系统部署方案

### 1、部署环境

* 系统部署结构及网络环境

系统以Microsoft Access Database为主体搭建数据库，在局域网内部运行，对于统计查询等功能主要基于python语言进行开发，便于相关领导和管理人员，随时随地通过内网登陆系统，按照权限来查询相关报表和数据。

系统采用集中式部署方案，系统用户均可通过医院内网登录系统。实施时要保证网络环境畅通，之间可以通过VPN专线或路由器等实现联接通信。在局域网内各台设备之间要用防火墙隔离，保障数据安全。

部署及应用架构如下所示:

* 局域网

最简单的局域网，可以采用一个路由器把几台计算机联起来。采用树形结构搭建局域网，网络成本低，结构简单。

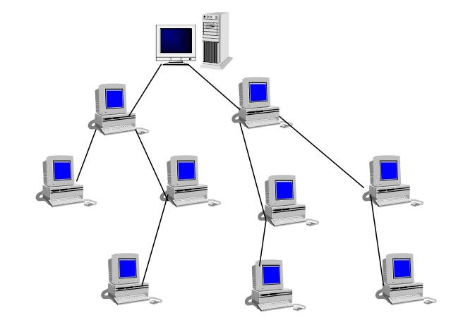


图1 树型拓扑结构

* 设备配置

|  |  |
| --- | --- |
| 硬件配置 |  |
| CPU位数 | 64位 |
| 内存 | 16GB及以上 |
| 硬盘 | 1TB及以上 |
| 电源 | 400W |

|  |  |
| --- | --- |
| 软件配置 |  |
| 操作系统及版本 | Microsoft Windows 10 |
| 数据库及版本 | Microsoft Access Database 2016及以上 |
| 防病毒软件 | 各类安全防护软件均可 |

### 2、数据库的搭建与使用

* Python配置

需配置python库：



1. 提取供货商邮件中附件的配置库名
2. zmail
3. os
4. sys

(2) 打开文件夹的配置库名

os

(3) 提取图像中合同信息的配置库名

1) base64

2) hashlib

3) time

4) requests

* Access数据库的环境调试

1. 创建一个plan.txt文件以供设备采购管理系统窗体中使用
2. 创建一个test.txt文件以供谈判记录及承诺书窗体中使用

完成以上环境搭建及调试即可正常使用本数据库。

### 3、系统安全保障

* 计算机防毒措施:

在整个网络的最末端，客户端的计算机是整个网络中为数最多也是容易遭受到病毒感染的一个环节。安装安全防护软件自动更新补丁，及杀毒软件。数据安全及备份配置

* 数据安全从两方面考虑实施:

一是硬件级别的，防止因硬盘损坏而造成数据丢失，需在服务器采购时就必须考虑做磁盘镜像（RAIDO1或RAID5)。

二是从软件角度考虑数据的日常备份，建立备份脚本，并通过操作系统中任务计划建立定期（例如每天夜晚0点〉自动运行备份任务。备份完成自动压缩，并将备份文件复制到指定的备份磁盘分驱。

1. 连入局域网
2. 设置登录用户及密码
3. 新建采购计划
4. 直接填写
5. 采用图片文字提取（需注意文件存放地址以及程序所在地址）
6. 上个步骤（2）中图片文件来自设备厂家发来的邮件的附件，需要用到邮件提取功能，需注意：1）邮件附件名称输入无误

2）所提取的附件的保存地址在局域网的主机上

5、对数据库中已有的可按OA单号，设备名称，计划号进行查询

6、其他问题还有从机上对数据库的权限问题需注意