Global Information Assurance Certification Paper

Author: Josh Drumwright
Version: 1.4b Option 1
Title: Securing Your Home Router/Firewall/Access Point
Certification: Security Essentials, GSEC
Date: 2 March 2004

Abstract
In the year 2002 broadband use grew 60% to more than 33 million users connected within the United States. While at the same time those using "dial-up declined by 10%" to 74 million users[1]. All the while "40 - 50% of all new computers [that were] bought [went] in [to] a home with an existing computer."[2] Of these households, many are now sharing their broadband connections to multiple computers. There are many different ways that a household could share their Internet connection, from the use of an always-on computer sharing it's connection with other computers, to the use of a switch directly connected to a broadband device, and finally to the use of a stand-alone router. Of these different methods for sharing a broadband connection, the router option is probably the easiest and most popular method in use today. Additionally it allows households to take advantage of additional features of these devices such as built in wireless access points supporting the 802.11b standard, integrated firewalls, and integrated switches all in one device; all for between $30 to $70 at the local electronics retailer[3]. This document examines the insecurity of three of the most common devices used to share a broadband internet connection, the D-Link DI-514, Netgear MR814, and/or the Linksys BEFW11S4, stepping the novice user through locking down these three devices explaining as it goes the features and risks inherent with these devices and the steps required to address these risks.

Securing Your Home Router/Firewall/Access Point

I remember the day when I used to rush home from school to dial-up and check my Juno e-mail. This was only 7 years ago, no longer do I dial up to a 9.6kbps connection to check my e-mail. Instead now I connect via broadband at speeds never once dreamed about. This seems to be the trend, for example in the year 2002 broadband use grew 60% to more than 33 million users connected with in the United States. While at the same time those using "dial-up declined by 10%" to 74 million users. [4] All the while "40 - 50% of all new computers are bought to go in a home with an existing computer."[5] With these new computers being bought for the household, and Internet access almost being taken for granted; households are looking for ways to share that single broadband connection to the house.

There are many different ways that a household could share their Internet connection, from the use of an always-on computer sharing it's connection with other computers, to the use of a switch directly connected to a broadband device, and finally to the use of a stand-alone router. Of these different methods for

[1] Lewin, James. "Broadband use on the rise; Surfers hate to wait"
[2] Holliday, Clifford. "We have Found the 'Killer App' and We Are Killing It!"
[3] Bestbuy.com, "D-Link 802.11b Wireless Router", "Linksys 802.11b Wireless Router", "Netgear 802.11b Wireless Router"
[4] Lewin, James. "Broadband use on the rise; Surfers hate to wait"
[5] Holliday, Clifford. "We have Found the 'Killer App' and We Are Killing It!"

sharing a broadband connection, the router option is probably the easiest and most popular method in use today. Additionally it provides households the ability to take advantage of additional features of these devices such as built in wireless access points supporting the 802.1b standard, integrated firewalls, and integrated switches all in one device; all for between $30 to $70 at the local electronics retailer[6].

The Equipment

This paper was written based on the use of the D-Link DI-514, Linksys BEFW11S4 ver.2, and the Netgear MR814 v. 2 devices, configured and accessed using an IBM T30 laptop with integrated ethernet card. Wireless Access was obtained using a Lucent WaveLan Silver 802.11b PCMCIA Card, based on the Orinoco chipset. Additionally the Lucent Orinoco Gold card was used to test the devices after configuring them for increased security. My connection to the internet is provided by cable modem however this document isn't dependent on a connection through a cable modem, and the settings addressed in this document are equally applicable to any type of always on connection such as DSL, Cable, or any other Broadband/Ethernet based connection. The three routers used are some of the most popular networking devices used to share a broadband connection. A basic list of their features is found below.

	D-Link DI-514[7]	Linksys BEFW11S4 v. 2[8]	Netgear MR814 v. 2[9]
Network Access Translation (NAT)	P	P	P
802.11b Compliant	P	P	P
4 Port Switch	P	P	P
Web Based Management	P	P	P
Wireless MAC Address Filtering	P	P	P
WEP Encryption 64bit/128bit	P	P	P
VPN Pass-Through	PPTP, L2TP, IPSec	PPTP, IPSec	L2TP, IPSec
Stateful Packet Inspection Firewall	P	P	P
Content Filtering	P		P
Outbound Connection Limiting	P	P	P
DHCP Server	P	P	P
Supports Exposed Hosts (DMZ)	P	P	P
Supports Port Forwarding	P	P	P

[6] Bestbuy.com, "D-Link 802.11b Wireless Router", "Linksys 802.11b Wireless Router", "Netgear 802.11b Wireless Router"
[7] D-Link "2.4 GHz Wireless Router"
[8] Linksys, "Wireless Access Point Router"
[9] Netgear, "Cable/DSL Wireless Router"

Configurable Firewall	P		
Wireless Range (Indoors/Outdoors)*	328'/984'	300'/1500'	660'/1485'
Warranty**	1 Year	1 Year	3 Year

* Actual results vary depending on operating environment; ** Conditions apply.

Understanding Device Features

Network Address Translation (NAT) – Commonly called NAT, Network Address Translation is the fundamental concept that allows multiple network devices to connect through a broadband sharing device such as a router. Essentially NAT takes the Internet Protocol (IP) address that was issued to you by your Internet Service Provider (ISP) and assigns that to the outside (Internet facing) port on your networking device (router). Your router then assigns a second set of private IP addresses to internal connections (those either directly plugged into one of the switched ports, or connections using the wireless network) such as your computer. The device running NAT then takes requests from the private IP range and sends them out over the Internet facing port with a public IP address (provided by your ISP).[10] As requests from various machines on the internal network are passed out through the ISP provided IP address, NAT keeps track of which request went out over which port so that it can route replies to the appropriate address on the internal network.

802.11b Compliant – The 802.11b standard is an IEEE standard for Wireless communication. It specifies how an 802.11b network card will interoperate with other 802.11b networking devices whether it is another network card or a wireless access point. What 802.11b compliance simply means is that a device supporting the standard will communicate with any other device that supports the standard, for example your Linksys Router would connect to a D-Link network card even though they are made by different companies.[11]

4 Port Switch – The four-port switch contained in each of these devices allows for multiple wired devices to connect to a single broadband-wired connection. While only four ports are provided directly in the device, additional ports could be added with another networking device such as stand alone hub or switch. Additionally the 4-port switch doesn't limit the number of wireless connections to only 4.

Web Based Management – Some networking devices are managed by Simple Network Management Protocol (SNMP) or via a telnet client. Web Based Management means instead that the device may be configured and managed via a web browser. Requiring only a connection to the device and a supported web browser. Web Based Management can be significantly easier to use than SNMP or telnet. This is achieved by providing a user friendly GUI that makes configuring a device with a Web Based Management Interface as easy as point and click, for even the most novice user.

[10] Tyson, Jeff. "How Network Address Translation Works"
[11] Brenner, Pablo. "A Technical Tutorial on the IEEE 802.11 Protocol"

Wireless MAC Address Filtering – Every network card has a unique identifying address called a MAC address. This address has nothing to do with the Macintosh computer, instead MAC stands for Media Access Control address. This address is a unique address assigned by the manufacturer of the device i.e., Intel or Linksys. Since MAC addresses are unique and no two devices are assigned the same address by manufacturers, MAC address filtering can be used as a measure to prevent unauthorized access to a wireless network.

WEP Encryption 64bit/128bit – WEP stands for Wired Equivalent Privacy and is part of the 802.11 standard. It is an algorithm based on the RC4 encryption algorithm and was designed to protect communication over wireless connections from eavesdropping. Additionally WEP can be used to prevent unauthorized devices from connecting to a network running WEP.[12]

VPN Pass-Through – Virtual Private Networking (VPN) pass-through is a feature that allows for computers connected to a networking device such as a router to use VPN to connect to a secured network, effectively passing through the router and firewall. This feature is typically used by telecommuters wishing to connect securely back to a corporate network. There are three main types of VPN's; those that use Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IP Secure (IPSec). However not every device claims to support pass-through of every protocol. Note: Just because a router supports VPN pass-through doesn't necessarily mean that you will be able to connect using VPN to a secure network, as your Internet Service Provider (ISP) may not support this type of connection across their network.

Configurable Firewall – The Firewall devices on most home Internet appliances such as the Netgear and Linksys Wireless Access Point/Firewall/Switch/Router use NAT and/or Stateful Packet Inspection (SPI) to provide a firewall protecting your computer only from inbound connections. Connections that you may not have originated from requests by clients within your network. However a truly configurable firewall will go a number of steps beyond this. The only device that contained a firewall that allowed advanced configuration was the D-Link device. The configurable firewall on this device allowed the administrator to limit which external IP addresses would be allowed to access which internal IP addresses and/or ports on the intranet. Additionally it limited which internal addresses could access specific external and/or internal addresses and/or ports. For example the administrator could block all internal users from accessing port 21 (FTP), or could allow all requests from 198.82.*.*(an external network block) to go to port 80 on 192.168.0.2 (an internal machine) and block all others requesting the same resource.[13]

Content Filtering – This feature is aimed at parents/employers wishing to restrict

[12] Borisov, Nikita, Goldberg, Ian and Wagner, David. "Security of the WEP algorithm"
[13] D-Link Router Help Files within Administrative Interface.

content that their children/employees may or may not be viewing, and works in different ways on different devices. However it generally involves blocking either domains and/or keywords.

Outbound Connection Limiting – This feature allows a router administrator to prevents certain hosts from gaining access to the Internet. These machines are still able to connect to other resources on the local network but connections could not be made from these machines outside the network. This feature might be used to prevent a user on your local intranet from using the Internet.

DHCP Server – DHCP stands for Dynamic Host Configuration Protocol, and is a protocol used to automatically configure the TCP/IP settings such as IP address, subnet mask, DNS servers and default gateway, all without user input.[14] This allows for new devices to essentially self configure themselves without the user having to have an understanding of either the address scheme in use or the settings for their internet service provider. Having a DHCP Server built into a broadband router also means that even if a users connection to the internet is lost they will still be able to maintain a connection with other devices on the local area network; and even obtain a new IP address when logging on.[15]

Supports Exposed Hosts (DMZ) – Exposing a host in a DMZ or De-Militarized Zone essentially sits the host out in the open on the Internet even though that device is physically connected to an internal port on your router. This functionality is typically used for machines used to play games, or that require certain port ranges to be open that are being blocked by the firewall. An alternative to having an exposed host would be to forward certain ports to a particular machine.

Supports Port Forwarding – Port forwarding is a function that allows a user to run a server behind the firewall on a specific port and have all requests to a specific port on the router forwarded to that port on the server. For example, a server may run the Apache web server on port 80. With port forwarding configured to forward all requests on port 80 to the Apache web server. If any request is received by the firewall on port 80 it will be forwarded to the Apache web server. If however a request came in on port 21 (FTP) and no port forwarding was configured for this port then the connection would simply be dropped. The difference between Port Forwarding and exposing a host by placing that machine in a DMZ is that port forwarding only opens up certain ports, where exposing a host, exposes the whole machine and every port on it.

Stateful Packet Inspection Firewall - A Stateful Packet Inspection Firewall examines packets that are received by the firewall and determines if they are the result of a request that originated within the Local Area Network, if they are then

[14] Droms, Ralph. “Resources for DHCP”.

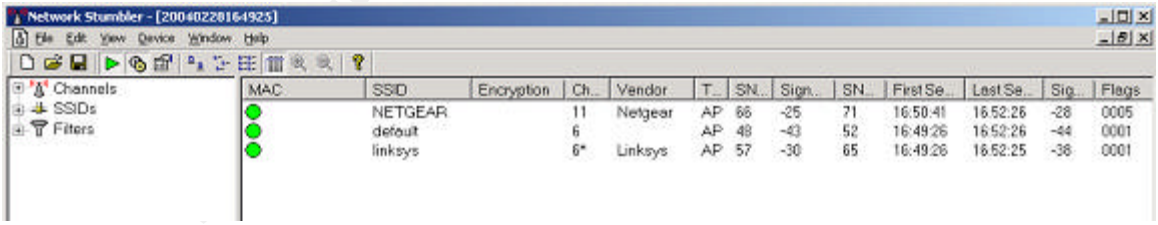
the firewall lets these packets through, if they are not, the firewall simply discards them. [16]

Wireless Range (Indoors/Outdoors) – The distance over which a wireless signal from the wireless access point can be received using a network card. The wireless range of any wireless device however can vary greatly depending on certain environmental factors, such as steel beams, microwaves, and other types of interference that limit a devices range. Additionally the range for some devices can even be increased using third party amplifiers, a subject not discussed here.

In-Security in the Devices Default Configurations

Now that you understand the basic features that each of these devices contains lets take a look to see how secure these devices are straight out of the box. To begin I setup all three devices resetting each one to it's default settings by using the hardware reset button on each device to purge any settings that I might have configured for each device. Note: If you plan on resetting your device in this manner, make sure to take note of your existing settings, as the resetting of your device will purge the devices settings.

After resetting each device to it's factory settings I began by opening up my laptop and using Network Stumbler (NetStumbler), to discover the wireless access points that were broadcasting in my area. Almost immediately I discovered the D-Link DI-514 (SSID of default), the Linksys BEFW11S4 v. 2 (SSID of Linksys), and the Netgear MR814 v. 2 (SSID NETGEAR). This tells us that all three Wireless Access Points are broadcasting their default SSID's, and that none of these devices have Wired Equivalent Privacy turned on which can be determined by looking at the Encryption column of the Network Stumbler results. This didn't surprise me in the least bit as these devices were likely designed for ease of setup as the number one goal instead of having been designed with security as the number one goal.

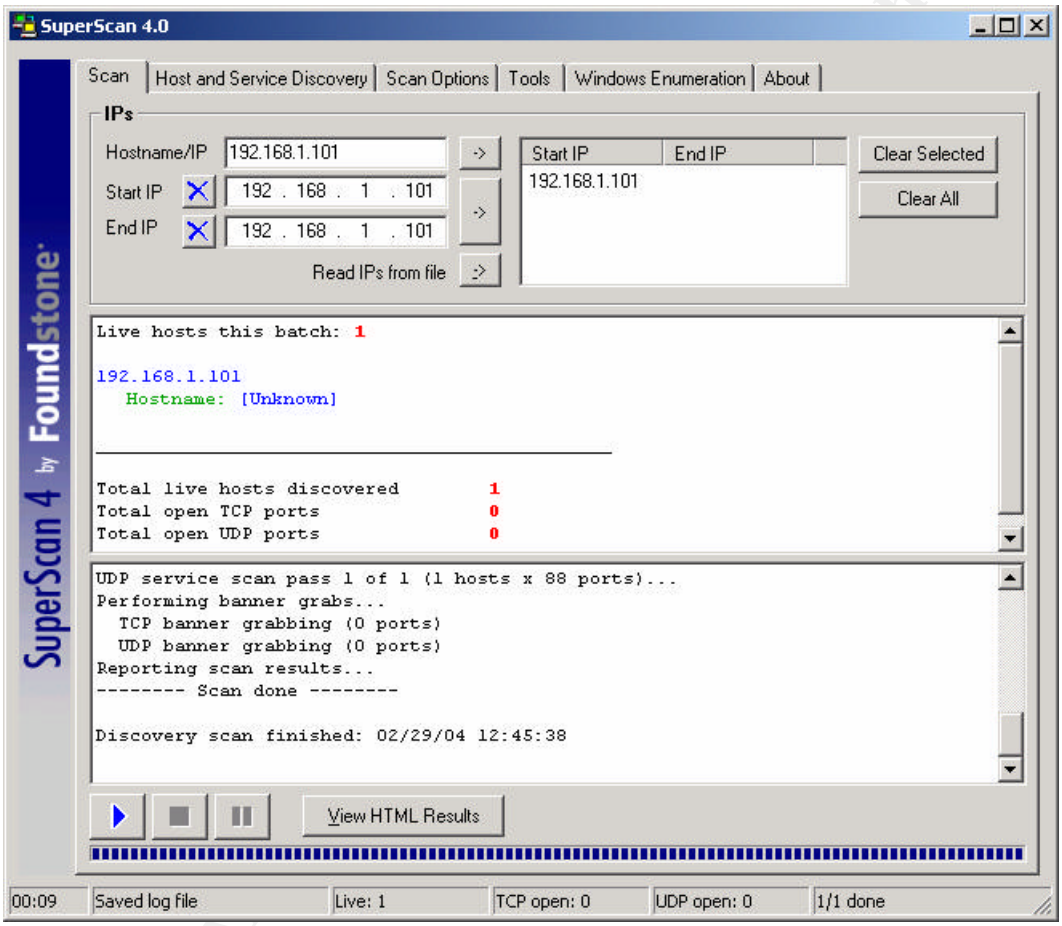


Network Stumbler (NetStumbler) Scan of my three Wireless Access Points. *Note: MAC addresses covered for privacy.* Network Stumbler can be downloaded free from http://www.netstumbler.com/.

Additionally I was able to connect and obtain an IP address lease through DHCP for each of these three devices without any type of authentication or authorization. This confirms that out of the box no MAC address filtering was in use. These devices each were essentially open wireless networks which

[16] Complex. "Stateful Packet Inspection Firewall"

presented a sizable security risk to a home network regardless of whether or not it is being used to access corporate applications on your companies corporate intranet or simply for checking your e-mail. After determining that the wireless connection had significant vulnerabilities I used version 4.0 of the SuperScan tool by FoundStone to scan each device Internet facing port to determine if the router had any open ports or was replying to ICMP pings. From my scans using SuperScan I didn't discover any ports open on any of the three devices. However SuperScan did discover that the D-Link DI-514 device did reply to ICMP pings with the manufacturers default configuration.



This is a discovery scan using SuperScan 4.0 on the D-Link DI-514 connected on 192.168.1.101. SuperScan 4.0 by FoundStone can be downloaded free from Foundstone, who can be reached at http://www.foundstone.com/.

The discovery scans for the D-Link DI-514 and Netgear MR814 v. 2 were performed with my laptop, and these two devices connected directly to internal ports on the Linksys BEFW11S4 v. 2. The scan of the BEFWS4 v. 2 was performed with a laptop and this device connected to the Netgear MR814 v. 2. Based on this configuration only the D-Link responded to any ICMP pings. To rule out false positives/false negatives I performed a remote ping using Tracert.com's ping tool available at http://www.tracert.com/cgi-bin/ping.pl. Based on the use of this site ICMP replies were still received from the D-Link device,

while both the Netgear and Linksys devices had 100% packet loss, meaning they didn't reply to ICMP pings on the WAN/Internet port.

Additionally each of the devices I configured contained a Web Based Administrative Interface residing on a standard port (80) at a known IP address (either 192.168.0.1 or 192.168.1.1) and was accessible using a well known user and password combination. To see how easy it was to determine the password for one of these devices I performed a Google search using Linksys+Router+Password as my search criteria, and the first link returned garnered me the default user name and password for the Linksys Router I was using. Needless to say there is a substantial security risk until a user changes this password. Someone might try to argue that Remote Administration isn't on by default, thus no one outside my network could access the administrative functions of the device. This is quite true, however in this case, anyone that is able to access your device by either wireless or via a switched local (non-internet facing) port on your router is considered part of your local network and could therefore access the administration interface of your device. This means that not just your computers can access this interface, but also computers of someone across the street if they are within range of your wireless network.[17]

So what does this mean?
The default configuration of these three networking device is akin to a double-edged sword; in that they provide a NAT firewall, yet they also ship with a completely open wireless network enabled. The firewall for these devices didn't have any ports open based on my tests, providing a reasonable level of protection from port scans and other such discovery scans originating on the Internet. However behind the firewall sits a completely open wireless network that anyone in range could join, thus bypassing the firewall. And this doesn't even address the fact that the administration interface is publicly available (via wireless) with a well-known address and user/password combination.

Essentially this means that you've increased the security of your networks internet facing port, by using a firewall; however you have reduced some of this protection by opening up your network to those around you. Picture this, you build a brick wall around your neighborhood to protect your house from the evil things that lurk outside your neighborhood, but you leave your back door wide open to neighbors whom you don't know, which might be just as evil. To succinctly say it "You're exposed!" Have no fear, the remainder of this document steps through remedying this exposure.

	D-Link DI-514	Linksys BEFW11S4 v. 2	Netgear MR814 v. 2
Secure with Default Configuration	**No**	**No**	**No**

[17] Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practices"

Following my initial testing of the D-Link DI-514 with it's default configuration, the device began to experience problems. For this reason the remainder of this document will not include step-by-step instructions for securing the D-Link DI-514. See the lessons learned section at the end of this document for a full description of the issues experiences with the D-Link DI-514.

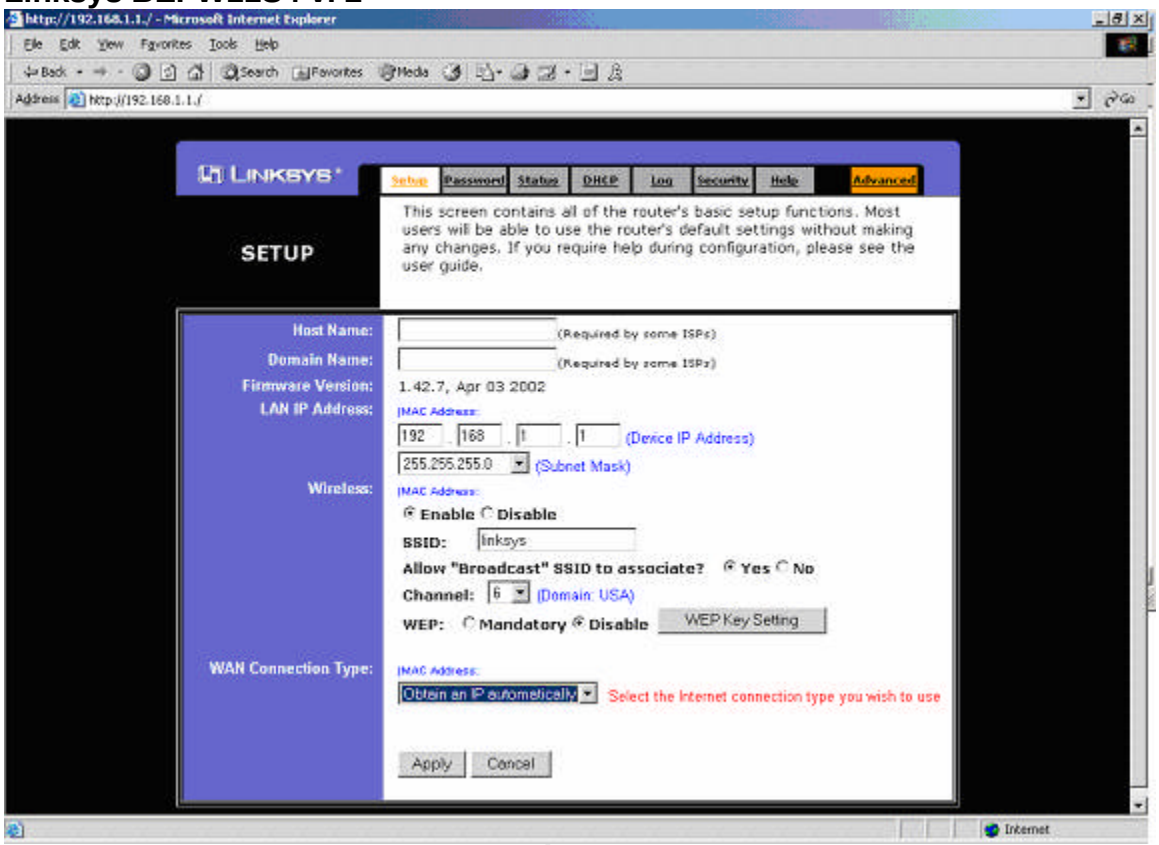
Securing the Out of the Box devices

Securing the D-Link DI-514, Linksys BEFW11S4 v.2, and Netgear MR814 v. 2 is actually a fairly simple process that even the most novice user can accomplish. The directions that follow will walk you through eight simple steps to providing a relatively secure wireless connection using any of these three devices. While other devices are not discussed here, the concepts addressed in the pages to follow can be applied to any device with the same functionality whether it is an 802.11a/b/g device by one of these manufacturers or another manufacturer. These concepts when implemented appropriately provide a reasonably secure wireless and wired network. By no means do these settings provide a absolutely secure network, to begin the Wired Equivalent Privacy used to encrypt transactions can be hacked, MAC addresses can be spoofed, etc. However without going as far as implementing a VPN solution (VPN between client and wireless access point) the use of WEP, MAC filtering, and other basic security measures will provide a reasonable level of security to your home environment. Regardless, the first step to providing this level of security is to login to the device. When logging into your device it is strongly recommended that you be physically connected to the device with a wired connection as settings that will be configured will take effect instantly. For this reason configuring your device via a wireless connection may result in a dropped connection, forcing you to connect to the device using a physical connection.

Logging in:

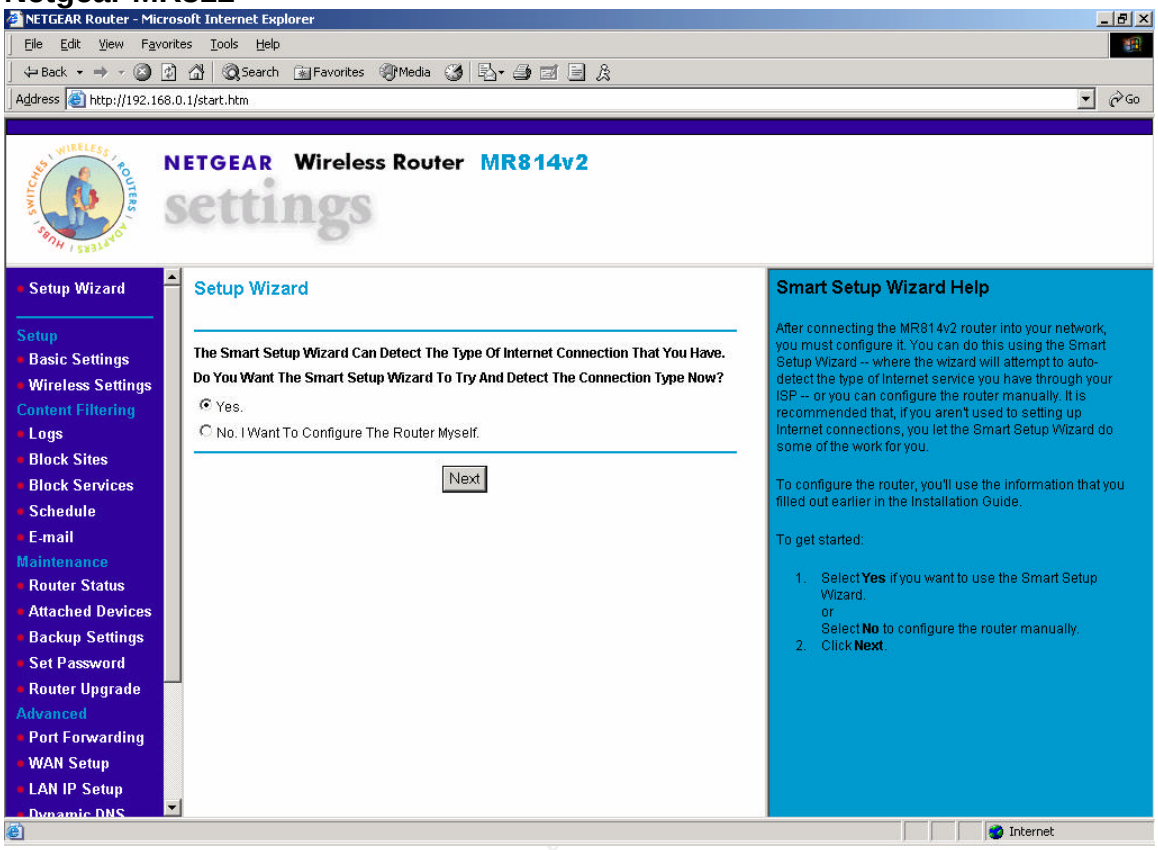
Begin by logging into to your networking device. This can be achieved by pointing your browser to the administrative interface address for your wireless router, and logging on using the credentials provided. (See below for a screen shot of the main router interface, the devices administrative interface address, and the standard login credentials used to connect to this interface.)

Linksys BEFW11S4 v. 2



Device Administration Address: http://192.168.1.1
User Name: admin
Password: admin

Netgear MR812



Device Administration Address: http://192.168.0.1
User Name: admin
Password: password

If you've gotten this far you've successfully logged into your networking device. Now it's time to begin the process of enhancing the security of your device.

Step One: Change your Administrator Password (Required)
The D-Link, Linksys, and Netgear routers each use a Web-Based Administration Interface to manage the configuration of their settings. Access to this interface is simply obtained by browsing to the devices administrative address i.e., 192.168.1.1. Such administrative addresses and their user name and password combinations are easily found on manufacturers websites. With a default user name and password and a completely unprotected wireless network with SSID that is broadcasting, anyone can attach to your network and begin to configure it. For this reason your very first step after plugging your device in should be to change it's password. Access to the administrative interface to your device could provide a potential attacker a list of all connected devices, allow an attacker to place a host outside the firewall by configuring them in a DMZ, provide a log of inbound/outbound activity, and/or allow an attacker to open up the remote administration port so they could manage your network from anywhere in the world at a later time. By obtaining a list of network devices attached to your network or a log of network activity a potential attacker could gain a better understanding of devices connected to your network and their use. This information might be useful to an attacker in planning an attack against your network. By configuring one of your devices to use the DMZ, an attacker could effectively place the device outside the protection of your firewall exposing it to the Internet. By opening the remote administration port for your router an attacker could open up weaknesses in your routers software and/or open up your router for configuration later from a location outside the range of your wireless connection. This step is simple to implement, waste no time in performing the steps required to change the default password for your device.

Linksys:

1. Click on the 'Password' tab at the top of the main page.
2. Delete the values in the fields to the right of 'Router Password:'
3. Enter a password into the first field to the right of 'Router Password:'
4. Enter this password into the second field to the right of 'Router Password:' to confirm your new password.
5. Click the 'Apply' button.

A message saying, "Settings are successful." will be displayed.

6. Click the 'Continue' button.

You will be required to login again since your password has changed.

Netgear:

1. Click on the 'Set Password' Link from the left menu.
2. Enter your old password (the original password is 'password') into the box labeled 'Old Password'
3. Enter your new password into the box label 'New Password'

4. Enter your new password again into the box labeled 'Repeat New Password'
5. Click the 'Apply' button.

You will be required to login again since your password has changed.

Step Two: Disable Wireless (Optional)

The D-Link, Linksys, and Netgear devices used in the document all contain a Wireless Access Point. It is this Wireless Access Point that gives others the opportunity to connect to your network through the use of wireless. These individuals could simply want to obtain free Internet access, or could have malicious intent, such as hacking into the FBI's website. Either way it would be you who would pay for their deeds; whether it is $39.95 to provide them with free Internet. Or having 15 armed federal agents show up at your door to confiscate your computer and networking equipment. If you don't plan on using the Wireless Access Point feature of your router, disable it to prevent potential abuses by unauthorized individuals using your network access. Then proceed to Step Eight. If you plan on using the Wireless Access Point feature frequently go to Step Three.

Linksys:

1. From the main page (Setup Tab) browse down to the 'Wireless:' section
2. Directly to the right and down one line are two radio buttons, select the 'Disable' button.
3. Click the 'Apply' button.

A message saying, "Settings are successful." will be displayed.

4. Click the 'Continue' button.

NetGear:

1. Click on the 'Wireless Settings' link from the left menu
2. Remove the check from the box labeled 'Enable Wireless Access Point' in the 'Wireless Access Point' section of this page.
3. Click the 'Apply' button to apply these settings.

You may be prompted to select the correct region for your location. If prompted, select the appropriate region for your location. And click 'Apply' again.

Step Three: Disable SSID Broadcast (Required)

Skip this step if you disabled wireless in Step Two

Imagine this, your friend boots up his computer with a built in wireless card. It instantly finds a network that it connects to. Kind of cool huh! Actually it is, unless that network is yours. What just happened is actually fairly simple. Your friend's computer's wireless card was set to associate with any SSID (network name). Since your Wireless Access Point was broadcasting its SSID, your friend's computer saw the broadcast. After seeing the broadcast your friend's computer tries to connect; connecting successfully. Chances are that if your friends computer can do this, so can other computers. What makes this possible is that

your router is broadcasting its SSID. This is essentially like putting up a billboard saying “free internet here”. By disabling SSID Broadcast you no longer are advertising that a wireless access point is available. This means that computers that are not configured to look for your SSID will not see your network as an available network. This also means that you will be required to configure each of your wireless network cards to look for your wireless access point.

Linksys:

1. From the main page (Setup Tab) browse down to the ‘Wireless:’ section
2. Find the ‘Allow "Broadcast" SSID to associate?’ options (yes/no).
3. Select the ‘No’ radio button.
4. Click the ‘Apply’ button

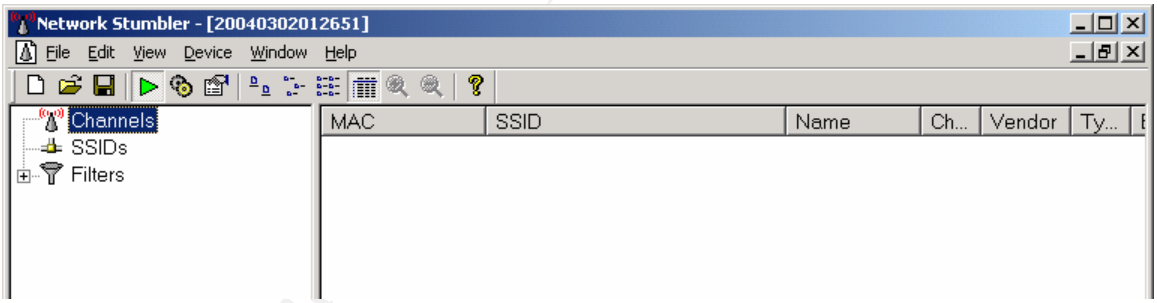
A message saying, “Settings are successful.” will be displayed.

5. Click the ‘Continue’ button.

Netgear:

1. Click on the ‘Wireless Settings’ link from the left menu
2. Remove the check from the box labeled ‘Allow Broadcast of Name (SSID)’ in the ‘Wireless Access Point’ section of this page.
3. Click the ‘Apply’ button to apply these settings.

You may be prompted to select the correct region for your location. If prompted, select the appropriate region for your location. And click ‘Apply’ again.



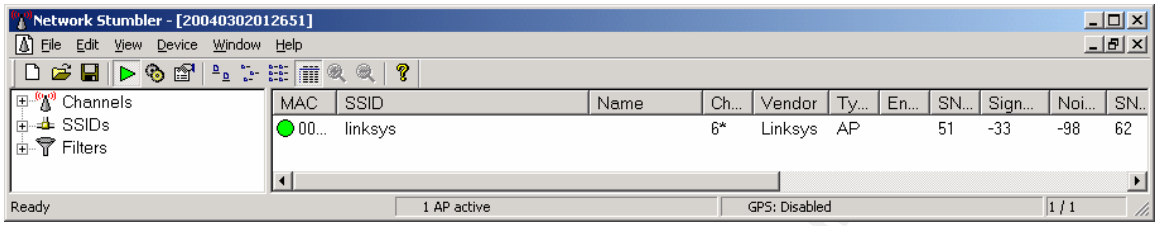
After disabling SSID broadcast, Network Stumbler no loner picks up any of the three Wireless Access Points.

Step Four: Change SSID (Required)

Skip this step if you disabled wireless in Step Two

While step three disabled the broadcasting of your SSID. You also must take into account the fact that there are only but so many different manufacturers of Wireless Access Points. Since your devices SSID is set to its default value, it is likely that someone around you will have a network card configured to listen to the default settings of your router. This may be by chance or it may be by intent. Either way someone could gain access to your network by trying a relatively short list of SSID values i.e., ‘linksys’, ‘NETGEAR’ or ‘default’. Not changing your SSID makes it trivial for someone actively looking for a wireless connection to find your device and ultimately gain access to the Internet. In choosing a SSID/network name make sure to avoid the obvious such as ‘wirelessnetwork’,

your families name, your address, your e-mail address, don't use any private information such as your password, nor should you use a name that might be easily guessed. Instead use an easy to remember name that others outside your family/organization wouldn't be able to guess. Take note however that this SSID is case sensitive and will need to be configured in every client that will be connecting to your network.[18]



Configuring my SSID to 'linksys' a known default SSID for Linksys devices instantly finds my Access Point even though it is not broadcasting.

Linksys:

1. From the main page (Setup Tab) browse down to the 'Wireless:' section
2. Find the box labeled 'SSID:'
3. Change the value in the box labeled 'SSID:' to your new SSID name.
4. Take note of the SSID you have entered, as you will be required to configure your network card using this SSID as the network name/SSID that you wish to connect to.
5. Click the 'Apply' button

A message saying, "Settings are successful." will be displayed.

6. Click the 'Continue' button.

Netgear:

1. Click on the 'Wireless Settings' link from the left menu
2. Within the 'Wireless Network' section find the text box labeled 'Name (SSID):'
3. Change the value in the box labeled 'Name (SSID):' to your new SSID name.
4. Take note of the SSID you have entered, as you will be required to configure your network card using this SSID as the network name/SSID that you wish to connect to.
5. Click the 'Apply' button.

Step Five: MAC Address Filtering (Required)

Skip this step if you disabled wireless in Step Two

As mentioned in step two open Wireless Access Points provide a ready opportunity for unauthorized individuals to connect to your network without your permission. These individuals could be in search of a free Internet connection. Or they could be in search of an Internet connection from which to launch an attack on a corporation or government entity. Either way it would be your Internet

[18] Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practices"

connection that was providing them with unrestricted access to the World Wide Web. Wireless networks unlike traditional wired networks lack defined borders. In a wired network you can physically secure who has access to a port by locking a door or a room. However in the wireless world you don't have this luxury. While hiding your access point by disabling the broadcast of it's SSID and changing it's SSID are good steps to protecting your network they still leave your network wide open. To address this issue we will implement MAC Address Filtering, which is one step that is commonly used to authorize machines to connect to a wireless network. A MAC address is a unique hardware address assigned by each networking devices manufacturer. It has nothing to do with the Macintosh computer. By setting up an Access Control List or Authorized MAC address list you essentially are telling your router which MAC addresses you wish to connect to your access point. Those devices that are not on this list will still be able to see that your access point exists but will not be able to readily receive a DHCP lease from your DHCP server. For most honest users, those that might have once inadvertently connected to your network this will likely be enough to prevent them from accessing your network.

Linksys:

1. Click on the 'Advanced' tab from the main page(Setup Tab highlighted).
2. Click on the 'Wireless' tab
3. Scroll down till you see a section labeled 'Station MAC Filter:'
4. Click on the button labeled 'Edit MAC Filter Setting'
5. Enter the MAC address you wish to allow to have access to your wireless access point.
6. Click the 'Apply' button.

A message saying, "Settings are successful." will be displayed.

7. Click the 'Continue' button.

Repeat from number 4 until all devices are added.

8. Select the 'Enable' radio button.
9. Click the 'Apply' button.

A message saying, "Settings are successful." will be displayed.

10. Click the 'Continue' button.

Netgear*:*

1. Click on the 'Wireless Settings' link from the left menu
2. Click on the 'Setup Access List' button
3. Place a check in the 'Turn Access Control On' box
4. Click the 'Add' button
5. Enter a label for your wireless card/device that will connect to your access point into the blank labeled 'Device name'
6. Enter the MAC address of your wireless card into the 'MAC address' field

For PCMCIA cards the MAC address is generally written on the bottom of the card and looks something like 00-00-00-00-00-00-00 and may contain letters, and may or may not contain dashes.

7. Click the 'Add' button.

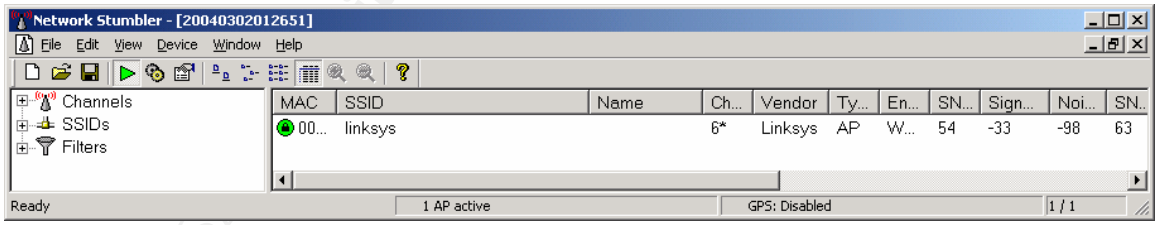
Repeat as needed to add each of your wireless devices

8. Click the 'Apply' button

Step Six: Implement WEP (Required)

Skip this step if you disabled wireless in Step Two

MAC address filtering was the first actual step we took towards limiting the individuals that have access to our network. It however doesn't address who has access to the information flowing across our wireless network. With a wired network, part of its security rests in the fact that physical access can be restricted. Restricting physical access allows us to control the devices and wires over which data flows. The same holds true for wireless connections, however the wires are now non-existent and the packets flow through the air. What this means is that the data that was previously being sent across a wire in plain text is now being sent in mid-air in plain text (with no encryption). Anyone that sniffs these packets would then be able to see your unencrypted traffic i.e., e-mail, the URLs you are requesting, even your plain text passwords. To address this issue, the Wired Equivalent Privacy (WEP) algorithm can be used[19]. Based on the RC4 algorithm WEP seeks to prevent eavesdropping through the use of a shared secret key. It encrypts data at the network card, which is then decrypted again at the access point. WEP essentially encrypts the contents flowing between the wireless access point and a wireless device preventing the average user from observing the contents of requests traversing a wireless network. While preventing eavesdropping was the only intended function of WEP specified in the 802.11 standard, WEP is also used for authorization. In using WEP for authorization an access point only allows communication with devices that share a secret key. Therefore devices that do not have this shared key are unable to communicate with the access point. This prevents them from accessing either the local area network (and hosts on it) or the Internet via the wireless access point. [20]



After configuring the Linksys network device for WEP a lock appears on the Green circle next to it's MAC address within the Network Stumbler utility.

Linksys:

1. From the main page (Setup Tab) browse down to the 'Wireless:' section
2. Find the 'WEP:' section
3. Select the 'Mandatory' radio button.
4. Click the 'WEP Key Settings' button

[19] Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practices"
[20] Borisov, Nikita, Goldberg, Ian, and Wagner, David. "Security of the WEP"

If you failed to 'select 'Mandatory' first and clicked on 'WEP Key Settings' you will be prompted with a box saying "Do you want to change WEP status to Mandatory?" Click 'OK'

5. Select the encryption strength supported by your card. Make sure to reference the documentation provided with your network card as your card my not support the 128bit encryption strength. For example my WaveLan card does not.
6. Enter a passphrase into the box labeled 'Passphrase'
7. Click the 'Generate' button.
8. Select which key to use, either 1, 2, 3, or 4.
9. Click the 'Apply' button.

A message saying, "Settings are successful." will be displayed.

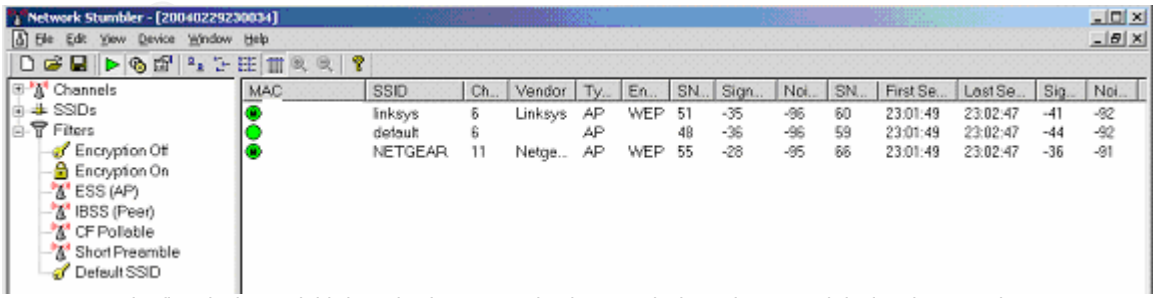
10. Click the 'Continue' button.

You will want to take note of the keys that were generated and which one you selected, as these values will be required for use by your network card.

Netgear:

1. Click on the 'Wireless Settings' link from the left menu
2. In the 'Security Encryption (WEP)' section set the 'Encryption Strength' to your desired encryption strength, either 64bit or 128bit.
3. Make sure to reference the documentation provided with your network card, as your card may not support the 128bit encryption strength. For example my WaveLan card does not.
4. In the 'Security Encryption (WEP) Key' section enter a pass phrase in the box labeled 'Passphrase'
5. Click the 'Generate' button.
6. Select which key you will use, either key 1, 2, 3, or 4 by selecting the radio button next to the key of your choice.
7. Take note of the keys that were generated and which one you selected, as these values will be required for use by your network card.
8. In the 'Security Encryption (WEP)' section set the 'Authentication Type' to *Shared Key*.
9. Click the apply button.

You may be prompted to select the correct region for your location. If prompted, select the appropriate region for your location. And click 'Apply' again.



You can see the first device and third Device have WEP implemented where the second device doesn't. The SSID's were turned on so NetStumbler could see these devices.

Step Seven: Reduce Number of DHCP Leases Issued (Recommended)
Each and every computer that connects to your networking device will require an IP address. Most of these network devices (i.e. a network card) will obtain their IP address via DHCP. To reduce the chance that a device accessing your network without authorization will receive an IP address through DHCP, you can do one of two things. Either turn DHCP off and use static IP addresses, or limit the total number of DHCP leases that are issued by the DHCP server. The easier of these two solutions is to limit the total number of IP address leases issued by the DHCP server. When determining the number of DHCP leases to issues you will want to consider the total number of devices using DHCP that you will want to have connected to your network. Once you make this determination you will be able to configure the DHCP server to only issue that many leases. Therefore once these leases have been issued, there will be no additional leases available for an unauthorized machine to obtain. However should an unauthorized device obtain an IP address you would quickly be able to determine that an issue was occurring, as another one of your devices would be unable to obtain a DHCP lease. [21]

Linksys:

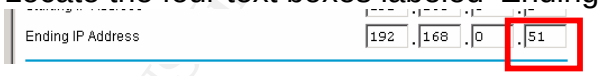
1. From the main page click on the 'DHCP' tab at the top of the page.
2. Change the text box labeled 'Number of DHCP Users:' to be the total number of devices that will be using DHCP to obtain network settings from your device. Make sure to include both wired and wireless devices in your count.
3. Click the 'Apply' button.

A message saying, "Settings are successful." will be displayed

4. Click the 'Continue' button.

Netgear:

1. Click on the 'LAN IP Setup' link found under the 'Advanced' section on the left hand side of the page.
2. Locate the four text boxes labeled 'Ending IP Address'



3. Change the fourth text box to be the one plus total number of devices that you will be using DHCP to obtain network settings from your device. Make sure to include both wired and wireless devices in your count. For example if have 8 devices that you wish to connect using DHCP you would want to enter the number 9 into this box.
   Additionally the Netgear router allows you to tie an IP address to a MAC address, however this feature is not discussed here.

[21] Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practices"

Step Eight: Disable ICMP Ping on WAN port

Both the Netgear and Linksys routers didn't respond to ICMP ping requests based on their default configuration. However the D-Link device did reply to ICMP ping requests. Essentially what this means is that the internet facing router port will confirm that a device is actually present at X.X.X.X should another device send a ICMP ping request to this address. This may sound harmless, and it likely is. However if the WAN port does not reply to an unsolicited request the requester will likely conclude that no device exists at the probed address, and will likely move on leaving your router alone. However since the D-Link device does reply to ICMP pings it confirms that a device does indeed exist at the specified address. This may result in a potential attacker taking a further look at your router. Disable this function on your router if it is enabled. Both the Netgear and Linksys routers come with this feature turned off. Unless there is a reason for it to be enabled, it should otherwise remain disabled.

Relatively Secure: A Recap

Looking back it is almost amazing to believe that 8 steps so simple go undone for many a router around the country. However since you followed these 8 simple steps your administrator password for your network device is no longer the default password. Your SSID has been changed and it is no longer being broadcast. Your Wireless Access Point is using WEP and MAC address filtering. And finally, you have limited the number of DHCP licenses available for issue. Or you disabled wireless altogether as are not using this functionality. These 8 simple steps have taken your device from completely wide open to invisible and nearly impossible to penetrate for the everyday user. No longer will a Network Stumbler Scan reveal even the presence of a network in your home, nor will a Super Scan discovery scan alert an attacker of the potential presence of a machine at your IP address. It should be mentioned however that while your network is now near impossible for the everyday user to gain access to your network. It however is not completely secure. The WEP protocol has known weaknesses. MAC addresses can and are spoofed everyday. However with adequate security precautions such as only accessing private information through the use of encryption (such as SSL) you shouldn't have any worries.[22]

Lessons Learned/Looking Back:

Whenever you go through a process, whether be it driving to work, or configuring a router you learn something. The primary lessons that I learned during the writing of this document center around the use of the D-Link DI-514 device. When I initially obtained this device I had no trouble configuring it, scanning it with both SuperScan 4 and NetStumbler and connecting via LAN ports. However through the use of this device (about 1 week) the device lost functionality. Specifically it began to take longer and longer to obtain a DHCP lease from the device. The WAN (internet facing port) had significant trouble requesting an IP address via DHCP from my Internet Service Provider (unlike either the Netgear

[22] Fisher, Ken. "Security Practicum: Essential Home Wireless Security Practices"

of Linksys devices). Additionally I had particular trouble accessing the administrative interface for the device. Furthermore I had particular difficulty achieving a connection via the wireless access point for this device despite the devices claim to be fully compatible with 802.11b. Specifically, I was never successfully able to make an outbound connection using the wireless connection. However I was able to obtain a DHCP lease from the router. Even when I wasn't able to connect out via wireless I was able to see the access point in NetStumbler This was extremely disappointing, as the D-Link device appeared to have the best feature set of all three devices. For example the D-Link device was the only device to provide both User and Administrator accounts and to provide a more restrictive firewall based on both port and address for both inbound and outbound connections.

References:

BestBuy.com. “D-Link 802.11b Wireless Router” URL:http://www.bestbuy.com/site/olspage.jsp?id=1057490485294&skuId=5765166&type=product (24 February 2004)

BestBuy.com. “Linksys 802.11b Wireless Router” URL:http://www.bestbuy.com/site/olspage.jsp?id=1051384294158&skuId=4221407&type=product (24 February 2004)

BestBuy.com. “Netgear 802.11b Wireless Router” URL:http://www.bestbuy.com/site/olspage.jsp?id=1051384568683&skuId=4790676&type=product (24 February 2004)

Borisov, Nikita, Goldberg, Ian and Wagner, David. “Security of the WEP algorithm” URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (29 Feb 2004)

Brenner, Pablo. “A Technical Tutorial on the IEEE 802.11 Protocol” 1997. URL: http://www.sss-mag.com/pdf/802_11tut.pdf (01 March 2004)

Compex. “Stateful Packet Inspection Firewall” URL: http://www.cpx.com/whitepapers/Compex%20SPI%20Firewall.pdf (29 Feb 2004)

D-Link. “2.4GHz Wireless Router” D-Link Di-514 Product Package (24 February 2004)

D-Link. Router Help Files within Administrative Interface (01 March 2004)

Droms, Ralph. “Resources for DHCP”. 22 November 2003. URL: http://www.dhcp.org/ (29 February 2004)

Fisher, Ken. “Security Practicum: Essential Home Wireless Security Practices” URL: http://www.arstechnica.com/paedia/w/wireless-security-howto/home-802.11b-1.html (01 March 2004)

HansenOnline.com. “Linksys Etherfast Cable/DSL Router” URL: http://www.hansenonline.net/reviews/linksys.html (02 March 2004)

Holliday, Clifford. “We have Found the 'Killer App' and We Are Killing It !” URL: http://www.igigroup.com/policy/app3.html (29 February 2004)

Lewin, James . “Broadband use on the rise; Surfers hate to wait” 29 January 2003. URL: http://www.itworld.com/nl/ecom_in_act/01292003/ (29 Feb 2004).

Linksys. “Wireless Access Point Router” BEFWS4 ver. 2 Product Package (25 Feb 2004)

Linksys. Router Help Files within Administrative Interface (01 March 2004)

Netgear. “Cable/DSL Wireless Router” MR814 Product Package. (25 Feb 2004)

Netgear. Router Help Files within Administrative Interface (01 March 2004)

Page, Sharon. “Secure Wireless At Home?” 3 February 2003.
URL: http://www.giac.org/practical/GSEC/Sharon_Page_GSEC.pdf (29 Feb. 2004).

Tracert.com. “Multiple Ping v0.96”
URL: http://www.tracert.com/cgi-bin/ping.pl (29 Feb 2004)

Tyson, Jeff. “How Network Address Translation Works”
URL: http://computer.howstuffworks.com/nat.htm (01 March 2004)

Webopedia. “DHCP” URL: http://www.webopedia.com/TERM/D/DHCP.html (29 Feb. 2004)

Webopedia. “NAT” URL: http://www.webopedia.com/TERM/N/NAT.html (29 Feb. 2004)

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor