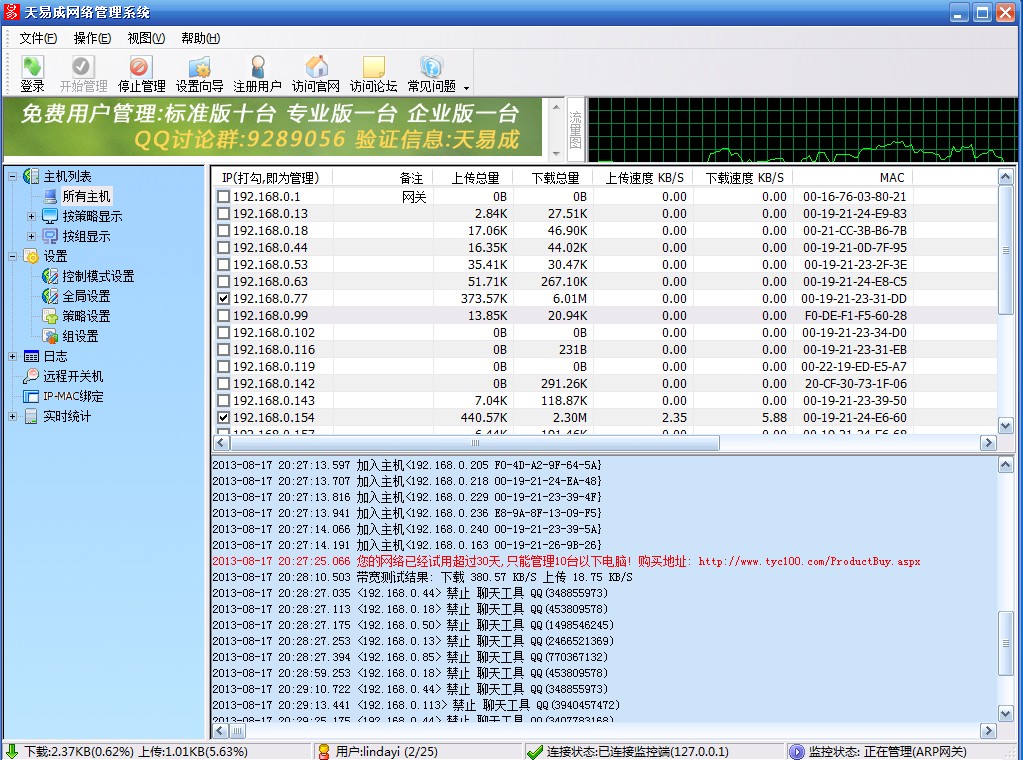
网络监控系统需求调研报告

# 需求

## 同类产品分析

目前市面上的局域网监控软件种类繁多，良莠不齐。经过多渠道的资料收集与分析，我们对目前使用较为广泛，评价较高的三款局域网监控软件——天易成网管，网眼监控软件，数据伞网络监控软件——进行了安装试用及操作分析，现具体分析如下：

### 天易成网管



天易成网管系统是由成都天易成软件有限公司研发的一款上网行为管理软件。该软件基于C/S（客户机/服务器）架构，无需调整网络结构，安装在局域网内任意一台电脑上，即可全面监控局域网内所有电脑的上网行为。天易成网管通过了360软件安全认证，是一款不含任何恶意代码的绿色软件。

**主要功能：**网页、下载、股票、聊天、视频、邮件监控，IP绑定，远程开关，远程监控管理，实时同步等。

|  |  |
| --- | --- |
| **优点：**  1. 有多种监控方式  2. 基于C/S架构，不需要任何客户端软件，安装任意一台电脑，即可监控整个网络的上网情况；  3. 支持分组策略管理  4. 对聊天工具控制最为严格的软件，控制QQ聊天国内最强，只需点击鼠标即可完全控制；  5. 远程监控管理。可以利用局域网、互联网上的任何一台电脑实现远程监控管理。利用互联网上的电脑远程管理时，需要在监控机上安装花生壳或者希网动态域名，并在网关上配置端口映射。 | **缺点：**  1.管理后网速变慢  2.开始管理后，可能会出现局域网内机不能上网的情况  3.出现IP冲突 |

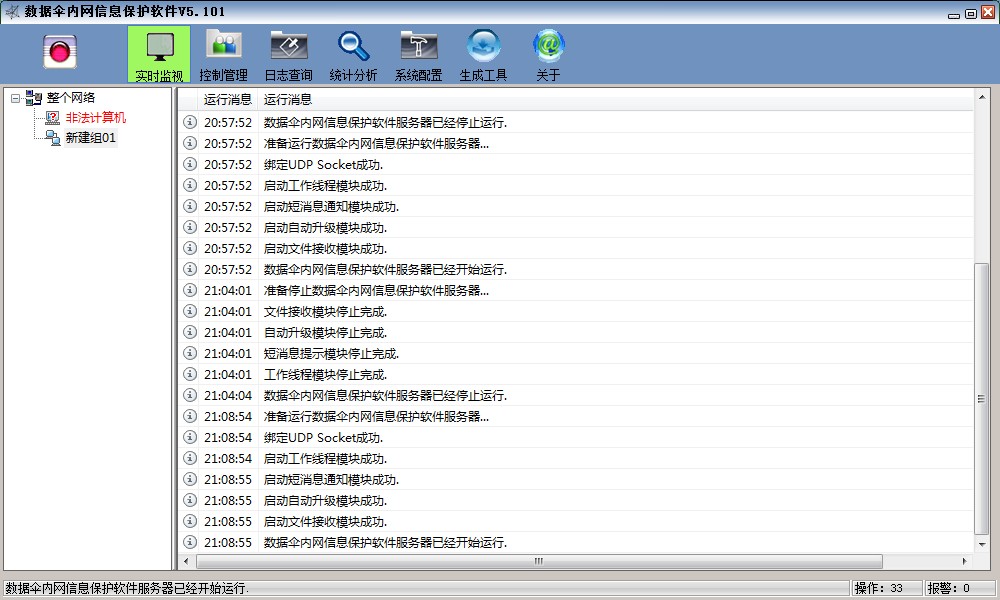
### 网眼监控软件



**主要功能：**上网监控，视频监控，聊天监控，屏幕监控，邮件监控，文件复制拷贝监控，插入U盘监控，网址过滤，端口封堵等等，即可监管，也可控制，让您对员工的一切电脑操作行为了如指掌。

|  |  |
| --- | --- |
| **优点：**   * 分为两个版本   Internet版本：  1. 拥有局域网版本的功能  2. 可以监控全球范围内的所有可以联网的员工  3. 可以在全球任意可以上网的计算机上对员工进行监控  家庭版本：  1. 对孩子浏览的网站了如指掌，可以正确引导孩子上网 。  2. 对孩子用电脑聊天内容，玩游戏等进行监控，及时掌握孩子 的心理以及实时了解情况。  Internet版本和局域网版本的管理端界面已经统一，用户可根据需要随时切换。   * 人性化UI设计 | **缺点：**   * 界面逻辑复杂 |

### 数据伞网络监控软件



数据伞网络监控软件象数据“保护伞”一样，时刻监视着局域网内的一举一动，任何对数据、端口、网络设备、互联网的操作都将纪录下来，一旦有信息泄漏等不法行为的发生，可以迅速取证、掌握失密内容和泄密途径，追查当事人的责任，并快速制定应急预案和补救措施，防止泄密影响扩大化。

**主要功能：**

1) 远程屏幕监控，能看到每台电脑的屏幕；

2) 查看员工以前做过什么，包括14种操作：QQ/MSN/SKYPE聊天监控、邮件内容、浏览了哪些网站、运行过哪些游戏软件或炒股软件等；

3) 禁止浏览指定的网站，禁止使用电驴、炒股、基金、BT、QQ、MSN等程序；

4) 限制员工通过U盘拷出重要文件或通过QQ/MSN/邮件发出机密资料；

5) 当被监控电脑通过U盘复制文件，或者通过邮件、MSN、QQ外传文件时能自动远程截屏并保存（远程屏幕截图）；

6) 统计24小时每个时段的聊天数量，迅速找出聊天最多的前10名对了，远程屏幕监控可以用。

|  |  |
| --- | --- |
| **优点：**  1.一个独特的功能，对非法计算机扫描  2. 安装之后客户端非常的隐蔽，不会让人家发现。采用自主开发设计的高性能专用管理平台，将监视、控制、管理、报警等功能模块有机结合，提供更多的安全 控制。结构先进、性能优异、功能强大、稳定可靠 | **缺点：**  1.使用逻辑复杂  2.界面不是很人性化 |

### 总结：

通过对市场的几款网络监控系统软件的测试，发现其基本功能大致为如下几点，网页、下载、股票、即时聊天工具、视频、邮件等监控。每个软件都有各自独特之处，比如天易成网管使用时不需要安装客户端，网眼监控系统的界面设计较为人性化，数据伞网络监控软件客户端较为隐蔽。总而言之，各有利弊。

## 窗体布局初稿

经过对系统需求的认真分析，结合开发周期及技术水平，我们拟定了如下界面设计稿：

（客户端无任何窗体，尽可能隐蔽自身，故不特别设计界面。）

**服务端：**

启动窗体：



主窗体：



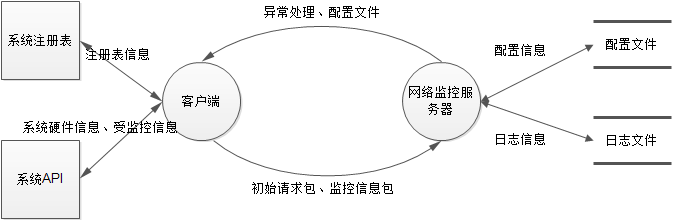




## 数据流分析初稿

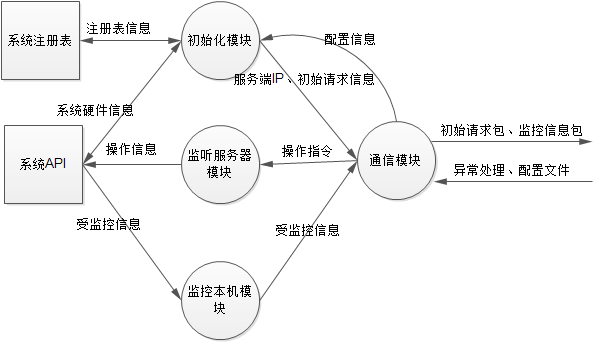
### 客户端数据流图

网络监控系统顶层DFD图

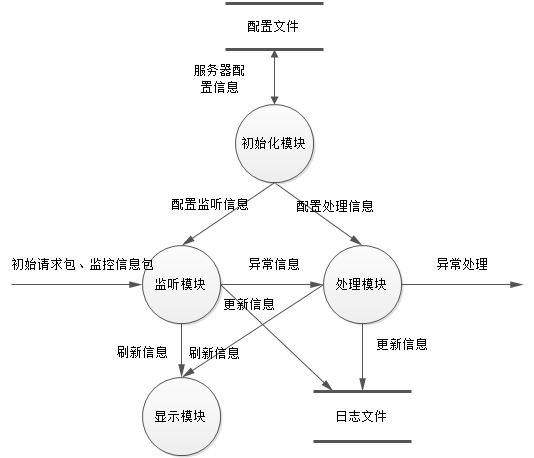


网络监控系统二层DFD图

第二层：加工“客户端”分解



第二层：加工“网络监控服务器”分解



### 数据流说明

#### 注册表信息

数据流名：注册表信息

数据组成：操作系统内的注册表项信息

数据来源：注册表

数据去向：客户端中的初始化模块

读取频率：客户端每启动一次，则读取一次

#### 系统硬件信息

数据流名：系统硬件信息

数据组成：系统IP，网关，MAC地址，基本硬件信息（内存、处理器、操作系统信息等）

数据来源：系统API提供

数据去向：初始化模块

读取频率：客户端每启动一次，则读取一次

#### 服务端IP

数据流名：服务端IP

数据组成：网络监控系统服务器对应的IP地址

数据来源：从初始化模块中处理获得

数据去向：通信模块

读取频率：客户端每启动一次，则获取一次

加工说明：IP地址由初始化模块扫描网段端口获得，用以设置通信模块中的目的IP地址，建立通信链接。

#### 初始请求信息

数据流名：初始请求信息

数据组成：该客户机IP地址+该客户机系统硬件信息

数据来源：从初始化模块中处理获得

数据去向：通信模块

读取频率：客户端每启动一次，则读取一次

加工说明：初始化模块对其上流获得的系统硬件信息作提取处理得到初始请求信息

#### 初始请求包

数据流名：初始请求包

数据组成：该客户机IP地址+该客户机系统硬件信息打包而成的XML格式的数据包

数据来源：通信模块

数据去向：网络系统监控服务器

发送频率：客户端启动时，发送一次

加工说明：将初始化模块传过来的初始请求信息封装为XML格式的数据包后发送给服务端

#### 受监控信息

数据流名：受监控信息

数据组成：该客户机当前系统进程列表信息+CPU及内存占用率+网卡上行、下行速度等

数据来源：监控本机模块

数据去向：通信模块

读取频率：根据配置文件中设置的读取频率读取

加工说明：包括本机所有网卡上行、下行（速度=两次间隔获取流量差/间隔时间）

#### 监控信息包

数据流名：监控信息包

数据组成：该客户机当前系统进程列表信息+CPU及内存占用率+网卡上行、下行速度打包而成的XML格式数据包

数据来源：通信模块

数据去向：网络监控系统服务器

发送频率：根据配置文件中设置的发送频率发送

加工说明：将监控本机模块传过来的受监控新信息封装为XML格式的数据包后发送给服务端

#### 配置文件

数据流名：配置文件

数据组成：受监控信息读取频率等配置信息打包而成的XML格式数据包

数据来源：网络监控系统服务器

数据去向：通信模块

读取频率：客户端每启动一次，则获取一次

加工说明：无

#### 配置信息

数据流名：配置信息

数据组成：受监控信息读取频率等配置信息

数据来源：服务端通信模块

数据去向：客户端通信模块

读取频率：客户端每启动一次，则读取一次

加工说明：将同服务器传来的配置文件数据包解封装得到

#### 异常处理

数据流名：异常处理

数据组成：异常处理命令

数据来源：网络系统服务器处理模块

数据去向：客户端通信模块

读取频率：若检测到进程异常则相应处理一次

加工说明：监听模块发送过来的异常信息，则激活处理模块做出相应异常处理

#### 异常信息

数据流名：异常信息

数据组成：异常对象IP+异常进程号

数据来源：网络系统服务器处理模块

数据去向：客户端通信模块

读取频率：若检测到进程异常则相应处理一次

加工说明：监听模块监听时检测出异常，则向处理模块发送异常信息

#### 服务器配置信息

数据流名：服务器配置信息

数据组成：账户信息+分组策略+进程黑名单等

数据来源：已存在的配置文件

数据去向：服务器初始化模块

读取频率：服务器每进行一次管理员登陆则读取一次

加工说明：账户信息中包含账户类型，不同账户类型，对应不同权限的操作

#### 配置监听信息

数据流名：配置监听信息

数据组成：监听频率

数据来源：初始化模块

数据去向：监听模块

读取频率：每启动一次，则读取一次

加工说明：无

#### 配置处理信息

数据流名：服务器处理信息

数据组成：处理权限

数据来源：已存在的配置文件

数据去向：服务器初始化模块

读取频率：服务器每进行一次初始化则读取一次

加工说明：根据配置文件中对账户类型的定义，设置处理权限

#### 刷新信息

数据流名：刷新信息

数据组成：刷新客户机IP+刷新内容

数据来源：监听模块、处理模块

数据去向：显示模块

读取频率：每收到一次监控信息包则刷新一次，或者每进行一次异常处理，刷新一次

加工说明：接受新数据刷新相应数据图示，杀死进程时改变相应客户机的当前系统进程显示

#### 更新信息

数据流名：更新信息

数据组成：程序自动终止的进程 | 管理员手动终止的进程 | 被监控机器上下线记录

数据来源：监听模块、处理模块

数据去向：日志文件

读取频率：每检测到监听的客户机系统进程与上次不同，则更新该信息；服务器每进行一次异常处理，则更新该信息

加工说明：无

# 技术

## 计划使用的技术

本项目基于C++ MFC类库开发，开发环境为VS2008，采用C/S架构，Socket(TCP)为通信协议，拟采用XML为客户端与服务端数据交换格式。

### 客户端

启动

· 进程保护，进程隐藏

* 注册表读写
* 扫描网段端口
* Socket(TCP)通信
* XML解析（MSXML.DLL）
* MFC ShellExecute

守护进程

监听服务端指令

监控本机信息

发送初始化包给服务端，接收服务端配置信息

隔5分钟重复

扫描网段特定端口

寻找服务端

写注册表

读取注册表

检测是否开机自启

否

是

未找到

找到

找到

### 服务端

* 文件读写
* MFC GDI曲线图绘制

记录IP，返回配置

日志

扫列表

手动添加黑名单

发结束进程指令

更新数据，画图

监听端口

权限验证

启动

通过

初始化包

数据包

发现黑名单进程

## 各技术点参考文档

### 进程保护，进程隐藏

http://www.cnblogs.com/BoyXiao/archive/2011/09/03/2164574.html

http://blog.csdn.net/lassewang/article/details/8622849

http://tieba.baidu.com/p/334524592

### 注册表读写

http://blog.csdn.net/zjg555543/article/details/6160525

http://hi.baidu.com/yn\_bg/item/40b6b129e7d60ffe50fd87e9

http://www.knowsky.com/440753.html

### 扫描网段端口

http://www.hackbase.com/tech/2006-12-16/29697.html

### Socket(TCP)通信

http://blog.csdn.net/aduovip/article/details/6422648

http://wenku.baidu.com/view/4095bfe981c758f5f61f6741.html

http://www.docin.com/p-413077107.html

### Xml解析（MSXML.DLL）

http://dev.yesky.com/413/2510413.shtml

http://www.codesky.net/article/200503/59503.html

http://www.poluoluo.com/jzxy/200801/7423.html

### MFC ShellExecute

http://wenku.baidu.com/view/b22faf9d51e79b8968022658.html

http://blog.sina.com.cn/s/blog\_565f47000100078e.html

http://wenku.baidu.com/view/8df7f5efaeaad1f346933f20.html

### 文件读写

http://wenku.baidu.com/view/8e16cb9d51e79b8968022661.html

http://www.2cto.com/kf/201107/98020.html

### MFC GDI曲线图绘制

http://wenku.baidu.com/view/a7524038580216fc700afdd3.html

http://zhidao.baidu.com/question/248201932.html

http://blog.csdn.net/dongliqiang2006/article/details/5466230