

Transparent Wireless Authentication For New Wireless Network

By

Timothy G. Krebs

A Proposal 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 2006

Transparent Wireless Authentication For New Wireless Network

By

Timothy Krebs

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

© Copyright 2006 Timothy G Krebs

The contents of this document are under copyright of the author. It may not be reproduced and distributed in whole or in part without the written permission of the author.

Timothy Krebs

Date

John Nyland

Date

Patrick C. Kumpf, Ed.D. Interim Department Head

Date

Acknowledgements

A special thanks to Cheviot United Methodist Church for granting me the opportunity to execute this project. I also thank Scott Eckner at SYSCO Food Services of Cincinnati, LLC for the donation of a computer for this project. In addition, I would like to acknowledge the support and assistance of advisors, John Nyland and Mark Stockman.

Table of Contents

Section	Page
Acknowledgements	i
Table of Contents	ii
List of Figures	iv
Abstract	v
1. Statement of Problem	1
1.1 Additional Benefits	1
1.2 A Secure Solution is Required	2
2. Reasons Why Security is Required	3
3. Project Explanation	4
3.1 Previous Infrastructure	4
3.2 Solution for Transparent Wireless Network Authentication	5
3.3 User Profiles	7
3.3.1 Guest User	7
3.3.2 Owner User	8
3.3.3 User Administration:	8
3.4 Design Protocols	10
4 Deliverables	15
5 Project Development	17
5.2 Project Budget	17
5.3 Hardware and Software Requirements	19
5.3.1 Hardware	19
5.3.2 Software	20
6 Proof of Design	20
6.1 Overall	20
6.2 Pastor:	22
6.3 Secretary:	23
7 Conclusion and Recommendations	24

Appendix A. NoCat Configuration File	25
Appendix B. Apache Configuration File	30
Appendix C. MySQL Tables	31
Appendix D. Packet Captures	32
Appendix E. User Documentation	34
References	47

List of Figures

Figure 1: Previous Network Infrastructure	4
Figure 2: Current Network Infrastructure	6
Figure 3: Current NoCat System Status	8
Figure 4: Webmin Logon Screen	9
Figure 5: User Modification Screen	10
Figure 6: Login Page For Access to Wireless Network	11
Figure 7: Successful NoCat Logon	12
Figure 8: NoCat Login Agent Window	13
Figure 9: NoCat Login Agent Logged Out Window	13
Figure 10: Snapshot of User Documentation	14
Figure 11: Comparisons of Original and New Sites	15
Figure 12: Time Line	17
Figure 13: Budget	18

Abstract

Transparent Wireless Access for the New Wireless Network at Cheviot United Methodist Church is a Linux gateway that operates between the primary church network and the new wireless network. The Linux gateway provides security for access to the primary network. The Linux gateway redirects any user associated with the church's wireless network to a login web page hosted on the Linux box. Once the Linux box receives the login request it compares it against a user database in MySQL. If the user is valid it allows it to enter the system and redirects the user to the original web page requested. In addition, to checking the user database the Linux box also looks for the user name as an owner in the gateway configuration file. If it finds it there, full network access is provided otherwise the user is considered a guest and is only allowed access to the web and not the computers on the primary network. All traffic submitted through the web page is a 128 bit encrypted. This solution provides an easy way for a normal user to access the wireless environment without the issues of setting up an encryption key.

Transparent Wireless Authentication For New Wireless Network

1. Statement of Problem

This project was originally started by a request to find Internet access for the pastor whose trial service with his current provider was running out. The church decided that since they were paying for Internet access already, that they could let the pastor use their access as a perk. The first thought was to let the pastor connect via dial up using the Fuse account that the church was paying for along with Zoomtown high-speed Internet access. Then there was the idea of connecting the pastor to the church network via a wireless access point. The possibility could be feasible because the parsonage is located just across the parking lot from the church. The wireless method would then allow the pastor full access to the church network as well as the high-speed Internet access. This would also permit his computer to stay current on virus definitions and windows security patches. It would prevent the possibility of the pastor's home machine from being infected from viruses. In addition this could protect the church system from incoming viruses via removable media ported from the pastor's home machine to the local office machine.

1.1 Additional Benefits

Along with benefiting the pastor the wireless network will serve the church. The church secretary uses a laptop to take minutes at meetings. Putting this wireless network in place could allow her to easily print off the minutes from her laptop and send files to her desktop without having to deal with floppy disks. In addition people at meetings who are giving presentations

could access their e-mail to retrieve PowerPoint presentations; instead of trying to get a floppy disk or CD to work in either their machine or the churches'. In the past the church has had some issues with burnt CD's not working in the church laptop.

The church is in the process of creating a contemporary worship service, which will require a computer. With the possibility of the contemporary worship computer being able to access the church network, it would allow them access to files such as sermon notes, PowerPoint presentations and song lyrics from one of the office computers. This would prevent incorrect duplicates from being used. Instead a centralized storage location could be used so changes made would be displayed. This also prevents having to update the second copy every time someone makes a change.

1.2 A Secure Solution is Required

The idea of a wireless network had raised the question of how could it be made secure, but be easily accessible for all types of users, whether they were technically inclined or not. In addition they did not want any setup to happen on the client side.

What the church was looking for was a solution to solve multiple problems.

- Have the pastor be able to access the Internet and church resources.
- Have the secretary be able to print meeting minutes from laptop.
- Have the secretary be able to easily move documents to her desktop computer.
- Have church members or guests be able to easily access the Internet for meetings or presentations.
- Have a secure wireless network that would prevent unauthorized user access.
- Allow network access for future contemporary worship computer.
- Be a low cost solution due to budget restraints.
- No client setup.

The primary emphasis for this project is on networking with some database and web work as well.

2. Reasons Why Security is Required

Security for a wireless network is different than that for a wired network. In a wired network you physically have to plug into the network to access it. In a wireless network however, you just have to be in range of the signal to access it. It makes hacking and packet sniffing a network much easier because you are already connected to the network. (Beginners Guides: Wireless Network Security - PCStats.com) It is easy to connect because most wireless access points broadcast their SSID and with Windows XP, it searches for them and usually automatically connects to the network.

All the security is disabled on the access point by default because it makes initial configuration easier. If the security is enabled by both the client and the router one must have exactly the same configuration. This includes SSID, encryption type, and level. Sometimes not all clients support all types of encryption. (Securing Your Wireless Network)

According to “Securing Your Wireless Network” on enterprisenetworkingplanet.com there are five ways to secure a wireless network. They are Physical Protection, User Authentication, Access Control, Encryption, and Security Management. To meet the church requirements, User Authentication, Access Control and Physical Protection will be implemented.

Since security is an issue the web login session must be encrypted. When Apache is initially setup it gives you a test certificate to use. Since it is a generic certificate, Internet Explorer contains some errors. Since these errors occurred a new certificate had to be created. Research was done on how to create a new self signed certificate. The resource at “How to Create a Self-Signed Certificate” provides information on how to create one. Every version of Linux is different so some tweaking was involved, but it was a good place to start.

3. Project Explanation

3.1 Previous Infrastructure

Previously, the church had a peer-to-peer network that looked like Figure 1 below.

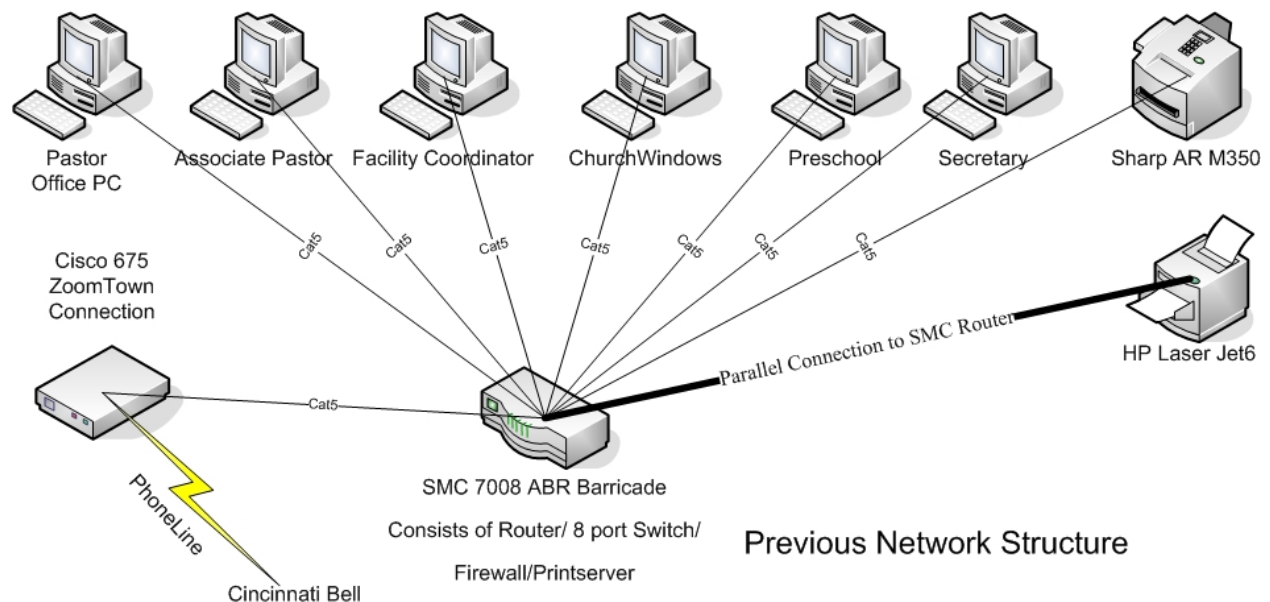


Figure 1: Previous Network Infrastructure

The network previously consisted of an eight port SMC 7008ABR Barricade broadband router/print server, six computers and one networked scanner/copier. Broadband access is Zoomtown by Cincinnati Bell who provided the Cisco 675 router. The church also has a laptop that was not connected to the network. All network wiring that is in place is CAT 5e with the exception of the HP laser Jet 6 which is connected via parallel cable to the router/print server.

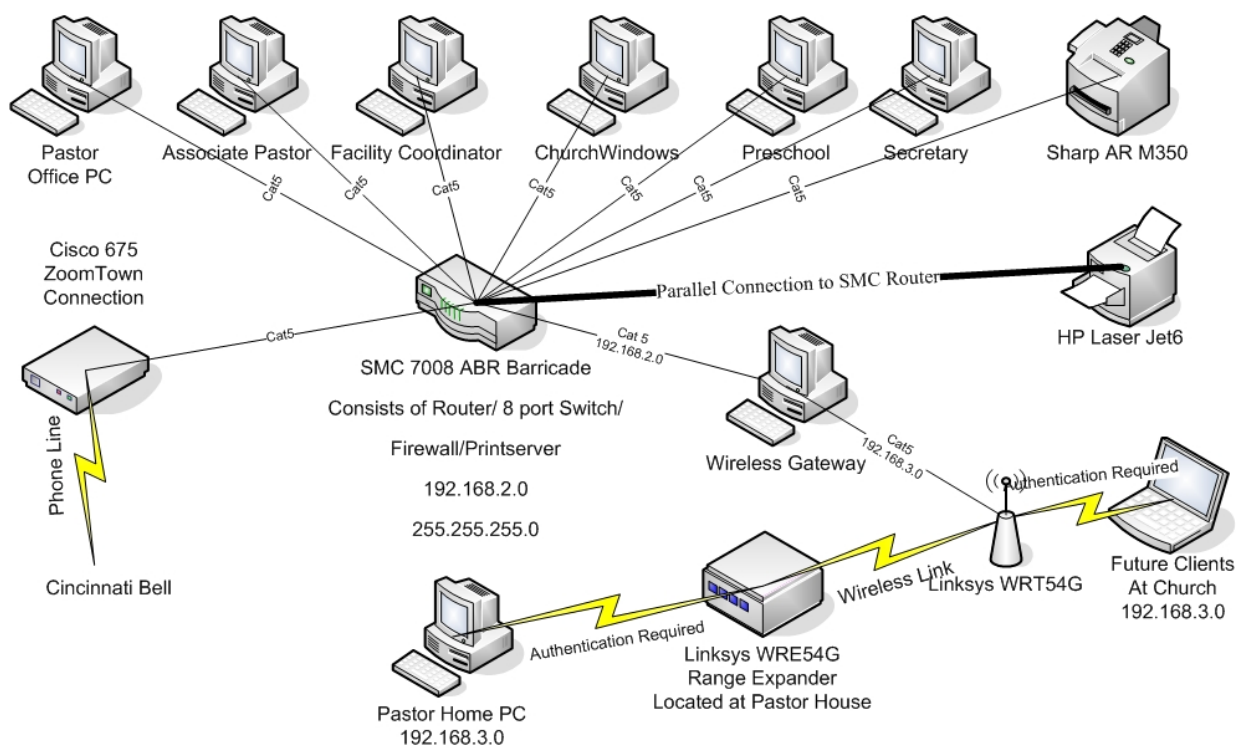
3.2 Solution for Transparent Wireless Network Authentication

My proposed solution was to implement a new wireless network along with a wireless gateway that would separate the main wired network and the wireless network. Initially, I planned on using a Linksys Wireless Access Point; but the Linksys Wireless Router was the same price so it was used. In addition, by doing this it gave the church future expandability. Additional access points can be connected via that router. The wireless network also consists of a Linksys PCMCIA card and Linksys USB Wireless Card. The USB wireless card was chosen so that it could be easily installed on the pastors' home desktop. If or when the pastor transfers to another church it could then be easily removed.

To prevent access to wireless computers all church computers are secured with their own personal firewall software. The gateway has two network cards one connected to each network. This gateway forces an authentication on the wireless network to gain access to the wired network and Internet. The gateway runs on Mandrake, a distribution of a Linux. Due to Linux's General Public License (GPL) agreement and low system requirements, this kept the cost low. MySQL and a authentication software called NoCatAuth are used. Both of these are also under the GPL agreement.

NoCatAuth is the software that provides the authentication and gateway services. Other services that are required on the Linux system are Apache, DHCP, DNS, Pearl, IPTables, GNU Privacy Guard, and Net Mask.

Below in figure 2 is a diagram of the current network, now that the project is implemented. The added pieces are the wireless gateway, the wireless router, and the two computers attached to the wireless network.



Current Network Structure

Figure 2: Current Network Infrastructure

The gateway required two network cards as mentioned before, one connected to each network. On the client side, wireless clients will associate with the access point encryption free. Then the user will open a browser window in which they will be automatically redirected to the login page. The user will then login to the system. Back on the server side it takes the login criteria and verifies it. Then depending on their user class Public, or Owner they will be allowed access to their specific material. The server will alter the IP tables to allow passage of that user for only their specified ports for that user class. As long as the user keeps the NoCat Agent window open they will remain online. As soon as they are out of the access point range, or have closed the window they are logged off.

3.3 User Profiles

The intended users for this system are the church staff, parishioners, and any guests that have church business. Most of the users have a basic understanding of computers. They know how to use the Microsoft Office and the Internet, but do not have an understanding of networking.

3.3.1 Guest User

There is two different user groups. One is the guest group that has access to ports 80, 443, 21, 23. They are allowed access to the Internet only. User names are created as requests are made to the church for required access. The UserID and password is in the following formats, for the user id it is first initial last name. For the password it is the current month and four-digit year. The user has only have access for the date they request. The account is then deleted the next morning.

3.3.2 Owner User

The other group, is the owner group that has full access to all ports and the wired computers on the network. Each person, on staff that needs access has his or her own user account and password. The user ids for owner accounts are for consistency, their Church AOL email addresses and passwords. These accounts will stay active on the system as long as that person is a staff member or requires access.

3.3.3 User Administration:

If there is a need to check the current status of the NoCat system the staff can navigate to the following URL <http://cheviotwireless:5028/status> or use the shortcut on their desktop. The user is presented with the screen shown in Figure 3. This page tells who is logged in to the system and for how long. It also gives some general information on the NoCat configuration.

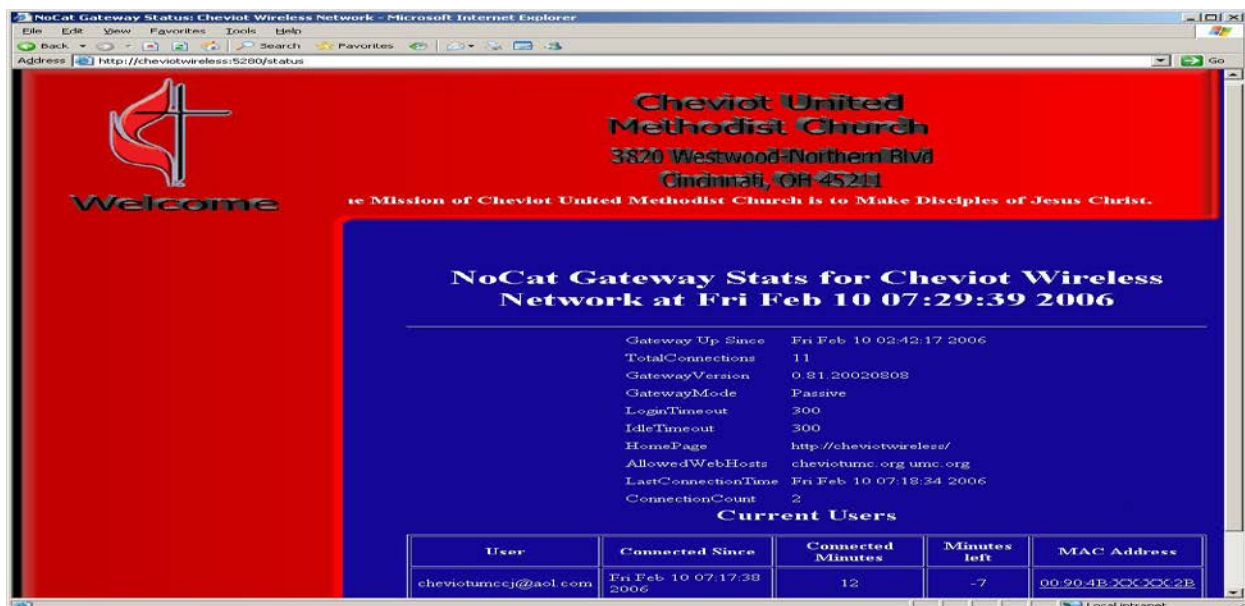


Figure 3: Current NoCat System Status

3.3.3.1 Webmin Administration

In order to make adding and removing users easier, a web interface called Webmin was implemented. This allows the staff to add, remove, and change users from a web interface instead of using complex Linux commands. There is a shortcut on their desktop that they can click on to get to this site. In addition one can view the site from the following URL <https://cheviotwireless/10000>. Figure 4 shows the login screen that the staff receives to enter the administration portion of the system.

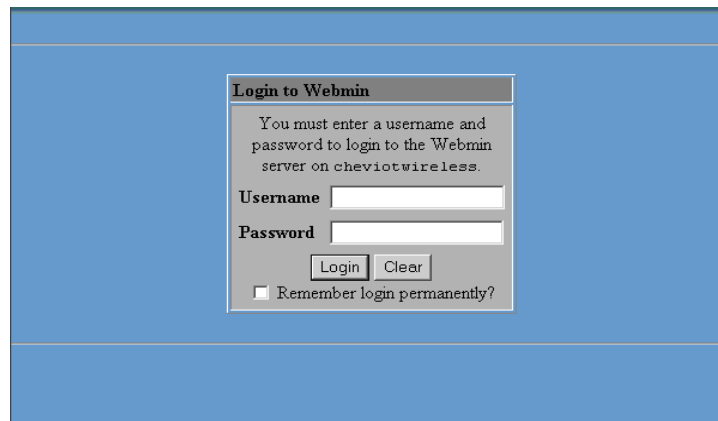


Figure 4: Webmin Logon Screen

After a successful login the user is presented with the screen shown in Figure 5. This is where they can add, change, and remove users. To add a user one would click “add user” then fill in the fields. If they wish to modify a user they would click on the user name and have the option to modify information or delete the account. This makes it much easier than trying to teach them Linux commands to do the same thing. This application is accessible from any of the wired computers. Wireless users are not able to access this site.

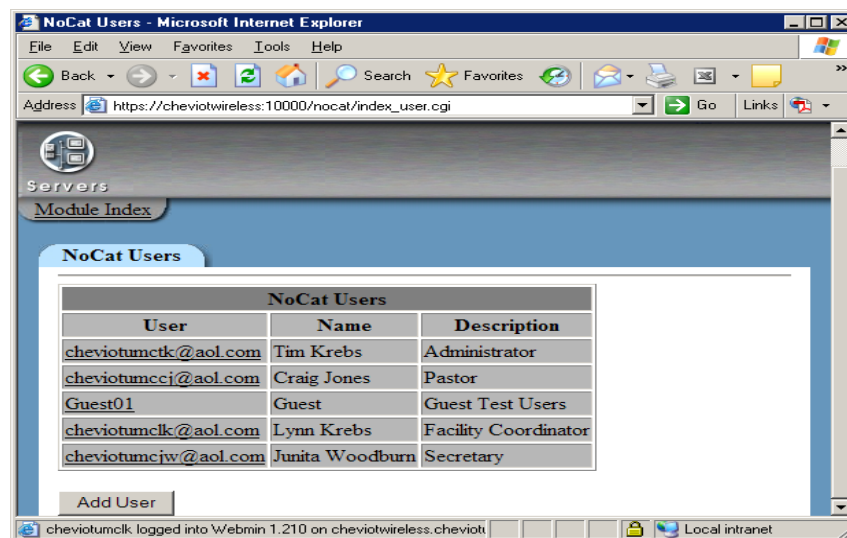


Figure 5: User Modification Screen

3.4 Design Protocols

Included, is one primary user interface that is used by everyone. In addition to that, there is a management interface for users to be added and removed easily as discussed above. If the user is running Windows Xp/SP2 there is no user setup. The only thing to check, is that the computer’s wireless card is associated to “CheviotUMC” Wireless Network. When associated with the access point, the user uses a web browser to access the network. In Figure 6 is an image

of what a user sees while trying to access the Internet via a web browser. The browser is automatically redirected to the page shown in Figure 6.

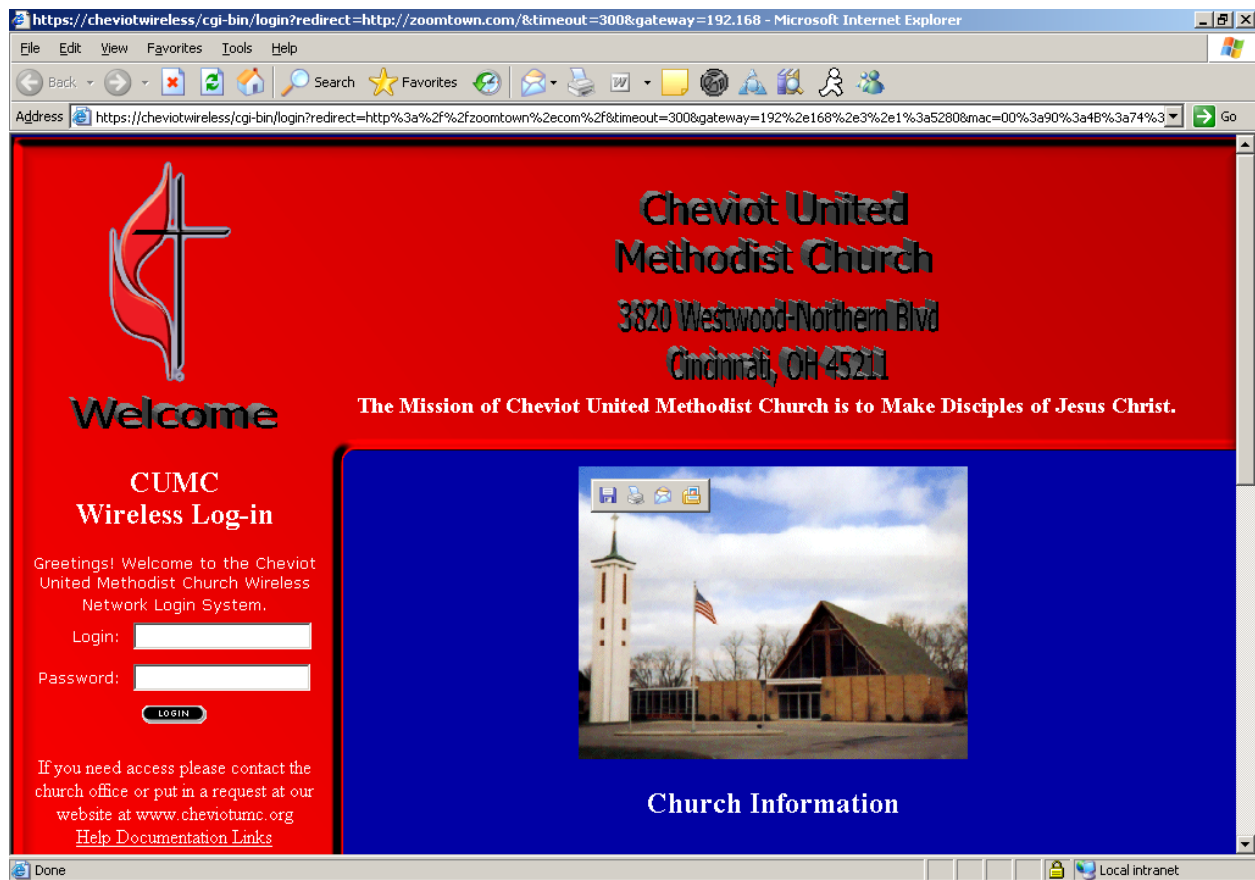


Figure 6: Login Page for Access to Wireless Network

In addition to the login, this page contains links to the Cheviot United Methodist Church website and the official United Methodist Church organization homepage. Users are able to access these sites without logging into the system. If users try to leave these sites they are redirected to the login page. These are the only two sites accessible at this time. There is the possibility, that in the future, additional sites will be added to this allowed list.

Figure 7 shows what the users sees when they enter a valid user name and password. From this page the larger window redirects users to their original web page requested. Otherwise, the system displays an error message that the login is invalid.

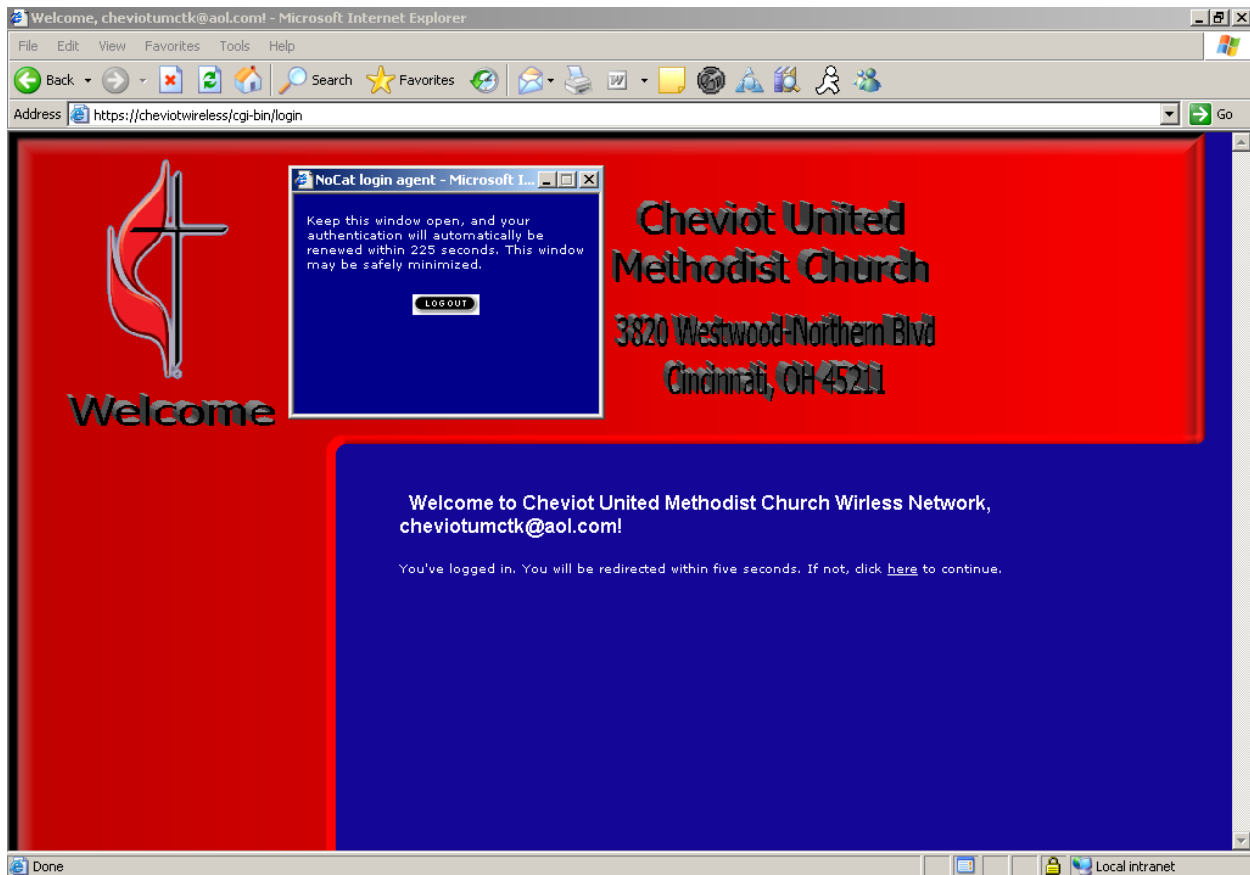


Figure 7: Successful NoCat Logon

The NoCat login agent window, shown in Figure 8, must stay open at all times while using the wireless connection; it can however be minimized. The NoCat login agent window shows a refresh time. This is how often the NoCat system validates to see if a user is still logged in. If the window is closed and that time expires, that user is automatically logged out of the

system. If a user closes this window while surfing and time expires, the user is prompted to re-authenticate. Otherwise, if the window is left open the login is extended.

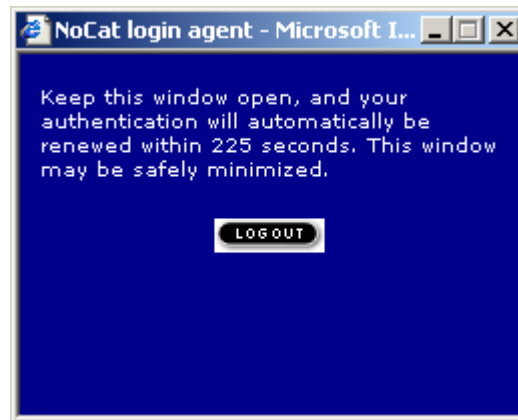


Figure 8: NoCat Login Agent Window

When the user is ready to log out they maximize the NoCat login agent and click logoff. Once logoff is clicked they see the window shown below in figure 9.

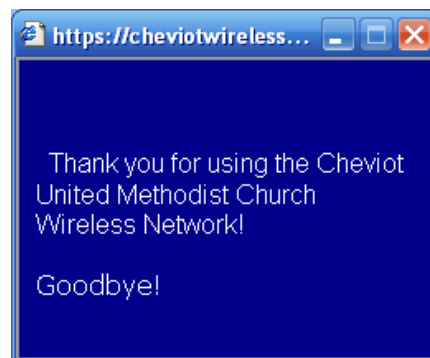


Figure 9: NoCat Login Agent Logged Out Window

There is also user documentation that has been created as part of the project. (see sample in Figure 10 and for full versions see Appendix E), both for the administration and usage of this

system. Some user training has taken place. Below are a few screen shots of some of the user documentation that was used for the training. Users that request access to the system are e-mailed documentation on how to establish the initial connection to the system.

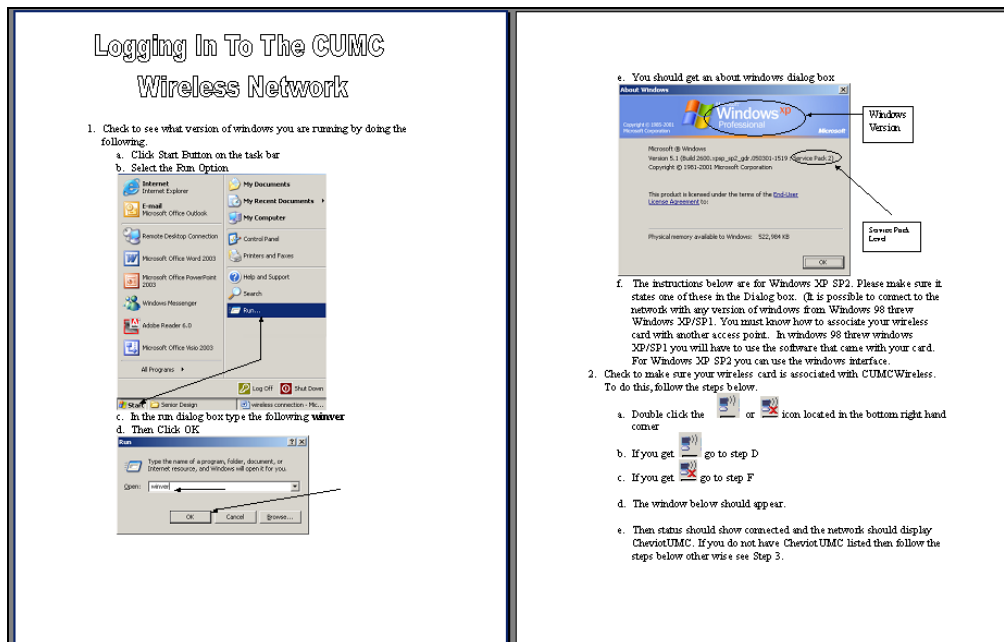


Figure 10: Snapshot of User Documentation

Previously, the login page was very bland and basic. Changes have been made to give it a cleaner and consistent look (see Figure 11 for comparison). Non-dated material was added about the church. This gives users that stumble upon the access point or known users some information on the church and free access to the church's official web page. Also added to these pages are links to the user documentation. Since all users do not have Microsoft Word, documents have been converted to Adobe PDF documents. In addition, there is a link to a copy of Adobe Acrobat Reader, which is locally stored on the machine.

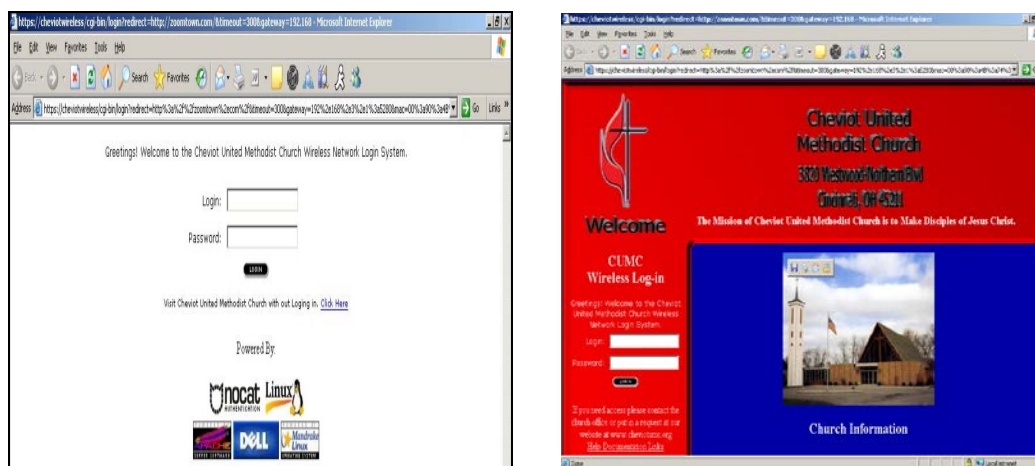


Figure 11: Comparisons of Original and New Sites

4. Deliverables

The following items are the deliverables and are completed.

Overall:

- A working wireless gateway that runs on Linux
- The users will be able to easily login and connect to required resources.
- There is no setup on the client guest machines to connect if they are running XP/SP2. If they are running this version they will be able to view the network and click “connect.”

Otherwise a connection to the access point will need to be setup first based on wireless card manufacture.

- Quick set of instructions for XP/SP2 users.
- The gateway is able to handle two types of users. A guest has access to the Internet only. Staff has access to the wired network computers and the Internet.

Pastor:

- The pastor has full network access from his home computer to the Internet and church network.
- The pastor's computer is able to retrieve software and antivirus updates.
- The pastor is able to remote desktop to his work machine from home.
- The pastor's computer is secure from rogue wireless connections on the network.
- The Pastor has directions on how to utilize these resources.

Secretary:

- The secretary's laptop has full access to the network as well as the Internet.
- The secretary's laptop has shortcuts setup to be able to easily move files from laptop to her desktop.
- The secretary's laptop is able to print to both printers.
- The secretary's laptop computer is secure from rogue wireless connections on the network.

5. Project Development

5.1 Project Timeline

Task	Start Date	End Date	Status
Senior Design 1	01/04/2005	03/08/2005	Completed
Project Research	01/04/2005	Mon 2/28/05	Completed
Progress Report 1	01/18/2005	Tue 1/25/05	Completed
Problem/Need Area of Inquiry	02/01/2005	Tue 2/8/05	Completed
Progress Report 2	02/15/2005	Fri 2/25/05	Completed
1st Proposal Draft	02/15/2005	Mon 2/21/05	Completed
Final Proposal	02/21/2005	Mon 2/28/05	Completed
Create PowerPoint Proposal	02/25/2005	Fri 3/4/05	Completed
Present Proposal	03/08/2005	03/08/2005	Completed
Read up on NoCatAuthenticataion	04/04/2005	04/12/2005	Completed
Install and Setup Stable Linux Enviornment	04/20/2005	05/01/2005	Completed
Senior Design 2	06/20/2005	08/22/2005	Completed
Experiment with Wirless Range.	06/20/2005	06/22/2005	Completed
Setup and Install Software Requirement for Gateway	06/20/2005	07/20/2005	Completed
Purchase Wireless Hardware	06/22/2005	06/23/2005	Completed
Setup Prottype Environment at home	06/23/2005	06/24/2005	Completed
Configure Linux Gateway	07/01/2005	07/31/2005	Completed
Start System Testing for Prottype	07/01/2005	07/31/2005	Completed
Progress Report 1	07/01/2005	07/11/2005	Completed
Draft of Project Description and Intended Use	07/01/2005	07/11/2005	Completed
Draft of Design Freeze	07/01/2005	07/25/2005	Completed
Progress Report 2	07/25/2005	08/01/2005	Completed
Create PowerPoint Presentation	08/01/2005	08/22/2005	Completed
Present Freeze	08/15/2005	08/22/2005	Completed
Senior Design 3	01/03/2006	03/13/2006	Completed
Create Greeting Page with Brief Information on Church	12/10/2005	12/11/2005	Completed
Configure Church Machine Firewalls	01/13/2006	01/13/2006	Completed
Progress Report 1	01/18/2006	01/18/2006	Completed
Cleanup Interface as Needed	12/10/2005	12/11/2005	Completed
Move from Prototpye Location to Permanent Location	01/20/2006	01/20/2006	Completed
1st Draft	02/10/2006	02/10/2006	Completed
Setup Advisor Appointment to View Network	02/18/2006	02/18/2006	Completed
Progress Report 2	02/18/2006	02/18/2006	Completed
Present Project	02/27/06	02/27/2006	Completed
Poster Board	02/18/2006	02/19/2006	Completed
Final Documentation	01/03/2006	02/25/2006	Completed

Figure 12: Time Line

5.2 Project Budget

All funding for this project was through the church's office software and hardware budget. Due to range limitations of the current wireless technology a range expander was needed. This was not accounted for in the initial phase but was accounted for in the design freeze. With

just the access point I was able to get a signal up to front of the pastor's house. With the extender placed on the wall inside the house full coverage was possible.

During the course of the project there was also the change of Linux distributions from Fedora Core 3 to Mandrake 9.0, which also took place prior to the design freeze. This was due to difficulties that configuring the gateway on Fedora Core 3. Due to the nature of Linux, there were many different versions of software available. The software that runs on Fedora Core 3 was not compatible with the NoCat software. By moving to Mandrake 9.0, configuration of the gateway was possible. Webmin was added to the software list. It will make maintenance and user configuration on the gateway easier for non-Linux users. Samba was also added strictly for implementing a NetBIOS. This allows a name to be used instead of an IP address. All of these additions and changes took place prior or during the design freeze.

Hardware	Description	Reason	Typical Cost	My Cost
Desktop PC	Dell GX110 P3 850	Donated	\$500.00	\$0.00
Linsys Wireless Router 54G	WRT54G	Retail Cost	\$79.00	\$79.99
Linsys USB Adapter	WUSB54G To be used in pastor's home machine	Retail Cost	\$59.99	\$59.99
Linsys Extender	WRE54G Extend Range to pastor's house	Retail Cost	\$79.00	\$79.00
CAT5	100ft from router to AP	Retail Cost	\$60.00	\$60.00
Test Client	Dell D600 use as outside client	Using Personal PC	\$0.00	\$0.00
Total			\$777.99	\$278.98
Software	Description	Reason	Typical Cost	My Cost
Mandrake 9.1	OS for Gateway	GPL agreement	0	\$0.00
NoCat 0.81	Gateway software	GPL agreement	0	\$0.00
MySql 3.32.52	Holds User database	GPL agreement	0	\$0.00
GNU Privacy Guard 1.0.7	Sign information between gateway and authserver	GPL agreement	0	\$0.00
Perl 5.8.0	Runs NoCat scripts	GPL agreement	0	\$0.00
Ethereal	Inspect packets	GPL agreement	0	\$0.00
Apache 1.3.26	Host NoCat login page	GPL agreement	0	\$0.00
Webmin 1.210	Manage system settings	GPL agreement	0	\$0.00
Samba 2.2.62	Used for netbios name	GPL agreement	0	\$0.00
Personal Firewall/Antivirus	Norton Personal Firewall/Norton Security	Both systems already have	\$50.00 *2	\$0.00
Total			\$100.00	\$0.00
Grand Total			\$877.99	\$278.98

Figure 13: Budget

5.3 Hardware and Software Requirements

5.3.1 Hardware

- Desktop Computer
 - System requirements
 - PC 486 processor or better
 - Two network interface cards (NICs); one for connecting to the AP, the other to connect to your outside network.
 - A hard disk with at least 10GB
 - 256Mb of RAM
 - System: To be donated from SYSCO Food Services of Cincinnati LLC
 - Planned system specs
 - Dell GX110 P3 667mhz
 - 256MB of RAM
 - 1 integrated 3c905b NIC
 - 2nd card will be donated by myself
 - Realtek RTL8029AS
 - Intel 810 Video card
 - 10GB hard drive

Linux does not need a powerful machine to operate that is the reason for the lower system requirements.

- Linksys Wireless Router 54mb
 - WRT54G
- Linksys USB Wireless Network Adapter
 - WUSB54G
 - If the pastor ever moves to another church or replaces the pc the adapter can be easily moved
 - Linksys was chosen because they are more of a mainstream name. In addition, it was one of the few companies that offered a range expander
- CAT 5e
 - To connect the Gateway computer to the SMC Router; and to connect the Linksys access point to the gateway desktop
- Client Test PC
 - Was my personal laptop
 - To use as a test machine for packet sniffing or network testing

5.3.2 Software

- Mandrake 9
 - For the operating system on the wireless gateway machine
- NoCatAuth
 - For gateway/authentication of wireless clients
- MySQL
 - To store user information for authentication
- Apache Web Server
 - To host the login webpage for NoCatAuth.
- GNU Privacy Guard and Net Mask
 - For security between the authentication software and the Gateway software.
- Pearl language
 - To run NoCatAuth Software.
- Ethereal Network Sniffer Software
 - For network packet testing.
- Norton Personal Firewall
 - For protecting Church PC's on wireless network.
- Webmin
 - Graphical user interface for user configuration and maintenance
- Samba
 - User for NetBIOS name resolution

These specific pieces of software were chosen because they were required for the authentication gateway to operate. In addition, these were selected to minimize the cost to the church.

6 Proof of Design

The deliverables for this project have been met by executing the following.

6.1 Overall

These are the primary deliverables:

- A working wireless gateway that operates on Linux

- o A Dell GX110 was setup with Mandrake Linux 9. The Linux box has two network cards in it. One card is connected to the wired network with an IP address in the 192.168.2.0 network. The other card was connected to the wireless network with an IP address of 192.168.3.1. DHCP on the Linux machine then issues IP to wireless clients.
- There is no setup on the client guest machines to connect if they are running XP/SP2. If they are running this version they are able to view network and click “connect.” Otherwise a connection to the access point needs to be setup first, based on wireless card manufacture.
 - o Users that have a Windows XP machine can easily connect to the network. The access point is broadcasting the SSID and has no encryption. By doing this there is no need to contend with finding the hidden SSID or guess whether or not the encryption key is typed correctly. This allows users to use “view available wireless network” features of Windows XP.
- The users are able to easily login and connect to required resources.
 - o The login is via a web page. Users that open a browser window are automatically directed to it. Since this happens there is no need to type or guess the URL. The user then enters a user id and password. If they enter a valid id and password they are redirected to the original requested web page.
- Quick set of instructions for XP/SP2 users.
 - o A set of user instructions has been created to help users that have never connected to a wireless access point before. This documentation has been created in Adobe PDF and Microsoft Word formats. In addition, there is a documents link on the login page for any additional help that might be needed. The documentation is very detailed and contains many screen shots so that users can walk through visually as well.
- The gateway is able to support two types of users. Guests have access to the Internet only. Staff have access to the wired network computers and the Internet.
 - o The owners group has all the staff members added to it. This group allows access to all resources on the network. The only way to add to this group is to modify the

nocat.conf file. This prevents users from being accidentally added to this group.

All other users are added as guest users. NoCat has been setup only to allow access to ports 21 80 443 and 53 to guest users. This prevents guests from accessing file shares, printers and other network resources.

6.2 Pastor:

The next grouping of deliverables is for the pastor's system.

- The pastor has full network access from his home computer to the Internet and church network.
 - The pastor has access to the wireless network from his home. A USB wireless card is installed on his system along with a wireless network range expander in the home. This allows the pastor to connect to the Linux Gateway to utilize church resources. The pastor is setup as a user in the owners group. By being in the owners group full access is given to the network. In addition, the church's printers are installed on his machine so that he may print at the church from his home.
- The pastor's computer is able to retrieve software and antivirus updates.
 - Since this system has access to a high-speed internet connection it is able to retrieve and install both windows and antivirus updates. This is also accomplished much faster and more often with the high-speed connection versus the dial up connection that was used.
- The pastor is able to remote desktop to his work machine from home.
 - Shortcuts are available on the desktop to connect to his work machine. Since there is now a network in place between his home and the church he is able to do this. In addition, documentation is available to explain how to use the remote desktop feature..
- The pastor's computer is secure from rogue wireless connections on the network.
 - The pastor's machine has both anti virus and firewall software. The firewall is modified to allow communications from the wired church network and the Linux

gateway only. In addition, the access point is setup in isolation mode causing each wireless connected client to be isolated from another.

- Directions on how to utilize these resources.
 - Documentation was created on how to use the remote desktop feature. In addition, a personal training session was presented to the pastor.

6.3 Secretary:

The next grouping of deliverables is for the laptop that the Secretary will use.

- The secretary's laptop has full access to the network as well as the Internet.
 - The secretary is setup as a user in the owners group. By being in the owners group full access is given to the network. In addition, a shortcut to a batch file is on the desktop, to map drives that she might need.
- The secretary's laptop has shortcuts setup for easy transfer of files from her laptop to her desktop.
 - A shortcut is in place on her laptop to the secretary's documents folder on her desktop machine.
- The secretary's laptop is able to print to both printers.
 - The church's printers are installed on the machine so that she may print to either printer. She was also informed that she must be logged into the gateway in order to use the printers.
- The secretary's laptop computer is secure from rogue wireless connections on the network.
 - The laptop has both anti virus and firewall. The firewall is modified to allow communications from the wired church network and the Linux gateway only. In addition, the access point is setup in isolation mode causing each wireless connected client to be isolated from another.

7 Conclusion and Final Additions

By implementing this wireless network and gateway; staff and guests can utilize church and Internet resources with ease. By using Linux and open source software, the budget was kept at a reasonable level. The only cost that the church incurred was the cost for the wireless devices and the cabling to setup the wireless infrastructure.

There were several primary deliverables. One, it is that it provides a fully implemented wireless infrastructure. Secondly, it has an easy to use interface with two access levels. Third, it allows the pastor access to the church network and resources along with user documentation. Finally, it is setup for the secretary's laptop so that she may print off minutes and move files to her desktop system. The solutions that were implemented met all theses deliverables. An addition to the project was the web administration interface that was not part of the original design. That implementation allows the staff to more easily add and remove users.

There were two additional components that were added near the end of the project. For much of 2005 the access point was connected to an extension cord that ran down the length of the suspend ceiling to an outlet. That was recently replaced with a Power Over the Ethernet solution, because of that the extension cord is no longer needed. In addition, high gain antennas were added to the access point. They will improve the signal strength and bandwidth between the range expander and the access point. The end result of this project is a long lasting expandable solution that the church may use for years to come.

Appendix A.

NoCatAuth Configuration File

```
##### Gateway application settings.
#
# GatewayName -- The name of this gateway, to be optionally displayed
# on the splash and status pages. Any short string of text will do.
#
GatewayName    Cheviot Wireless Network

##
#
# GatewayMode -- Determines the mode of operation of the gateway. Possible
# values are:
#
# Captive    - Allow authentication against an auth service. LEGACY.
# Passive    - Like Captive, but YOU MUST USE THIS if your gateway
#              is behind a NAT. Will work anyway if not. *RECOMMENDED*.
# Open       - Simply require a user to view a splash page and accept
#              a use agreement.
#
# If Captive or Passive Mode is set, you will need to have values set for
# AuthServiceAddr, AuthServiceURL, and LogoutURL. You will want to leave a
# short value for LoginTimeout (probably <600).
#
#
# If Open Mode is set, you will need to have values set for SplashForm,
# HomePage, and possibly DocumentRoot (or provide an absolute path for
# SplashForm). Also, you will want to set a large value for LoginTimeout
# (probably >3600).
#
GatewayMode    Passive

##
# LoginTimeout - Number of seconds after a client's last
# login/renewal to terminate their connection. Probably
# don't want to set this to less than 60 or a lot of
# bandwidth is likely to get consumed by the client's
# renewal attempts. Defaults to 300 seconds.
#
# For Captive Mode, you want to set this to something
# fairly short (like 10 minutes) to prevent connection
# spoofing.
#
LoginTimeout   300
```

```

##### Active/Passive Portal settings.
#
##
# TrustedGroups - A list of groups registered with the auth server
# that a user may claim membership in order to gain Member-class
# access through this portal. The default magic value "Any" indicates
# that a member of *any* group is granted member-class access from
# this gateway.
#
# TrustedGroups NoCat NYCWireless PersonalTelco
#
TrustedGroups Any
##
# Owners - Optional. List all local "owner" class users here, separated
# by spaces. Owners typically get full bandwidth, and unrestricted
# access to all network resources.
#
# Owners rob@nocat.net schuyler@nocat.net
Owners cheviotumctk@aol.com cheviotumccj@aol.com cheviotumclk@aol.com
cheviotumcjw@aol.com cheviotumc3820@aol.com

##
# AuthServiceAddr - Required, for captive mode. Must be set to the address of
# your authentication service. You must use an IP address
# if DNS resolution isn't available at gateway startup.
#
# AuthServiceAddr 208.201.239.21
#
AuthServiceAddr 192.168.3.1

##
# AuthServiceURL - HTTPS URL to the login script at the authservice.
#
AuthServiceURL https://cheviotwireless/cgi-bin/login

##
# LogoutURL - HTTP URL to redirect user after logout.
#
LogoutURL https://cheviotwireless/logout.html

#### Network Topology
#
# ExternalDevice - Required if and only if NoCatAuth can't figure it out
# from looking at your routing tables and picking the interface

```

```

# that carries the default route. Must be set to the interface
# connected to the Internet. Usually 'eth0' or 'eth1'
# under Linux, or maybe even 'ppp0' if you're running
# PPP or PPPoE.
#
ExternalDevice eth0

##
# InternalDevice - Required if and only if you have ethernet devices
# on your gateway besides your wireless device and your 'Net connection.
# Must be set to the interface connected to your local network, normally
# your wireless card. In Linux, some wireless devices are named 'wvlan0'
# or 'wlan0' rather than 'ethX'.
#
InternalDevice eth1

##
# LocalNetwork - Required if and only if NoCatAuth can't figure out
# the network address of your local (probably wireless) network,
# given your InternalDevice(s). Must be set to the network
# address and net mask of your internal network. You
# can use the number of bits in the netmask (e.g. /16, /24, etc.)
# or the full x.x.x.x specification.
#
LocalNetwork 192.168.3.0/24

##
# DNSAddr - Optional. *If* you choose not to run DNS on your internal network,
# specify the address(es) of one or more domain name server on the Internet
# that wireless clients can use to get out. Should be the same DNS that your
# DHCP server hands out. If left blank, NoCatAuth will presume that you
# want to use whatever nameservers are listed in /etc/resolv.conf.
#
DNSAddr 192.168.2.2

##
# AllowedWebHosts - Optional. List any domains that you would like to
# allow web access (TCP port 80 and 443) BEFORE logging in (this is the
# pre-'skip' stage, so be careful about what you allow.)
#
# AllowedWebHosts nocat.net
AllowedWebHosts www.cheviotumc.org umc.org

##
# IncludePorts - Optional. Specify TCP ports to allow access to when
# public class users login. All others will be denied.

```

```

#
# For a list of common services and their respective port numbers, see
# your /etc/services file. Depending on your firewall, you might even
# be able to specify said services here, instead of using port numbers.
#
IncludePorts 21 80 443 53

### Fin!

##### authserv.conf -- NoCatAuth Authentication Service Configuration.
#
# Format of this file is: <Directive> <Value>, one per
# line. Trailing and leading whitespace is ignored. Any
# line beginning with a punctuation character is assumed to
# be a comment.

##### Authservice-specific settings.
#
# HomePage -- The authservice's notion of a default
# redirect.
#
HomePage http://cheviotwireless/

# DocumentRoot -- Where all of the application templates (including
# SplashPage) are hiding. Can be different from Apache's DocumentRoot.
#
DocumentRoot /usr/local/nocat/htdocs

##### Authservice authentication source.
#
# DataSource -- specifies what to authenticate against.
# Possible values are DBI, Passwd, LDAP, RADIUS, PAM, Samba, IMAP, NIS.
#
DataSource DBI

##
# Auth service database settings.
#
# If you select DataSource DBI, then Database, DB_User, and DB_Password
# are required.
#
# Database is a DBI-style data source specification.
#
# For postgres support:
# Database dbi:Pg:dbname=nocat
#

```

```

# For mysql support:
Database      dbi:mysql:database=nocat
DB_User       nocat
DB_Passwd     *****

##### Auth service user table settings.
#
# UserTable names the table containing the user ID data.
#
# UserIDField names the column containing the ID that the
#   client uses to uniquely identifying themselves, i.e. their
#   e-mail address or username.
#
# UserPasswdField stores the user's MD5-hashed password.
#
# UserAuthField is deprecated and will go away.
#
UserTable     member
UserIDField   login
UserPasswdField pass
UserAuthField status
UserStampField created

GroupTable    network
GroupIDField  network
GroupAdminField admin

##### Auth service web application settings.
#
# MinPasswdLength -- Enforced minimum user password length.
#   Not much other checking is done on the user's p/w.
#
MinPasswdLength 6

# LocalGateway -- If you run auth service on the same subnet
#   (or host) as the gateway you need to specify the hostname
#   of the gateway. Otherwise omit it. (Requires Net::Netmask)
#
LocalGateway 192.168.3.1

##### Fin.

```

Appendix B.

Apache Configuration File

```
NameVirtualHost *
<VirtualHost 192.168.3.1:443>
  DocumentRoot /usr/local/nocat/htdocs
  # ServerName localhost:443
  # ServerAdmin root@localhost
  SSLEngine On
  SSLCertificateFile /etc/ssl/apache/server.crt
  SSLCertificateKeyFile /etc/ssl/apache/server.key
  Options FollowSymLinks Includes Indexes MultiViews
  ScriptAlias /cgi-bin/ /usr/local/nocat/cgi-bin/
  <Directory "/usr/local/nocat/htdocs">
    AllowOverride All
    Options FollowSymLinks Includes Indexes MultiViews
    <Limit GET POST OPTIONS PROPFIND>
      Order allow,deny
      Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS PROPFIND>
      Order deny,allow
      Deny from all
    </LimitExcept>
  </Directory>
  <Directory "/usr/local/nocat/cgi-bin">
    AllowOverride All
    Options ExecCGI
    <IfModule mod_access.c>
      Order allow,deny
      Allow from all
    </IfModule>
    #
    # $PERL5LIB tells Perl where to find the NoCat libraries.
    SetEnv PERL5LIB /usr/local/nocat/lib
    #
    # $NOCAT tells NoCat where to find its configuration file.
    SetEnv NOCAT /usr/local/nocat/nocat.conf
    SSLOptions +StdEnvVars
  </Directory>
  <IfModule mod_setenvif.c>
    SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown \
      downgrade-1.0 force-response-1.0
  </IfModule>
  <IfModule mod_rewrite.c>
```

```

RewriteEngine On
RewriteOptions inherit
</IfModule>
</VirtualHost>
Include conf/addon-modules/php.conf
Include conf/ssl/mod_ssl.conf
Include conf/ssl/ssl.default-vhost.conf

```

Appendix C.

MySQL Tables

```
mysql> desc member;
```

Field	Type	Null	Key	Default	Extra
url	varchar(255)	YES		NULL	
description	text	YES		NULL	
created	datetime	YES		NULL	
modified	timestamp(14)	YES		NULL	
status	tinyint(3) unsigned	YES		NULL	
login	varchar(250)		PRI		
pass	varchar(255)				
name	varchar(255)	YES		NULL	

8 rows in set (0.00 sec)

url	description	created	modified	status	login	pass
	Administrator	2005-06-22 05:19:06	20060130035252	0	cheviotumctk@aol.com	uwGTdQJfwAKaOb3
	Pastor	2005-06-22 05:19:54	20060210044857	0	cheviotumccj@aol.com	bmTyLZUE9CUiAOK
	Guest Test Users	2006-01-30 03:52:41	20060130035241	0	Guest01	PJQwFs9x15X3Qfc
	Facility Coordinator	2006-02-10 04:49:26	20060210044926	0	cheviotumclk@aol.com	XlrPvt0ey51TKBr
	Secretary	2006-02-10 04:49:56	20060210044956	0	cheviotumcjw@aol.com	aP0EwDQjJNFP36e
	Account For Contemporary Worship	2006-02-13 07:15:53	20060217065023	0	cheviotumc3820@aol.com	510RsNJ/RRiSwuk

Appendix D. Packet Captures

Redirect Capture

	A	B	C	D
1	Source	Destination	Port	Info
2	"192.168.3.99"	"216.68.4.69"	"TCP"	"3521 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260"
3	"216.68.4.69"	"192.168.3.99"	"TCP"	"http > 3521 [SYN
4	"192.168.3.99"	"216.68.4.69"	"TCP"	"3521 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0"
5	"192.168.3.99"	"216.68.4.69"	"HTTP"	"GET / HTTP/1.1"
6	"216.68.4.69"	"192.168.3.99"	"TCP"	"http > 3521 [ACK] Seq=1 Ack=274 Win=6432 Len=0"
7	"216.68.4.69"	"192.168.3.99"	"HTTP"	"HTTP/1.1 302 Moved"
8	"192.168.3.99"	"216.68.4.69"	"TCP"	"3521 > http [FIN
9	"216.68.4.69"	"192.168.3.99"	"TCP"	"http > 3521 [FIN
10	"192.168.3.99"	"216.68.4.69"	"TCP"	"3521 > http [ACK] Seq=275 Ack=568 Win=17074 Len=0"
11	"192.168.3.99"	"216.68.4.69"	"TCP"	"3527 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260"
12	"216.68.4.69"	"192.168.3.99"	"TCP"	"http > 3527 [SYN
13	"192.168.3.99"	"216.68.4.69"	"TCP"	"3527 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0"
14	"192.168.3.99"	"216.68.4.69"	"HTTP"	"GET / HTTP/1.1"
15	"216.68.4.69"	"192.168.3.99"	"HTTP"	"HTTP/1.1 301 Moved Permanently (text/html)"
16	"192.168.3.99"	"216.68.4.69"	"TCP"	"3527 > http [ACK] Seq=435 Ack=599 Win=17042 Len=0"
17	"192.168.3.99"	"208.197.227.117"	"TCP"	"3529 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260"
18	"208.197.227.117"	"192.168.3.99"	"TCP"	"http > 3529 [SYN
19	"192.168.3.99"	"208.197.227.117"	"TCP"	"3529 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0"
20	"192.168.3.99"	"208.197.227.117"	"HTTP"	"GET / HTTP/1.1"
21	"208.197.227.117"	"192.168.3.99"	"TCP"	"http > 3529 [ACK] Seq=1 Ack=445 Win=6432 Len=0"
22	"208.197.227.117"	"192.168.3.99"	"HTTP"	"HTTP/1.1 302 Found"
23	"192.168.3.99"	"208.197.227.117"	"TCP"	"3529 > http [ACK] Seq=445 Ack=301 Win=17340 Len=0"
24	"192.168.3.99"	"208.197.227.117"	"HTTP"	"GET /index.php HTTP/1.1"

SSL Packet Capture

	C	D	E	F
1	Source	Destination	Port	Info
2	"192.168.3.99"	"192.168.3.1"	"TCP"	"3522 > https [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260"
3	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 3522 [SYN
4	"192.168.3.99"	"192.168.3.1"	"TCP"	"3522 > https [ACK] Seq=1 Ack=1 Win=17640 Len=0"
5	"192.168.3.99"	"192.168.3.1"	"SSLv2"	"Client Hello"
6	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 3522 [ACK] Seq=1 Ack=79 Win=5840 Len=0"
7	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Server Hello"
8	"192.168.3.99"	"192.168.3.1"	"SSLv3"	"Client Key Exchange"
9	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Change Cipher Spec"
10	"192.168.3.99"	"192.168.3.1"	"TCP"	"3522 > https [ACK] Seq=283 Ack=766 Win=16875 Len=0"
11	"192.168.3.99"	"192.168.3.1"	"SSLv3"	"Application Data"
12	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 3522 [ACK] Seq=766 Ack=705 Win=7504 Len=0"
13	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Application Data"
14	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Continuation Data"
15	"192.168.3.99"	"192.168.3.1"	"TCP"	"3522 > https [ACK] Seq=705 Ack=2810 Win=17640 Len=0"
16	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 3522 [FIN
17	"192.168.3.99"	"192.168.3.1"	"TCP"	"3522 > https [ACK] Seq=705 Ack=2811 Win=17640 Len=0"
18	"192.168.3.99"	"192.168.3.1"	"TCP"	"3522 > https [FIN
19	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 3522 [ACK] Seq=2811 Ack=706 Win=7504 Len=0"
20	"192.168.3.99"	"192.168.3.1"	"TCP"	"3523 > https [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260"
21	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 3523 [SYN
22	"192.168.3.99"	"192.168.3.1"	"TCP"	"3523 > https [ACK] Seq=1 Ack=1 Win=17640 Len=0"

Login Packet Capture from Linux Server

No.	Time	Source	Destination	Protocol	Info
4	"17.172649"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2056 > https [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260"
5	"17.172840"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2056 [SYN]
6	"17.176908"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2056 > https [ACK] Seq=1 Ack=1 Win=17640 Len=0"
7	"17.178790"	"192.168.3.99"	"192.168.3.1"	"SSLv3"	"Client Hello"
8	"17.179016"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2056 [ACK] Seq=1 Ack=103 Win=5840 Len=0"
9	"17.179296"	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Server Hello"
10	"17.203186"	"192.168.3.99"	"192.168.3.1"	"SSLv3"	"Change Cipher Spec"
11	"17.207921"	"192.168.3.99"	"192.168.3.1"	"SSLv3"	"Application Data"
12	"17.208172"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2056 [ACK] Seq=147 Ack=1142 Win=8748 Len=0"
13	"17.936987"	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Application Data"
14	"17.937028"	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Continuation Data"
15	"17.942063"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2056 > https [ACK] Seq=1142 Ack=2667 Win=17640 Len=0"
16	"17.942195"	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Continuation Data"
17	"17.949219"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2056 [FIN]
18	"17.950609"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2056 > https [ACK] Seq=1142 Ack=3009 Win=17299 Len=0"
19	"18.017423"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2056 > https [FIN]
20	"18.017486"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2056 [ACK] Seq=3009 Ack=1143 Win=8748 Len=0"
21	"18.327806"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2057 > https [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260"
22	"18.327943"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2057 [SYN]
23	"18.329286"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2057 > https [ACK] Seq=1 Ack=1 Win=17640 Len=0"
24	"18.330437"	"192.168.3.99"	"192.168.3.1"	"SSLv3"	"Client Hello"
25	"18.330653"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2057 [ACK] Seq=1 Ack=103 Win=5840 Len=0"
26	"18.330930"	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Server Hello"
27	"18.333565"	"192.168.3.99"	"192.168.3.1"	"SSLv3"	"Change Cipher Spec"
28	"18.335748"	"192.168.3.99"	"192.168.3.1"	"SSLv3"	"Application Data"
29	"18.372578"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2057 [ACK] Seq=147 Ack=619 Win=6432 Len=0"
30	"18.924778"	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Application Data"
31	"18.924819"	"192.168.3.1"	"192.168.3.99"	"SSLv3"	"Continuation Data"
32	"18.928251"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2057 > https [ACK] Seq=619 Ack=2033 Win=17640 Len=0"
33	"18.936032"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2057 [FIN]
34	"18.937429"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2057 > https [ACK] Seq=619 Ack=2034 Win=17640 Len=0"
35	"19.037835"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2057 > https [FIN]
36	"19.037906"	"192.168.3.1"	"192.168.3.99"	"TCP"	"https > 2057 [ACK] Seq=2034 Ack=620 Win=6432 Len=0"
37	"22.397273"	"192.168.3.99"	"192.168.2.2"	"NBNS"	"Refresh NB RIKER21LAP<20>"
38	"23.546158"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2058 > 5280 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260"
39	"23.546314"	"192.168.3.1"	"192.168.3.99"	"TCP"	"5280 > 2058 [SYN]
40	"23.547615"	"192.168.3.99"	"192.168.3.1"	"TCP"	"2058 > 5280 [ACK] Seq=1 Ack=1 Win=17640 Len=0"

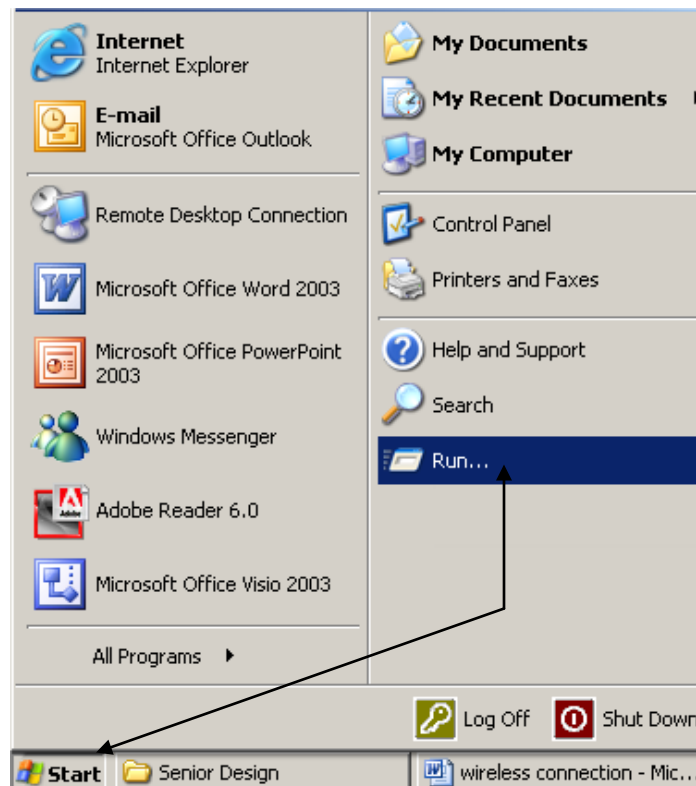


Complete Packet
Capture From Server

Appendix E. User Documentation

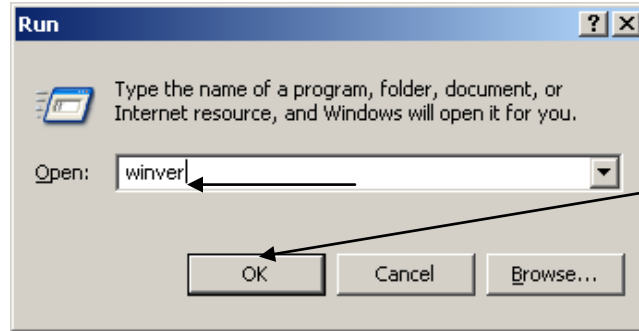
Logging In To The CUMC Wireless Network

1. Check to see what version of Windows you are running by doing the following.
 - a. Click the “Start” Button on the task bar
 - b. Select the “Run” Option

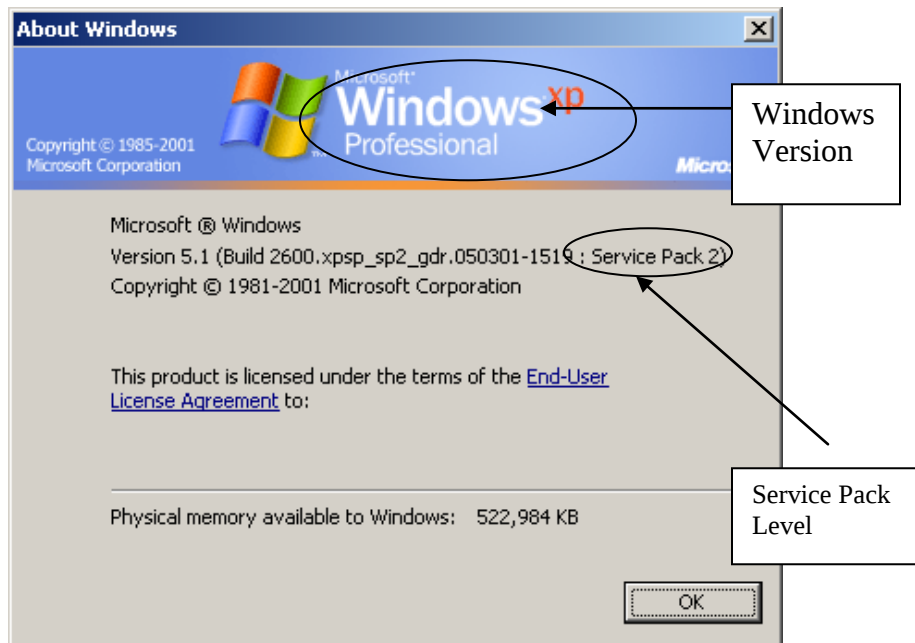


- c. In the “Run” dialog box type the following **winver**

- d. Then Click “OK”

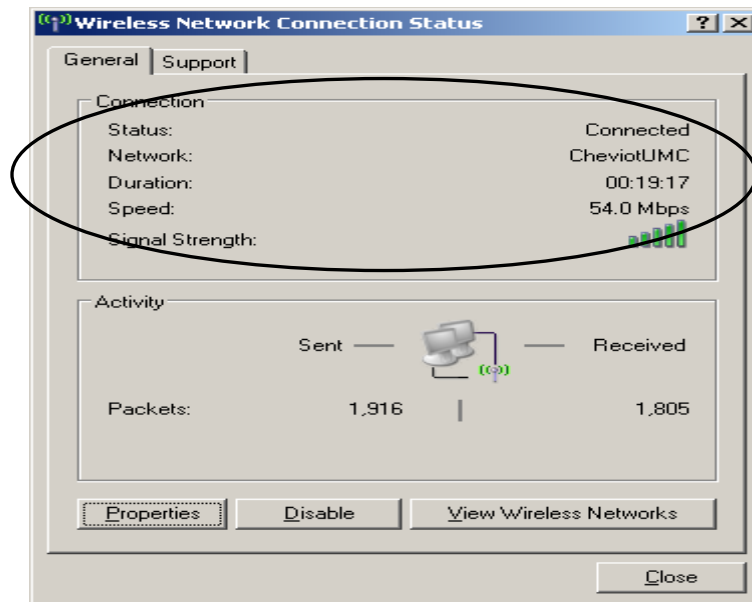


- e. You should get an “About Windows” dialog box

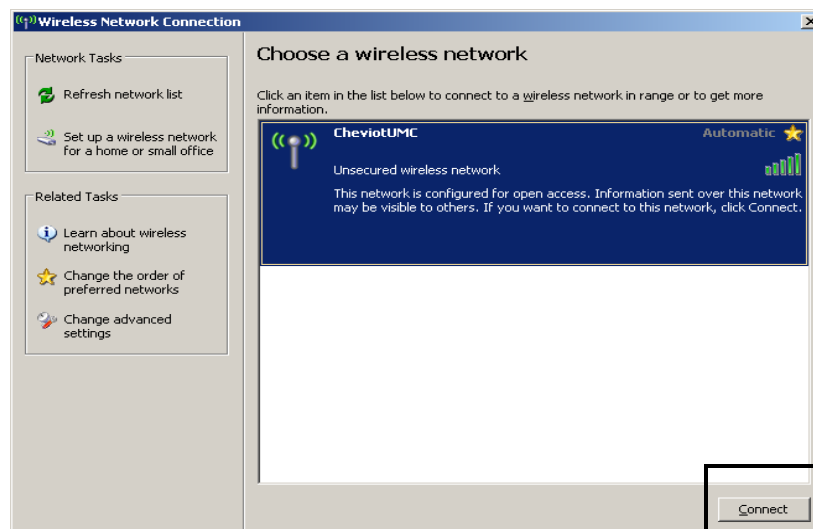


- f. The instructions below are for Windows XP SP2. Please make sure it states one of these in the Dialog box. (It is possible to connect to the network with any version of Windows from Windows 98 through Windows XP/SP1. You must know how to associate your wireless card with another access point. In Windows 98 through Windows XP/SP1 you will have to use the software that came with your card. For Windows XP SP2 you can use the Windows interface.
2. Check to make sure your wireless card is associated with CUMCWireless. To do this, follow the steps below.
- a. Double click the  or  icon located in the bottom right hand corner
- b. If you get  go to step D

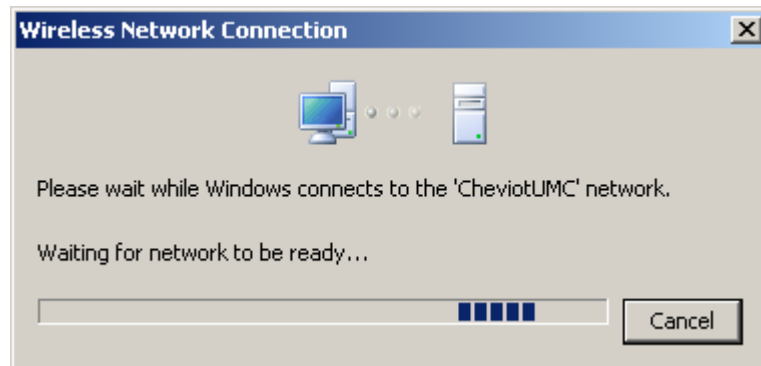
- c. If you get  go to step F
- d. The “Wireless Network Connection Status” window should appear.
- e. Then status will show connected and the network will display CheviotUMC. If you do not have CheviotUMC listed then continue following steps “f” though “i,” otherwise see Step 3.



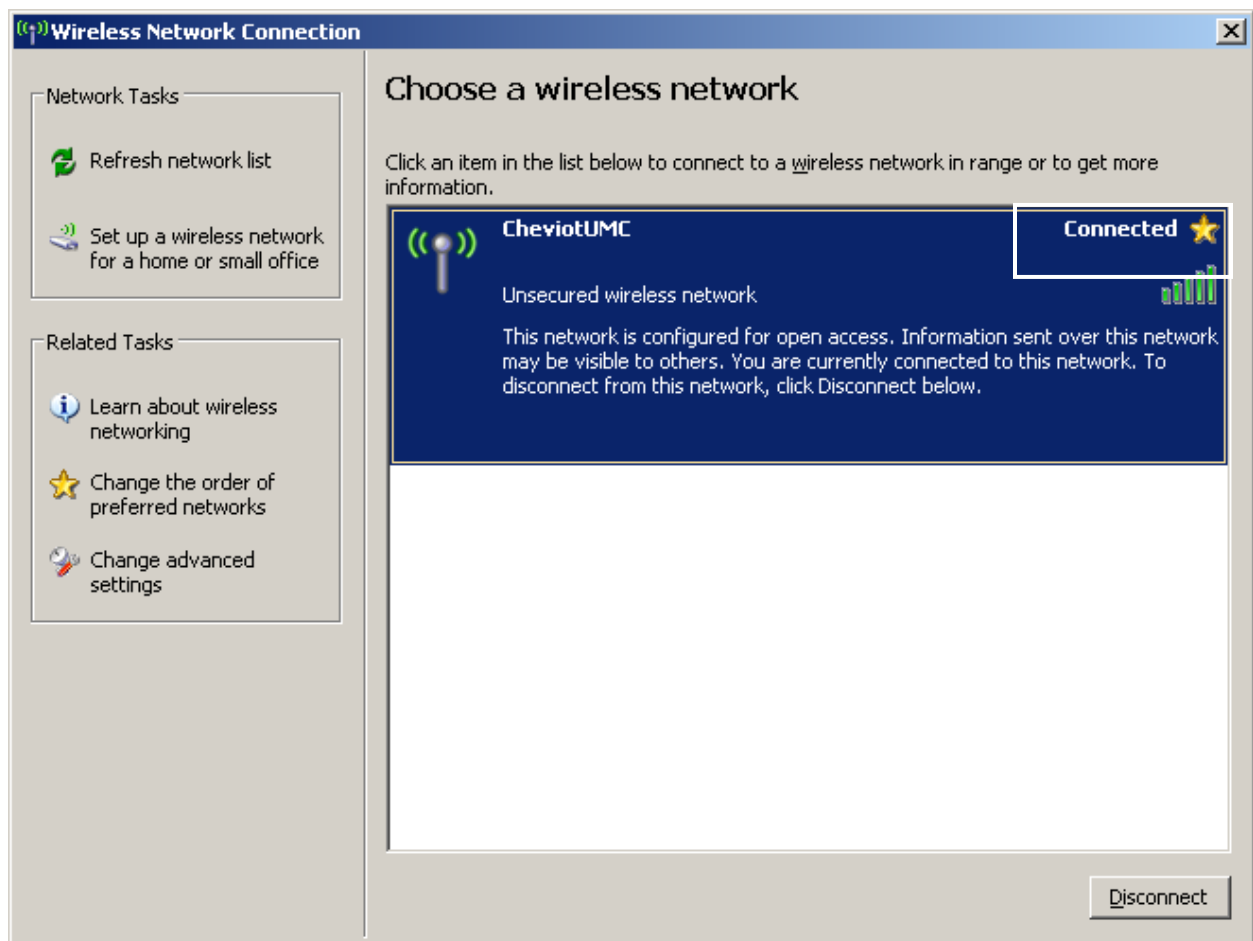
- f. Double click the .
- g. You will see a window like the one below. Select the CheviotUMC network then click the connect button.



h. You will then see the following window pop up



i. It should now say connected next to the network name

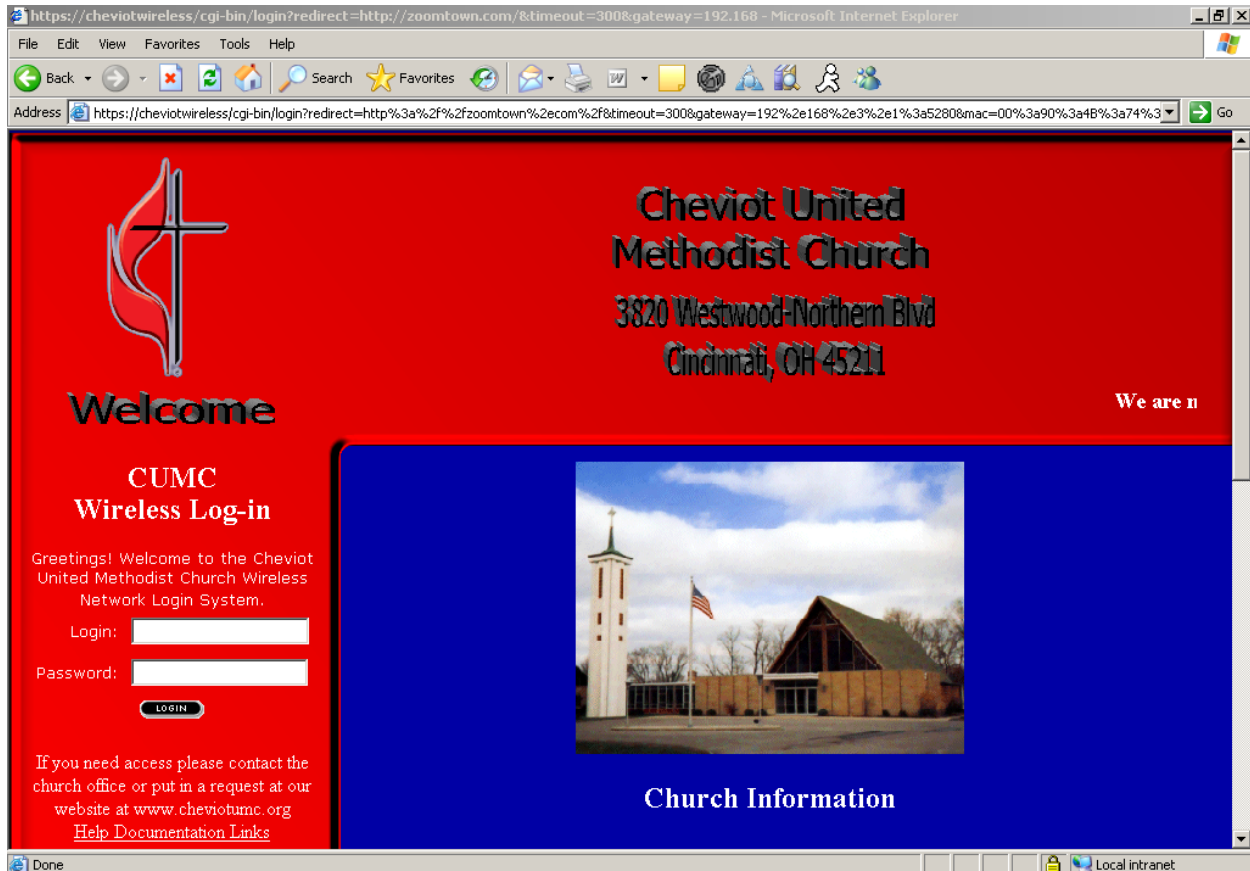


3. Once your card has been associated with the access point, click the Internet Explorer Icon.

4. Your browser will automatically be redirected to the Login Page.

- a. NOTE: You may get the following screen below. This screen is informing you that a third party has not signed the certificate. This will not affect the system in anyway. Press the yes button and the Login screen will appear.

5. You will see a page displayed like the window below.

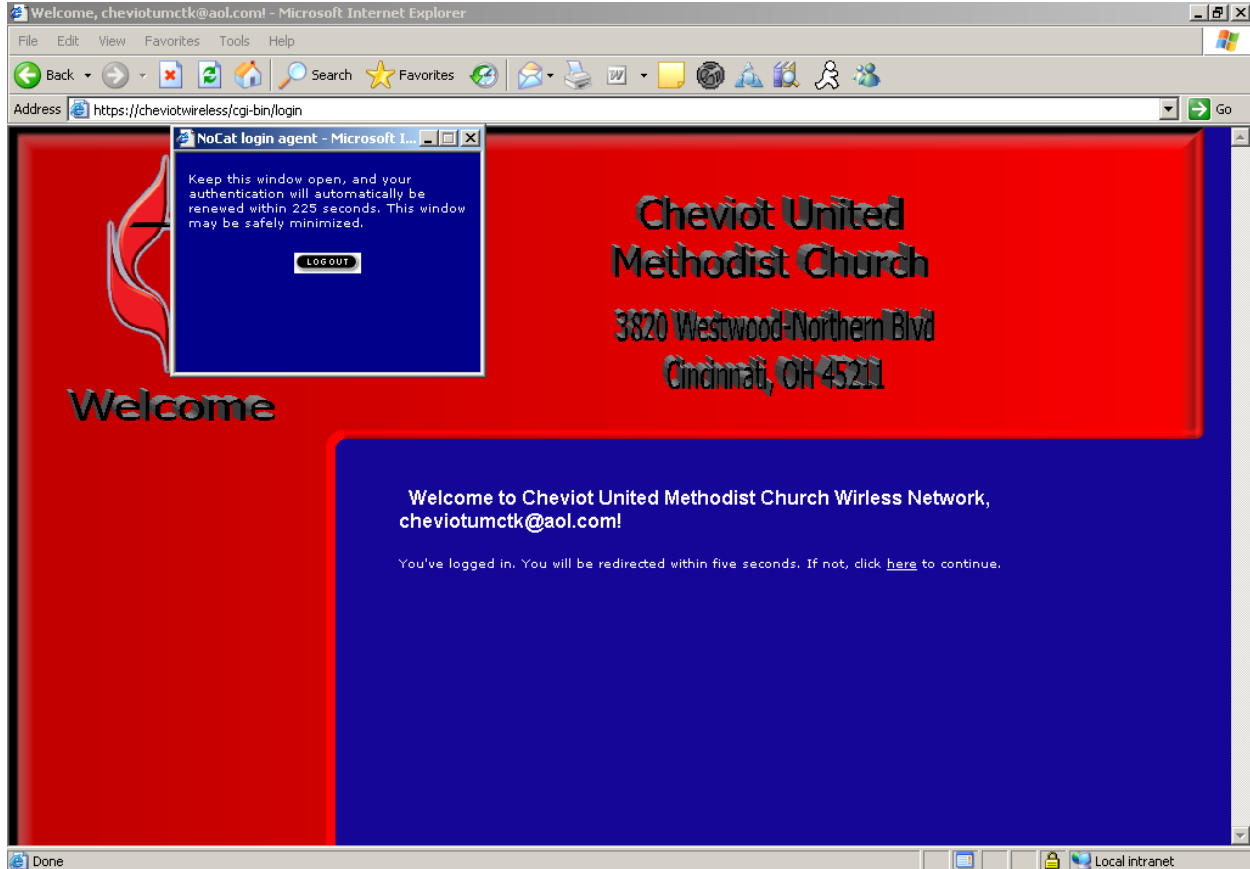


6. Enter the user name and password that was e-mailed or told to you.

PLEASE NOTE!

- a. If you have an old password from a prior login this password and/or username will not be valid, please make sure you acquire a new password and username from the church.
- b. If you did not receive an e-mail or if the password was not included please speak with or email Church Secretary at 513-662-2048 (cheviotumcjw@aol.com), Facility Coordinator at 513-662-2048 (cheviotumclk@aol.com) or contact the Network Administrator at cheviotumctk@aol.com.

7. When you are correctly logged in you will see the following screen.



a. It will inform you if an incorrect username or password has been entered.

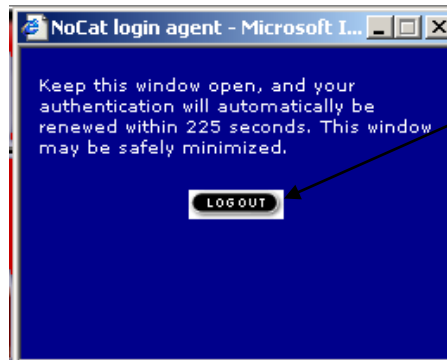
PLEASE NOTE!

b. **Make sure your caps lock key is off because password and user name are case sensitive.**

8. You may now use the Internet for your demonstration or to retrieve your presentation from e-mail.

a. **Please Note: you will not be able to print from this account unless you're a church staff member.**

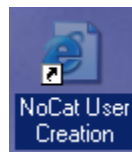
9. Make sure you keep the popup window shown below open so that you are not logged out automatically.



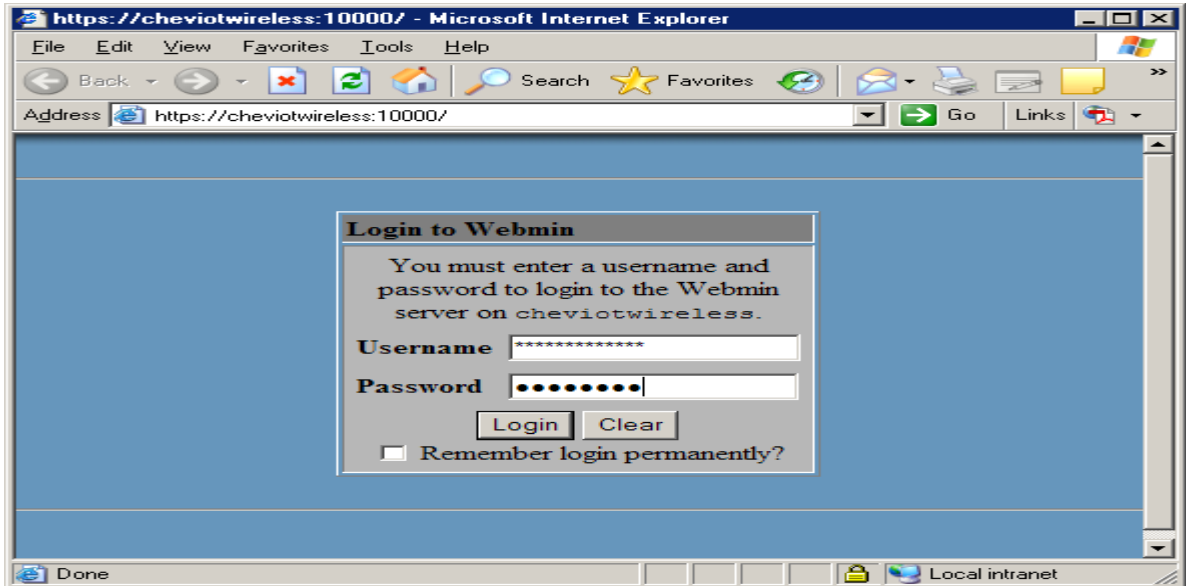
10. Once completed with your internet session please click the "Log Out" button.

Adding or Removeing NoCat Users

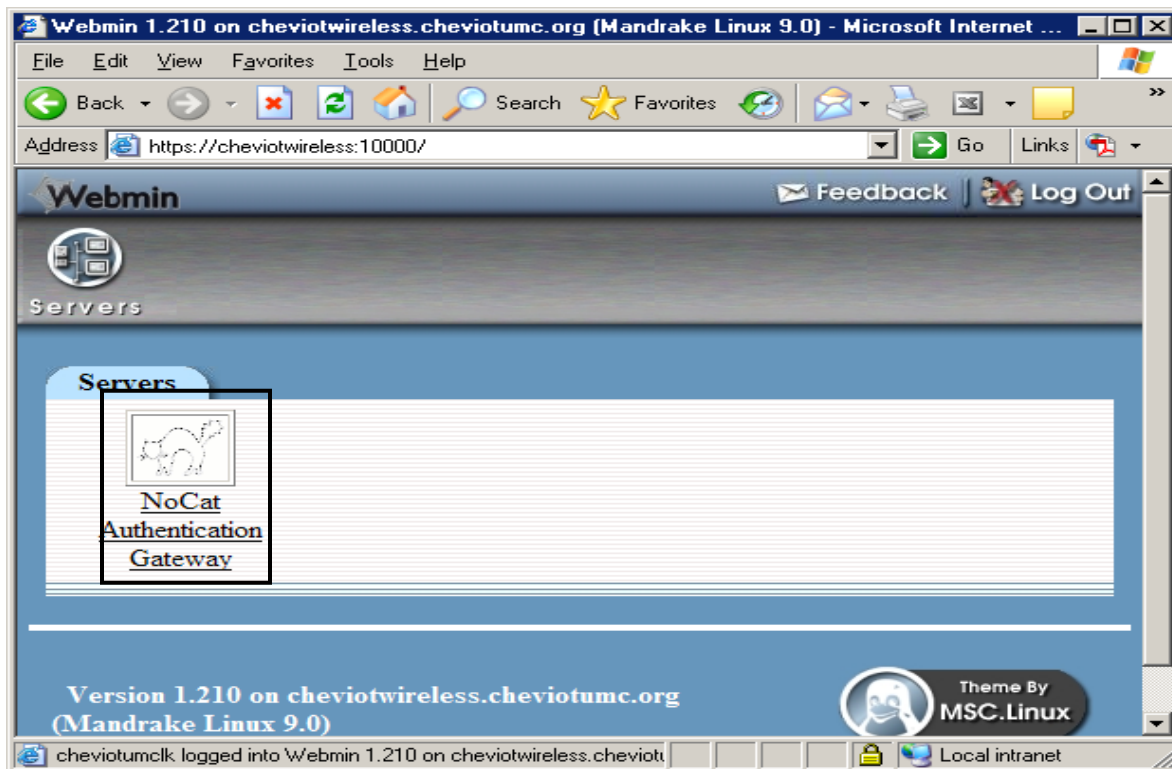
1. Double click on the icon on your desktop called "NoCat User Creation."



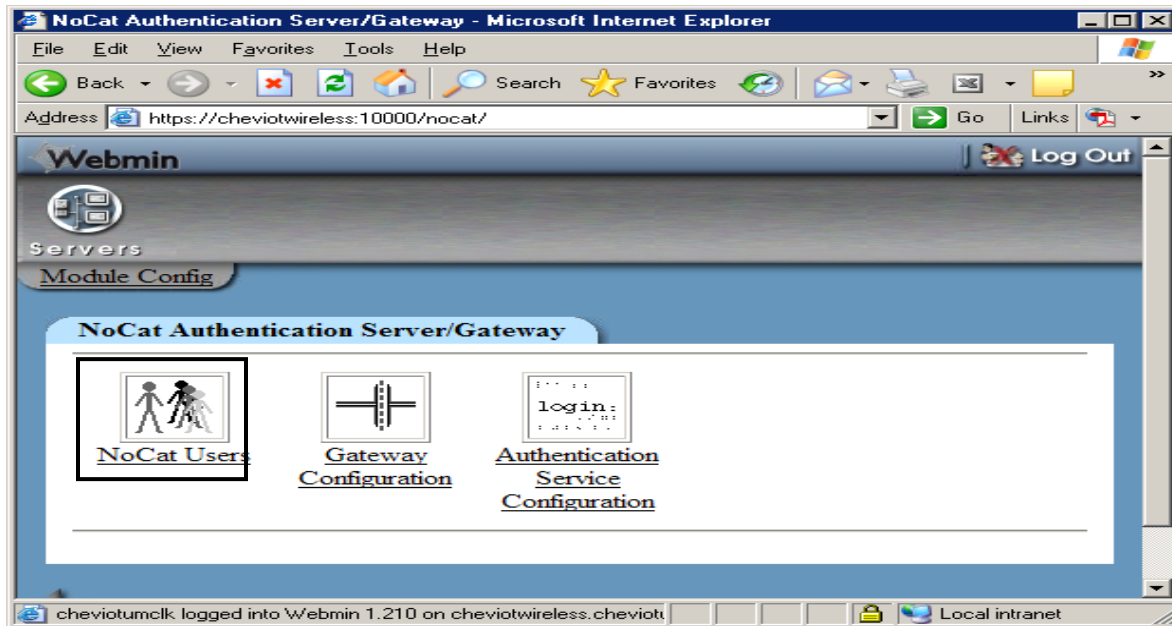
2. A new window will open like the following below



3. Enter your user id and password then click “Login.”
4. Once you login you will see the following. Click on “NoCat Authentication Gateway.”



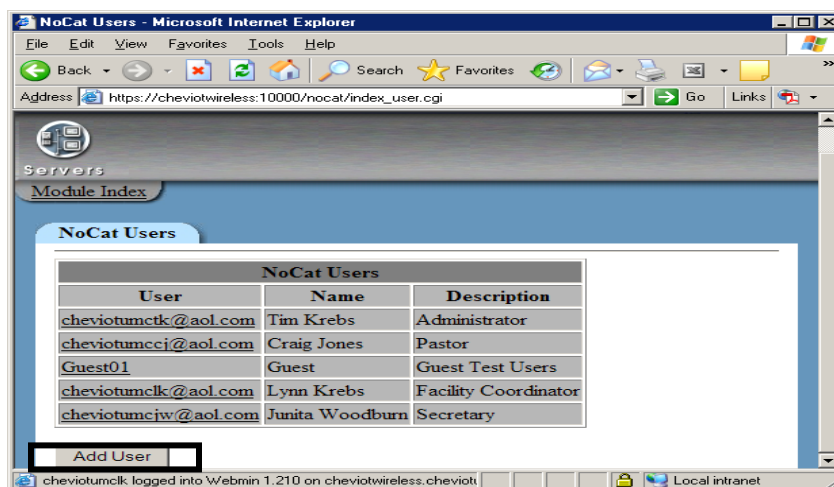
5. You will then come to another window. Click on “NoCat Users.”



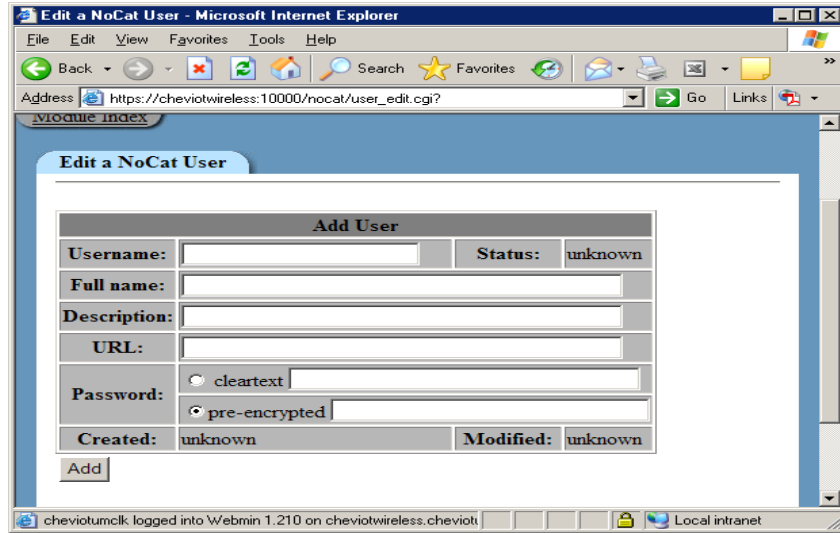
6. Now you have the option to Add, Remove, or Edit users.

a. TO ADD USER

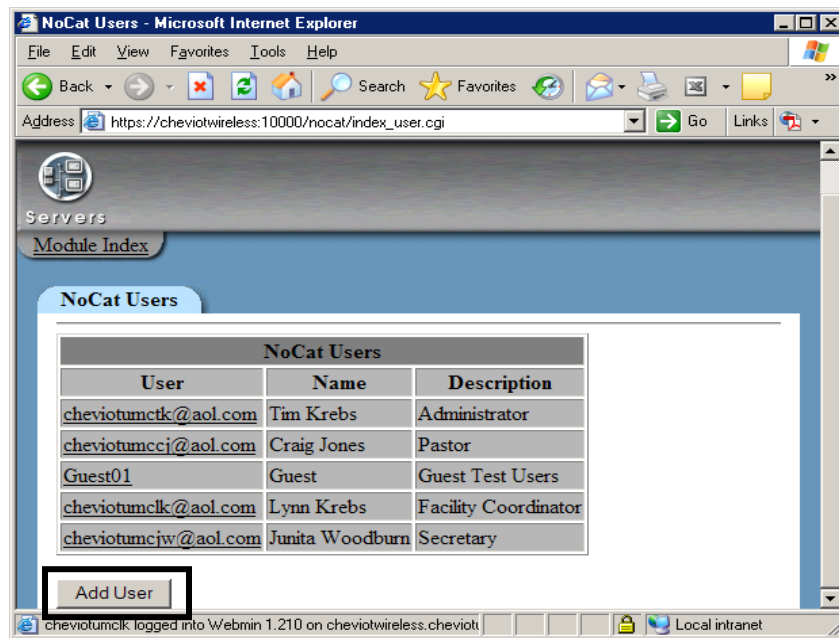
i. Click on the “Add User” button



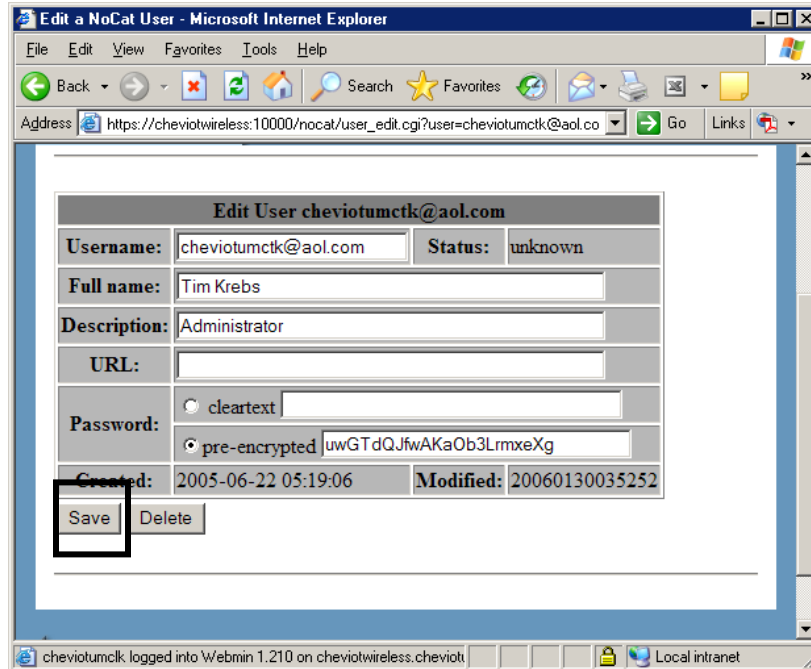
- ii. Enter user name; the name the user will log in with
- iii. Enter their full name
- iv. Enter why they need access and for how long
- v. Select button next to clear text
- vi. Enter user password
- vii. Click “Add User” button
- viii. The user is now a “NoCat User.”



- b. TO EDIT A USER
 - i. Click on one of the user ID's

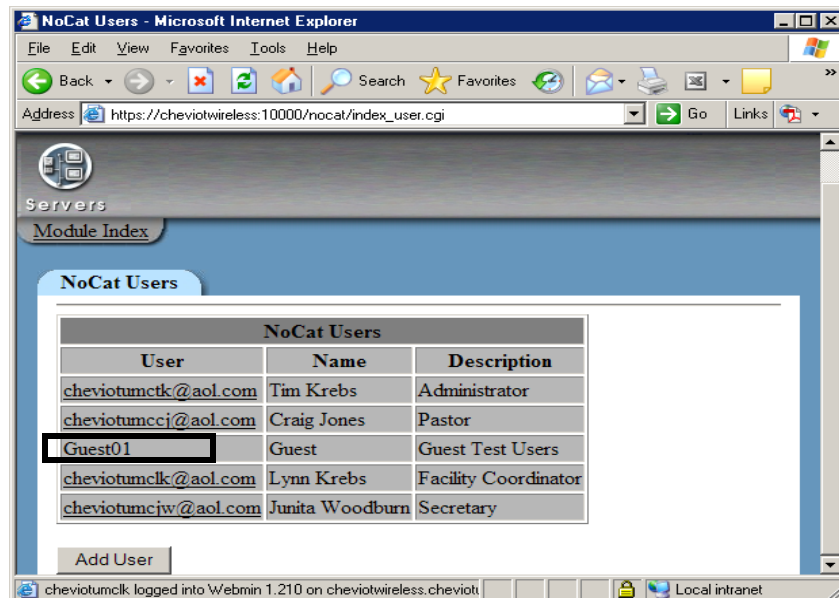


- ii. Change the options you wish to edit
 - iii. Then click the "Save" button

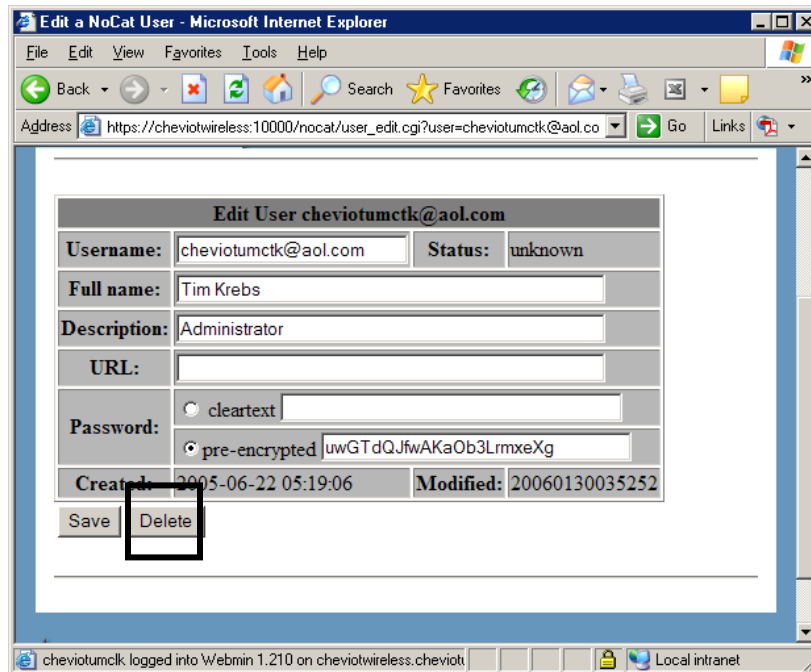


c. TO REMOVE A USER

i. Click on one of the user ID's



ii. Then click the "Delete" button that user is removed.



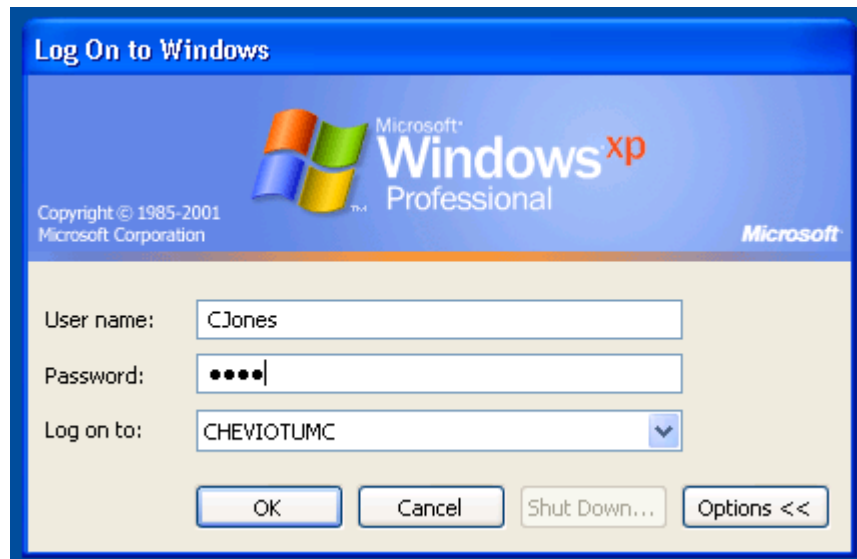
7. When you are done click the “Log Out” button at the top right hand corner then close the window.

Connecting to Work PC via Remote Desktop

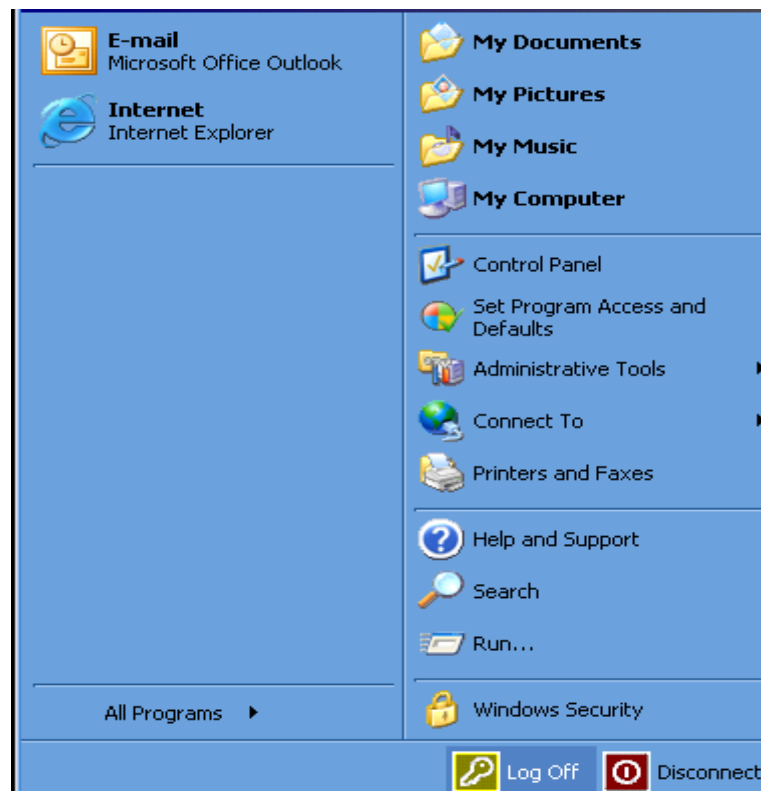
1. Login to the NoCat System by clicking on Internet Explorer and entering information as you normally would for surfing the internet.
2. Next minimize the NoCat window.
3. Double click on “Connect To Work PC” icon on your desktop.



4. This should bring open a new window with the windows “Log On to Windows” screen information.



5. Enter your work user id and password.
6. After a successful login use interface as you normally would.
7. When done log out as normal by clicking the “Start” button, then select the “Log Off” button.



8. You will then return to your local desktop.

References

Most references were used to troubleshoot during the initial project phases.

“The Apache HTTP Server Project”

[Http://httpd.apache.org](http://httpd.apache.org) February 25, 2005

Beginners Guides: Wireless Network Security - PCStats.com

[Http://www.pcstats.com/articleview.cfm?articleID=1489](http://www.pcstats.com/articleview.cfm?articleID=1489) February 28, 2005

Building Wireless Community Networks

Implementing the Wireless Web

By Rob Flickenger

1st Edition November 2001

ISBN: 0-596-00204-1

Collins, Jamin W. Thomas, Kristin E. “Linux.Com”

[Http://www.linux.com/howtos/Authentication-Gateway-HOWTO/intro.shtml](http://www.linux.com/howtos/Authentication-Gateway-HOWTO/intro.shtml) February 25, 2005

Enockson, Eric “Nocat Protocol”

[Http://lists.nocat.net/pipermail/nocat/2002-July/001791.html](http://lists.nocat.net/pipermail/nocat/2002-July/001791.html) February 25, 2005

Ferrarini, Elizabeth M. The Five-Access Point Security Plan

[Http://www.enterprisenetworkingplanet.com/netsecur/article.php/752421](http://www.enterprisenetworkingplanet.com/netsecur/article.php/752421) February 28, 2005

Flickenger, Rob O'Reilly Network: NoCatAuth: Authentication for Wireless Networks

[Http://www.oreillynet.com/pub/a/wireless/2001/11/09/nocatauth.html](http://www.oreillynet.com/pub/a/wireless/2001/11/09/nocatauth.html) February 25, 2005

Gunter, Matt NoCatAuth Gateway Server Configuration

[Http://www.wi-fiplanet.com/tutorials/article.php/3111111](http://www.wi-fiplanet.com/tutorials/article.php/3111111) February 20, 2005

How to Create a Self-Signed Certificate

[Http://www.akadia.com/services/ssh_test_certificate.html](http://www.akadia.com/services/ssh_test_certificate.html) November 23, 2005

How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN

By Lee Barken CISSP, CCNA, MCP, CPA

Publisher : Prentice Hall PTR

Pub Date : August 26, 2003

ISBN : 0-13-140206-4

Managing and Using MySQL, 2nd Edition

By Tim King, George Reese, Randy Jay Yarger

Publisher : O'Reilly

Pub Date : April 2002

ISBN : 0-596-00211-4

“MySQL: The World’s Most Popular Open Source Database”

[Http://www.mysql.com](http://www.mysql.com) February 25, 2005

“Netfilter/Iptables Project Homepage”

[Http://www.netfilter.org](http://www.netfilter.org) February 25, 2005

“The NoCat Community Wireless Network Project”

[Http://nocat.net/nocatrfc.txt](http://nocat.net/nocatrfc.txt) February 25, 2005

Pearson Education, Que Publishing Securing Your Wireless Network

[Http://www.quepublishing.com/articles/article.asp?p=339052](http://www.quepublishing.com/articles/article.asp?p=339052) February 28, 2005