



An All Linux Network with Integrated Monitoring Systems

Jay Schutte

Elton Vinson

Submitted to
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Engineering Technology

University of Cincinnati
College Of Applied Science
March 2005

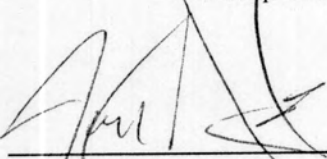
An All Linux Network with Integrated Monitoring Systems

By

Jay Schutte
And
Elton L. Vinson

Submitted to
The Faculty of the Information Engineering Technology Program
In Partial Fulfillment of the Requirements for
The Degree of Bachelor of Science
In Information Engineering Technology

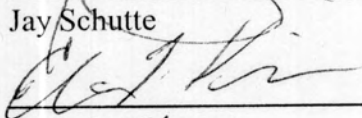
The authors grant to the Information Technology Program permission
To reproduce and distribute copies of this document in whole or in part.



Jay Schutte

3/7/05

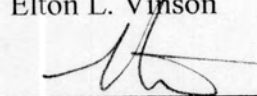
Date



Elton L. Vinson

3/7/05

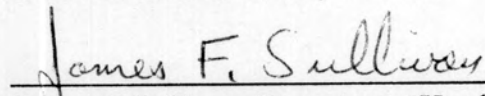
Date



Mark Stockman, Faculty Advisor

3/7/05

Date



James F. Sullivan, Department Head

7 March, 2005

Date

Acknowledgments

We would like to give special thanks to Mitsui Sumitomo Insurance Group for the donation of the hardware for this project. They donated nine Compaq PC's for the completion of our project. Along with the PC's they provided keyboards, mice, power cords, and monitors. Without this funding our project would not have been completed without holding a fundraiser to raise money to purchase equipment.

We would also like to thank Nettie Vinson for putting up funding for our budget. Her agency also has a lot of other priorities, but made sure that the office space was the first area of the facility to be completed so that we could setup the network in a timely fashion. We also want to thank her and the rest of the members of the ANPCA for venturing away from something familiar and trying out Linux on the desktop.

Table of Contents

Section	Page #
List of Figures	6
Abstract	7
1. Statement of Problem	8
2. Description of Solution	9
2.1 User Profiles	11
2.2 Design Protocols	12
3. Deliverables	16
4. Design & Development	16
4.1 Timeline	18
4.1.1 Senior Design I Accomplishments	18
4.1.2 Senior Design II Accomplishments	17
4.1.3 Senior Design III Accomplishments	18
4.2 Budget	20
5. Proof of Design	21
5.1 Linspire Desktop	21
5.2 Directory Searches	22
5.3 Network Shares	23
5.4 IP Cam & Favorites	23
5.5 Network Printer Information	23
5.6 Rsync	23
6. Recommendations	25
Appendix A - DIRECSERV1 Configuration. Files	27
A.1 SAMBA	27
A.2 LDAP	27
A.3 Partitions	29
A.4 RSYNC	30
Appendix B - BACSERV1 Configuration. Files	31
B.1 Partitions	31
B.2 LDAP	31
B.3 RSYNC	34
B.4 CRON	34
Appendix C- Client Configuration Files	36
C.1 PAM	36

C.2 LDAP	37
C.3 SAMBA	38
Notes	39
References	40

List of Figures

<u>Figure #</u>	<u>Page #</u>
Figure 1. Adding database entry	13
Figure 2. Base LDIF entry	14
Figure 3. User LDIF	14
Figure 4. Sample smb.conf file	15
Figure 5. Budget	21
Figure 6. Linspire Desktop	22
Figure 7. Linspire Email Contacts	23
Figure 8. Network Share	23
Figure 9. Favorites List to Choose IP Cam	24
Figure 10. IP Cam Sample View	24
Figure 11. Network Printer Setup	25

Abstract

Aunt Net's Professional Care Agency, Inc. (ANPCA) is a new non-profit organization that provides emergency respite care and supportive living for the mentally challenged and elderly. The management of ANPCA is obligated to monitor their staff for quality assurance purposes. ANPCA would like the presence of Information Technology in their agency to make their jobs easier, and allow them to do more with less.

We have designed a client/server Linux network with the addition of donated Compaq 866MHZ computers and an IP camera for monitoring staff and clients. This will ensure that the members of the organization that need computers will have them. They will be able to save money by sharing resources such as internet access, printers and file storage. This network consists of 4 client PCs and 2 servers. The building that our network is setup in had no network connections, so Cat 5 cabling has been run throughout the selected floor in the building. Internet access has been made available through Cincinnati Bell. The PCs have Linspire 4.5 installed with necessary applications and configured to use LDAP for authentication and employee lookups. There are two categories of system users; Management and Administrators.

An All Linux Network with Integrated Monitoring Systems

1. Statement of the Problem

Aunt Net's Professional Care Agency, Inc. (ANPCA) is a new non-profit organization that provides emergency respite care and supportive living for the mentally challenged and elderly. The bulk of ANPCA's business requires them to provide apartments for consumers and staffing to assist those consumers in daily routines. The management of ANPCA is obligated to monitor their staff for quality assurance purposes. This helps ensure that their consumers are receiving the care they need. Currently the agency is a small company of four management level employees and most of the work is done out of their homes on home computers. Soon they will be leasing a building. The building will house their offices and will be one site that they will be using for adult day care and supportive living.

ANPCA's former CEO, Sylvia Hill, and Program Director, Nettie Vinson, stated that they needed a small local area network (LAN) setup that will grow as the company grows. The two would also like the presence of Information Technology in their agency to make their jobs easier, and allow them to do more with less. According to Nettie, "The network should be as inexpensive as possible, but functional and reliable" (13). Due to the fact that the agency will be dealing with confidential records of the mentally challenged and elderly, the network should be secure as possible. There is no central file location for checking and updating of confidential client files and databases. Currently everyone has to have a copy of the same file and updates have to be e-mailed.

2. Description of Solution

To serve the needs of ANPCA we will create a LAN composed of four workstations running Linspire 4.5 operating system, a printer, an IP (Internet Protocol) camera, and two servers which will both be running Debian Linux. One server will be used as a PDC (Primary Domain Controller) by means of Samba^C and LDAP (Lightweight Directory Access Protocol)^D, while the other will function as a file server, BDC (Backup Domain Controller), and also to share a printer. The BDC will provide redundancy for the PDC in case of hardware malfunction. The second server described will also be backed up on a removable hard drive for disaster recovery. These nodes will be connected in a star topology by a switch. The switch will be connected to the Internet through a router and a DSL modem. A diagram of the described network can be seen in Figure 1. The primary emphasis of this project will be networking.

This design will meet all seven of the before mentioned requirements. It will ensure that all of the current employees have a computer to work on, meeting requirement number one. The network will allow all the users to share the same printer and Internet connection saving the agency money, meeting requirements two, three, and seven. The file server will house client records and other data that shouldn't be duplicated on every machine, which satisfies requirement number four. The network will also allow expandability for future growth. When more computers are needed another switch can be connected to the current one, allowing more computers to connect to the network, this meets requirement number five.

The sixth requirement of ANPCA is a secure IT environment. Security is a state that can almost be reached, but never totally achieved. But there are things that can be

done to make the job of securing the network easier. The LAN will be protected from the Internet through the router, which will act as a firewall blocking unwanted traffic. The domain controller will create a centralized point of security administration, and will force users to authenticate into the network in order to gain access to resources. Finally, we believe that centralized storage of sensitive data will make it easier to focus security efforts to protect it.

All of our solutions in some way help the agency save money, but we came up with one solution specifically for the purpose of saving ANPCA money. We will implement IP cameras that can be securely accessed through authentication over the local network and Internet via web browser. The user accounts can be added with an administrative account; the cameras have onboard web servers and network interface cards to make this possible. We would like to integrate the user accounts from LDAP with the IP cameras' onboard web servers to eliminate the need to add users in both places; we will know if this is possible after further research. IP cameras can be mounted where ever necessary at different apartments around the city where they provide supportive living. This will give management the power to check on staff and consumers from anywhere there is a computer with Internet access. This will reduce gas expenses and create free time that can be invested in other tasks.

2.1 User Profiles

There are two categories of users. The two levels include Management and Administrators.

Management

Upper management will be the daily users of the client PCs. They will have experience working with Microsoft Office products and be able to adapt to using Open Office. They will have experience with e-mail clients and web browsers. This user will vary in regards to technical literacy. The portion of the applications that will be used by the end users will require very little technical literacy. Our end users will be using computers for word processing, working with spreadsheet, sending emails, web browsing, and in the future they will have a need for using databases. For their work they need an office suite. At the moment they don't use very many of the advanced features that Microsoft Office offers. So, all they need is a computer that has a familiar office suite, with a web browser, and email client.

Systems Administrators

The System Administrator will have knowledge of LANs and Linux operating systems. The System Administrator will also be responsible for managing user accounts, maintaining the availability of network services, and security.

2.2 Design Protocols

OpenLDAP

OpenLDAP is an open source implementation of Lightweight Directory Access Protocol (LDAP). LDAP is the protocol that allows connections to a backend database and allows entries to be manipulated and accessed for directory lookups. OpenLDAP is a service called slapd that can be configured by a text file called slapd.conf. OpenLDAP can also be used in combination with other services (nss-ldap, libnss-ldap, and pam-ldap configuration files can be seen in the Appendix) to achieve authentication in several situations; in our case it will be logging on to the clients. The default database that will be used is called bdb (Berkeley Database). The directory entries are entered by a file format called LDAP Data Interchange Format or LDIF. From the command line on the server side the process for adding an entry in the database would be:

```
# /etc/init.d/slapd stop
# slapadd -v < /tmp/example.ldif
# slapindex -v
# /etc/init.d/slapd start
```

Figure 1: Adding database entry

The first command stops the OpenLDAP service. When working from the command line on the server side it is a good idea to stop OpenLDAP service to prevent any data corruption. When making modifications on an OpenLDAP replica or some third party tools it's not necessary to stop the service. The second command adds an LDIF entry that is written in a text file. There is an option to index the database after the entry, this is suggested when the service has been

stopped, otherwise it's done automatically at a later time. The last command restarts the OpenLDAP service.

Before adding user entries in to the database the database schema must be created. An example of our initial LDIF file that is used to develop the database schema would be:

```
dn: dc=anpca,dc=org
dc: anpca
o: anpca.org
objectClass: top
objectClass: dcObject
objectClass: organization

dn: ou=people,dc=anpca,dc=org
ou: people
objectClass: top
objectClass: organizationalUnit

dn: cn=admin,dc=example,dc=com
cn: admin
userPassword: secret
objectClass: top
objectClass: organizationalRole
objectClass: simpleSecurityObject
```

Figure 2: Base LDIF entry

This is a simple setup that works for authentication, but it's not that detailed when it comes to using it for an address book. For that, other object classes need to be added. An example of a user entry in LDIF just for authentication would be:

```
dn: uid=nvinson,ou=people,dc=anpca,dc=org
uid: nvinson
cn: Nettie Vinson
uidNumber: 1001
gidNumber: 100
homeDirectory: /home/nvinson
userPassword: password
loginShell: /bin/bash
```

Figure 3: User LDIF

After the users were added into OpenLDAP, Directory-Administrator was used to manipulate the directory. Another GUI called GQ was used to view the directory tree.

Samba

Samba will be used for sharing the /home and /share1 partition on DIRECSERV1 with the clients. Like OpenLDAP, Samba is a service (nmbd and smbd are the processes that make up the service) that runs on the servers that can be configured by a text file called smb.conf. Samba also comes preinstalled on the clients and its configuration file can be manipulated by GUI tools. The following example is a smb.conf file that would create a file share called share1, which happens to be on a separate partition.

```
#smb.conf

[global]
workgroup = anpca.org
netbios name = DIRECSERV1
security = share

[docs]
comment = "Departmental Shares"
path = /share1
guest ok = yes
read only = no
```

Figure 4: Sample smb.conf file

Rsync and Cron

Automated backups of home directories and shares to BACSERV1 will be achieved by rsync being installed on both servers in conjunction with cron, which comes with Debian. The directories that are to be backed up are defined in a

configuration file, /etc/rsyncd.conf, as well as the machine that is allowed to access DIRECSERV1 and a means for authentication. A copy of our rsyncd.conf file can be viewed in the Appendix. On BACSERV1 a script has been created and placed into a cron job that runs every weekday at 4:30 pm. A copy of our script and cron jobs can be seen in the Appendix also. At the end of the work day the hard drive that contains the backups can be removed, in case of disaster.

Security

The router is a physical firewall that will help shield the LAN from the internet. By default all ports are closed and they can be opened as needed. On the software side, firewalls are included with the Linux operating systems. Like the router, all unnecessary ports can be closed. The ports and services on our machines can be controlled through /etc/services and /etc/inetd.conf.

Another security measure that has been taken is the use of user passwords. With OpenLDAP we are enforcing strong passwords (seven alphanumeric characters) that need to be changed every ninety days.

The server file systems were divided into separate partitions. The folders /tmp and /var were given their own partition as another measure to protect the servers if the firewalls were compromised. Since everyone has write access to /tmp and /var it is a way for hackers to make a server useless by filling those directories to the hard drive's maximum capacity. If /tmp and /var are on separate partitions hackers can only fill those partitions and not effect the rest of the system.

Management of IP Cam and Network Printer

Both are on the network and accessed by IP addresses. The IP camera has an internal web server, which is managed by the web browser. There will be shortcuts on the desktops to access the IP camera. Security on the IP camera will be utilized by user name and password profiles. The IP Camera is currently located in the front room, on the first floor, monitoring the group activities.

The printer will be connected via parallel cable to a HP JetDirect Box and then to the router by a network cable, because the printer is not capable of an internal network card. Other ways to set up the printer are attaching it to one of the client's machines and sharing it. The only drawback is that machine has to be on at all times for other clients to print.

3 Deliverables

DIRECSERV1

- Running Debian 3.0
- Static IP address from the router
- Running OpenLDAP for authentication and company contacts
- Samba for user's home directories and shares
- rysnc/cron for automated backups of home directories and shares to

BACSERV1

BACSERV1

- Running Debian 3.0
- A static IP address from the router
- Replication of the directory server on DIRECSERV1 for redundancy

- A second larger removable hard drive for backing up the file server and some configuration files

PC001 – PC004

- Will be running Linspire 4.5
- Needed applications installed
- Configured to authenticate through LDAP
- Configured to do employee lookups through LDAP
- Shortcut to the IP camera website on the desktop
- Network printer installed
- Shared Internet connection through Cincinnati Bell

Network Peripherals

- The printer and IP camera will be connected to the network by the router and be assigned static IP addresses.

4 Design and Development

Below is our timeline and overall budget.

4.1 Timeline

Our Timeline is spaced out between each Senior Design Course.

4.1.1 Senior Design I Accomplishments – Spring 2004

Week 1-5

- Research and Analysis
- Documentation
- Write Draft Proposal

Week 6-10

- Write Senior Design Proposal
- Present Proposal to IET Faculty

4.1.2 Senior Design II Accomplishments – Fall 2004

Week 1-5

- Initial Network Setup
- Testing
- Workstation/Server Hardware Modifications
- Development of Standard Images
- Rough Draft of Design Freeze

Week 6-10

- Configure File Server
- Configure Domain Controllers
- Integrate LDAP with systems
- Complete Final Draft of Design Freeze
- Meeting with Advisor: Professor Stockman
 - Met with advisor at project site
- Senior Design Presentation and Project Demo for IET Faculty

4.1.3 Senior Design III Accomplishments – Winter 2005

Week 1-5

- Configure cron for automated backups of home directories and shares to BACSERV1
- Configure replication of directory
- Look into a wireless network system for the 4 workstations and network printer

Week 6-10

- Senior Design Finished Product
- End User support
- Finish Final Paper
- Final Presentation to IET Faculty

4.2 Budget

Budget

Item	Manufacturer/Model/Version	Cost	Quantity	Subtotal	Source
Computers	Compaq Deskpro EN Minitower PIII 866Mhz	\$0.00	4	\$0.00	Mitsui Sumitomo
File/Print Server	Compaq Deskpro EN Minitower PIII 866Mhz	\$0.00	1	\$0.00	Mitsui Sumitomo
Domain Controller	Compaq Deskpro EN Minitower PIII 866Mhz	\$0.00	1	\$0.00	Mitsui Sumitomo
Hard Drive	160 Gigabyte Samsung Hard Drive	\$89.99	1	\$89.99	www.microcenter.com
Hard Drive Rack	Hard Drive Rack	\$19.99	1	\$19.99	www.compusa.com
Switch/Router	D-Link DI-707 7-Port Router	\$60.80	1	\$60.80	www.ebay.com
Switch	D-Link 5 Port Switch	\$0.00	1	\$0.00	Cinergy
Network Jacks	Network Jacks	\$1.99	3	\$5.97	www.microcenter.com
IP Camera	D-Link DCS-900	\$88.00	1	\$88.00	www.ebay.com
DSL Modem	Speedstream	\$0.00	1	\$0.00	www.cincinnatiatibell.com
Network Cable	CAT 5 Network Patch Cable 300-foot	\$45.95	1	\$45.95	www.microcenter.com
LaserJet Printer	Brother Laser Printer HL-1440	\$129.99	1	\$129.99	www.microcenter.com
Surge Protectors	Surge Protector	\$2.99	2	\$5.98	www.microcenter.com
Operating System	Linspire 4.5	\$49.95	1	\$49.95	www.linspire.com
Internet Service	Zoomtown ADSL	\$64.95	1	\$64.95	www.cincinnatiatibell.com
Toner	Brother Toner	\$34.95	1	\$0.00	www.microcenter.com

Current Total: \$561.67

▼Hardware ▼Software Recurring Cost

Figure 5: Budget

5 Proof of Design

To meet our deliverables established in Senior Design II a network had to be put in place and many operating system configuration changes were made.

A makeshift network closet was put together with an available shelf to house two servers and a router. Cables were ran thru out the floor for the printer, IP camera, and 2 clients. Later, two other computers will be placed on the network as the need arises.

After a client PC is booted the user is prompted by the generic Linspire login prompt. After the user types in a username, password and clicks OK; they are authenticated into the system by DIRECSERV1 and there desktop appears. If DIRECSERV1 is down or overwhelmed by other network request BACSERV1 will authenticate the user.

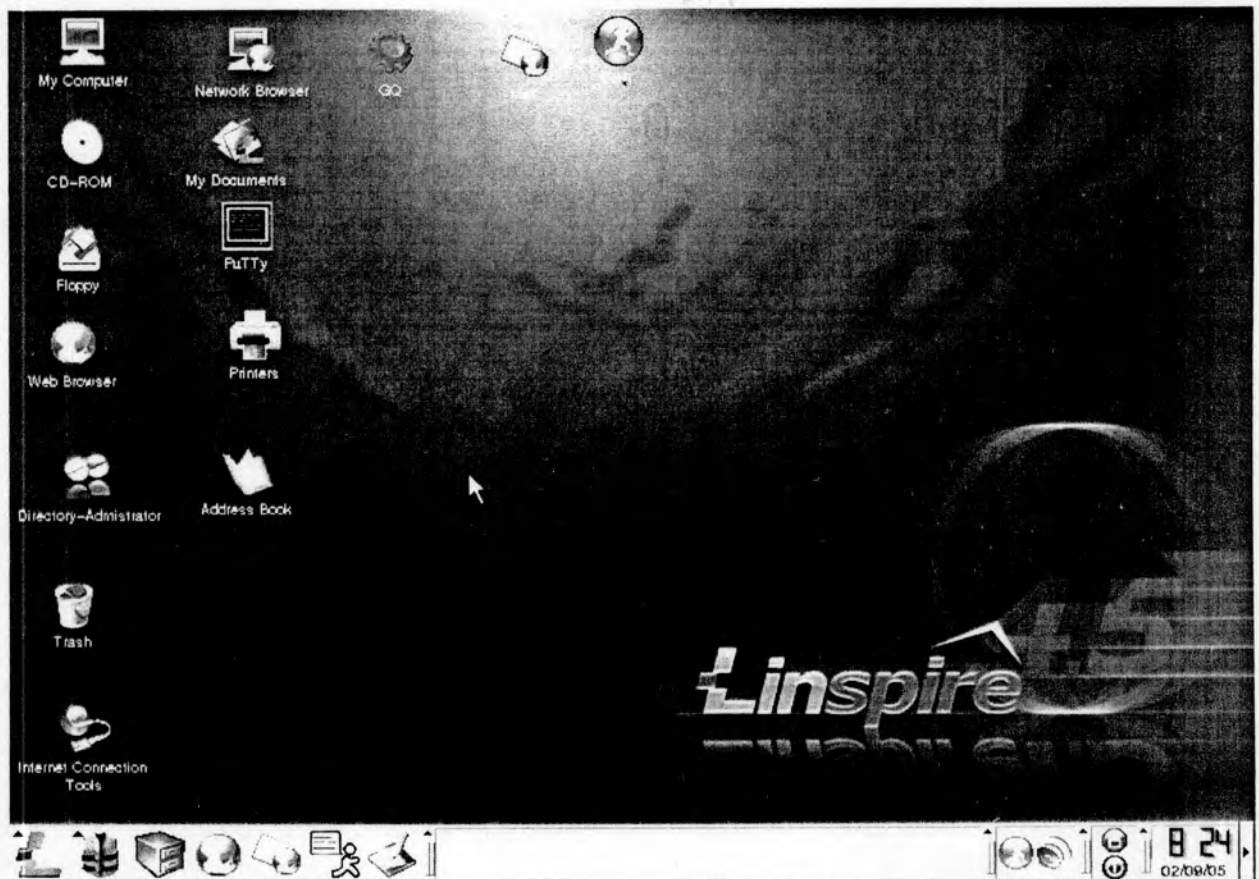


Figure 6: Linspire Desktop

By being part of a network many services can be made available to the Linspire desktops. When using Linspire's email client, email addresses and other organizational information can be found by the OpenLDAP servers.

The screenshot shows a web-based interface for searching and viewing contact information. At the top, there is a search bar labeled "Name or Email contains:" with the text "Vinson" entered. To the right of the search bar are two buttons: "Clear" and "Advanced...". Below the search bar is a table with the following columns: Name, Email, Department, Title, and Work Phone. The table contains two entries:

Name	Email	Department	Title	Work Phone
Elton Vinson	evinson@anpcainc.org	IT	CIO	513-961-4434
Nettie Vinson	nvinson@anpcainc.org	Executive	Director	513-961-4434

Below the table, there is a section titled "Card for Nettie Vinson". This section displays the following information:

- Display Name: Nettie Vinson
- Email: nvinson@anpcainc.org
- Work: 513-961-4434
- Director
- Executive
- Aunt Net's Professional Care Agency Inc.
- Cincinnati

At the bottom right of the card section is a button labeled "Get Map". At the bottom left of the interface, there are several icons (a folder, an envelope, a magnifying glass, and a document) followed by the text "2 matches found".

Figure 7: Linspire email contacts

A user can navigate to the department shares either from typing the path of the share at the run command or by navigating to it from the Network Browser.

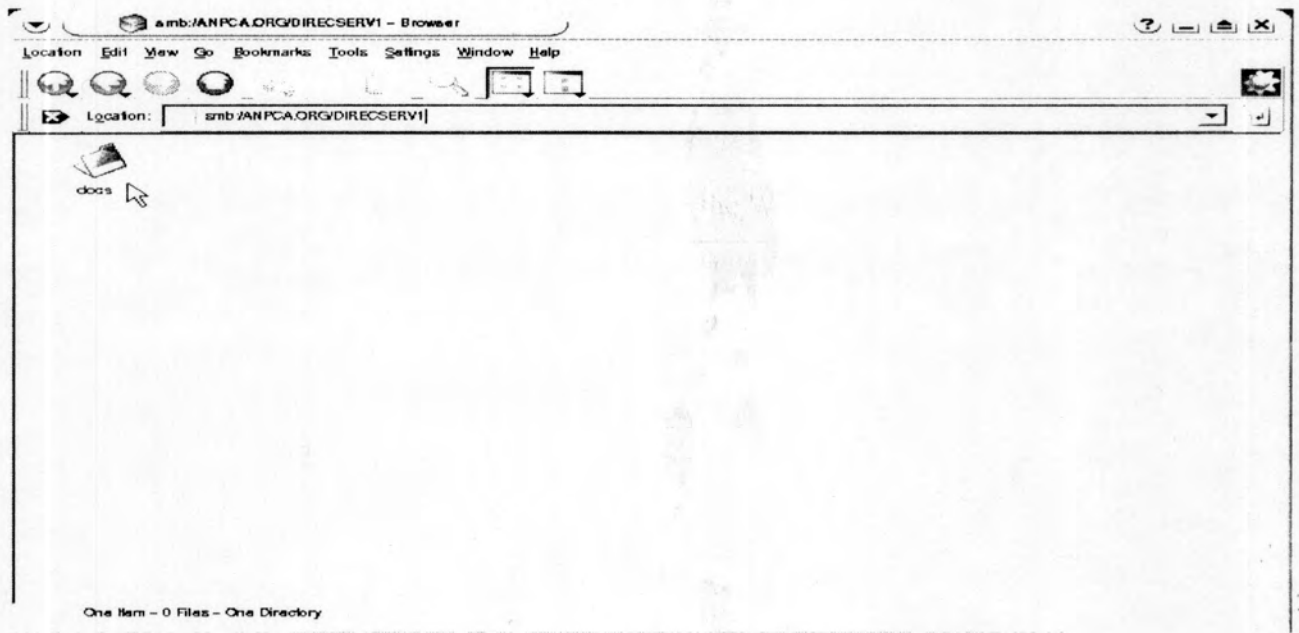


Figure 8: Network Share

Video from the IP camera can be viewed by going to the Web Browser and clicking on the IP camera listing in the Favorites menu.

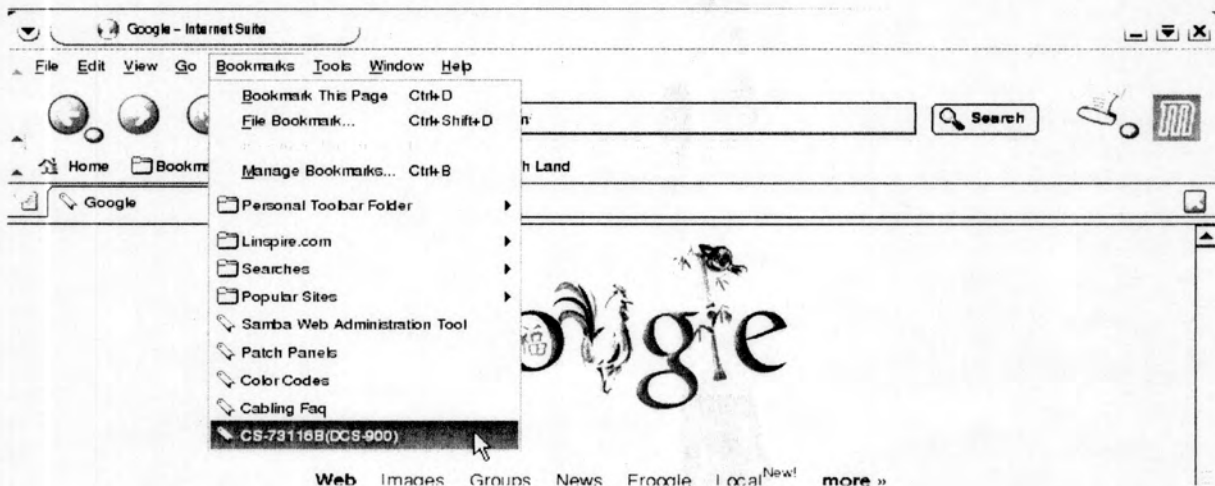


Figure 9: Bookmarks Menu to access IP camera

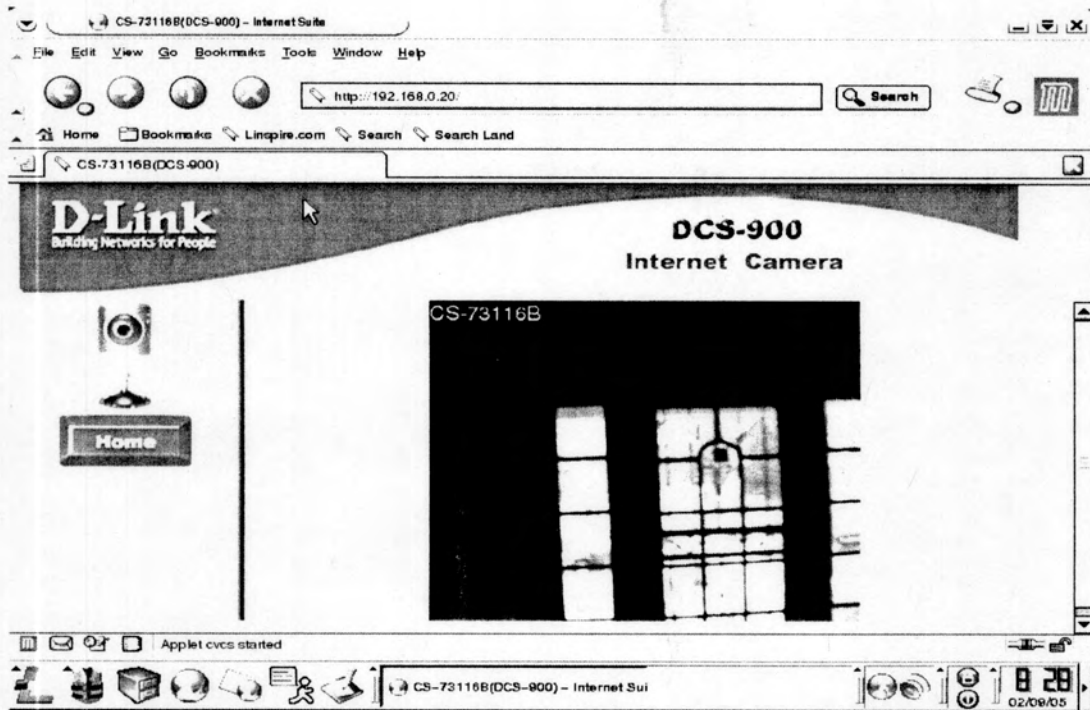


Figure 10: IP camera Sample View

To add a network printer the user can click the printer icon and follow the wizard's instructions to add a network printer.

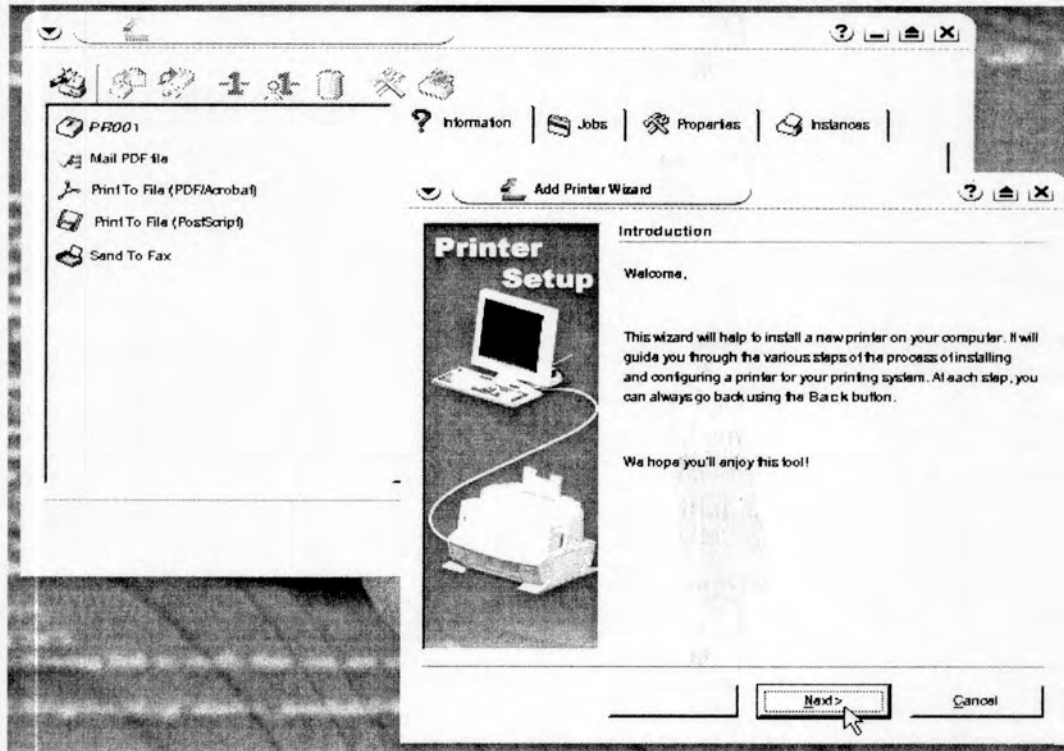


Figure 11: Network Printer Setup

On the server side, backups of all the users' network shares are made by an automated script every weekday at 4:30 p.m. Rsync is the service that actually backs up the shares. When the backups rotate only files that have changed since the previous backup are recopied. This makes the backups faster after the initial backup. By using this method an administrator can retrieve a backup of lost data up to a week old. The backups are saved on a removable hard drive, so at the end of the workday the drive can be taken to another location in case of disaster.

6 Recommendations

Our project presented some problems that we couldn't quite resolve, because of lack of time or some things weren't quite feasible the way we originally planned. Those

problems that we couldn't resolve were solved with "work arounds". All of our deliverables were meant, but maybe not quite as we had originally planned. This section addresses some of the issues that were encountered and the actions we took or will take.

For convenience the IP camera only has two accounts. One account for administrators and one account for users. Ideally we would of liked to have the IP camera's authentication page use the LDAP accounts for authentication so that would could have a single sign on, but because the web server is hard coded in the camera we could not make changes. A solution to this problem could have been to create a middle tier web application that authenticated our users by their LDAP account, and then forwarded them to the IP camera page. The solution was beyond the range of this project, so we decided to keep it as is.

Another problem that we encountered that was on the verge of being solved was the need to have a separate password database for Samba instead of Samba using LDAP as it's password database. In theory it should work, but due to time constraints, we will continue to maintain a Samba and a LDAP password database, and synchronize them as needed.

One last recommendation for aesthetics more than anything would be to replace our wired network with a wireless one. This would eliminate the need for network cables to be run along the base boards of the floor. In the future if ANPCA wishes we may incorporate wireless technology.

Appendix A

DIRECSERV1 Configuration Files

A.1 SAMBA

smb.conf

```
# /etc/samba/smb.conf
[global]
    workgroup = ANPCA.ORG
    server string = %v
[homes]
    valid users = %S
    read only = No
    browseable = No
[share1]
    path = /share1
    read only = No
    guest ok = Yes
[root]
    path = /
    read only = no
    guest ok = yes
```

A.2 LDAP

ldap.conf

```
#/etc/ldap/ldap.conf
BASE dc=anpca,dc=org
URI ldap://localhost
```

```
#/etc/ldap/slapd.conf
# Schema and objectClass definitions
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck on
```

```

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile          /var/run/slapd.pid

# List of arguments that were passed to the server
argsfile         /var/run/slapd.args

# Where to store the replica logs
repllogfile      /var/lib/ldap/repllog

replica host=192.162.0.120:389
      suffix="dc=anpca,dc=org"
      binddn="cn=admin,dc=anpca,dc=org"
      credentials=directserv
      bindmethod=simple

loglevel         0

#####
#####
# ldbm database definitions
#####
#####

# The backend type, ldbm, is the default standard
database         ldbm

# The base of your directory
suffix           "dc=anpca,dc=org"

# Where the database file are physically stored
directory        "/var/lib/ldap"

# Indexing options
index objectClass eq

# Save the time that the entry gets modified
lastmod on

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
access to attribute=userPassword
      by dn="cn=admin,dc=anpca,dc=org" write
      by anonymous auth

```

```

        by self write
        by * none

# The admin dn has full write access
access to *
        by dn="cn=admin,dc=anpca,dc=org" write
        by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
access to dn=".*,ou=Roaming,o=morsnet"
        by dn="cn=admin,dc=anpca,dc=org" write
        by dnattr=owner write

```

A.3 Partitions

fstab

```

# /etc/fstab: static file system information.
#
# <file system>    <mount point>    <type>    <options>
<dump>           <pass>
/dev/hda1        /                ext2      errors=remount-ro 0      1
/dev/hda2        none            swap      sw                0      0
proc             /proc           proc      defaults          0      0
/dev/fd0         /floppy         auto      user,noauto       0      0
/dev/cdrom       /cdrom          iso9660   ro,user,noauto    0      0
/dev/hda3        /usr            ext2      defaults          0      0
/dev/hda5        /var            ext2      defaults          0      0
/dev/hda6        /tmp            ext2      defaults          0      0
/dev/hda7        /home           ext2      defaults          0      0
/dev/hda8        /share1         ext2      defaults          0      0

```

A.4 Rsync

rsyncd.conf

```
# /etc/rsyncd.conf
[rsync_home]
    path = /home
    use chroot = no
    max connections = 4
    auth users = root
    hosts allow = BACSERV1.anpca.org
    secrets file = /etc/.rs_sec
    uid = root
    gid = root
[rsync_docs]
    path = /share1
    use chroot = no
    max connections = 4
    auth users = root
    hosts allow = BACSERV1.anpca.org
    secrets file = /etc/.rs_sec
    uid = root
    gid = root
```

Appendix B

BACSERV1 Configuration Files

B.1 Partitions

fstab

```
# /etc/fstab: static file system information.
#
# <file system>    <mount point>    <type>    <options>
<dump>            <pass>
/dev/hda1          /                ext2      errors=remount-ro 0      1
/dev/hda2          none             swap      sw                0      0
proc               /proc            proc      defaults           0      0
/dev/fd0            /floppy          auto      user,noauto        0      0
/dev/cdrom          /cdrom           iso9660    ro,user,noauto     0      0
/dev/hdb1           /backup          ext2      defaults           0      0
```

B.2 LDAP

ldap.conf

```
# /etc/ldap/ldap.conf
BASE dc=anpca, dc=org
URI ldap://192.168.0.120
```

```
# /etc/ldap/slapd.conf
# Allow LDAPv2 binds
allow bind_v2
```

```
# This is the main slapd configuration file. See
slapd.conf(5) for more
# info on the configuration options.
```

```
#####
#####
# Global Directives:

# Features to permit
#allow bind_v2
```

```

# Schema and objectClass definitions
include          /etc/ldap/schema/core.schema
include          /etc/ldap/schema/cosine.schema
include          /etc/ldap/schema/nis.schema
include          /etc/ldap/schema/inetorgperson.schema

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck      on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile          /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile         /var/run/slapd.args

# Read slapd.conf(5) for possible values
loglevel         0

# Where the dynamically loaded modules are stored
modulepath       /usr/lib/ldap
moduleload       back_bdb

#####
#####
# Specific Backend Directives for bdb:
# Backend specific directives apply to this backend until
another
# 'backend' directive occurs
backend          bdb

#####
#####
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until
another
# 'backend' directive occurs
#backend         <other>

#####
#####
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this database
until another
# 'database' directive occurs
database         bdb

```

```

# The base of your directory in database #1
suffix          "dc=anpca,dc=org"

# Where the database file are physically stored for
database #1
directory       "/var/lib/ldap"

# Indexing options for database #1
index           objectClass eq

# Save the time that the entry gets modified, for database
#1
lastmod         on

# Where to store the replica logs for database #1
# relogfile     /var/lib/ldap/replog

updatedn        "cn=admin,dc=anpca,dc=org"
updateref       ldap://192.168.0.119

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attribute=userPassword
    by dn="cn=admin,dc=anpca,dc=org" write
    by anonymous auth
    by self write
    by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms. Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
    by dn="cn=admin,dc=anpca,dc=org" write

```

```

        by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
#access to dn=".*,ou=Roaming,o=morsnet"
#       by dn="cn=admin,dc=anpca,dc=org" write
#       by dnattr=owner write

#####
#####
# Specific Directives for database #2, of type 'other' (can
# be bdb too):
# Database specific directives apply to this database
until another
# 'database' directive occurs
#database      <other>

# The base of your directory for database #2
#suffix        "dc=debian,dc=org"

```

B.3 Rsync

Rsync Script

```

# /etc/rsync.homes
ext=$1
rsync=/usr/bin/rsync
mount=/bin/mount
umount=/bin/umount
rsync_opts="-av --delete --delete-excluded"
password="--password-file=/etc/.rs_pass"
exclude_list=""
excludes=""
for exclude in $exclude_list; do
excludes="$excludes -- exclude=$exclude"
done

$rsync $rsync_opts $excludes $password
DIRECSERV1::rsync_home /backup/DIRECSERV1_${ext}
/backup/DIRECSERV1_error_${ext}/

```

B.4 Cron

Cron Jobs

```
# /etc/cron.d/rsync_daily_jobs
30 16 * * 1 root sh /etc/rsync.homes Mon
30 16 * * 2 root sh /etc/rsync.homes Tue
30 16 * * 3 root sh /etc/rsync.homes Wen
30 16 * * 4 root sh /etc/rsync.homes Thu
30 16 * * 5 root sh /etc/rsync.homes Fri
```

Appendix C

Client Configuration Files

C.1 PAM

kde

```
# /etc/pam.d/kde
auth required pam_nologin.so
auth sufficient pam_ldap.so
auth sufficient pam_unix.so shadow use_first_pass
auth required pam_deny.so

account sufficient pam_unix.so
account sufficient pam_ldap.so
account required pam_deny.so
```

login

```
#/etc/pam.d/login
auth required pam_nologin.so
auth sufficient pam_ldap.so
auth sufficient pam_unix.so shadow use_first_pass
auth required pam_deny.so

account sufficient pam_unix.so
account sufficient pam_ldap.so
account required pam_deny.so

session required pam_mkhomedir.so skel=/etc/skel
umask=0022
```

pam_ldap

```
#/etc/pam_ldap.conf
# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host 192.168.0.119
```

```

# The distinguished name of the search base.
base dc=anpca,dc=org

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
uri ldap://192.168.0.119

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=padl,dc=com

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=anpca,dc=org

# The port.
port 389

# Use the OpenLDAP password change
# extended operation to update the password.
pam_password exop

```

C.2 LDAP

libnss-dap

```

# /etc/libnss-ldap.conf
host 192.168.0.119
uri ldap://192.168.0.119/      ldap://192.168.0.120
base dc=anpca,dc=org

```

nsswitch.conf

```
# /etc/nsswitch.conf
passwd:      files ldap
group:       files ldap
shadow:      files ldap

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files
netgroup:    nis
```

C.3 SAMBA

smb.conf

```
# /etc/samba/smb.conf
[global]
    workgroup = ANPCA.ORG
    security = domain
    password server = *
```

Notes

A. The term “consumers” refers to the mentally challenged or elderly consumers who Aunt Net’s Professional Care, Inc cares for.

B. The term “staff” refers to non management employees that provide direct care for clients.

C. SAMBA is a Windows compatible file sharing service

D. LDAP is a protocol for accessing directory information.

E. The term “distribution” refers to a commercial or non-commercial release of an operating system based on the Linux kernel.

References

1. Carter, G. *LDAP System Administration*. O'reilly, 2003
2. CDW, www.cdw.com May 25, 2004.
3. Cincinnati Bell, www.cincinnati-bell.com May 25, 2004.
4. Debian GNU/Linux, www.debian.org May 30, 2005.
5. Injuryboard.com, "Surveillance Cameras Monitor Nursing Home Staff"
<http://www.injuryboard.com/view.cfm/Article=308> May 25, 2001.
6. Linspire, www.linspire.com May 25, 2004.
7. News Factor Top Tech News, "Linux Servers Seeing Upsurge"
http://www.newsfactor.com/story.xhtml?story_id=23258 Feb 24, 2004.
8. News Factor Top Tech News, "Linux Growth Means Security Test Ahead"
http://www.newsfactor.com/story.xhtml?story_title=Linux_Growth_Means_Security_Tests_Ahead&story_id=23932 May 4, 2004.
9. Metaconsultancy, www.metaconsultancy.com September 3, 2004.
10. Micro Center, www.microcenter.com May 25, 2004.
11. Terpstra, J. *The Official Samba-3 HOWTO and Reference Guide*. Prentice Hall, 2004
12. Tomsho, Greg, Ed Tittel, and David Johnson. *Guide to Networking Essentials*. Massachusetts: Thomson Course Technology, 2003.
13. Vinson, Nettie. Program Director of Aunt Net's Professional Care, Inc. Interview. April 10, 2004.