靠性，能长时间连续工作，并且有容错措施；
- 支持通用大型数据库，具有广泛的软件支持，软件兼容性好，并支持多种传输协议；
- 能与Internet互联，可提供互联网的应用；
- 支持SNMP网络管理协议，具有良好的可管理性和可维护性；
- 方案应合理分配带宽，使用户不受网上“塞车”的影响；
- 该网络应是面向连接的，能够实现虚拟网(VLAN) 连接；

4.2 网络设计原则

（1）开放性：采用开放的网络体系以方便网络的升级、扩展和互联；

（2）可管理性：利用合理的网络规划策略提供强大的网络管理功能；

（3）可扩充性：从主干网络设备的选型及其模块、管理软件和网络整体机构以及技术的开放性来保证系统的可扩充性；

（4）安全性：内部网络之间、内部网络与外部公网之间的互联，利用VLAN/ELAN以及防火墙等对访问进行控制，确保网络的安全。

4.3 子网设计原则

（1）服务器区采用私IP地址，NAT后供人员远程访问；

（2）与Internet 互联设备IP地址采用真实IP地址；

（3）部分内部互连采用私有IP地址；

（4）面向用户的私有IP地址，由统一出口的边缘设备（路由器、防火墙）进行地址翻译。

4.4 网络设备的选择原则

根据已制定的网络系统设计原则，我们所选择的网络设备必须具有以下一些特点：

（1）网络设备应具备安全性、稳定性和可靠性的特点；

（2）应选择具有一定扩展能力的设备；

（3）先进的设备必须配合先进的管理和维护方法，才能够发挥最大的作用。

五、校园网系统详细设计方案

5.1 逻辑结构设计

5.1.1 网络拓扑结构的分层设计

校园网分为3层结构，即核心层、汇聚层和接入层。主干网一般采用星型拓扑结构，主流技术是千兆以太网。校园网核心层一般采用双核心路由交换机，核心层到汇聚层具有冗余链路，以提高网络可靠性。为了便于校园网的管理，一般按部门划分子网和VLAN。网络分层设计示意图如下所示：

5.1.2 网络拓扑结构各层设计

（1）网络核心层设计

（2）网络接入层设计

（3）网络汇聚层设计

（4）网络拓扑各层的设计目标和策略

5.1.3 网络安全和管理策略的设计

防火墙只允许内网访问外网https，http；

5.1.4 网络综合布线设计

结构化布线应该满足以下目标：

（1）满足学院各大楼主要需求，同时兼顾未来升级能更好的实施。

（2）满足当前和长远的数据传输要求，兼顾质量。

（3）布线系统遵循国际标准和国家建设部门和电信部门标准，根据逻辑设计中的拓扑星型结构采用国际标准施工。

（4）布线设备的安装将支持语音、文本、视频等综合数据的高质量传输， 重点强调各设备的兼容问题。

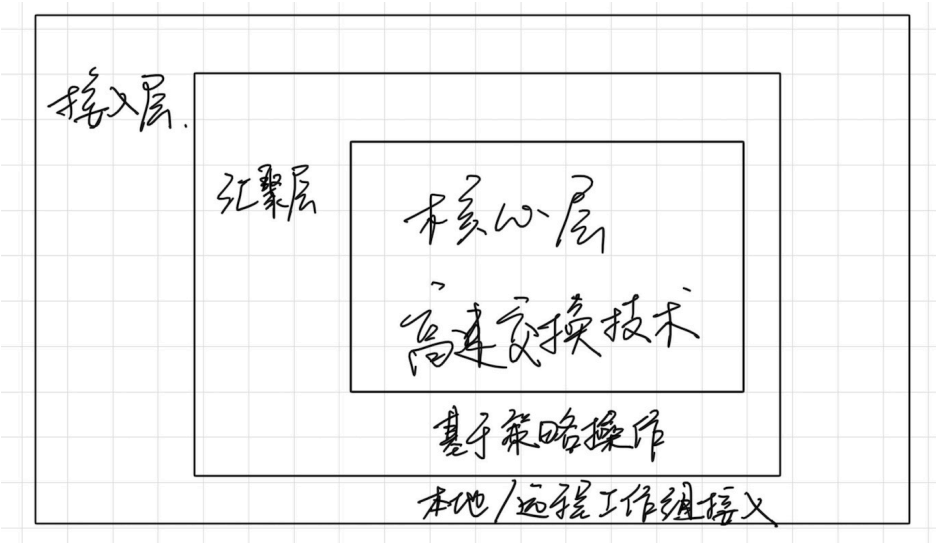
（5）布线系统信息出口主要才用现在流行的通用RJ45接口插座，按统一规格进行线路铺设和连接接口，使之数据畅通。

5.2 物理结构设计

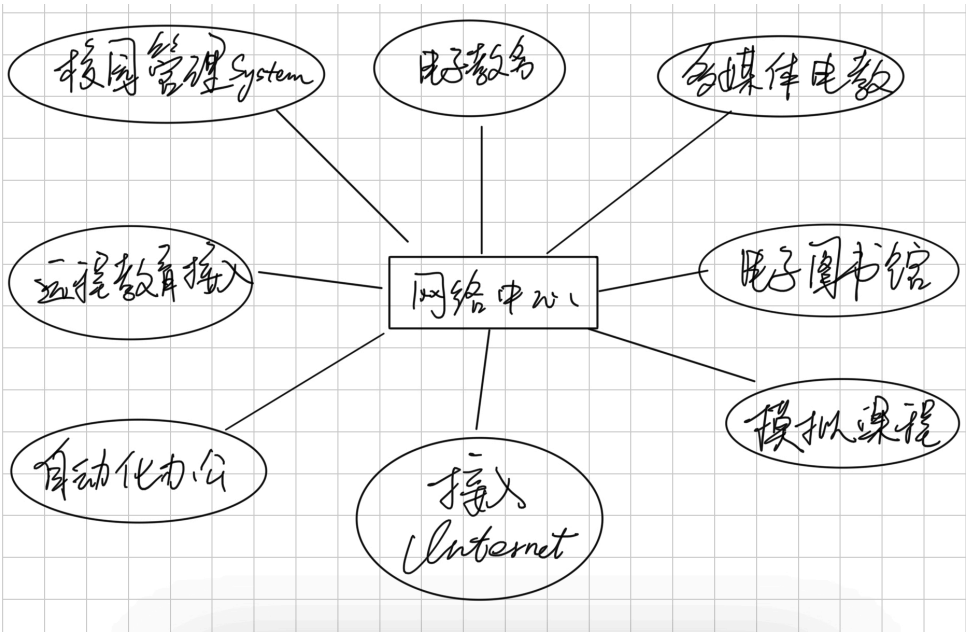
组建所需设备的选择，包括硬件设备（服务器、路由器、交换机、网卡、传输介质、信息插座等等）、软件设备（操作系统软件、应用软件等）。在组建局域网选择网络设备的时候，需要从多方面去考虑。选择的设备要能满足学校的实际功能需求，设备的性能和费用等等这些都是设备选型时应该考虑的。选择的设备既能使网络运行达到高效率，又经济实惠关系到校方的利益。根据对本校园网的实际要求、信息点数量和建筑物布局的分析，得出了本校园组网所需的各类硬、软件设备。

5.3 校园网光纤布线设计

骨干光纤布线采用星型结构，中心机房设在行政楼，考虑把图书馆、学生宿舍、食堂、各二级学院楼、全部光纤与位于网络信息联合中心相连。

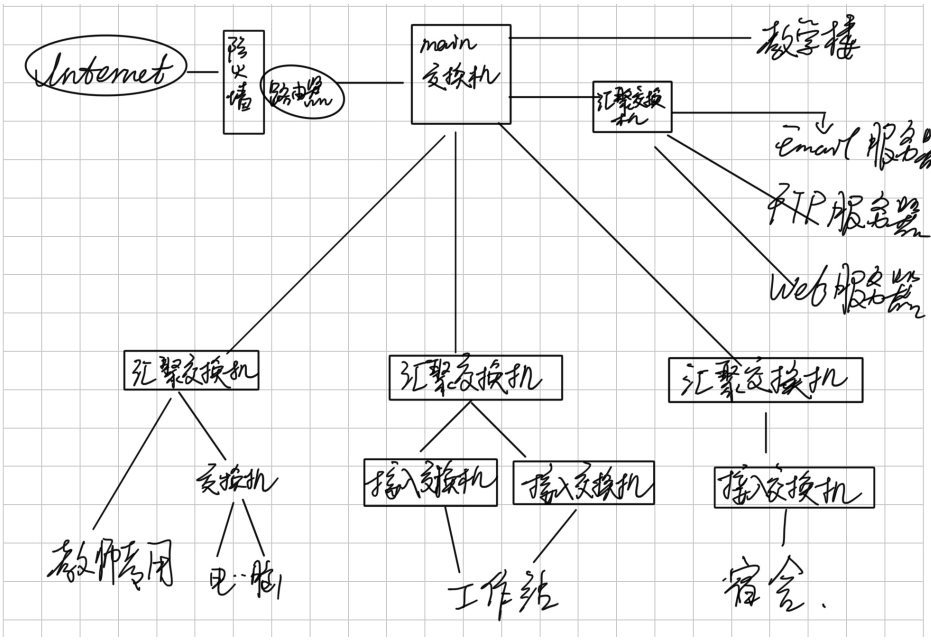


六、基本架构：



6.1 校园网网络的方案设计：

校园主干网采用一台千兆多层交换机作为中心交换机，配置多台二层换机为二级交换机；在网络中心配置多台工作站，一台主机工作站，一台连接外部网络的路由器和校内的两台FTP服务器供存储和访问校内资料。二级交换机通过千兆光纤连接到主干交换机上，构成星形的拓扑结构，使得主干网具有较好的可扩展性和可管理性。



七、网络安全：

7.1 校园网主要的安全威胁：

(1)非法访问
非法访问主要有假冒、身份攻击、非法进入网络、未授权操作等。在校园网中主要表现为有意或无意闯入学生记录和考试数据库。

(2)信息丢失或泄露
通常包括信息在传输或存储介质中丢失或泄露。如“黑客” 们利用电磁泄漏或搭线窃听等方式截取机密信息;或通过对信息流向、流量、通信频度和长度等参数的分析,推断出用户口令、账号等重要信息;还可以通过建立隐蔽隧道等方式窃取敏感信息等。

(3)破坏数据完整性
破坏数据完整性通常指以非法手段窃得对数据的使用权,删除、修改、插入或重发某些重要信息,以取得有益于攻击者的响应,同时干扰用户的正常使用。

(4)破坏性攻击
破坏性攻击是一种旨在干扰用户正常使用计算机的侵袭行为, 它不断地对网络服务系统进行干扰 , 改变其正常的作业流程, 执行无关程序使系统响应减慢甚至瘫痪, 影响正常用户的使用 , 甚至使合法用户不能进入计算机网络系统或不能得到相应的服务器。

(5)利用网络传播病毒
网络的普及为病毒检测与消除带来了极大的难度, 使病毒的破坏性大大高于单机系统 ,而且用户很难防范,成为计算机及其网络安全的一大公害。

(6)来自内部网的安全问题
现在,黑客攻击工具在网上泛滥成灾,而个别学生的心理特点决定了其利用这些工具进行攻击的可能性。解决这类问题,好的管理体制是必不可少的,但还须结合对校园网内部实行全面的监控措施,才能较为彻底地防范此类问题的危害。

7.2 防火墙：

7.2.1防火墙技术

防火墙是计算机网络上一类防范措施的总称，它使得内部网络与Internet之间或其它外部网络互相隔离、限制网络互访，用来保护内部网络。防火墙简单的可以只用路由器实现，复杂的则可以用主机甚至一个子网来实现，设置防火墙的目的都是为了在内部网与外部网之间设立惟一的通道来自简化网络的安全管理。防火墙的功能主要是过滤掉不安全服务和非法用户与控制对特殊站点的访问以及提供监视Internet安全和预警的方便端点。由于网络具有天生的开放性，所以有许多防范功能的防火墙也有一些防范不到的地方，如防火墙不能防范不经由防火墙的攻击和感染了病毒的软件或文件的传输。因此，防火墙只能是一种整体安全防范政策的一部分。
实现防火墙技术从层次上大概可以分为报文过滤和应用层网关。报文过滤是在IP层实现的，它的原理是根据报文的源IP地址、目的IP地址、源端口、目的端口报文信息来判断是否允许报文通过，因

此它可以只用路由器完成。在用应用层网关实现的防火墙有多种方式，如应用代理报务器和网络地址转换器等。
在校园网中大部分的应用都是内部网络用户，而内部用户通常具有较大的访问权限，因此局域网络系统的安全是整个网络系统安全中最重要的部分。但相对而言，内部的安全问题是可以预测的，并可据此制定相应的防范措施。

7.2.2 防火墙设计

（1）防火墙设计策略基于特定的Firewall，定义完成服务访问策略的规则。通常有两种基本的设计策略：

① 允许任何服务除非被明确禁止；

② 禁止任何服务除非被明确允许。

第一种的特点是安全但不好用， 第二种是好用但不安全，通常采用第二种类型的设计策略。 而多数防火墙都在两种之间采取折衷。

（2）防火墙的安全策略:
① 所有从内到外和从外到内的数据包都必须经过防火墙；
② 只有被安全策略允许的数据包才能通过防火墙；
③ 防火墙本身要有预防入侵的功能；
④ 默认禁止所有服务，除非是必须的服务才被允许。

（3）防火墙的设计：
① 保障校园内部网主机的安全，禁止外部网用户连接到内部网；
② 只向外部用户提供HTTP、SMTP和POP等有限的服务；
③ 向内部记账用户提供所有Internet服务，但--律通过代理服务器；
④ 要求具备防IP地址欺骗和IP地址盗用功能；
⑤ 要求具备记账和审计功能，能有效记录校园网的一切活动。