

# Northeastern University Secure Wireless Network: A Proposal

**Randy Heins**

*College of Computer Science, Northeastern University Boston, MA. 02115*

Addressed to:

Robert Weir - *Vice President of Information Services, Northeastern University*  
Robert Whelan - *Director of Network Services, Northeastern University*

*Northeastern University would benefit in many ways from a wireless network. The advantage of a wireless network would be noticeable by advancements in enrollment, the public view of Northeastern University, University sales and by easing the overcrowding situation. However, modern day wireless networks are insecure by default. The insecurities in the Wired Equivalent Privacy security protocol render information accessible to the public, which is not acceptable in an educational facility. My proposal describes the faults of wireless networking, and offers a specific solution for Northeastern University. The solution involves a combination of MAC address authentication, RFC 1918 private address space, router-based access control lists, and a virtual private network. These complimentary technologies will show that WEP is not necessary in a modern day wireless network. The proposal will rely upon the built-in strong encryption that is provided with Virtual Private Networking to make an easy to manage and secure wireless network for Northeastern University.*

## **Introduction**

Not only does the modern day computer user demand connectivity, but they also want versatility. To accommodate this desire, wireless networking has become an important part of mainstream corporations, universities, and even some home networks. Simply put, a wireless network is an extension of a traditional data network. This complementary network provides access to the traditional network via radio waves in the 2.4 GHz frequency. Wireless nodes are physically installed in places where network access is needed, meanwhile users communicate to the network using a wireless network card for their laptop computer. Wireless networks are beneficial due to their inherent lack of cabling. The side effect of wireless networking is a loss of privacy, which needs to be solved before you establish a wireless network.

Each year, computer networks play an increasingly important role in the University environment. Northeastern University has stayed ahead of the curve in regards to the upkeep of their network; allowing it to expand and evolve as the demands of its students increase. I believe that the next logical step in the evolution of Northeastern University's network is the implementation of a wireless network to accommodate their students. However, wireless

networking implies a breach of security on any network unless the further measures are taken. A makeshift security solution will not adhere to IEEE standards, that is why it is important to build on trusted technologies to secure the network. In my proposal, I will discuss the measures that should be taken to implement a secure wireless network for Northeastern University.

## **How Wireless Benefits Northeastern University**

A wireless expansion to Northeastern University is beneficial to the students, but also benefits the school in return. The existing wired network at Northeastern University provides access from dormitories, classrooms, and the library. The proposed wireless network will increase the range to include areas that remain inaccessible by traditional wired networks. This advantage will introduce Northeastern University to benefits that cannot be achieved by traditional wired networks.

### **Increased Enrollment**

A wireless network is beneficial to Northeastern University for several reasons. The first reason confronts the traditional concern of Universities: enrollment. Northeastern's Information Technology department has acquired advertisements in the

student newspaper, stating that the Northeastern network is one of the “best in Boston.” It is easy to understand how boasting the network will give the appearance that the University cares about meeting the students’ needs, and this will help enrollment. However, not all colleges in Boston have a wireless network to brag about. Northeastern should welcome the chance in becoming one of the first colleges in Boston to tout their own state of the art wireless network. In this manner, a wireless network will help appearance of Northeastern University, and in turn help enrollment.

**Enhanced Reputation**

Northeastern University has a large public presence. There are many visitors to Northeastern on a daily basis; these people are prospective students, contributing alumni, and possible co-op employers. These people notice small things about the University, and their views of the University are based on how they perceive it. A wireless network would be visible to anyone visiting the University. Students using the wireless network would be noticed in the library, Marino center, dorm lobbies, conference rooms, or even out on the lawn in the Krentzman Quadrangle. Northeastern’s visitors would put the University in higher regard if they noticed a state-of-the art wireless network in use.

**Increased Demand for Northeastern Goods**

Additionally, the presence of a wireless network will be attractive to Northeastern’s large commuter population. Between classes, commuters spend their time at computer labs doing homework or simply browsing the internet. However, the University does not gain any money from commuter students sitting at a computer lab, tying up precious bandwidth. A wireless network can approach this problem from another standpoint. If a wireless network were to be implemented around the University, it would not be difficult to expand the wireless academic network to encompass local Northeastern owned establishments, such as eateries, bookstores, and cafés. If this was the case, commuter students would be enticed to stray away from their internet browsing, and rather buy products from Northeastern’s establishments.

**Overcrowding Solution**

The sudden rise in population at Northeastern University has created a shortage of real estate. Not only are classrooms and dorms over-occupied, but computer labs are at a premium. Students fight for a seat at the library to gain access to the Internet. When there are no unoccupied seats at the library, students go to the computer labs in Dodge Hall or

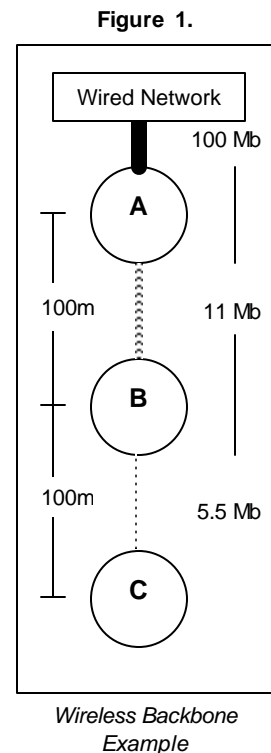
Cullinane Hall. These computer labs are intended for the College of Business Administration and the College of Computer Science at Northeastern University, however they are currently being used to compensate for the overcrowding occurring at the library. However, when wireless networking is incorporated into public areas at Northeastern University, people will be able to bypass wait lines for computers at the library. A user can sit down with a laptop in any wireless equipped area in the University, and gain access to the network without tying up a Northeastern computer. A wireless network at Northeastern University would free the valuable computer space which remains a premium today.

**Wireless networking overview**

Wireless networking (also known as IEEE 802.11) reaps all the benefits of a wired network along with the implicit benefit of having no wires. This important benefit has placed this seemingly new technology on the front burner of most corporations’ IT departments. Wireless network nodes are radio devices that are physically connected a wired network. A laptop is then equipped with a wireless network card which receives radio messages from the network node, thus providing a link to the network.

A wireless network can only be seen as a complement to an already existing wired network, not as a supplement. A wireless network will only extend an already existing physical network backbone; it will not be able to create a network backbone.

The incorporated diagram explains the limitations of wireless network design. The first wireless node “A” is directly connected to the wired network at 100 megabits/second. If you wish to provide access to the second



wireless node “B” via “A”, the maximum bandwidth will be the maximum speed for the 802.11 standard, or 11 megabits/second. After the third hop, the bandwidth will be reduced by half to yield only 5.5 megabits/second. The bandwidth that is provided by wireless node C is not sufficient to provide access for the smallest of corporations. The speed is limited to approximately 18% of the capacity of a traditional wireless network. Because of this limitation, wireless networks cannot efficiently handle a backbone for a network. That is why a wireless network should only be seen as a complement to a wired network, and not as a replacement.

### **Physical network security**

Similar to libraries, networks are of little value unless they are easy to access by the people who are authorized to use them. And just like libraries, some networks are open to the public, and some are private. It is very important to designate which users are allowed access to the network, that way intrusions will be limited. However, not all intrusions are carried out by outside attackers. Internal attacks account for a large number of intrusions. Attacks are carried out by users that have access to the network, but use it for unauthorized purposes. In our library example, this would be the equivalent of a librarian looking up private information in the town archives. This explains the need for security in places where private information is held. Not only is it important to guard against external attacks, but internal attacks can be just as devastating.

#### **Physical Wired Network Security**

When considering networks, the most important aspect of security is physical access. A network can be immune from outside attackers, but if someone physically gains access to an internal network jack, all traditional security measures will be rendered useless. Once an eavesdropper is part of the internal network, they can view all information that crosses their path. This method defined as “packet analyzing” or “sniffing” is quite simple and can be achieved by nearly anyone. Most network cards are set to only receive packets that are destined for itself. However, network cards can also be set to a “promiscuous mode” which receives all packets that are viewed [3]. A common tool called a “packet analyzer” will examine all traffic and show various information. This information includes: usernames, passwords, email correspondence, network

configuration information and many other forms of sensitive material on the network.

Physical security on a wired network is relatively easy to manage. For the most part, locking office doors is the solution that will protect from outside attackers. The solution for internal attackers is based on hardware. The only way to solve internal physical attacks is by network technology. A hub will allow all users on a network segment to view all other users’ data, thus creating insecurity. On the other hand, a switch will only transmit data to the desired network card. This leaves all data private on a network, and solves the issue of internal network security.

#### **Physical Wireless Network Security**

Physical security on a wireless network presents a more difficult problem compared its wired counterpart. As mentioned earlier, wireless network nodes broadcast data over radio waves. These radio waves behave similar to wired network hubs, allowing everyone to receive your private data. The waves can travel as far as 100 meters, sometimes broadcasting information far beyond the physical area that you wish to allow access to your network. This aspect puts a new twist on physical security; eavesdroppers no longer have to inconvenience themselves with gaining physical access to your office to view sensitive data. With wireless networking, they can park their car across the street from your office building, install a wireless network adapter in their laptop, and intercept data as it is broadcast from the wireless nodes.

### **Wireless encryption security standards**

A new standard, the Wired Equivalent Privacy protocol, was introduced to protect wireless network segments from eavesdropping.

*“The 802.11 standard for wireless LAN communications introduced the Wired Equivalent Privacy (WEP) protocol in an attempt to address these new problems and bring the security level of wireless systems closer to that of wired ones” [2].*

The WEP protocol was meant to be the answer to physical wireless network security. The only method for a user to gain access to a WEP equipped wireless network is to enter a password called the WEP key. However, we assume that there is an eavesdropper who can guess the password off-line without the interaction of your network [5]. The best defense against this form of attack is to increase the frequency that the WEP key is changed. The important job of key administration relies upon

network administrators, most of whom are too busy with other matters to keep up with changing the WEP key on every wireless network node. Also, once the key is changed, all users must be informed of the new key. This would present a never ending administration cycle that no one would want to manage. Any administrator will inform you that WEP key authentication poses the first problem for this standard.

WEP worked in theory, but failed in practice. The algorithm that lies in the heart of WEP is weak, and easy to exploit due to the random initiation variable (IV). However, the algorithm and IV's are not the root cause for the failures of WEP. The limitations of wireless hindered the processor design for wireless network nodes. In turn, this hindered the encryption algorithm design.

It is important to understand the failings of the current WEP standard to further understand that additional technologies must be included in a design for a secure wireless network at Northeastern University.

**Encryption Algorithm**

WEP uses an algorithm called "RC4" to encrypt data. Once data is encrypted, it is transmitted to the wireless node, where it is then decrypted and forwarded on just like wired network traffic. However, there are flaws in the RC4 algorithm that make the protocol insecure.

The critical flaw in WEP starts with the design in the wireless network nodes. The nodes are designed to be placed in small areas where minimal power was available, such as on top of a suspended ceiling in an office building. For this reason, the processor for the wireless node is much less powerful compared to its wired counterpart.

*"Since the wireless local area networks are intended for portable battery operated wireless stations, low power consumption is a very important consideration. Therefore, the security mechanisms developed should use relatively low complexity cryptographic algorithms" [7].*

Therefore, a weaker encryption was needed to accommodate for the slower CPU. The result was a watered down 40-bit WEP encryption that proved to be too weak to secure wireless networks.

**Random Initial Variables**

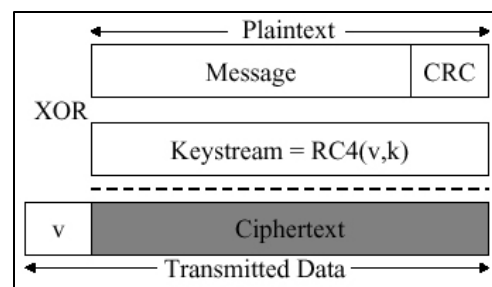
To gain the initial authentication, WEP performs a private/public key exchange with the access node. A 24-bit number called the random initial variable is generated to give a different key exchange for every

transaction. The random number is the factor that is meant to keep eavesdroppers guessing. In a real life comparison, you could consider the wireless communication to be compared to telephone system. Every time you use the telephone, you are assigned a new "code name" to be used instead of your real name. Therefore, if there was an eavesdropper tapping your phone line, he would be confused as to who you are and with whom you are talking. On a wireless network, you are assigned a different IV (codename) for every connection, therefore if there is an eavesdropper on the network; they will have to crack your IV before you are assigned with another IV (a totally different codename).

Random numbers help to secure wireless transactions; however they are also a fault. Due to the limited processor capability, the wireless nodes have a relatively small pool of "random numbers" to choose from. To relate this to our example, the eavesdropper who is tapping your phone line only has a few different "codenames" to choose from when narrowing down your identity. If the wireless processor was more powerful, true "random" numbers could be generated, thus making the pool of codenames nearly infinite.

Reuse is another problem with the wireless IV. Wireless designers recommend that the IV be reset after every packet. The constant changing of the IV will make it more difficult for eavesdropping to occur. However, the wireless network card will "reset the IV to 0 each time it is re-initialized, and then increment the IV to 0 by one for each packet transmitted" [2]. A relation to our example goes as follows. You are given a numbered list of "codenames." Every morning, you communicate using the first codename on the list during the first phone call, the second codename on the second phone call and so on. The eavesdropper has been clued in to your true identity if you use the same codenames, in the same order, every day. Figure 2 helps illustrate the importance of IV privacy. If the

Figure 2.



Ciphertext construction [2]

eavesdropper has the encrypted ciphertext, and has also discovered the IV key, then a simple XOR will give the original unencrypted message. If the IV is not truly random, eavesdroppers will find it easy to analyze wireless transactions.

### **Insecurity Proof of Concept**

To fully understand the importance of wireless security, it is beneficial to be familiar with the process in which a wireless network is compromised. There exists software which exploits WEP, and it is readily available to the public for free. One of these programs, AirSnort (<http://airsnort.shmoo.com>), exploits the weaknesses in the RC4 algorithm to accomplish the job.

In order for AirSnort to analyze packets, the wireless network card must be set to “promiscuous” mode. Once the card is set in this fashion, every packet that reaches the network card will be analyzed. “Out of the sixteen million keys which can be generated by WEP cards, about nine thousand are weak (for 128 bit encryption.) Call these packets with weak keys ‘interesting’ “ [1]. Once enough “interesting” packets are logged by the program, it takes less than two seconds to actually break the encryption.

If a WEP-equipped wireless network were to be analyzed without the aid of programs such as AirSnort, you would only view encrypted data such as: “1efb483292ac.” However, with AirSnort’s ability to exploit the WEP algorithm, such encrypted data can be translated into: “Username: bjefferson Password: LetMeIn!” The most alarming fact is that this decryption can happen within a day on most networks.

Sometimes the implications of problems are not always clear. This example serves as a proof of concept for WEP insecurity. It also expresses the need for additional technologies to secure a wireless network at Northeastern University.

### **Recommendations for a wireless Northeastern network**

It is obvious that WEP is not the best answer for a secure wireless network. Along with its security failures, the WEP algorithm is very slow, and therefore cuts network speeds. On a typical 802.11b network node, the maximum bandwidth is 11 megabits per second. “When WEP is enabled, most Access Points exhibit a severe decrease in useable bandwidth (as much as 50%)” [8]. WEP renders a wireless network twenty times slower than a typical

wired network connection. With the addition of WEP, users will view the disadvantages of WEP to outweigh the advantages of wireless networking, and this proposal will fail. Due to these factors, WEP is not the answer for securing Northeastern’s wireless network.

WEP is the IEEE standard for wireless encryption. Individual corporations may design their wireless nodes with their own proprietary encryption standards; however, it will not always be compatible with other technologies. In order to find a true way to secure a wireless network, the following complementary technologies must be incorporated in the design. By introducing these new technologies, the network will still adhere to IEEE standards thus making troubleshooting feasible.

### **MAC Authentication**

MAC address registration is currently used on all RESNET equipped computers. Every user on the Northeastern network is forced to register their unique MAC address before they are allowed access to the network. Denying foreign network card assures that only authorized users can gain access to resources. With MAC address authentication enabled an intruder would need possession of a registered Northeastern network card to gain access.

MAC address registration will be the first layer of security for the proposed wireless network. Implementing this on the wireless network will assure that every user is registered with the University. Each individual user will register their wireless network card’s MAC address with RESNET. At this point, only users with valid MAC addresses will be allowed access to the network. Since every MAC address is unique, it corresponds to one individual user which gives RESNET the ability to monitor their users.

### **RFC 1918**

The second step to secure the Northeastern wireless network is through the use of RFC 1918 private address space. Every node on the internet is assigned a unique Internet Protocol (IP) address. It is the function of routers to advertise your unique IP address, so others know how to communicate with you. However, RFC 1918 maintains a list of IP addresses that routers cannot advertise. Since a router cannot advertise these IP addresses, it makes them private to the outside world.

When a user connects to the proposed wireless network at Northeastern University, they will be automatically assigned an RFC 1918 private IP

address by DHCP. Since this private address space is not advertised by Northeastern's border router, the user can only access resources within Northeastern's local network. If the user was to try to access a foreign resource, say <http://www.yahoo.com>, Northeastern's border router would drop the data request, and the user would be presented with an error message. Another benefit to assigning private addresses is that users on the wireless network will not be visible to the outside world. However, this advantage does not affect eavesdropping. Private addressing provides the second layer of security on the wireless network, and it merges nicely with other technologies to make a complete solution.

**Access Control Lists**

Northeastern University's routers are equipped with packet filtering Access Control Lists (ACL) which make it easy to direct network traffic. These ACL's can help secure the proposed wireless network. An ACL can be implemented on routers to permit or deny traffic between hosts on a network, thus giving the administrator more control over the flow of information.

MAC address authentication and RFC 1918 address space contribute to the security of the proposed network. Although these are two major steps in securing the network, it does not guarantee that every user on the network is a valid user. Registered network cards can be stolen, and MAC addresses can be spoofed to resemble registered network cards. These aspects create the possibility of unauthorized access to the network, thus creating an untrusted network. Since a users validity is not assured at this stage of authentication, it is important to secure all Northeastern University resources.

Since it is plausible for any user to have unauthorized access to the network, all users' access will be controlled by router-based access control lists. In order to protect all local Northeastern resources, the ACL's will deny all IP access to any part of the network. The only access allowed is via port 80 (HTTP), which is also filtered to stop unauthorized access. The router will have a static route in place to filter any port 80 traffic to a specific URL within Northeastern's network. This web page will contain an explanation of how the user can connect to the final stage of authentication, virtual private networking (see Figure 6).

Northeastern's wired and proposed wireless networks essentially reside on the same network. By default, there is an implicit trust between the two networks, which creates holes in the security model. Any user could take advantage of these trust relationships and exploit Northeastern services. With ACL's in place, the wired and wireless networks will become two virtually separate networks. ACL's will help protect Northeastern's network from interior attacks from unauthorized users.

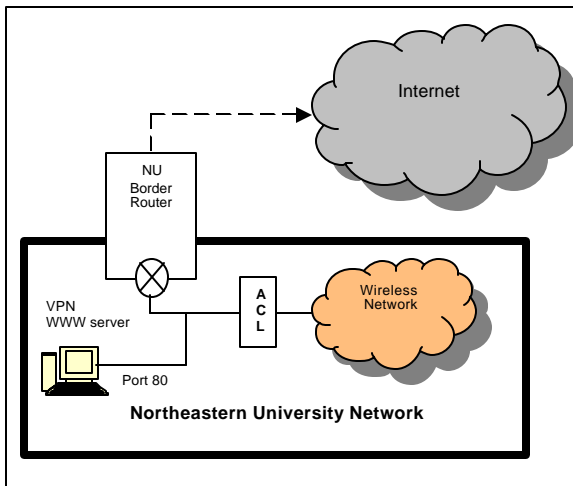
**Virtual Private Networking**

Combined with ACL's and private addressing, virtual private networking will provide the security cornerstone in the plan to implement a secure wireless network at Northeastern University. Virtual Private Networking (VPN) is a secure and transparent way to bridge two networks.

The most common usage of a VPN is for traveling employees. This example is similar to the wireless situation. In the example, an employee is visiting a foreign network which has an unknown security structure. In order to communicate with his home network in a secure fashion, the employee uses VPN technology. VPN creates a secure tunnel from the foreign network to the employee's home network, thus guaranteeing that eavesdropping will be ineffective. Any data destined for his corporate network will travel over the secure tunnel, and then is decrypted by the VPN concentrator at his corporate network. This insures that all data that is transferred between the two locations is secure.

*"The end result is a secure VPN that operates automatically and transparently to the user. Employees residing in the VPN work normally. They go on-line, send email to customers and suppliers or download presentations, and the VPN determines which of their tasks are to be conducted secured and which should continue in the clear. Full privacy is maintained, communications costs are reduced, but efficiency and employee output remain unchanged" [6].*

**Figure 3.**



*Wireless network implemented with RFC 1918 address space and access control lists.*

The traveling employee situation will help explain the relation between VPN and the proposed wireless network. Here is a review of the current characteristics of a user connected to the proposed wireless network:

- *The user is assigned a RFC 1918 private address space, limiting their access to Northeastern resources. The user has no access to the external internet.*
- *Due to insecurities of wireless, the user is granted limited network access. All other communications are denied by router-based access control lists.*

At this point, the wireless user is limited to the operations that they can perform. The role of VPN is to break these restrictions.

Every member of the Northeastern University community will be provided with a VPN account. This account will grant the user a valid public Northeastern IP address. This allows the user to access internal resources and the external Internet without any restrictions. We allow this to happen because of VPN's secure tunneling protocol (PPTP). The strong VPN encryption now carries the load that was previously carried by the insecure WEP algorithm, thus making eavesdropping nearly impossible. The wireless connection is no longer hindered by the insecurities of wireless networking.

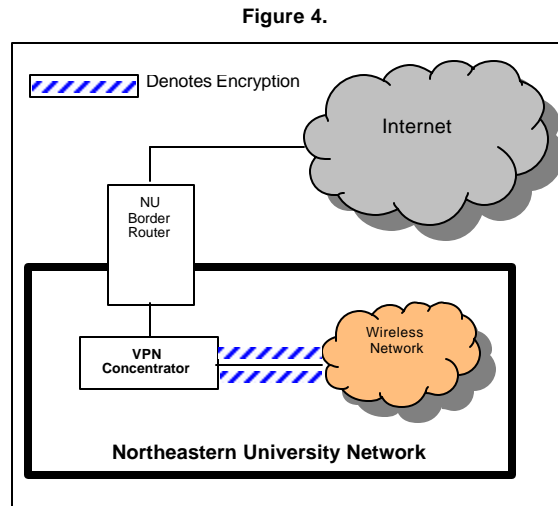
The problem that most organizations have with VPN is participation. Connecting to VPN is as simple as entering a username and a password, however, most corporations give little incentive for a user to take advantage of VPN. In my proposal, the incentive is access. If a user does not take advantage of VPN, they are not granted access because they are sending vital information to anyone who cares to listen to their connection. I feel that that access will encourage users to take advantage of VPN, which is the best method for securing a wireless network at Northeastern University.

## Conclusion

### Cost Analysis

As stated earlier, I believe that a wireless network will enhance the public view of Northeastern University. Advances in enrollment, alumnae contributions, and local sales will make the wireless network feasible. However, the largest cost of this project will be a virtual private network concentrator to secure all wireless communications. A wireless network can be implemented without the use of VPN; however, it will rely on WEP, which is insecure.

The cost of VPN can be seen as a tradeoff. One can properly invest in the future of the wireless network and incorporate a VPN concentrator into the design. This will provide a secure wireless network infrastructure that will be scalable for coming years.



*Wireless network implemented with Virtual Private Networking (VPN)*

Conversely, a wireless network can be implemented with WEP authentication. Due to the design of WEP, this network will run at 1/10<sup>th</sup> the speed of a wireless network without WEP enabled. This means that ten times the investment is needed to provide an equivalent VPN network – and it will still be insecure.

Sensitive data that is gathered by eavesdroppers costs money. The wireless network will be a playground filled with credit card numbers, social security numbers, usernames/passwords, bank account PIN's, and other forms of sensitive data. The VPN investment will prove to be less expensive than the potential loss due to the insecurities of wireless. Investing in secure technologies is essential to the success of a wireless network.

### Concluding Thoughts

Northeastern University will benefit from a wireless network in many different ways, ranging from the alleviation of overcrowding to increased enrollment. The time for a wireless network has come for the University. However, the adoption of such a network will pose a security threat for all users. The security threat stems from a flaw in the wireless security protocol, WEP. My proposal has focused on complementary technologies to solve the security flaws posed by wireless networking. The following

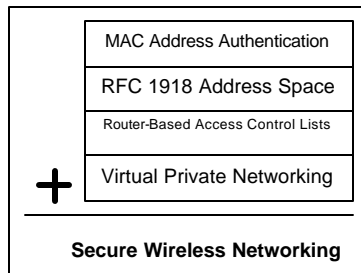
components compose the core security structure for a wireless network at Northeastern University.

- *Virtual private networking*
- *Access control lists*
- *RFC 1918 private address space*
- *MAC address authentication*

These technologies cannot provide a secure infrastructure by themselves, which is why they have been introduced in such a way that they build on each other to produce the final product (Fig 5).

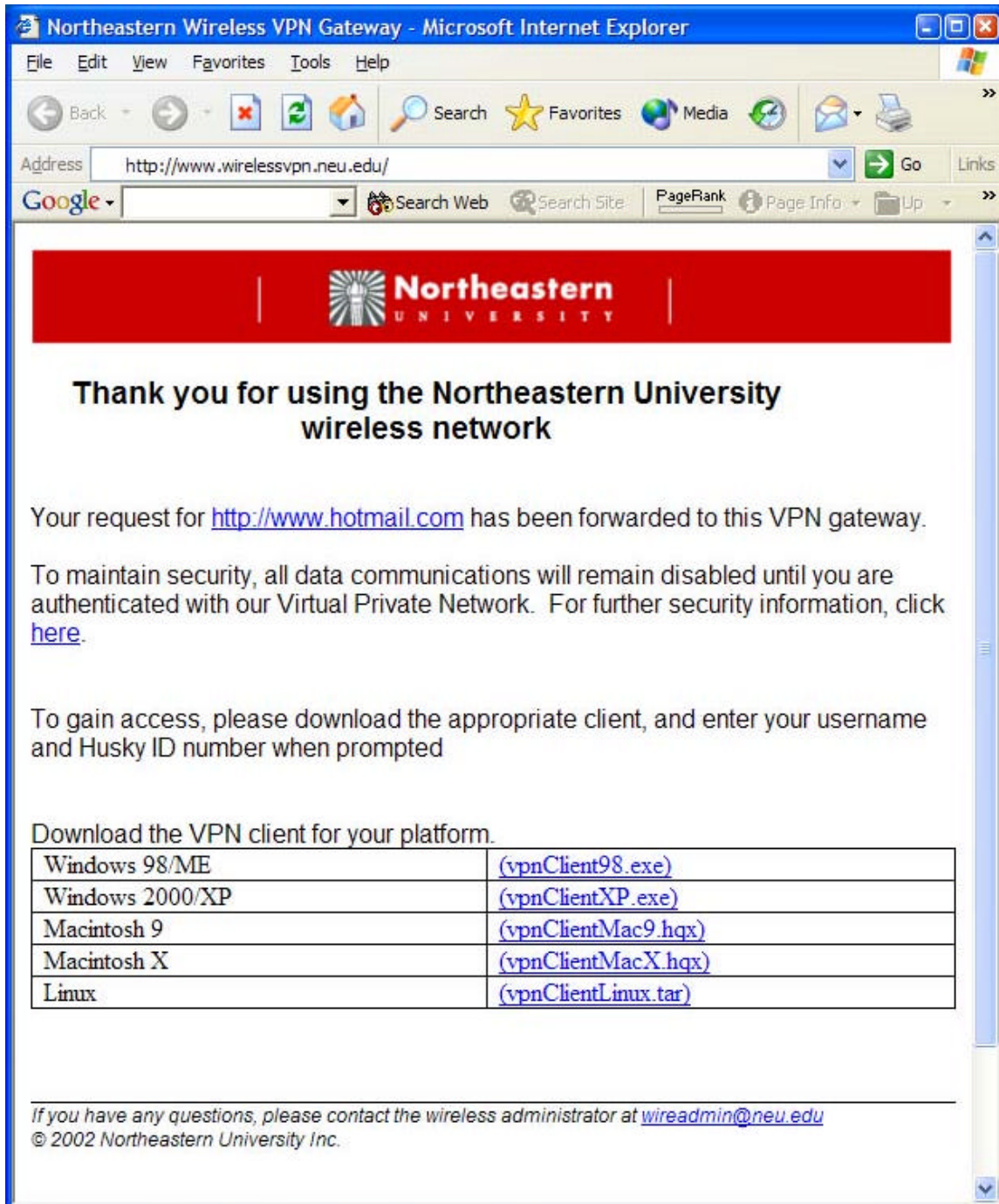
The components that were introduced in this proposal exist as separate entities that can be replaced and upgraded with equivalent technologies when needed. The technologies all follow IEEE standards to alleviate the pains of troubleshooting non-standard technologies. This proposal serves as an integrated plan to implement a secure wireless network at Northeastern University.

**Figure 5.**



*Component summary for secure wireless networking proposal*

Figure 6.



VPN gateway web interface

## Works Cited

- [1] AirSnort Homepage. "Frequently Asked Questions," AirSnort [Online] Available: <http://airsnort.shmoo.com/>
- [2] N. Borisov, I. Goldberg, D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *Proc. Of the seventh annual international conference on Mobile computing and networking*, ACM Press, New York, NY. pp 180-189
- [3] Enterasys Networks, "WLANA Security White Paper," Enterasys Knowledge Base [Online] Available: <http://www.enterasys.com/roamabout/WLANAsecwp.htm>
- [4] V. Gupta, G. Montenegro, "Secure and Mobile Networking," Mobile Networks and Applications, vol. 3 no. 4 1999 pp 381-390
- [5] S. Halevi, H. Krawczyk. "Public-key cryptography and password protocols," ACM Transactions on Information and System Security, vol. 2 no. 3, Aug. 1999 pp 230-268
- [6] E. Herscovitz. "Secure virtual private networks: the future of data communications," International Journal of Network Management, vol.9 no. 4, July-Aug 1999 pp 213-220
- [7] S.H. Park, A. Ganz, Zvi Ganz, "Security Protocol For IEEE 802.11 Wireless Local Area Network," Mobile Networks and Applications, vol. 3 no. 3, Sept. 1998, pp 237-246
- [8] E. Schirmer, "Technology in the Workplace," Buildings [Online] Dec 2001. Available: <http://www.buildings.com/Articles/detail.asp?ArticleID=564>