Design for a Home Network

by

Mary O’Brien

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

August 2005

Design for a Home Network

by

Mary O’Brien

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

Mary O’Brien Date

John Nyland, Faculty Advisor Date

Patrick Kumpf, Interim Department Head Date

Acknowledgements

I would like to give special thanks the technical instructors at the College of Applied Sciences who have through their insightful instructions empowered me with the ability to complete this project. In addition, my appreciation goes to my fellow students who by their excitement in the field of computer technology have shared ideas, suggestions, and recommendations.

And finally, thanks to my family who offered encouragement, support, and patience throughout this project.

Table of Contents

List of Illustrations

Abstract

Design for a Home Network is a local area network (LAN) project completed for the personal use of my family. I have constructed an Ethernet client/server network composed of various operating systems, a switch, and wired and wireless devices, security, and provisions for scalability. The server has two network interface cards, one to connect to the Internet through a router and a DSL modem, and the other connecting to the switch. The wireless access point (WAP) was configured as a bridge to segment the wireless portion network; network addresses were statically configured for security. The primary function of this home computer network is to share resources, bandwidth, files and applications. Overall, the design elements presented in this project can be recreated in any home or office environment.

Design for a Home Network

1. Product Description

This project is a client/server local area network (LAN) for a homeowner. This system is composed of a server, various operating systems, wired and wireless devices, with security, and growth potential. I have selected Fedora® Core release 3 as the Linux distribution for the server. The client stations' operating systems are Microsoft ® WindowsXP. Application programming was done using Samba, which is a suite of UNIX applications that speak the Server Message Block (SMB) protocol. Many operating systems use SMB to perform client-server networking. By supporting this protocol, Samba allows UNIX servers to communicate with the same networking protocol as Microsoft® Windows products. Thus, a samba-enabled UNIX machine can masquerade as a server on a Windows network.

1.1 Problem

The Shane, Sharp, and O'Brien household is a prime example of a normal, typical dysfunctional family. This blended household each has specific and unique computing uses and needs. Because of the various interests and skill levels, specific problems need to be addressed. For example, one member has an adapted technology device that can be attached to any computer. He would like to have more freedom to be able to log onto any machine to retrieve his files. The family also likes gaming and would like to play each other, with friends joining who have wired and wireless devices. Also, some financial information is stored on hard drives, so the solution would need to be as secure as possible.

1.2 The Solution

My solution is to build a home local area network that will provide for various operating systems, wired and wireless devices, growth potential, security, and a server. I have constructed an Ethernet network using category 5e cable, cat 5e, in a star configuration topology connecting each location to a switch. The server has two network interface cards, one to connect to the Internet through a router and a DSL modem, and the other connecting to the switch. The operating system for the server is a distribution of Linux. Linux was chosen as the operating system because it was created and distributed according to the principles of open source. Open source requires the distribution of the original source materials that can be studied, altered and built upon, with the results being freely distributed. Most operating systems, drivers and utility programs are written by commercial organizations that distribute executable versions of their software, versions that cannot be studied or altered. Linux was also selected because it has enabled individual users to have greater control over how their devices behave. I have selected Fedora® core release 3 as the Linux distribution for the following reasons:

- On-line documentation
- Written documentation
- Intel compatibility

Each of the personal computers currently owned operate with Microsoft® Windows XP, so application programming thru Samba has allowed the PC's to communicate with the server. Each of PC's is a station on the switch. The wireless router has enabled wireless device connectivity. This router also is a station on the switch.

A layered solution has addressed security through hardware and software configurations in a defense in depth approach. The LAN is protected from Internet attacks through the DSL router which acts as a firewall blocking unwanted traffic from entering the perimeter. The internal network has private subnet addressing, so the individual operating system information is not broadcast over the Internet. Each station and the server within the network has current software virus protection and anti spy-ware protection. The wireless router has been configured as a bridge with static address assignments to prohibit wireless hacking and to protect bandwidth. Nessus, a software application, has been installed on the server and is testing security and vulnerability. All unused ports, services, and protocols have been blocked either at the router level or the server. Also, an effective backup and recovery schedule has been implemented on the server and on each individual workstation.

1.3 Intended Use

This project is intended to be a home network of computer systems for the personal use of my family. This configuration has enabled us to share the Internet connection, printers, local area gaming, and files. The setup of the network includes securing sensitive files, Internet access and financial data, thereby keeping this system free from worms and viruses.

2. User Profile

The intended users will be myself as administrator, my husband, a special needs child, and a heavy gamer. As the administrator, I am controlling all aspects of this network including assigning file permissions, sharing folders, and managing users. I also am responsible for implementing and monitoring all network and computer security with a defense in-depth approach. My husband is using these systems to complete work, surf the Internet, and handle our finances. My special needs child uses the computer system to play games and for personal enjoyment. My other child is a heavy gamer and is using this network for Internet and Local Area Gaming with his friends. This user is my current concern as a security threat. Other threats are unknown hackers, spy wear, and malicious programmers.

3. Project Design

This project design utilizes both networking and application programming components. I have designed a star configuration topology using cat5e cable. Because wireless devices will be included in the network, I have selected a Linksys wireless access point to incorporate their use within the network. This router has been configured as a bridge to alleviate problems with segmentation.

3.1 Wire Diagram

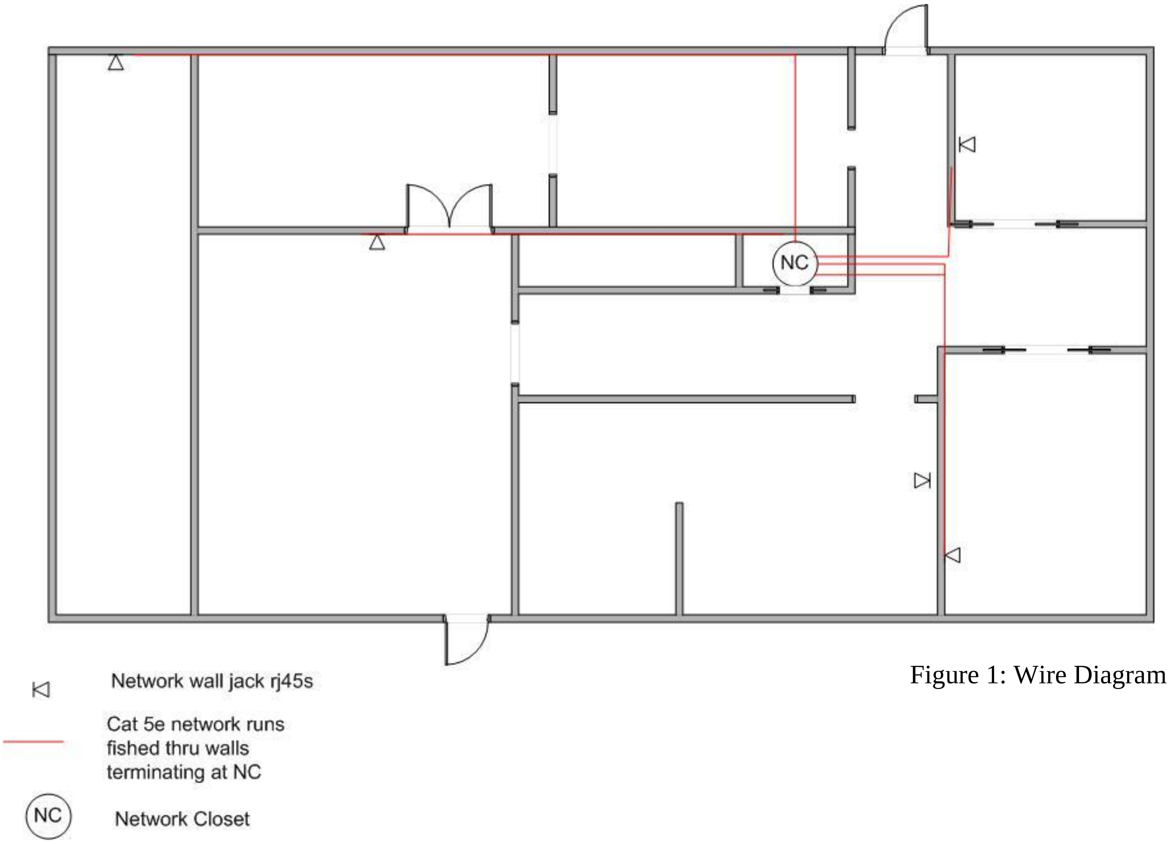


Figure 1: Wire Diagram

Figure 2: Wire drops

Figure 3: Wire drops

Figure 4: Wire outlet

3.2 Network Closet

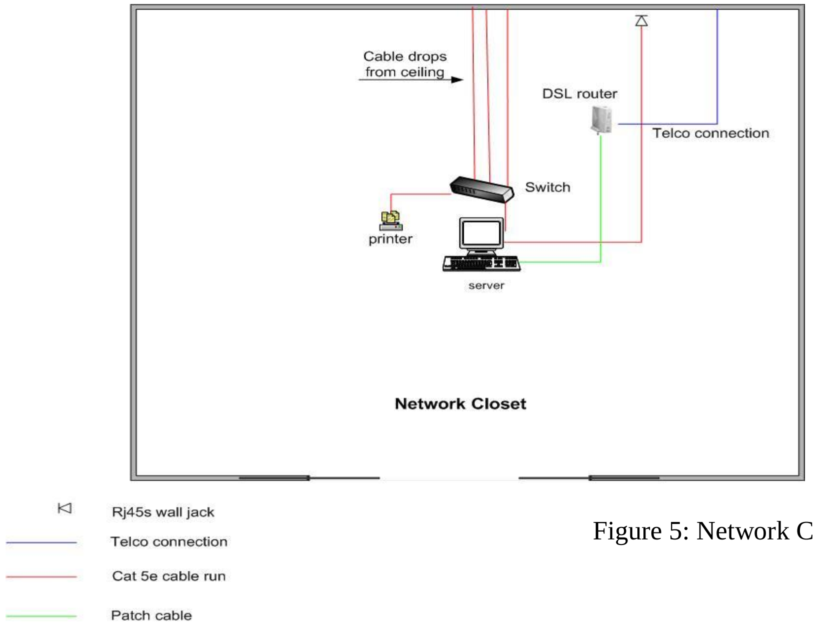


Figure 5: Network Closet

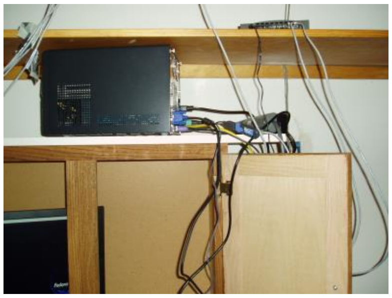


Figure 6: Network Closet

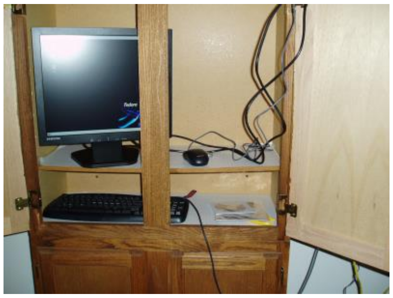


Figure 7: Network Closet

3.3 Logical Diagram

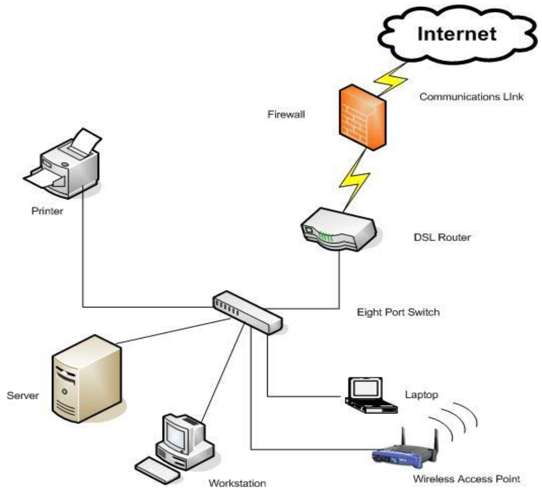


Figure 8: Logical Diagram

3.4 Software

In order to build and test the proposed home network, I am using the following operating systems: Microsoft Windows XP Pro, Fedora® distribution of Linux, and Samba. I already have the windows applications, and the UNIX based software is open source.

3.5 Hardware

Currently I am using a standard IBM based desktop and a laptop; additional client stations will be added as the scope of this project increases. The server equipment is a shuttle barebones system with Pentium P4/3.2GHz and the switch is an 8 port with auto sensing by SMC Networks.

4. Budget

The following is an approximation of costs for the project.

Item	Approximate Cost
Server	**$900.00**
SMC switch	**30.00**
Linksys WAP	**70.00**
USB Nic	**80.00**
Cat 5e cable	**54.00**
cover plates	**70.00**
rj45s jacks	**10.00**
Miscellaneous	**500.00**
Total	**$1714.00**

5. Timeline

5.1 Winter Quarter weeks 1-10

- Diagram wire locations
- Research and development
- Progress reports 1&2
- Area of inquiry
- Presentation
- Proposal

5.2 Spring quarter weeks 1-10

- Wired and labeled cate5e locations
- Researched Linux distribution and selected Fedora®
- Downloaded iso's
- Ordered equipment
- Progress report 1
- Rough draft of design freeze

5.3 Summer quarter weeks 1-10

- Complete installation of server
- Presentation for Spring quarter
- Submission of design freeze for Spring quarter
- Progress reports
- Final paper draft
- Final paper
- Presentation

6. Deliverables

6.1 System Deliverables

- Cat 5e ethernet in a star configuration
- Hardware firewall
- Software firewalls
- Linksys wireless access point

- Scalability

6.2 Server Deliverables

- Linux distribution Fedora® core 3
- Samba
- Domain controller
- User level security
- Roaming profiles
- User authentication
- Backup and recovery strategy and implementation
- Software firewall
- Nessus

6.3 Client Deliverables

- Microsoft® Windows backup and recovery strategy and implementation
- Software firewalls on each machine
- Wiring

7. Testing

Different testing implemented and completed throughout the project:

- Wire mapping and continuity testing
- Nessus security and vulnerability testing
- Hacker exploit testing using OPNET
- Wireless access testing
- Server and workstation compatibility

- Ethereal packet sniffing

8. Proof of Design

To meet my deliverables established in Senior Design II, a network was put in place, a wiring scheme was designed and completed, equipment was ordered and assembled, and software was installed. A closet that is located centrally was transformed into a network closet. This closet was selected not only for its location but also for its amenities and size. Because the home is one story, cable was run over the ceiling and jack locations were cut into specific location in various rooms with the terminating ends being dropped into the network closet.

The server hardware and software was ordered, assembled, downloaded, and installed. After the installation of Linux Fedora® core release 3 on the server, procedures were completed for the connecting of computers via a LAN.

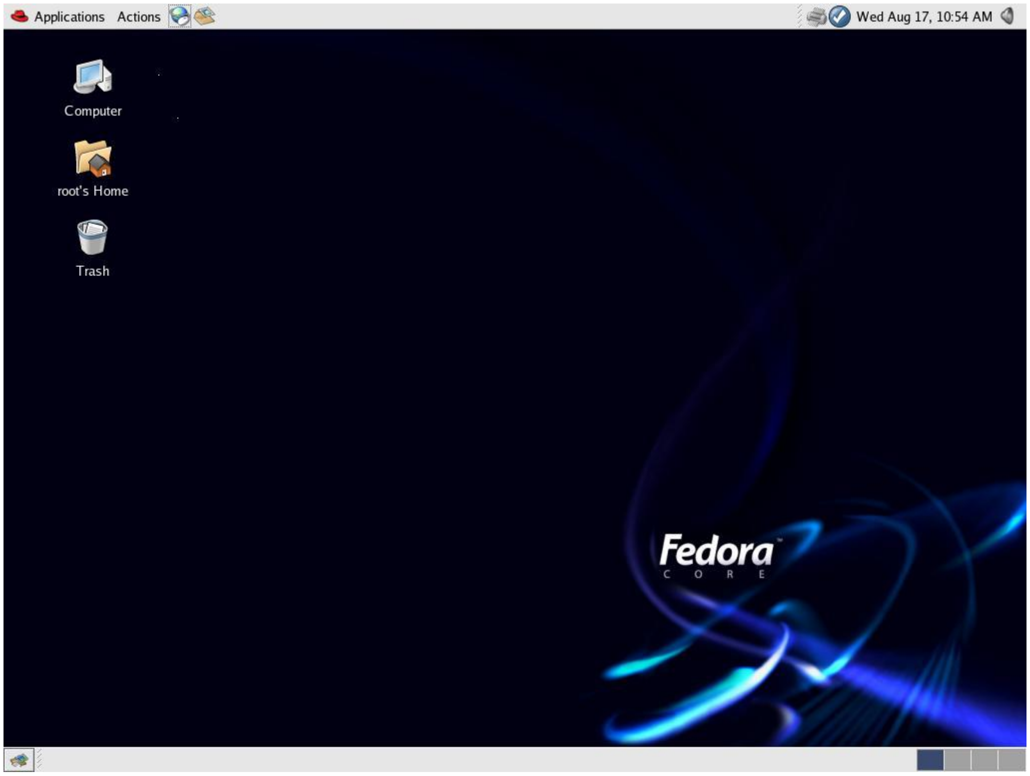


Figure 9: Fedora® Desktop

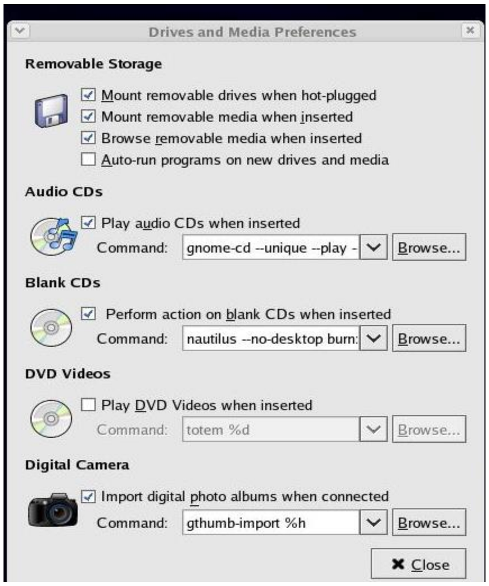
The creation of a network makes many services and resources available. For this network a subnet mask was created for the internal network; it is connected to the server by the addition of an additional network interface card, eth1. The addressing schema of the subnet was created for the addition of workstations, WAP, and for security.

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
IPV6INIT=no

cat ifcfg-eth1
IPV6INIT=no
ONBOOT=yes
USERCTL=no
PEERDNS=no
TYPE=Ethernet
DEVICE=eth1
HWADDR=00:10:60:85:3d:e1
BOOTPROTO=none
NETMASK=255.255.255.0
IPADDR=192.168.0.2
```

Figure 10: etho and eth1 configuration

The GNOME desktop, provided by Fedora® core release 3 installation default, is the desktop environment that one sees when logging in. The look-and feel-framework is provided by the window manager. The enhancements include a CD-burning feature, improved panels, plug-and-play, and accessibility features to improve ease-of-use for people with disabilities. The windows and icons visible are arranged on the desktop area. This area also supports a drag-and-drop between applications, a desktop menu, and icons for launching applications.



Drives and Media Preferences

Removable Storage

☑ Mount removable drives when hot-plugged
☑ Mount removable media when inserted
☑ Browse removable media when inserted
□ Auto-run programs on new drives and media

Audio CDs

☑ Play audio CDs when inserted
Command: gnome-cd --unique --play -

Blank CDs

☑ Perform action on blank CDs when inserted
Command: nautilus --no-desktop burn:

DVD Videos

□ Play DVD Videos when inserted
Command: totem %d

Digital Camera

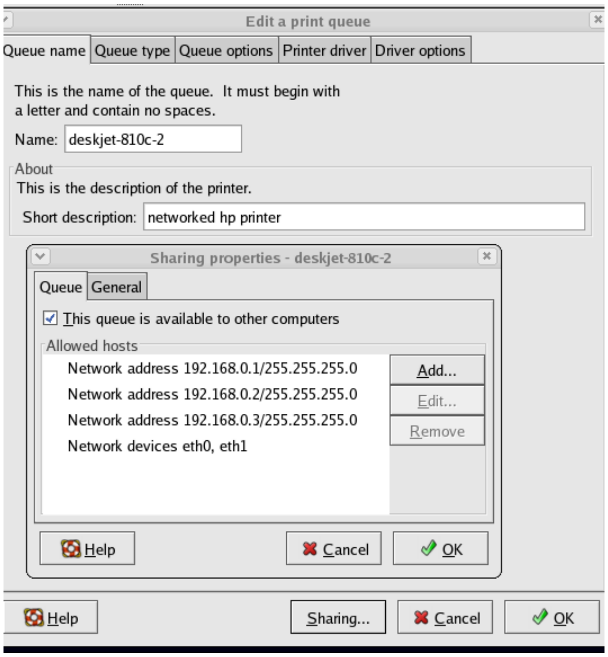
☑ Import digital photo albums when connected
Command: gthumb-import %h

Figure 11: Application GUI

Network printing was enabled by the configuration file Common UNIX Printing Service (CUPS), which is the recommended print service for this Linux version. Once a local printer is configured, print commands are available for carrying out the actual printing. Commands also exist for querying print queues, manipulating print queues, and removing print queues. A local printer can also be shared as a print server to users on the network.

```
<Location /printers/deskjet-810c-2>
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
AuthType None
Allow from 192.168.0.1/255.255.255.0
Allow from 192.168.0.2/255.255.255.0
Allow from 192.168.0.3/255.255.255.0
Allow from @IF(eth0)
Allow from @IF(eth1)
Listen 192.168.0.2:631
Listen 72.49.106.163:631
Listen 127.0.0.1:631
```

Figure 12: Print Allow



This is the name of the queue. It must begin with
a letter and contain no spaces.

Name: deskjet-810c-2

About

This is the description of the printer.

Short description: networked hp printer

☑ This queue is available to other computers

Allowed hosts

Network address 192.168.0.1/255.255.255.0
Network address 192.168.0.2/255.255.255.0
Network address 192.168.0.3/255.255.255.0
Network devices eth0, eth1

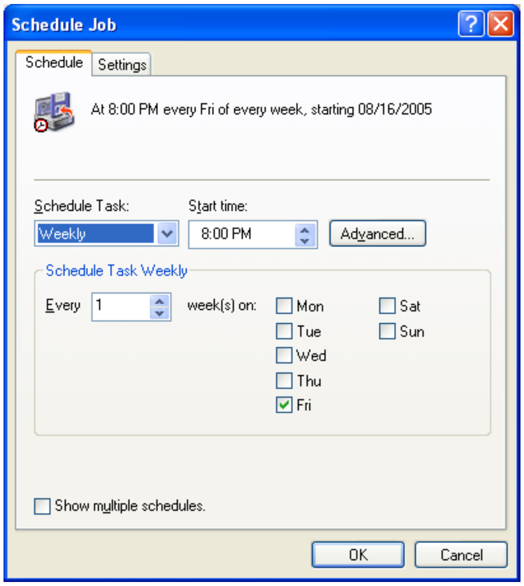
Figure 13: Print GUI

On the server side, backups of all the files that have been changed are appended and saved to a file. The files are saved in /etc/cron.weekly/backup and the file will launch the file, mirrorthis, which mounts an external device to save the backup.

```
mirrorthis
#!/bin/sh
cd `dirname $1`
2>&1 rsync --stats -a --delete --force ./$1
/mnt/externaldrive/. 2>&1 >/synclogs/$1sync.log
```

Figure 14: Server Backup File

An automatic backup schedule has also been implemented to run on the Windows XP client workstations. This plan has been scheduled to run weekly.



At 8:00 PM every Fri of every week, starting 08/16/2005

Schedule Task: Weekly

Start time: 8:00 PM

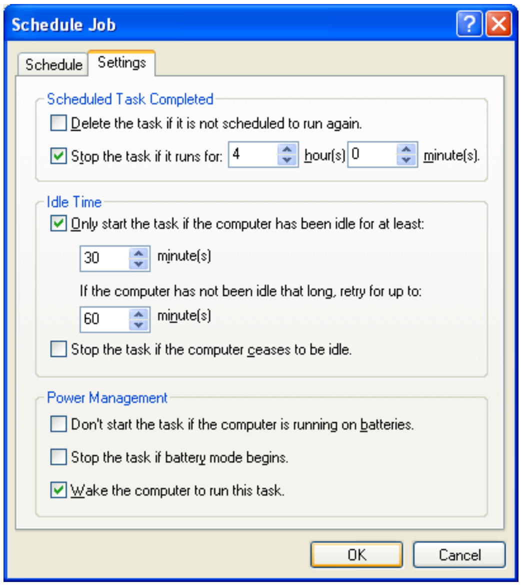
Schedule Task Weekly

Every 1 week(s) on:

□ Mon
□ Tue
□ Wed
□ Thu
☑ Fri
□ Sat
□ Sun

□ Show multiple schedules.

Figure 15: Windows Backup Schedule



Scheduled Task Completed

□ Delete the task if it is not scheduled to run again.

☑ Stop the task if it runs for: 4 hour(s) 0 minute(s).

Idle Time

☑ Only start the task if the computer has been idle for at least:

30 minute(s)

If the computer has not been idle that long, retry for up to:

60 minute(s)

□ Stop the task if the computer ceases to be idle.

Power Management

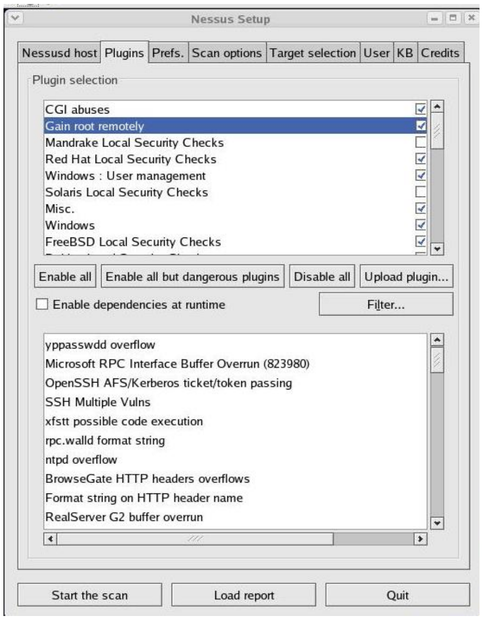
□ Don't start the task if the computer is running on batteries.

□ Stop the task if battery mode begins.

☑ Wake the computer to run this task.

Figure 16: Windows Backup Schedule

Nessus, a vulnerability scan utility, has also been implemented on the network. The configuration files and instructions were obtained from Nessus. A GUI interface allows the administrator to select specific plugins (pre-scripted applications) to check to security weaknesses in the network.



Plugin selection

CGI abuses ☑
Gain root remotely ☑
Mandrake Local Security Checks □
Red Hat Local Security Checks ☑
Windows : User management ☑
Solaris Local Security Checks □
Misc. ☑
Windows ☑
FreeBSD Local Security Checks ☑

□ Enable dependencies at runtime

yppasswdd overflow
Microsoft RPC Interface Buffer Overrun (823980)
OpenSSH AFS/Kerberos ticket/token passing
SSH Multiple Vulns
xfstt possible code execution
rpc.walld format string
ntpd overflow
BrowseGate HTTP headers overflows
Format string on HTTP header name
RealServer G2 buffer overrun

Figure 17: Nessus Plug in GUI

9. Conclusion and Recommendations

9.1 Conclusion

This project was created to satisfy a particular need for the members of my household. Though this project was custom created, the overall design concepts can be recreated in any home or small office. The performance of the completed network has far surpassed my expectations. Small problems involving both hardware and software, that individual computers were experiencing have been eliminated and performance and user satisfaction has increased. This project has fulfilled all Design Freeze deliverables. Testing was implemented and performed throughout the project. In particular, the vulnerability testing using Nessus has been essential.

9.2 Recommendations

While working on this project, I encountered several challenges. All of the problems were resolved; however, one resolution (the performance of my DSL line) was out of my control. All of my deliverables were met but some required more time to implement than previously anticipated. This section addresses some of the issues that were encountered and the actions taken.

Samba 3.0 has increased the performance level between the various operating systems, especially since the domain controller configuration feature has been added. I would have saved a lot of time if I had had previous experience with the release. My lack of expertise in this area increased my research time pushing the implementation of this feature to the last minute.

The other major problem that I experienced was with the performance of the DSL line. The DSL line was to be transmitting at speed close to that of a T1 line; however, at this speed my network performance would begin to degrade. I began experiencing packet loss. The network provider lowered my speed; the problem was eliminated. I have since contacted the provider to question when my neighborhood would be upgraded.

Appendix A

Configuration Files

A.1 Samba

Smb.conf

```
#
```

Global Settings [global]

```
# workgroup = NT-Domain-Name or Workgroup-Name
   workgroup = MYGROUP

# server string is the equivalent of the NT Description field
   server string = Samba Server

# This option is important for security. It allows you to restrict
# connections to machines which are on your local network.
   hosts allow = 192.168.1. 192.168.2. 127.

# if you want to automatically load your printer list rather
# than setting them up individually then you'll need this
   printcap name = /etc/printcap
   load printers = yes
   printing = cups

# This option tells cups that the data has already been rasterized
cups options = raw

# Uncomment this if you want a guest account, you must add this to /etc/passwd
  guest account = pcguest

# this tells Samba to use a separate log file for each machine that connects
  log file = /var/log/samba/%m.log

# Put a capping on the size of the log files (in Kb).
   max log size = 50

   security = user

# Password Level allows matching of _n_ characters of the password for
# all combinations of upper and lower case.
   password level = 8
   username level = 8
```

```
# You may wish to use password encryption.
   encrypt passwords = yes
   smb passwd file = /etc/samba/smbpasswd

# The following are needed to allow password changing from Windows to
# update the Linux system password also.
  unix password sync = Yes
  passwd program = /usr/bin/passwd %u
  passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n
*passwd:*all*authentication*tokens*updated*successfully*

# Unix users can map to different SMB User names
   username map = /etc/samba/smbusers


# Configure Samba to use multiple interfaces
# If you have multiple network interfaces then you must list them

    interfaces = 192.168.12.2/24 192.168.13.2/24

# Configure remote browse list synchronization
    remote browse sync = 192.168.3.25 192.168.5.255
# Cause this host to announce itself to local subnets here
   remote announce = 192.168.1.255 192.168.2.44

# Browser Control Options:
   local master = no

# OS Level determines the precedence of this server in master browser

   os level = 33

# Domain Master specifies Samba to be the Domain Master Browser.
  domain master = yes

   preferred master = yes

# Enable this if you want Samba to be a domain logon server for

   domain logons = yes


# Where to store roving profiles (only for Win95 and WinNT)
#      %L substitutes for this servers netbios name, %U is username
#       You must uncomment the [Profiles] share below
    logon path = \\%L\Profiles\%U
```

```
# All NetBIOS names must be resolved to IP Addresses
     name resolve order = wins lmhosts bcast

# Windows Internet Name Serving Support Section:
   WINS Support - Tells the NMBD component of Samba to enable it's WINS Server
   wins support = yes

 WINS Server
 wins server = w.x.y.z

 WINS Proxy - Tells Samba to answer name resolution queries on
   wins proxy = yes
```

Share Definitions

```
   idmap uid = 16777216-33554431
   idmap gid = 16777216-33554431
   template shell = /bin/false
   winbind use default domain = no
[homes]
   comment = Home Directories
   browseable = no
   writable = yes

# Un-comment the following and create the netlogon directory for Domain Logons
  [netlogon]
   comment = Network Logon Service
    path = /home/netlogon
    guest ok = yes
    writable = no
    share modes = no


# Un-comment the following to provide a specific roving profile share
  [Profiles]
     path = /home/profiles
     browseable = no
      guest ok = yes


# NOTE: If you have a BSD-style print system there is no need to
# specifically define each individual printer
[printers]
   comment = All Printers
   path = /var/spool/samba
   browseable = no
```

```
# Set public = yes to allow user 'guest account' to print
   guest ok = no
   writable = no
   printable = yes
```

A.2 Nessus-user

```
nessusd_host = isaac
nessusd_user = mary
paranoia_level = 1
begin(SCANNER_SET)
 10180 = yes
 10278 = no
 10331 = no
 10335 = yes
 10841 = no
 10336 = no
 10796 = no
 11219 = no
 14259 = no
 14272 = no
 14274 = no
 14663 = no
end(SCANNER_SET)

begin(SERVER_PREFS)
 max_hosts = 20
 max_checks = 4
end(SERVER_PREFS)

/nessus/nessusd.users
#

# Basically, this is
# username:[password]
# rules for the user
#

# User foo, with password bar :
#foo:bar
#accept 192.168.0.0/16
#default deny

# User oof :
#oof:rab
#deny 192.168.1.1/24
```

```
#default accept

# Default users, authenticated via their public key, and their rules :
*:
default accept
```

A.3. IPTABLES

```
Table: nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Table: filter
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:21
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:515
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:139
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:901
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
DROP       tcp  --   0.0.0.0/0           0.0.0.0/0          tcp dpt:445
DROP       udp  --  0.0.0.0/0            0.0.0.0/0          udp dpt:137
DROP       udp  --  0.0.0.0/0            0.0.0.0/0          udp dpt:138
DROP        tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:1241

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-          INPUT  all  --        0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --       192.168.0.0/24       0.0.0.0/0
ACCEPT     all  --       0.0.0.0/0                 192.168.0.0/24
DROP         all  --       !192.168.0.0/24      0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
```

```
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp - 0.0.0.0/0              0.0.0.0/0           icmp type 255
ACCEPT     esp  -  0.0.0.0/0             0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  -  0.0.0.0/0             224.0.0.251         udp dpt:5353
ACCEPT     udp  -  0.0.0.0/0             0.0.0.0/0           udp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
```

A.4. FSTAB

```
# This file is edited by fstab-sync -
LABEL=/                 /                       ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
none                    /dev/pts                devpts  gid=5,mode=620  0 0
none                    /dev/shm                tmpfs   defaults        0 0
LABEL=/home             /home                   ext3    defaults        1 2
none                    /proc                   proc    defaults        0 0
none                    /sys                    sysfs   defaults        0 0
LABEL=/var              /var                    ext3    defaults        1 2
LABEL=SWAP-hda3         swap                    swap    defaults        0 0
/dev/hdb                /media/cdrecorder       auto    pamconsole,exec,noauto,managed 0 0
/dev/sdc1               /media/APRICORN         vfat
pamconsole,exec,noauto,iocharset=utf8,managed 0 0
```

A.5. YUM (for nightly updates)

```
/etc/cron.daily/yum.cron
#!/bin/sh

if [ -f /var/lock/subsys/yum ]; then
        /usr/bin/yum -R 10 -e 0 -d 0 -y update yum
        /usr/bin/yum -R 120 -e 0 -d 0 -y update
Fi
/usr/include/fstab.h
/usr/sbin/fstab-sync
/usr/share/vim/vim63/syntax/fstab.vim
/usr/share/man/man5/fstab.5.gz
/usr/share/man/man8/fstab-sync.8.gz
/etc/hal/device.d/50-fstab-sync.hal
```

A.6. CUPS

```
# cupsd.conf.in,v 1.16 2004/08/18 17:53:47 mike Exp $".
#
<Location /printers/deskjet-810c-2>
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
AuthType None
Allow from 192.168.0.1/255.255.255.0
Allow from 192.168.0.2/255.255.255.0
Allow from 192.168.0.3/255.255.255.0
Allow from @IF(eth0)
Allow from @IF(eth1)
</Location>
Browsing Off
Listen 192.168.0.2:631
Listen 72.49.106.163:631
Listen 127.0.0.1:631
```

Appendix B

Checklist

Router Considerations

Check	Description
□	Latest patches and updates are installed.
□	You subscribed to router vendor's security notification service.
□	Known vulnerable ports are blocked.
□	Ingress and egress filtering is enabled. Incoming and outgoing packets are confirmed as coming from public or internal networks.
□	ICMP traffic is screened from the internal network.
□	Administration interfaces to the router are enumerated and secured.
□	Web-facing administration is disabled.
□	Directed broadcast traffic is not received or forwarded.
□	Unused services are disabled (for example, TFTP).
□	Strong passwords are used.
□	Logging is enabled and audited for unusual traffic or patterns.
□	Large ping packets are screened.
□	Routing Information Protocol (RIP) packets, if used, are blocked at the outermost router.

Firewall Considerations

Check	Description
□	Latest patches and updates are installed.
□	Effective filters are in place to prevent malicious traffic from entering the perimeter
□	Unused ports are blocked by default.
□	Unused protocols are blocked by default.
□	IPsec is configured for encrypted communication within the perimeter network.
□	Intrusion detection is enabled at the firewall.

Switch Considerations

Check	Description
□	Latest patches and updates are installed.
□	Administrative interfaces are enumerated and secured.
□	Unused administrative interfaces are disabled.
□	Unused services are disabled.
□	Available services are secured.

Appendix C

Nessus Scan Report

Nessus Scan Report
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	0
Number of security warnings found	2

Host List	
Host(s)	**Possible Issue**
buddybelle.homelinux.com	Security warning(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
buddybelle.homelinux.com	general/tcp	Security notes found
buddybelle.homelinux.com	microsoft-ds (445/tcp)	Security notes found
buddybelle.homelinux.com	netbios-ssn (139/tcp)	Security notes found
buddybelle.homelinux.com	netbios-ns (137/udp)	Security warning(s) found
buddybelle.homelinux.com	http (80/tcp)	Security notes found
buddybelle.homelinux.com	ssh (22/tcp)	Security warning(s) found

Security Issues and Fixes: buddybelle.homelinux.com		
Type	**Port**	**Issue and Fix**
Informational	general/tcp	 However the execution of the command "uname -a" failed, so local security checks have not been enabled Nessus ID : 12634
Informational	general/tcp	72.49.106.163 resolves as buddybelle.homelinux.com. CVE : CAN-2004-0500 BID : 10865 Nessus ID : 12053
Informational	microsoft-ds	A CIFS server is running on this port Nessus ID : 11011

	(445/tcp)	
Informational	microsoft-ds (445/tcp)	It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000). Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$ Please see http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html All the smb tests will be done as ''/'whatever' in domain ARACOMA CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117 BID : 494, 990, 11199 Nessus ID : 10394
Informational	microsoft-ds (445/tcp)	The remote native lan manager is : Samba 3.0.10-1.fc3 The remote Operating System is : Unix The remote SMB Domain Name is : ARACOMA Nessus ID : 10785
Informational	netbios-ssn (139/tcp)	An SMB server is running on this port Nessus ID : 11011
Warning	netbios-ns (137/udp)	The following 9 NetBIOS names have been gathered : ISAAC ISAAC ISAAC __MSBROWSE__ ARACOMA ARACOMA ARACOMA ARACOMA ARACOMA . This SMB server seems to be a SAMBA server (this is not a security risk, this is for your information). This can be told because this server claims to have a null MAC address If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621 Nessus ID : 10150
Informational	http (80/tcp)	The following directories were discovered: /cgi-bin, /error, /icons, /manual While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards Nessus ID : 11032
Informational	http	The remote web server type is :

	(80/tcp)	Apache/2.0.53 (Fedora) Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers. Nessus ID : 10107
Warning	ssh (22/tcp)	The remote host is missing the patch for the advisory SUSE-SA:2004:025 (gaim). Gaim is an instant messaging client which supports a wide range of protocols. Sebastian Krahmer of the SuSE Security Team discovered various remotely exploitable buffer overflows in the MSN-protocol parsing functions during a code review of the MSN protocol handling code. Remote attackers can execute arbitrary code as the user running the gaim client. The vulnerable code exists in SUSE Linux 9.1 only. Solution : http://www.suse.de/security/2004_25_gaim.html Risk factor : High CVE : CAN-2004-0500 BID : 10865 Nessus ID : 10882
Informational	ssh (22/tcp)	Remote SSH version : SSH-1.99-OpenSSH_3.9p1 Remote SSH supported authentication : publickey,gssapi-with-mic,password Nessus ID : 10267

This file was generated by Nessus, the open-sourced security scanner.

Notes

DSL modem- Digital subscriber line modem designed to allow high speed data communication over the existing copper telephone lines between end-users and telephone companies.

GNOME- Fedora® default desktop environment provided with the installation package of the operating system.

GUI- Graphical User Interface. A computer terminal interface, such as Windows, that is based on graphics instead of text.

LAN- Local area network is a collection of computers and other networked devices that fit within the scope of a single physical network

Nessus-Nessus is a vulnerability scanner, a program that looks for security bugs in software.

OPNET- OPNET Technologies Inc. is a company that creates management software for communications networks. Its simulation-based products are used to design, build, and operate new networks and services.

Samba- An open source software suite that makes a Linux server look and act like a Windows server. It permits Windows clients to access Linux.

Server- A computer whose job is to respond to requests for services or resources from clients elsewhere on a network.

Sharing- This is the fundamental justification for networking. Sharing is the way in which resources are made available to the network.

Subnet address- A portion of a network that shares a common address, Internet Protocol IP, component creating an internal network.

Topology- Network design

WAP- Wireless access point is a device that connects wireless networking components of the LAN to the switch. It forwards traffic from the wired side to wireless side.

Resources

1. Anderson, Harry. "Introduction to Nessus." August 15, 2005. URL http://www.securityfocus.com/print/infocus/1741/ (2005).

2. Ciampa, Mark. *Guide To Wireless Communications.* United States: Thompson Course Technologies, 2002.

3. Das, Sumitabha. *Your UNIX, The Ultimate Guide*. Boston: McGraw-Hill, 2001.

4. Eckstein, Robert and David Collier-Brown and Peter Kelly. *Using Samba.* California: O'Reilly & Associates, Inc., 2000.

5. Graham, Steven, and Steve Shah. *Linux Administration-A Beginners Guide*. New York: McGraw-Hill/ Osborne, 2003.

6. Kochan, Stephen G., and Patrick H Wood. *UNIX Shell Programming*. United States: Hayden Books UNIX System Library, 1990.

7. Microsoft corp. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/CL_SecuNet.asp. No date.

8. Negus, Christopher. *Red Hat Linux Bible: Fedora and Enterprise Edition.* Indiana: Wiley Publishing, Inc. 2004.

9. Northcutt, Stephen, Lenny Zeltser, Scott Winters, Karen Kent Frederick, and Ronald W. Ritchey.. *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPN's), Routers, and Intrusion Detection Systems.* United States: New Rider, 2003.

10. Skoudis, Ed. *Counter Hack.* New Jersey: Prestice-Hall, Inc, 2002.

11. Tomsho, Greg, and Ed Tittel, and David Johnson. *Guide to Networking Essentials.* United States: Thompson Course Technology, 2003.

12. Verity, Beth. *Guide to Network Cabling Fundamentals.* United States: Thompson Course Technologies, 2003.

13. "Wireless-G Access Point, Linksys Users Guide." No date. Online manual Linksys® A Division of Cisco Systems, Inc. <http://www.linksys.com/wap54>.