

《计算机网络》课程设计个人报告

（2020——2021 年度第一学期）

|  |  |
| --- | --- |
| 题 目 |  |
|  | ——个人设计报告 |
| 专 业 | 计算机科学与技术（非师范） |
| 班 级 |  |
| 姓 名 |  |

**《计算机网络》课程设计**

**成 绩 评 定**

|  |  |  |  |
| --- | --- | --- | --- |
| **学号** | **姓名** | **个人成绩** | **备注** |
|  |  |  | 组成员 |

指导教师： 李臻

目录

[摘要 1](#_Toc59550844)

[1 FTP服务器的搭建 1](#_Toc59550845)

[1.1 概述 1](#_Toc59550846)

[1.2 FTP的工作方式 1](#_Toc59550847)

[1.3 用户授权 2](#_Toc59550848)

[1.4 传输模式 3](#_Toc59550849)

[1.5 配置FTP服务器 3](#_Toc59550850)

[2 计算机局域网络背景介绍及需求分析 6](#_Toc59550851)

[2.1 学校背景概况 6](#_Toc59550852)

[2.2 学校平面图 7](#_Toc59550853)

[2.3 网络应用和服务需求 7](#_Toc59550854)

[2.4 用户概况和信息点需求 8](#_Toc59550855)

[2.5 安全需求 8](#_Toc59550856)

[2.6 威胁网络安全因素分析 8](#_Toc59550857)

[2.7 网络管理需求 9](#_Toc59550858)

[2.8 网络可扩展、优化需求 10](#_Toc59550859)

[3 小结 10](#_Toc59550860)

# 摘要

科学技术的发展日新月异，在计算机技术和通信技术结合下，网络技术得到了飞速的发展。如今，不仅计算机和整个网络紧密结合，整个社会都不能脱离网络而存在。网络技术已经成为现代信息技术的主流，人们对网络的认识也随着网络应用的逐渐普及而迅速改变，网络逐渐成为人们生活中必不可少的一部分。但是网络也会存在一定的安全隐患，为了使整个网络正常运作、便于管理，我们需要对网络安全、网络管理做出合理的分析。本文将详细阐述这些，需求并搭建FTP服务器实现文件的传输。

**关键字：** 需求分析、管理、FTP服务器

# 1 FTP服务器的搭建

## 1.1 概述

FTP（File Transfer Protocol）即文件传输协议，是一种基于TCP的协议，采用客户/服务器模式。通过FTP协议，用户可以在FTP服务器中进行文件的上传或下载等操作。虽然现在通过HTTP协议下载的站点有很多，但是由于FTP协议可以很好地控制用户数量和宽带的分配，快速方便地上传、下载文件，因此FTP已成为网络中文件上传和下载的首选服务器。同时，它也是一个应用程序，用户可以通过它把自己的计算机与世界各地所有运行FTP协议的服务器相连，访问服务器上的大量程序和信息。FTP服务的功能是实现完整文件的异地传输。

## 1.2 FTP的工作方式

工作方式FTP支持两种模式，一种方式叫做Standard (也就是 PORT方式，主动方式)，一种是 Passive(也就是PASV，被动方式)。 Standard模式 FTP的客户端发送 PORT 命令到FTP服务器。Passive模式FTP的客户端发送 PASV命令到 FTP Server。

（1）Standard (也就是 PORT方式，主动方式)：PortFTP 客户端首先和FTP服务器的TCP 21端口建立连接，通过这个通道发送命令，客户端需要接收数据的时候在这个通道上发送PORT命令。 PORT命令包含了客户端用什么端口接收数据。在传送数据的时候，服务器端通过自己的TCP 20端口连接至客户端的指定端口发送数据。 FTP server必须和客户端建立一个新的连接用来传送数据。

（2）Passive(也就是PASV，被动方式)：Passive在建立控制通道的时候和Standard模式类似，但建立连接后发送的不是Port命令，而是Pasv命令。FTP服务器收到Pasv命令后，随机打开一个高端端口（端口号大于1024）并且通知客户端在这个端口上传送数据的请求，客户端连接FTP服务器此端口，通过三次握手建立通道，然后FTP服务器将通过这个端口进行数据的传送。很多防火墙在设置的时候都是不允许接受外部发起的连接的，所以许多位于防火墙后或内网的FTP服务器不支持PASV模式，因为客户端无法穿过防火墙打开FTP服务器的高端端口；而许多内网的客户端不能用PORT模式登陆FTP服务器，因为从服务器的TCP 20无法和内部网络的客户端建立一个新的连接，造成无法工作。

（3）FXP：FXP说简单点就是一个FTP客户端控制两个FTP服务器，在两个FTP服务器之间传送文件。FXP的全称为File Exchange Protocol――文件交换协议，可以认为FXP本身其实就是FTP的一个子集，因为FXP方式实际上就是利用了FTP服务器的Proxy命令，不过它的前提条件是FTP服务器要支持PASV，且支持FXP方式。FXP传送时，文件并不下载至本地，本地只是发送控制命令，故FXP传送时的速度只与两个FTP服务器之间的网络速度有关，而与本地速度无关。因FXP方式本地只发送命令，故在开始传送后，只要本地不发送停止的命令，就算是本地关机了，FXP仍在传送，直至一个文件传送完成或文件传送出错后，FTP服务器等待本地发送命令时，才会因不能接收到命令而终止FXP传送。因为上述的原因，FXP传送出错时，本地的用户进程还留在FTP服务器中，并没有退出，如此时再次连接FTP服务器，可能会因用户线程超过允许，FTP服务器提示客户已登陆并拒绝客户端的连接，直至服务器中的傀儡进程因超时或其他原因被FTP服务器杀死后，才能再次连接FTP服务器。成功FXP有两个必要条件：首先两个FTP服务器均支持FXP；其次两个FTP服务器均支持PASV方式。但并不是说满足这两个条件的FTP服务器均经本地操作成功FXP，这还与本地与FTP服务器的网络状况有关。故有时会出现同样两个FTP，别人可以FXP，而你不可以的情况。

## 1.3 用户授权

1. 授权：要连上 FTP 服务器（即“登陆”），必须要有该 FTP 服务器授权的帐号，也就是说你只有在有了一个用户标识和一个口令后才能登陆FTP服务器，享受FTP服务器提供的服务。
2. 地址格式：FTP地址如下：ftp://用户名：密码@FTP服务器IP或域名：FTP命令端口/路径/文件名上面的参数除FTP服务器IP或域名为必要项外，其他都不是必须的。
3. 匿名：互联网中有很大一部分 FTP 服务器被称为“匿名”（Anonymous）FTP 服务器。这类服务器的目的是向公众提供文件拷贝服务，不要求用户事先在该服务器进行登记注册，也不用取得FTP服务器的授权。Anonymous（匿名文件传输）能够使用户与远程主机建立连接并以匿名身份从远程主机上拷贝文件，而不必是该远程主机的注册用户。用户使用特殊的用户名“anonymous”登陆FTP服务，就可访问远程主机上公开的文件。许多系统要求用户将Email地址作为口令，以便更好地对访问进行跟综。匿名FTP一直是Internet上获取信息资源的最主要方式，在Internet成千上万的匿名FTP主机中存储着无以计数的文件，这些文件包含了各种各样的信息，数据和软件。人们只要知道特定信息资源的主机地址，就可以用匿名FTP登录获取所需的信息资料。虽然使用WWW环境已取代匿名FTP成为最主要的信息查询方式，但是匿名FTP仍是 Internet上传输分发软件的一种基本方法。如red hat 、autodesk等公司的匿名站点。

## 1.4 传输模式

FTP协议的任务是从一台计算机将文件传送到另一台计算机，它与这两台计算机所处的位置、联接的方式、甚至是是否使用相同的操作系统无关。假设两台计算机通过ftp协议对话，并且能访问Internet，你可以用ftp命令来传输文件。每种操作系统使用上有某一些细微差别，但是每种协议基本的命令结构是相同的。FTP的传输有两种方式：ASCII传输模式和二进制数据传输模式。

1. ASCII传输模式。假定用户正在拷贝的文件包含的简单ASCII码文本，如果在远程机器上运行的是不同的操作系统，当文件传输时ftp通常会自动地调整文件的内容以便于把文件解释成另外那台计算机存储文本文件的格式。但是常常有这样的情况，用户正在传输的文件包含的不是文本文件，它们可能是程序，数据库，字处理文件或者压缩文件（尽管字处理文件包含的大部分是文本，其中也包含有指示页尺寸，字库等信息的非打印字符）。在拷贝任何非文本文件之前，用binary 命令告诉ftp逐字拷贝，不要对这些文件进行处理，这也是下面要讲的二进制传输。
2. 二进制传输模式：在二进制传输中，保存文件的位序，以便原始和拷贝的是逐位一一对应的。即使目的地机器上包含位序列的文件是没意义的。例如，macintosh以二进制方式传送可执行文件到Windows系统，在对方系统上，此文件不能执行。如果你在ASCII方式下传输二进制文件，即使不需要也仍会转译。这会使传输稍微变慢 ，也会损坏数据，使文件变得不能用。（在大多数计算机上，ASCII方式一般假设每一字符的第一有效位无意义，因为ASCII字符组合不使用它。如果你传输二进制文件，所有的位都是重要的。）如果你知道这两台机器是同样的，则二进制方式对文本文件和数据文件都是有效的。

## 1.5 配置FTP服务器

（1）在服务器上找到FTP，然后启用这个服务，设置用户名和密码，开启读、写、删除、重命名及列表功能。如图1、图2所示。

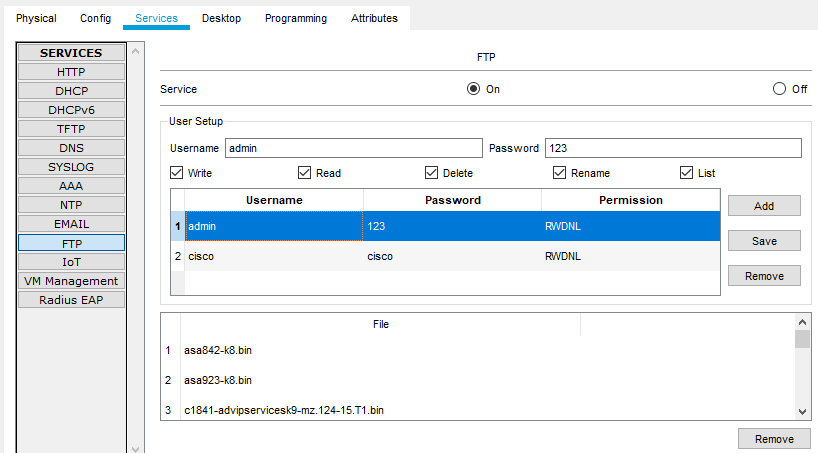


图1 内网FTP服务器的配置

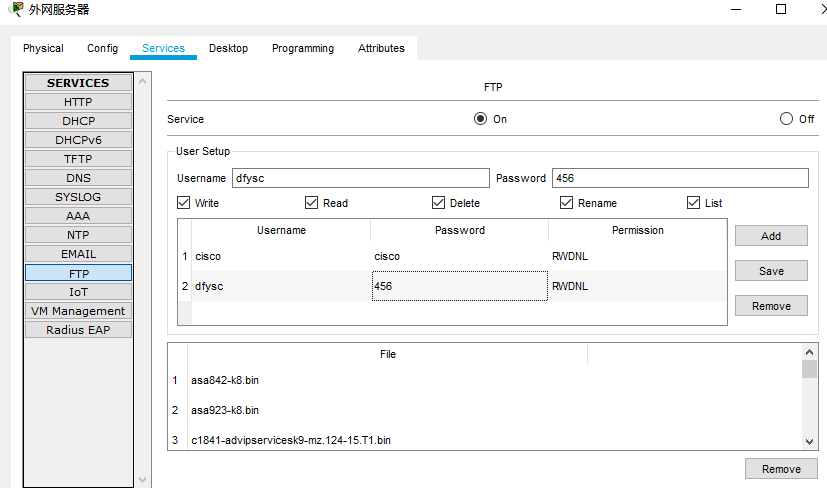


图2 外网FTP服务器的配置

1. 通过PC机进入FTP服务

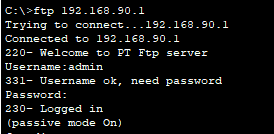
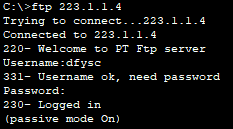


图3 内网FTP服务登入 图4 内网FTP服务登入

1. 查看FTP操作命令

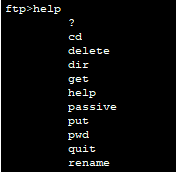
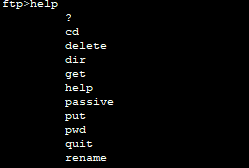
 

图5 查看内网FTP操作命令 图6 查看外网FTP操作命令

1. 查看FTP文件

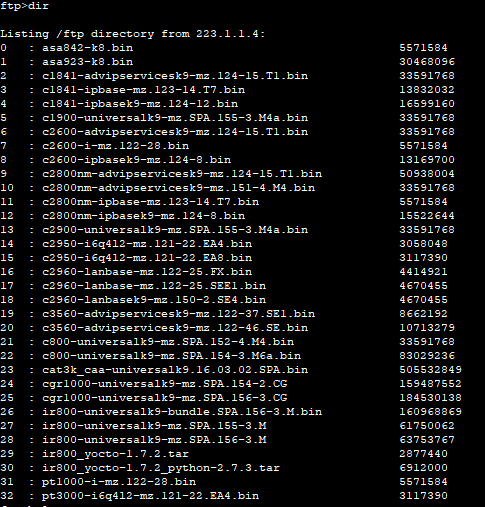


图7 查看内网FTP服务文件

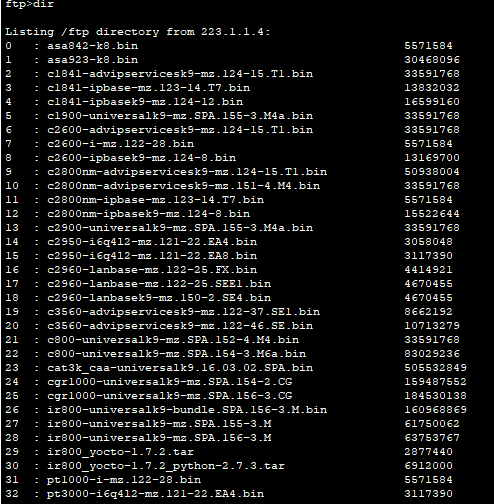


图8 查看外网FTP服务文件

1. 下载FTP服务文件

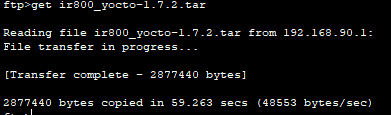


图9 下载内网FTP文件

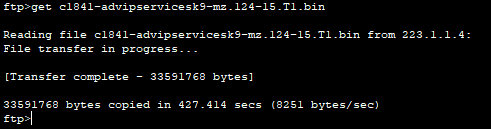


图10 下载外网FTP文件

# 2 计算机局域网络背景介绍及需求分析

## 2.1 学校背景概况

大肥羊学校始建于2020年，位于青青草原东边，青青河北岸的羊村，占地面积260亩，在校生969人，共有48个教学班，259名教职工，学校着力培养学生全面发展，以学生自主合作探究学习打造高效课堂。为此，我们要建立一个连接教学楼、宿舍楼、食堂、图书室、体育馆和综合楼（网络中心）等区域的校园网，能有效管理学校的各层面信息，实现信息和设备资源的及时交换与共享。

## 2.2 学校平面图

****

图11 平面图

## 2.3 网络应用和服务需求

1）信息交流功能。

1. 使任何一个办公室的计算机都能实现网上浏览、查询信息的功能，使教师能够拓宽视野，充分利用互联网上的资源辅助教学，提升教学理念。
2. 可以充分利用互联网资源来宣传学校，展示学校的办学能力与办学水平，展示教师的教训能力与科研成果，提升学校的办学形象。校内信息服务能为教育教学和管理决策提供各项信息服务。
3. 能为全校师生提供相互交流、相互学习的平台。

2）教学服务功能

（1）建立课件、基件、教学信息资源库，实现课件点播和辅助教学将教学资源库建设成为包括各科的教材、教案、试题、录像、图片等对教师有参考价值的多媒体素材库。

（2）利用网络技术，实现多媒体信息交换、远程教育等功能。

3）学生学习功能

（1）利用网络自主学习，提高学生的学习能力。

（2）利用网络查阅资料，相互交流、相互学习。

（3）可实现网上资源远程学习。

4）学校管理功能

（1）行政办公系统

（2）教务管理系统

（3）学生管理系统

（4）财务管理系统

## 2.4 用户概况和信息点需求

主要信息点集中在综合楼、教学楼、实验楼、生活区等。详细分布如表1所示。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 栋数 | 信息点/楼（个） | 信息点总数 |
| 综合楼（网络中心） | 1 | 107 | 67+50（网络中心）=107 |
| 教学楼 | 3 | 40、40、40 | 120 |
| 实验楼 | 1 | 38 | 38 |
| 生活区（宿舍，食堂） | 2 | 232 | 464 |
| 食堂 | 1 | 2 | 2 |
| 体育馆 | 2 | 10 | 3+7=10 |
| 门卫 | 1 | 2 | 2 |
| 合计 |  |  | 743 |

表1 主要信息点分布

综合楼主要有领导办公室、教研办公室和网络中心，领导办公室主机数量少，分配信息点数每个房间3个；教研办公室使用主机人数多，需在办公室安置4个信息点；网络中心是整个校园网的中心，一部分维护内部校园网络，一部分负责校内资源共享，信息点数较密集。

教学楼每个教室有2个信息点，会议室3个信息点。

实验楼除信息技术机房外，每个实验室2个信息点，信息技术机房每个教室52台电脑，4个信息点。

生活区，每间宿舍3个信息点，食堂2个信息点

## 2.5 安全需求

校园网的安全威胁主要来源于两大块，一块来自于内网，一块来自于网外。来源于网内的威胁主要是病毒攻击和和黑客行为攻击，根据统计，威胁校园网安全的攻击行为大概有40%左右来自内部网络。虽然计算机系统本身或多或少地具有安全防范措施，网络系统的安全防范却是整个系统安全性的第一道防线。

（1）网络硬件安全：网络系统中各通信计算机设备以及相关设备的物力保护。

（2）网络配置安全：

信息完整性：计算机系统能够防止非法修改和删除数据和程序；

保密性：信息不泄露给未经授权的人；

可用性：系统能够防止非法防止独占计算机资源和数据，合法用户的正常请求能及时、正确、安全的得到服务或回应。

## 2.6 威胁网络安全因素分析

1. 非授权访问。指对网络设备及信息资源进行非正常使用或越权使用等。如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享。
2. 冒充合法用户。主要利用各种假冒或欺骗的手段非法获得合法用户的使用权限，以达到占用合法用户资源的目的。
3. 破坏数据的完整性。指使用非法手段，删除、修改、重发某些重要信息，以干扰用户的正常使用。
4. 干扰系统正常运行、破坏网络系统的可用性。指改变系统的正常运行方法，减慢系统的响应时间等手段。这会使合法用户不能正常访问网络资源，使有严格响应时间要求的服务不能及时得到响应。
5. 病毒与恶意攻击。指通过网络传播病毒或恶意JAVA、active X 等，其破坏性非常高，而且用户很难防范。
6. 软件的漏洞和“后门”。软件不可能没有安全漏洞和设计缺陷，这些漏洞和缺陷最易受到黑客的利用。另外，软件的“后门”都是软件编程人员为了方便而设置的，一般不为外人所知，可是一旦“后门”被发现，网络信息将没有什么安全可信。如Windows的安全漏洞便有很多。
7. 电磁辐射。电磁辐射对网络信息安全有两方面的影响。一方面，电磁辐射能够破坏网络中的数据和软件，这种辐射的来源主要是网络周围电子电气设备产生的电磁辐射和试图破坏数据传输而预谋的干扰辐射源。另一方面，电磁泄露可以导致信息泄露。

## 2.7 网络管理需求

网络管理性能是衡量一个网络系统性能高低的重要因素之一。网络管理系统完成设置网络设备、监控网络运行、保障网络安全，查找并隔离网络故障，记录网络中的各种事件以及划分虚拟网络等功能。网管通常结合硬件和软件的手段来实施，对不同的拓扑结构及不同的物理和逻辑部件进行监控和分析。为了便于校园网络管理人员的管理及维护，我们选购Quidview网络管理软件，该软件基于灵活的组件化结构，用户可以根据自己的管理需求和网络情况灵活选用自己需要的组件，真正实现“按需建构”。Quidview支持多种操作系统平台，并能够与多种通用网管平台集成，实现从设备级到网络级全方位的网络管理。

（1）网络集中监视

Qiudview网络管理软件提供一拓扑发现功能，实现全网监控，并根据网络运行环境变化提供合适的方式对网络参数进行配置修改，保证网络以最佳性能正常运行。

（2）故障管理

故障管理功能对全网设备的告警信息和运行信息进行实时监控，查询和统计设备的告警信息。

（3）性能监控

Quidview网管系统通过性能任务的配置，可自动获得网络的各种当前性能数据，并支持设置性能的门限。通过统计不同线路、不同资源的利用情况，为优化或扩充网络提供依据。

（4）设备配置文件管理

当网络规模较大时，网络管理员的配置文件管理工作十分繁重，如果没有好的配置文件维护工具，网络管理员就只能动手备份配置文件。这样就给网络管理员管理、维护网络带来一定的困难。Quidview网络配置中心支持对设备配置文件的集中管理，包括配置文件的备份、恢复以及批量更新等操作，同时还实现了配置文件的基线化管理，可以对配置文件的变化进行比较跟踪。

（5）设备软件升级管理

使用Quidview管理员可以方便地查询设备上运行的软件版本，并利用升级分析功能来确定设备运行软件是否需要升级。当升级软件版本时，可以利用Quidview集中备份设备运行软件，然后进行批量升级。升级之后，可以使用该软件进行升级结果验证，确保升级操作万无一失

1. 集群管理

针对二层交换机设备的应用环境，Quidview网络管理软件提供集群管理功能，通过一个指定公网IP的设备对网络进行管理。

1. 堆叠管理

Quidview网络管理软件通过堆叠管理，可以集中管理较大量的低端设备，并且为用户提供统一的网管界面，方便用户对大量设备的统一管理维护。

1. 故障定位与地址反查

针对最为常见的端口故障，Quidview网络管理系统提供了便捷的定位检测工具——路径跟踪和端口环回测试；当用户报告网络端口使用异常时，网络管理员可以通过网管对指定用户端口做环回测试，直接定位端口故障。

## 2.8 网络可扩展、优化需求

采用层次化结构。在网络设计中。模块化具有的特性使网络增长时的复杂性能够限制在子网中，而不会蔓延到网络的其他地方。如果采用扁平化和网状设计，任何节点的变动都将对整个网络产生很大影响。同时层次化设计可将网络拓扑分解为易于理解的子网，网络管理者可容易地确定网络故障的范围，简化排错过程，易于优化。

# 3 小结

1. 通过本次实验对FTP服务器有了更深入的了解。进一步掌握了FTP的配置方法。
2. 明确的信息点的分布，为后来VLAN的划分奠定了良好的基础。
3. 应用和服务需求分析，明确了校园网搭建的目的，安全需求的分析为网络建设提供了良好的服务，网络管理需求分析为校园网的正常运作提供了保障。