

# 基于 IP 与 MAC 绑定的透明代理在 LINUX 系统下的实现

指导教师	马玉军	13569229622
小组成员	李佩星	15003772680
	王 安	15036236547
	史明凤	15938467367

南阳理工学院

2008-11-20

## 摘 要

在 LINUX 系统中搭建透明的代理服务器，不仅节省了大量的 IP 地址，而且还提高了用户上网的安全性。通过对用户的 IP 地址与 MAC 地址绑定，可以很好防止局域网中 ARP 病毒的侵扰，给用户提供一个安全、快捷的上网环境。

通过建立代理服务器，本系统创造性的应用 WEB 服务来实现管理员对系统的操作和对用户的管理，包括用户的身份，主机的 IP 地址，以及每个 IP 的详细上网记录等等。确保每个用户都能高效，顺畅的浏览网络，而不必再受 ARP 病毒的困扰；同时也极大的方便了网络管理员对整个网络的管理，而且还节省了大量的人力，物力和财力。

**【关键字】** ARP 病毒 LINUX 透明代理 局域网

# 目 录

一. 项目背景 .....	4
二. 需求分析 .....	4
三. 系统设计 .....	5
(一) 相关原理 .....	5
(二) 整体架构 .....	5
(三) 整体设计 .....	6
四. 系统实现 .....	7
(一) 相关软件介绍 .....	7
(二) 系统具体实现 .....	8
五. 系统运行测试 .....	19
六. 设计感言 .....	21

## 一．项目背景

截至 2008 年 6 月底，中国网民数量达到 2.53 亿，网民规模跃居世界第一位。但是分给我国的 IPv4 地址数量只有 1.58 亿个（来源于中国互联网信息中心）。数量严重不足。根据 IPv4 地址的剩余数量状况,预计到 2012 年,全球 IPv4 地址将会完全耗尽。虽然国家在积极地推进 IPv4 到 IPv6 的过渡工作,但目前 IPv6 地址的技术还处于试验阶段,IPv6 在国内利用率极低,并且从 IPv4 向 IPv6 过渡需要投入大量的资金和人力。所以在现有的条件下,通过架设代理服务器通过代理上网,不仅可以节省大量的 IP 地址,而且还能提高网络的安全性。

## 二．需求分析

随着我国网民的急剧增加,有大量用户需要上网。但是 IP 地址日益紧缺,没有足够的 IP 地址可供分配。并且由于 IPv4 自身的局限性,对于普通的用户来说,公网 IP 地址不够安全。如果保护不周,就会给用户带来不必要的麻烦。通过代理服务器上网,可以很好的保护网内的用户的上网安全。代理服务器分为需要在浏览器中设置代理服务器的 IP 地址和端口的普通的代理服务器和不需要有任何的设置透明代理服务器。普通的代理服务器,虽然可以解决 IP 地址紧缺和用户主机安全的问题,但是设置比较复杂,很容易给网络管理员带来不必要的麻烦。而使用透明代理,用户使用起来感觉不到自己是在通过代理服务器连接网络。用户通过代理服务器上网时,由于 IP 地址是用户自己设置的,没有经过任何的规划,所以经常会出现 IP 地址冲突,影响用户的正常上网;而对于网络管理员来说,用户对 IP 地址冲突的反馈也是一件很头疼的事情,而且用户的 IP 地址如果可以随意改动,就不能对用户的上网情况进行有效的管理,也给网络安全带来一定的隐患。采用 IP 与 MAC 地址绑定的方案后,管理员会分给用户一个固定的 IP 地址,使用户不能够再随意的更改,这样既便于网络管理员对网络进行管理,又提高网络的安全性。

本系统就是基于以上的需求,在深入了解 Linux 系统的运行机制后,开发的一套基于 Web 服务的软件。用来绑定用户 IP 与 MAC 地址,对用户的上网情况进行管理并记录日志。

这套系统适用于通过代理上网的中小型网络。例如:中小型公司网络,生活小区局域网等。为用户提供安全、快捷的网络支持。

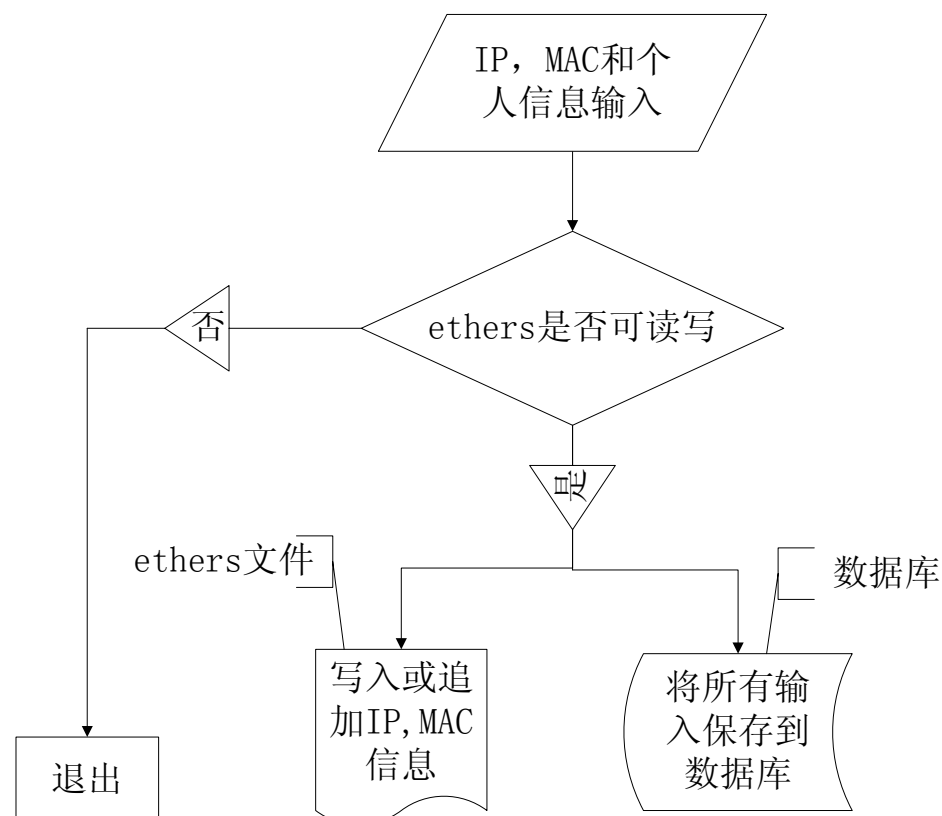
### 三. 系统设计

#### (一) 相关原理

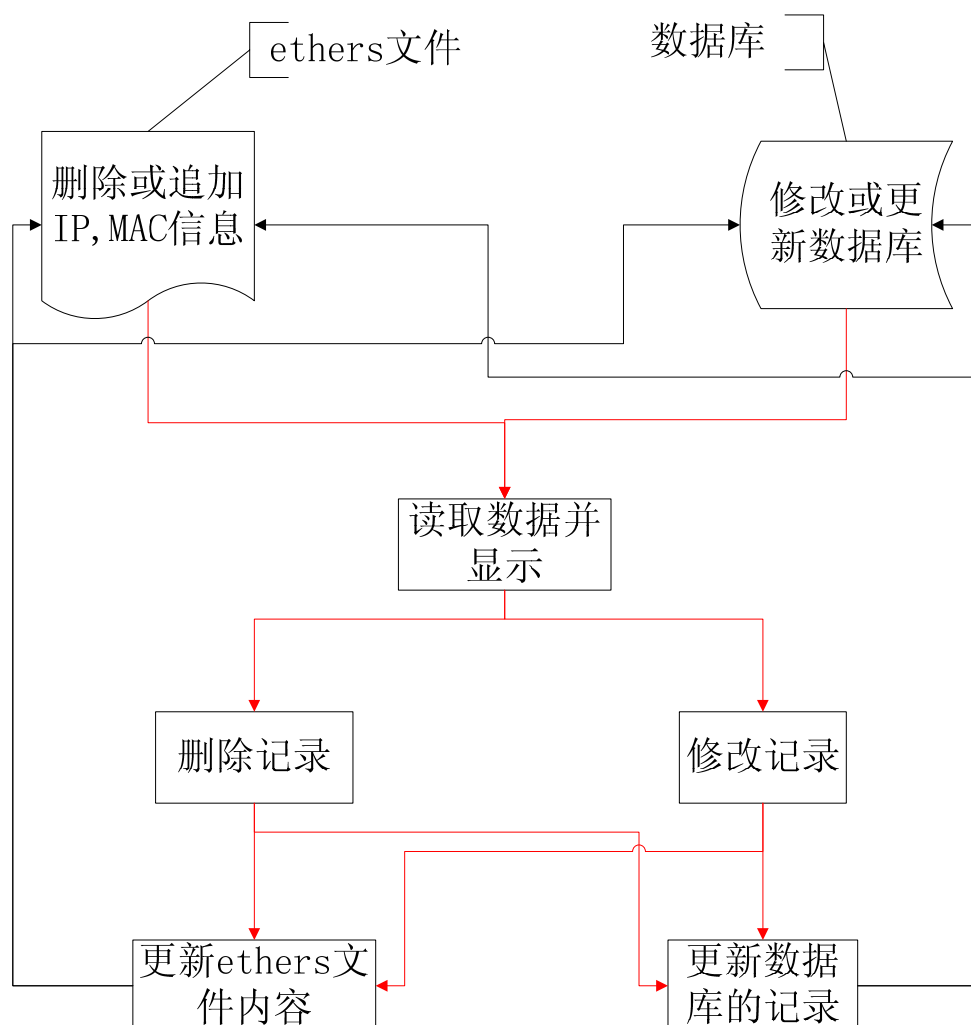
ARP 协议是“Address Resolution Protocol”（地址解析协议）的缩写。它主要负责将局域网中的 32 位 IP 地址转换为对应的 48 位物理地址,即网卡的 MAC 地址。在每台安装有 TCP/IP 协议的电脑里都有一个 ARP 缓存表,这个缓存表是主机通过广播动态获取的（这里的 IP 地址与 MAC 地址是一一对应的）。获取的内容可能是真实的,也可能是虚假的。主机也可以静态地读取 IP 与 MAC 信息,将 IP 与 MAC 人为的对应,也称为绑定。根据静态的优先级高于动态的规则,一旦主机静态地读取这些信息,就不会再接受广播过来的 ARP 信息,这样在 ARP 缓存当中就只有系统读取的 IP 与 MAC 信息,达到了绑定的目的。Linux 系统可以很好的完成这一任务。

在 Linux 下搭建 Web 服务器,通过页面程序人为地去控制读取含有 IP 与 MAC 信息的文件,将用户 IP 与 MAC 地址绑定。同时将用户的个人信息与主机的 IP、MAC 地址一起保存到数据库中,方便网络管理员对用户进行管理。

#### (二) 整体架构



信息的录入：分别将用户的 IP 与 MAC 地址和用户的所有信息保存到 ethers 文件和数据库中。



信息的管理：从数据库中读取用户的信息，经过管理员修改或删除用户的信息后，再将更改后的信息重新保存到指定的文件中。

### （三）整体设计

在 Linux 系统下，通过 Web 程序将用户的 IP，MAC 以及个人信息分别输入到数据库和 ethers 文件中。在将 IP 与 MAC 写入 ethers 文件后用程序执行 `arp -f /etc/ethers` 命令,从 ethers 文件读取用户的 IP 与 MAC 地址到 ARP 缓存表，绑定用户的 IP 地址。在添加用户之前要初始化 ethers 文件，即在 ethers 文件中添加所有可用的 IP 地址和错误的 MAC 地址。如：

```

172.16.0.2  00:00:00:00:00:00
172.16.0.3  00:00:00:00:00:00
172.16.0.4  00:00:00:00:00:00
... ..
  
```

172.16.0.254 00:00:00:00:00:00

添加错误的 MAC 地址的作用是防止用户通过 ARP 广播动态地生成 MAC 表。这样用户的 IP 与 MAC 没有被绑定，就会造成 IP 地址冲突。所以，在系统刚开始运行时要首先静态的生成 MAC 表，当添加用户的时候再更改为正确的 MAC 地址，使用户处于可控的状态。

## 四．系统实现

本系统是基于 IP 与 MAC 绑定的代理服务器在 Linux 系统下实现的，所以需要有一个切实可行的网络环境。需要有一台装有 Linux 系统的主机作为服务器，还有几台通过它来上网的电脑。但考虑到实际拥有的资源，最后决定在虚拟机（VMware Workstation6.0）中来实现。在 Linux 服务器中需要添加两个网卡，一个网卡用来连接外部的网络，本系统使用的是 eth0；一个网卡用来连接内部网络，本系统使用的是 eth1。

### （一）相关软件介绍

1. LAMP (Linux+Apache+MySQL+PHP) 指一组用来运行动态网站的开源软件。包括:Linux 操作系统, Apache 网络服务器, MySQL 数据库, PHP 编程语言。虽然这些开放源代码程序本身并不是专门设计成同另外几个程序一起工作的, 但由于它们都是影响较大的开源软件, 拥有很多共同特点, 这就使得了这些组件经常在一起使用。在过去的几年里, 这些组件的兼容性得到不断完善, 将它们整合到一起使用也更加普遍。并且它们为了改善不同组件之间的协作, 已经创建了某些扩展功能。目前, 几乎在所有的 Linux 发布版中都默认包含了这些产品。Linux 操作系统、Apache 服务器、MySQL 数据库和 PHP 语言, 这些产品共同组成了一个强大的 Web 应用程序平台。

2. Squid 是一种在 Linux 系统下使用的优秀的代理服务器软件。它是一个可以缓存 Internet 数据的软件, 用来接收用户的下载申请, 并自动处理所下载的数据。也就是说, 当一个用户想要下载一个页面时, 它向 Squid 发出一个申请, 请求 Squid 替它下载, 然后 Squid 连接所申请网站并请求该页面, 接着把该主页传给用户同时保留一个备份, 当别的用户申请同样的页面时, Squid 把保存的备份立即传给用户, 使用户觉得速度相当快。对于 Web 用户来说, Squid 是一个高性能的代理缓存服务器, 可以加快内部网浏览 Internet 的速度, 提高客户机的访问命中率。Squid 不仅支持 HTTP 协议, 还支持 FTP、Gopher、SSL 和 WAIS 等协议。和一般的代理缓存软件不同, Squid 用一个单独的、非模块化

的、I/O 驱动的进程来处理所有的客户端请求。Squid 将数据元缓存在内存中，同时也缓存 DNS 查寻的结果，除此之外，它还支持非模块化的 DNS 查询，对失败的请求进行消极缓存。Squid 支持 SSL，支持访问控制。由于使用了 ICP，Squid 能够实现重叠的代理阵列，从而最大限度的节约带宽。

3. Sarg 的全称是：Squid Analysis Report Generator。Sarg 作为一款 Squid 日志分析工具，它采用 html 格式，详细列出了每一位用户访问 Internet 的站点信息：时间、占用信息、排名、连接次数、访问量等。用户上网的日志以文本的形式存放在 access.log 中。Sarg 的作用是将文本日志以网页的形式呈现给管理员。

4. Iptables 是一种功能强大的基于包过滤的网络工具，利用它可以构建一个网络防火墙。Iptables 由两个子系统组成，即内核模块和用户接口应用程序，它可以被编译进系统内核，也可以编译成可装卸的内核模块，之后还可以选择安装一些能够完成一定功能的部件，这些部件实现了 IP 地址伪装，端口映射，包过滤等等一系列功能。

## （二）系统具体实现

### 1. 相关平台的搭建

①安装代理服务软件 squid。从 [www.squid-cache.org/Version/](http://www.squid-cache.org/Version/) 网站上下载 squid 软件并进行安装。为了操作方便，通常在系统的根目录下通过 `mkdir /squid` 命令创建用来存放 squid 软件的目录。之后，使用下边的命令会自动拆包并解压 squid 压缩文件，并显示解压过程中的文件和文件名。

```
tar -zxvf squid-2.6.STABLE22.tar.gz
```

得到源文件后，通过 `cd squid-2.6` 进入 squid-2.6 文件夹对源文件进行操作。squid 这套软件支持多种语言，在这里设置默认的出错语言为简体中文，并指定 squid 安装到 /squid 文件夹下。

```
./configure --prefix=/squid --enable-default-err-language="Simplify_Chinese"
```

现在对解压过的进行编译安装。

```
make all
```

```
make install
```

squid.conf 是 squid 软件的配置文件。要使 squid 能正常工作需要使用 vi 编辑器对 squid.conf 文件进行编辑，使用 `vi /squid/etc/squid.conf` 命令对 squid.conf 编辑，进入 squid.conf 的编辑页面后，就可以修改配置文件。下边是需要修改的配置，修改完



以后要保存退出。下边是 squid.conf 需要修改的地方。

配置 squid.conf 文件

```
http_port 3128 transparent
//将服务器的类型配置为透明代理的模式
http_access allow all
//将 squid 代理服务器配置为允许所有的主机都可以访问
access_log /squid/var/logs/access.log squid
//配置日志文件的目录
```

通过以上的步骤 squid 代理服务器就安装完成了。下面需要通过 iptables 添加访问规则。

② iptables 在安装系统的时候，都是被默认安装的。只需要打开 iptables 的功能，并添加相应的规则就可以达到相应的目的。

打开内核的包转发功能

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

也可以对内核的配置文件操作实现同样的功能：

```
vi /etc/sysctl.conf
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

添加 iptables 的规则

给 nat 表添加一条规则：凡是通过 eth1 进来的符合 TCP 协议的目的端口是 80 的数据包都跳转到 3128 端口

```
iptables -t nat -A PREROUTING -i eth1 -s 172.16.0.0/24 -p tcp
--dport 80 -j REDIRECT --to-ports 3128
```

在 nat 表中添加一条规则：源地址在 172.16.0.0/24 的数据包都要从 eth0 出去。

```
iptables -t nat -A POSTROUTING -s 172.16.0.0/24 -j MASQUERADE -o
eth0
```

经过以上配置，透明代理服务器便配置成功。下面安装 squid 的日志分析软件 sarg。

③安装 sarg。登录 <http://sarg.sourceforge.net/sarg.php> 网站下载 sarg-2.2.5.tar.gz。sarg 的安装和 squid 一样。通过 tar -zxvf sarg-2.2.5.tar.gz 命令将 sarg-2.2.5.tar.gz 拆包并解压，在这个过程中显示解压过程中的文件和文件名。然后进入 sarg-2.2.5 文件夹 cd sarg-2.2.5。通过 ./configure 将 sarg 软件安装到默认的文件夹中。

编译安装

```
make
make install
```

配置文件的修改方法同 squid 一样，sarg.conf 是 sarg 软件的配置文件，需要对这个文件进行编辑，修改必要的配置才能在指定的目录中显示出通过代理上网的用户上网的详细日志。

```
vi /usr/local/sarg/sarg.conf //指定 squid 日志文件绝对路径
access_log /squid/var/logs/access.log //指定网页标题，可以写
中文网页
title "Squid 用户审计" //指定输出页面的标题
background_color #7bb6e7 //指定日志页面的背景颜色
output_dir /var/www/html/access //指定网页报告文件输出路径
overwrite_report yes //覆盖已经存在的日志数据
charset UTF-8 //语言修改成支持中文的语言
topuser_fields NUM DATE_TIME USERID CONNECT BYTES %BYTES
IN-CACHE-OUT USED_TIME MILLISEC %TIME TOTAL AVERAGE
datafile_fields
user;date;time;url;connect;bytes;in_cache;out_cache;elapsed
squidguard_log_format #year#-#mon#-#day#
#hour##tmp#/#list#/#tmp#/#tmp#/#url#/#tmp# #ip#/#tmp#
#user# #end# //显示日志页面
show_sarg_info no //不显示软件的信息
show_sarg_logo no //不显示软件的 logo
www_document_root /var/www/html/ //设置 web 目录为 /www
```

#### ④搭建 Web 平台

在安装 Asianux3.0 时可以安装系统自带的整套的 Web 服务平台。也可以自己安装。这里采用系统自带的 WEB 服务平台。

查找 httpd.conf 文件的位置并配置 httpd.conf

```
vi /etc/httpd/conf/httpd.conf
编辑 httpd.conf 文件
```

```
Port 80 //设置 httpd 服务于的端口为 80
DocumentRoot "/var/www/html/" //配置/www 为 apache 的根目录
User apache //配置系统中运行 httpd 服务的用户
Group apache //配置系统中运行 httpd 服务的用户组
Timeout 300 //连接超时时间为 300 秒
KeepAlive On //配置服务中用户完成一次访问后，继续保持连接
```

KeepAliveTimeout	15	//在同一个客户连接中，等待下一个请求的等待时间
EnableSendfile	off	//关闭 sendfile 功能
MaxClients	150	//最大用户数
MaxKeepAliveRequests	100	//最大保持连接数
MinSpareServers	5	//最少的空闲服务进程数
StartServers	5	//打开的服务进程数

特别需要说明的是，在livecd中Apache不能传输html、css、js文件和较大的图片，但是默认却能显示It Works。需要将EnableSendfile设为off，主要原因是这个指令控制httpd是否可以操作系统内核的sendfile支持来将文件发送到客户端。默认情况下，当处理一个请求并不需要访问文件内部的数据时(比如发送一个静态的文件内容)，如果操作系统支持，Apache将使用sendfile将文件内容直接发送到客户端而并不读取文件。这个sendfile机制避免了分开的读和写操作以及缓冲区分配。由于默认是打开的，但系统对sendfile系统调用支持不够。所以会出现无法传输大于一定容量的html页面或图片。关掉并不影响正常使用。(参考系统之家网站内容)

修改过配置文件，要想使新的文件起作用，需要重新启动服务  
service httpd restart

最后在/var/www/html/下建立 access 目录，用来存放 sarg 生成的上网日志页面。

MySQL 默认用户是 root，而密码为空。可以在浏览器上输入http://localhost/phpMyAdmin/ 进入数据库管理界面。然后点击修改密码，输入新的密码，提高系统的安全性。phpMyAdmin 是一款图形化操作 MySQL 的软件，它存放在 Apache 的根目录下。

总结，通过以上步骤就在 Linux 系统上配置好透明代理，日志分析工具和用来管理用户上网的 Web 服务器，通过例行性命令的在指定的时间将用户每天的上网日志文件以网页的形式保存到 Apache 的目录(/var/www/html/access)中。

## 2. 网络管理程序的设计和实现

经过 Linux 相关服务的配置，已经搭建起一个用来管理用户的平台。这一部分将重点介绍在这个平台下应用程序的设计、实现过程以及相关代码。通过搭建 LAMP 就可以知道，本系统要采用的是 PHP 程序设计语言。不仅是因为 PHP 与 Linux, Apache 和 MySQL 结合的很紧密，还考虑到 PHP 程序设计语言自身比较成熟，并且对 Linux 文件具有很好的

操作性。

① 首先进入 MySQL 建立 user 数据库，在数据库中建立 admin 和 userinfo 两个数据表。

admin 表用来存放系统管理员的用户和密码。

字段	注释
id	用来标记用户的编号，设置为自动增加
username	网络管理员的登录系统的用户名(admin)
pwd	网络管理员的登录系统的密码(admin)

创建 admin 数据表的 SQL 语句：

```
CREATE TABLE `admin` (  
  `id` int(5) NOT NULL auto_increment,  
  `username` varchar(50) NOT NULL,  
  `pwd` varchar(50) NOT NULL,  
  PRIMARY KEY (`id`)  
) ENGINE=MyISAM DEFAULT CHARSET=utf8 AUTO_INCREMENT=1 ;
```

userinfo 表用来存放用户的所有信息。

字段	注释
id	用来标记用户的编号，设置为自动增加
ip	用户的 IP 地址
mac	与用户 IP 地址绑定的 MAC 地址
mac2	MAC 地址的备份与启用或禁用用户的账号有关
name	用户的名称
sex	用户的性别
phone	用户的电话
phone2	用户的手机
duty	用户的职称
email	用户的电子邮件
birthday	用户的生日
address	用户的地址
flag	是否启用或禁止用户的账号

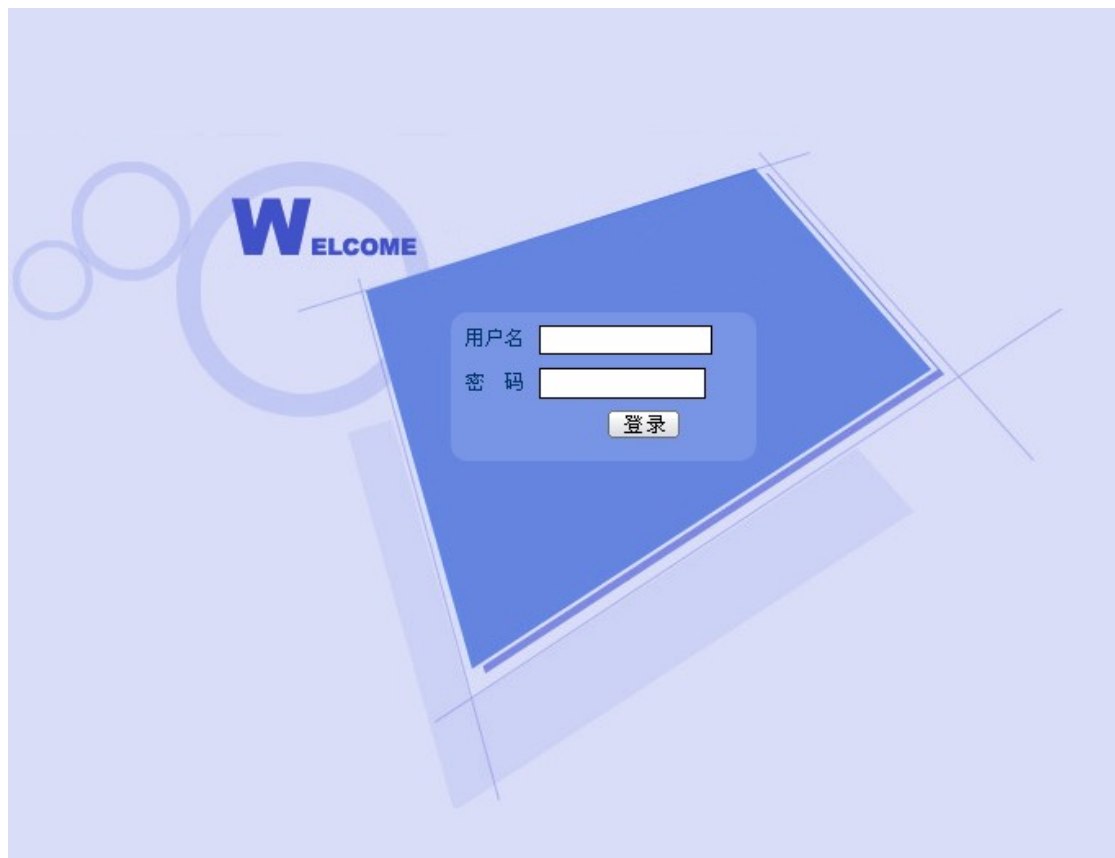
创建 userinfo 数据表的 SQL 语句：

```
CREATE TABLE `userinfo` (  
  `id` int(11) NOT NULL auto_increment,  
  `ip` varchar(100) NOT NULL,  
  `mac` varchar(100) NOT NULL,  
  `mac2` varchar(100) default NULL,  
  `name` varchar(50) NOT NULL,  
  `sex` varchar(5) NOT NULL,  
  `phone` varchar(30) NOT NULL,  
  `phone2` varchar(30) NOT NULL,  
  `duty` varchar(20) NOT NULL,  
  `email` varchar(50) NOT NULL,
```

```
`birthday` varchar(50) NOT NULL,  
`address` varchar(100) NOT NULL,  
`flag` int(2) NOT NULL,  
PRIMARY KEY (`id`)  
) ENGINE=MyISAM DEFAULT CHARSET=utf8 COMMENT='user_ip_mac'  
AUTO_INCREMENT=1 ;
```

数据库只是存放用户信息的地方。系统要绑定用户的 IP 与 MAC 地址，还需要在 /etc 目录下建立一个 **ethers** 文件用来存放用户的 IP 与 MAC 地址。系统通过执行 `arp -f /etc/ethers` 从文件 **ethers** 中读取 IP 与 MAC 信息。然后将这些信息放置到 ARP 缓存当中，以达到绑定的目的。（需要 创建 ethers 文件 `touch ethers`）

②设计 **Web** 页面，给管理员提供一个登录系统，管理网络的窗口，如下图所示：



登录窗口 用户名：admin 密码：admin

服务器的有关参数		组件支持有关参数	
服务器名:	192.168.0.21	mysql数据库:	✓ 支持
服务器IP:		odbc数据库:	✓ 支持
服务器端口:	80	SQL Server数据库:	✗ 不支持
服务器时间:	2008年11月15日14点11分42秒	msql数据库:	✗ 不支持
PHP版本:	5.1.6	SMTP:	✗ 不支持
WEB服务器版本:	Apache/2.2.3 (Asianux)	图形处理 GD Library:	✓ 支持
服务器操作系统:	Linux	XML:	✗ 不支持
脚本超时时间:	30 秒	FTP:	✗ 不支持
站点物理路径:	/	Sendmail:	✗ 不支持
脚本上传文件大小限制:	2M	显示错误信息:	✗ 不支持
POST提交内容限制:	8M	使用URL打开文件:	✓ 支持
服务器语种:	zh-cn	压缩文件支持 (Zlib):	✓ 支持
脚本运行时可占最大内存:	16M	ZEND支持 (1.3.0):	✓ 支持

管理首页

添加用户	
IP (*)	172.16.0. [ ]
MAC地址 (*)	[ ] : [ ] : [ ] : [ ] : [ ] : [ ]
用户姓名 (*)	[ ]
性别 (*)	男 <input type="radio"/> 女 <input type="radio"/>
联系电话 (*)	[ ]
手机 (*)	[ ]
电子邮箱 (*)	[ ]
职务 (*)	[ ]
出生日期 (*)	[ ] 如1980-11-12
[ 添加 ]	

添加用户页面

主要的程序集中在用户管理上边。包括：添加用户和管理用户。  
 添加用户：需要管理员输入用户的 IP 地址与 MAC 地址以及用户的个人信息。所要填写处，我们都采用了严格的匹配规则，例如 IP 只能填写 2-254，手机号必须是 11 位，生日必须用我们提示的格式等等。如添加用户页面所示。点击添加后程序将所填的这些信息自动的添加到数据库和 ethers 文件中。代码如下：

将用户信息添加到数据库的主要代码：

```
if($_POST["submit"]=="添加")
{
    $name=$_POST["name"];
    $sex=$_POST["sex"];
    $phone=$_POST["phone"];
    $phone2=$_POST["phone2"];
    $email=$_POST["email"];
    $duty=$_POST["duty"];
```

```

$birthday=$_POST["birthday"];
$address=$_POST["address"];
$ip="172.16.0.". $_POST["ip"];
$mac=$_POST["mac1"].":": $_POST["mac2"].":": $_POST["mac3"].":": $_
POST["mac4"].":": $_POST["mac5"].":": $_POST["mac6"];
AddArpUser($ip,$mac);//将 IP 与 MAC 写入 ethers 文件的函数
//////////信息写入数据库
$query="INSERT INTO $userinfo ( `id` , `ip` , `mac` , `mac2`,`name` ,
`sex` , `phone` , `phone2` , `duty` , `email` , `birthday` , `address` ,
`flag`
                                )                                VALUES
(' ', '$ip', '$mac', '$mac2', '$name', '$sex', '$phone', '$phone2', '$duty', '$
$email', '$birthday', '$address', '1')";
$sql->query($query);
$sql->msg("添加用户成功!", "Manage_User.php");
//////////
}

```

将用户 IP 与 MAC 地址写入 ethers 文件的主要代码:

```

function AddArpUser($ip,$mac)
{
    $filename="/etc/ethers";
    if(is_writable($filename))
    {
        $str="$ip $mac";
        $farray=file($filename);//echo $farray[0];
        for($i=0;$i<count($farray);$i++)
        {
            $arr=explode(" ", $farray[$i]);//echo $arr[0];
            if(trim($arr[0])==$ip)
            {
                $newfp.=$str."\n";
            }
            else
            {
                $newfp.=$farray[$i];
            }
        }
        if(!$fp=fopen($filename,"wb"))
        {
            echo "<script>alert('文件打开失败');</script>";
            exit;
        }
        if(flock($fp,2))
        {
            if(fwrite($fp,$newfp) == FALSE)
            {
                echo "<script>alert('写入文件数据失败');</script>";
            }
        }
    }
}

```

```

        exit;
    }
    flock($fp, 3);
}
else
{
    echo "<script>alert(' 锁定命令文件失败!');</script>";
}

fclose($fp);
exec("../bin/arp -f");
}
else
{
}
echo "<script>alert(' 文件不可写');</script>";
exit;
}
}

```

被添加过的用户都可以通过代理服务器上网。现在还需要对用户上网进行管理。

≡ 首选服务 ≡

✦ 管理首页

✦ 退出管理

≡ 用户管理 ≡

✦ 添加用户

✦ 管理用户

≡ 用户行为 ≡

✦ 上网记录

≡ 其它设置 ≡

✦ 修改密码

≡ 操作说明 ≡

✦ 操作说明

当前位置: 管理用户页面

管理导航: 新增用户 管理用户

用户管理							
选中	用户姓名	IP	MAC地址	职务	手机	出生日期	操作
<input type="checkbox"/>	王安	172.16.0.2	FF:FF:FF:FF:FF:FF	在校学生	15036236547	1987-02-28	<a href="#">启用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/>	史明凤	172.16.0.3	FF:FF:FF:FF:FF:FF	在校学生	15938467367	1987-01-11	<a href="#">启用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/>	ddd	172.16.0.4	00:0c:29:66:E2:35	dd	13503877880	1987-02-02	<a href="#">禁用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/>	项老师	172.16.0.85	20:04:12:30:31:7c	老师	13503877880	1975-09-03	<a href="#">禁用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/>	李佩星	172.16.0.58	00:11:58:78:93:9E	4424	33333333333	1980-11-12	<a href="#">禁用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/> 全选	<a href="#">删除</a>						<a href="#">刷新</a>

共有5条记录 当前1/1页 [首页](#) [尾页](#) [第1页](#)

上图就是用户的管理页面。管理员可以通过可视化的页面对用户进行管理。可以单个删除，也支持批量操作（选中全选）。删除的主要代码为：

```

if($_POST["Submit"]=="删除")
{
    if(count($_POST["id"])!=0)
    {
        $id=$_POST["id"];
        for($i=0;$i<count($id);$i++)
        {
            $query="select `id`,`flag`,`ip` from $userinfo where id=$id[$i]";
            $arr=$sql->fetch($query);
            $ip=$arr[0]["ip"];
            $mac="00:00:00:00:00:00";

```



```

        AddArpUser($ip, $mac);
        $query="delete from $userinfo where id=$id[$i]";
        $sql->query($query);
    }
    echo "<script>history.back(-1);</script>";
}
}

```

管理员还可以在线禁止或启用用户上网,上图红色的矩形所在的位置就是操作的触发器。主要代码为:

```

if($session_arr[0]["level"]!=0)
{
    echo "<meta http-equiv=refresh content='0;url=../error.htm'>";
    exit();
}
$user_id=$_GET["user_id"];
$query="select    `id`,`flag`,`ip`,`mac2`    from    $userinfo    where
id=' $user_id' ";
$arr=$sql->fetch($query);
$ip=$arr[0]["ip"];
$mac="FF:FF:FF:FF:FF:FF";
$mac2=$arr[0]["mac2"];
if($arr[0]["flag"]==0)
{
    AddArpUser($ip, $mac2);
    $ban_query="update    $userinfo    set    flag=1,mac=' $mac2'    where
id=' $user_id' ";
    $sql->query($ban_query);
}
else
{
    AddArpUser($ip, $mac);
    $start_query="update    $userinfo    set    flag=0,mac=' $mac'    where
id=' $user_id' ";
    $sql->query($start_query);
}

```

如果发现用户的信息填写错误可以点击管理页面的修改信息进入修改信息页面,进行修改。

<div> <div>首连服务</div> <div> <div>管理首页</div> <div>退出管理</div> </div> </div> <div> <div>用户管理</div> <div> <div>添加用户</div> <div>管理用户</div> </div> </div> <div> <div>用户行为</div> <div>上网记录</div> </div> <div> <div>其它设置</div> <div>修改密码</div> </div> <div> <div>操作说明</div> <div>操作说明</div> </div>	<div>当前位置: 修改用户页面</div> <div>管理导航: <a href="#">新增用户</a> <a href="#">管理用户</a></div> <div> <div>修改用户</div> <table border="1"> <tr> <td>IP(*)</td> <td>172.16.0.58</td> <td>MAC地址(*)</td> <td>00 : 11 : 5B : 78 : 93 : 5E</td> </tr> <tr> <td>用户姓名(*)</td> <td>李佩星</td> <td>性别(*)</td> <td>男 <input checked="" type="radio"/> 女 <input type="radio"/></td> </tr> <tr> <td>联系电话(*)</td> <td>234</td> <td>手机(*)</td> <td>3333333333</td> </tr> <tr> <td>电子邮箱(*)</td> <td>s814.com</td> <td>职务(*)</td> <td>4424</td> </tr> <tr> <td>出生日期(*)</td> <td>1980-11-12 如1980-11-12</td> <td>住址(*)</td> <td>24242</td> </tr> <tr> <td colspan="4" style="text-align: right;"><a href="#">修改</a></td> </tr> </table> </div>	IP(*)	172.16.0.58	MAC地址(*)	00 : 11 : 5B : 78 : 93 : 5E	用户姓名(*)	李佩星	性别(*)	男 <input checked="" type="radio"/> 女 <input type="radio"/>	联系电话(*)	234	手机(*)	3333333333	电子邮箱(*)	s814.com	职务(*)	4424	出生日期(*)	1980-11-12 如1980-11-12	住址(*)	24242	<a href="#">修改</a>			
IP(*)	172.16.0.58	MAC地址(*)	00 : 11 : 5B : 78 : 93 : 5E																						
用户姓名(*)	李佩星	性别(*)	男 <input checked="" type="radio"/> 女 <input type="radio"/>																						
联系电话(*)	234	手机(*)	3333333333																						
电子邮箱(*)	s814.com	职务(*)	4424																						
出生日期(*)	1980-11-12 如1980-11-12	住址(*)	24242																						
<a href="#">修改</a>																									

修改信息的主要代码为:

```

if($_POST["submit"]=="修改")
{
    $name=$_POST["name"];
    $sex=$_POST["sex"];
    $phone=$_POST["phone"];
    $phone2=$_POST["phone2"];
    $email=$_POST["email"];
    $duty=$_POST["duty"];
    $birthday=$_POST["birthday"];
    $address=$_POST["address"];
    $ip=$_POST["ip"];
    $mac=$_POST["mac1"].":".$_POST["mac2"].":".$_POST["mac3"].":".$_POST["mac4"].":".$_POST["mac5"].":".$_POST["mac6"];
    AddArpUser($ip,$mac);
    //////////////////////////////////信息写入数据库
    $query="update $userinfo set `mac`=' $mac', `mac2`=' $mac',`name`=' $name' , `sex`=' $sex', `phone`=' $phone',`phone2`=' $phone2' , `duty`=' $duty', `email`=' $email' ,`birthday`=' $birthday' , `address`=' $address' where id='$id'";
    $sql->query($query);
    $sql->msg("修改用户成功!", "Manage_User.php");
    //////////////////////////////////
}

```

本系统还提供了强大的用户上网的日志管理功能，这主要是由 Linux 系统下的 Sarg 软件实现的。只要将 Sarg 输出的目录指定到 Apache 的目录下，在本系统中引用这些网页，就可以将 Sarg 软件兼容到本套系统中。前边一部分已经就这一点进行了详细的说明。

通过以上的步骤，一个拥有强大功能的通过透明代理上网的网络管理系统就完成了。

### 3. 日志文件的循环生成

将用户上网的日志文件生成方便管理员查看的网页，需要运行 sarg 软件。但是如果管理员在需要查看日志的时候去手工去运行，这样既不方便，又不容易查找想要的日志。为了解决这个问题，本系统采用了让系统自动循环执行 sarg 软件的方法。创建 sarg.sh 文件，控制

sarg 去将昨天一天的用户上网的日志生成网页文档放到 WEB 服务的目录下。然后通过 crontab 命令,让系统每天执行一次 sarg.sh 这个文件。这样就可以将用户上网的详细记录以天为单位分别放置在不同的目录中。创建 sarg.sh 文件 touch sarg.sh, 然后设置 sarg.sh 文件的权限为所有的人都可以执行 chmod 755 sarg.sh。

编写 sarg.sh 文件

```
#!/bin/bash
/usr/bin/sarg -l /squid/var/logs/access.log -o /var/www/html/access -d
$(date --date "1 day ago" +%d/%m/%Y)-$(date +%d/%m/%Y)
exit 0
```

文件中间一句 bash 语句的作用是通过 sarg 软件整理用户昨天一天的上网日志,并将生成的网页放到 /www/access 目录下。这个文件只有在执行的时候才能将日志以网页的形式输出到 access 目录中。由于用户上网日志的信息量非常的大,将所有的日志都放到一个文件夹中时查看不方便,所以要将用户的每一天日志分割到一个单独的文件夹中,这样方便管理员管理。这就需要每天都去执行一次 sarg.sh 这个文件。Linux 系统下的 crontab 命令就是对事件进行循环执行的。

对 sarg.sh 文件进行循环操作。通过 crontab -e 命令编辑 crontab

```
01 00 * * * /root/sarg.sh
```

这句话的意思是每天的 0 点 1 分执行 sarg.sh 文件,这样就达到了目的。

## 五. 系统运行测试

测试环境: VMware Workstation6.0 虚拟机。Linux 系统登录的用户 root 密码 123456。

在系统测试之前要先连接好网络,配置好 IP 地址。网络管理员需要在 Linux 服务器上的 eth0 网卡上配置正确的 IP 地址(避免使用 172.16.0.0 这个网段),用来连接外网。在 eth1 网卡上配置 IP 地址: 172.16.0.1 子网掩码: 255.255.255.0, 填写一个可以使用的域名解析服务器,用来连接内网。配置好这些后,在客户端的浏览器中输入 http://172.16.0.1 进入网络管理系统,添加用户。网络管理系统的登录的用户名 admin 密码 admin。进入用户添加页面,按照规则添加用户信息(用户的 MAC 地址一定要真实的用户主机网卡的 MAC 地址)。然后将添加的用户 IP 地址分配给用户使用。在用户的 PC 上输入管理员分配的 IP 地址,子网掩码 255.255.255.0,网关 172.16.0.1, DNS 服务器和 Linux 服务器一样。之后对 ethers 文件进行初始化,考虑到信息的安全性,系统里边不能看到初始化的页面,相关内容在

/var/www/html/user\_manage 的 arpf.php 文件中。Livecd 中已经对 ethers 文件进行了初始化。

然后就可以开始测试。

结果如下：

≡ 首选服务 ≡

➤ 管理首页

➤ 退出管理

≡ 用户管理 ≡

➤ 添加用户

➤ 管理用户

≡ 用户行为 ≡

➤ 上网记录

≡ 其它设置 ≡

➤ 修改密码

≡ 操作说明 ≡

➤ 操作说明

当前位置:管理用户页面

管理导航: 新增用户 管理用户

用户管理							
选中	用户姓名	IP	MAC地址	职务	手机	出生日期	操作
<input type="checkbox"/>	王安	172.16.0.2	00:E0:5C:40:1B:16	在校学生	15036236547	1987-02-28	<a href="#">禁用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/>	史明凤	172.16.0.3	00:E0:4C:F6:8F:C1	在校学生	15938467367	1987-01-11	<a href="#">禁用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/>	ddd	172.16.0.4	00:0c:29:66:E2:35	dd	13503877880	1987-02-02	<a href="#">禁用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/>	项老师	172.16.0.85	20:04:12:30:31:7e	老师	13503877880	1975-09-03	<a href="#">禁用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/>	李佩星	172.16.0.58	00:11:58:78:93:9E	4424	33333333333	1980-11-12	<a href="#">禁用帐户</a> <a href="#">修改信息</a>
<input type="checkbox"/> 全选						<a href="#">删除</a>	<a href="#">刷新</a>

共有5条记录 当前1/1页 [首页](#) [尾页](#) [第1页](#)

添加过的用户都可以正常上网。

由于系统设定的是在每天的 00:01 时刻执行 sarg 将访问日志生成网页。在测试的时候要想查看到详细的信息，需要手工的执行一下 sarg。命令如下：

```
/usr/bin/sarg -l /squid/var/logs/access.log -o /var/www/html/access -d $(date --date "1 day ago" +%d/%m/%Y) - $(date +%d/%m/%Y)
```

≡ 首选服务 ≡

➤ 管理首页

➤ 退出管理

≡ 用户管理 ≡

➤ 添加用户

➤ 管理用户

≡ 用户行为 ≡

➤ 上网记录

≡ 其它设置 ≡

➤ 修改密码

≡ 操作说明 ≡

➤ 操作说明

Squid 用户审计

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2008Nov15-2008Nov15	2008年 11月 15日 星期六 03:10:38 CST	1	9.14K	9.14K
2008Nov13-2008Nov14	2008年 11月 14日 星期五 03:59:55 CST	4	210.71M	52.67M
2008Nov13-2008Nov13	2008年 11月 13日 星期四 23:06:39 CST	2	188.06M	94.03M

≡ 首选服务 ≡

➤ 管理首页

➤ 退出管理

≡ 用户管理 ≡

➤ 添加用户

➤ 管理用户

≡ 用户行为 ≡

➤ 上网记录

≡ 其它设置 ≡

➤ 修改密码

≡ 操作说明 ≡

➤ 操作说明

Squid 用户审计

Period: 2008Nov13-2008Nov14

Sort: BYTES, reverse

Topuser

Topsites

Sites & Users

Downloads

Denied

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME
1	172.16.0.85	7.98K	189.29M	89.83%	0.58%	99.42%	00:30:30	1.830.021 36.04%
2	172.16.0.2	3.42K	18.33M	8.70%	8.49%	91.51%	00:53:20	3.200.205 63.02%
3	172.16.0.3	272	2.01M	0.95%	21.37%	78.63%	00:00:28	28.879 0.57%
4	172.16.0.4	148	1.07M	0.51%	39.71%	60.29%	00:00:18	18.817 0.37%
TOTAL		11.82K	210.71M	1.67%	98.33%		01:24:37	5.077.922
AVERAGE		2.95K	52.67M				00:21:09	1.269.480

= 首选服务 =		Squid 用户审计							
+ 管理首页		Period: 2008Nov13-2008Nov14							
+ 退出管理		User: 172.16.0.3							
		Sort: BYTES, reverse							
		User Report							
= 用户管理 =		ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME
+ 添加用户		www.icbc.com.cn	123	468.43K	23.28%	0.00% 100.00%	00:00:08	8,332	28.85%
+ 管理用户		www.sina.com.cn	2	417.63K	20.76%	0.00% 100.00%	00:00:00	959	3.32%
		www.pcpop.com	4	322.99K	16.06%	0.00% 100.00%	00:00:03	3,494	12.10%
= 用户行为 =		d1.sina.com.cn	27	248.58K	12.36%	70.47% 29.53%	00:00:01	1,755	6.08%
+ 上网记录		images.movie.xunlei.com	15	123.60K	6.14%	0.00% 100.00%	00:00:01	1,844	6.39%
		i0.sinaimg.cn	12	86.62K	4.31%	100.00% 0.00%	00:00:00	44	0.15%
= 其它设置 =		movies.xunlei.com	1	83.28K	4.14%	0.00% 100.00%	00:00:00	551	1.91%
+ 修改密码		i3.sinaimg.cn	12	77.12K	3.83%	100.00% 0.00%	00:00:00	82	0.28%
		i1.sinaimg.cn	11	49.15K	2.44%	100.00% 0.00%	00:00:00	49	0.17%
= 操作说明 =		33.pcpop.com	2	44.46K	2.21%	0.00% 100.00%	00:00:00	329	1.14%
+ 操作说明		pfp.sina.com.cn	10	25.19K	1.25%	21.06% 78.94%	00:00:01	1,017	3.52%
		i2.sinaimg.cn	4	22.32K	1.11%	100.00% 0.00%	00:00:00	14	0.05%
		error:unsupported-request-method	8	9.46K	0.47%	100.00% 0.00%	00:00:00	2	0.01%
		bj.house.sina.com.cn	5	6.16K	0.31%	0.00% 100.00%	00:00:06	6,727	23.29%
		beacon.sina.com.cn	2	2.89K	0.14%	0.00% 100.00%	00:00:00	59	0.20%
		updatem.360safe.com	3	1.99K	0.10%	0.00% 100.00%	00:00:00	199	0.69%
		589.adsina.allyes.com	1	1.97K	0.10%	0.00% 100.00%	00:00:00	33	0.11%
		image.sinajs.cn	2	1.90K	0.09%	100.00% 0.00%	00:00:00	72	0.25%
		data.house.sina.com.cn	4	1.81K	0.09%	73.39% 26.61%	00:00:00	114	0.39%
		631.adsina.allyes.com	1	1.53K	0.08%	0.00% 100.00%	00:00:00	56	0.19%
		630.adsina.allyes.com	1	1.53K	0.08%	0.00% 100.00%	00:00:00	308	1.07%
		analytics.xunlei.com	1	1.48K	0.07%	0.00% 100.00%	00:00:00	178	0.62%
		allyes.nie.163.com	1	1.42K	0.07%	0.00% 100.00%	00:00:00	265	0.92%
		44.adsina.allyes.com	1	1.22K	0.06%	0.00% 100.00%	00:00:00	35	0.12%
		movie.xunlei.com	1	1.06K	0.05%	0.00% 100.00%	00:00:00	84	0.29%
		fav.qq.com	2	910	0.05%	0.00% 100.00%	00:00:00	122	0.42%
		news.sina.com.cn	2	862	0.04%	44.32% 55.68%	00:00:00	51	0.18%

这里是用户上网的详细记录。当点击用户操作的禁用帐户后，该帐户的用户不能与网路进行连接。点击用户的修改信息操作，修改用户的个人信息，发现在管理页面上用户的信息已经改变。当修改用户的 IP 或 MAC 地址后，用户不能正常上网。将用户的 IP 与 MAC 修改正确，提交。用户重新可以与网路连接。

至此，经过测试，这套系统已经正常工作。

## 成员分工

李佩星	系统分析，服务的搭建和论文撰写
王安	系统分析，程序实现，裁减模块和 Livecd 制作
史明凤	系统分析，搜集资料和论文校验

## 六．设计感言

上传文档的最后期限马上就要到了。可心中总是有点遗憾，因为联合文件系统我们没有安装成功。为了安装 unionfs，将我们作品的功能完美的呈现出来，我们付出了巨大的努力。特别是在最后一个星期，我们每天都研究到很晚，期间还阅读了大量的英文文献。但是到目前为止，还没能成功。作品要交了，但我们不会就此罢手，研究将继续进行，直到问题解决。不过值得欣慰的是，在整个过程当中，我学到了很多知识，积累了大量调试系统的经验。对 Linux 系统的运行机制，内核版本等知识有了新的认识。这或许就是我在过程当中最大的收获。

经验：

1. 做系统之前，原理一定要十分的清楚，不能有半点的含糊。否则将会走很多的弯路，有很多的疑惑。
2. 设计要从整体入手，不能总是盯着细节问题。另外，步骤一定要规范，这样可以节省很多时间和精力。
3. 不管遇到什么问题，要想办法去解决问题，不能选择逃避。逃避解决不了问题。
4. 写作论文要用简明的语言让读者明白你要表达的内容。要注意论文的格式和排版。
5. Baidu、Google 都是非常不错的工具。从大量的信息当中快速的查找到对自己有用的内容也是一种很好的技能。

太高兴了，之前我们的系统在制作成 livecd 后不能显示图片，不能传送 html 文件，一直都以为是没有安装联合文件系统造成的。为了解决这个问题，我们整整忙碌了两天两夜，搜集阅读了大量的文件，还想了很多折中弥补的方案，包括手工将所有的 html 日志文件的后缀名该成.php。可就是在刚才，在指导教师的帮助下，我们找到了问题的所在：需要在 Apache 服务中关闭 sendfile 功能(Enable sendfile off)。现在我们的系统可以显示美丽的图片了，详细的日志文件也不需要手工更改了，完全实现自动化。今天已经是上传系统的最后一天，我们的系统的终于可以完美无缺的去参与竞争，这一时刻真是太激动人心了，心中已不再有遗憾。

——李佩星

经过一个多月的实际项目设计，感触颇多，期间有过欣喜，也有过苦恼，当初设计时认为做好项目里的每一个功能就可以了，并且如何用程序去实现它，因而觉得只要按照步骤就能生成 LiveCD，所以直到 11 月 18 号的时候才开始去生成 LiveCD，当然第一次没有成功，原因是我的虚拟机根目录太小了不能生成 iso 文件了，最后我通过创建符号连接把 /tmp 目录指向空间比较大的 /home 分区 又一次生成 LiveCD，生成一次要几个小时(其实最后发现并不用重新生成一次，只要执行一下 make\_iso.sh 就可以生成 iso 文件几秒钟就可以)结果还是没有成功。最后无可奈何只好重装系统把根目录设大点。重装系统时我没有完全安装，免得以后还要裁减，装好后把所有的服务功能都移植到新的系统后终于生成了 LiveCD，590M。可运行后发现我原来在根目录建的 /squid 没有，当时相当郁闷，难道是不能自己建目录？我有点不大相信，我想

本来 linux 的灵活性就比较强，一般都可以定制的。于是回到 livecd 的目录下找答案，原来它有一个隐藏的 .config 文件，编辑它，发现确实可以让它生成自己想生成的一些目录。我加上 squi 重新执行 ./build 几个小时后生成了 LiveCD。其实最后验证发现并不需要让它生成所有的目录因为很浪费时间，配置文件修改成只生成 squid 这个目录的内容，把生成的 squid.lzm 这个文件拷贝到之前没有 squid.lzm 的那个 /tmp/live\_data\_4188/RedFlag-LiveCD/base 目录下，然后执行 /tmp/live\_data\_4188/RedFlag-LiveCD 目录下的 make\_iso.sh 即可生成新的 iso 文件。

最让人头痛的并不只是这而是我们的管理平台上不显示图片和 css 样式，我们开始认为可能是 apache 没配好，试了很多次还是不行，最后又请教其它人发现是 CD 不支持临时文件写入，要用到一项新的技术联合文件系统 unionfs，整了几天，每天都熬到三四点才睡觉，早上 8 点多起来接着做最后还是没有成功。就是在 21 号的晚上发现系统已经用了 aufs 文件系统是支持光盘写数据的，也就是说问题不是出在联合文件系统，最后又回到 apache 的配置文件上找答案，发现原来只要打开 EnableSendfile off 就可以了。在这次设计过程中确实学到了许多课堂上都学不到的东西，当然我也感受到了团队合作的重要性。也感谢给我们指导的老师。

——王 安

这次竞赛对我来说是一次终身难忘的经历，面对这么多高手的比赛，想要从中脱颖而出是有多困难我相信我们的队友每个人都很清楚！可是我们也知道这是对我们的一次考验，要想证明自己，这又是一次难得的机会！

我们的设计过程可以说是从无从下手，到找到突破口，到分工合作，到细致工作，到遇到难题，到分析问题，到查阅资料，到解决问题，到再次遇到问题到解决问题，可以说形成了一个死循环，但是我们始终耐心细致地做好每一个工作，走好每一步，遇到问题了及时反应，及时解决，我们的团队是团结而有力的，遇到问题一起解决，一起想办法。

当我们遇到问题的时候从来没有过埋怨，更没有过放弃的念头，我们总是抱着不到最后一分钟决不放弃的想法继续前进着，团队合作在我们这个队一直坚持贯彻始终，让我充分感受到了团队的力量！这就是我的最大的收获！

### 教师评语

该组三位同学在做此项目期间，勤奋好学，踏实肯干，和睦相处，在项目操作中遇到不懂的地方，能够虚心向有经验的老师、同学请教，善于思考，举一反三。对于别人提出的建议能虚心听取。在时间紧迫的情况下，加班加点完成任务，并能将在学校所学的知识灵活应用到该项目中去，保质保量完成此项任务。

他们所开发的系统，是基于 Linux 下 ip 与 mac 绑定的代理服务。平时本人在工作中也有遇到此类问题，感觉该队此次所开发这套系统具有实用性、创新性、挑战性，实现了网络管理的简单化和智能化，可直接将此系统应用于公司、学校、小区中。

祝愿他们通过共同努力，能取得好的成绩。

指导教师：马玉军