Global Information Assurance Certification Paper

Securing Your Wireless Access Point: What Do All Those Settings Mean Anyways?

Joe Scolamiero

Version 5.1b

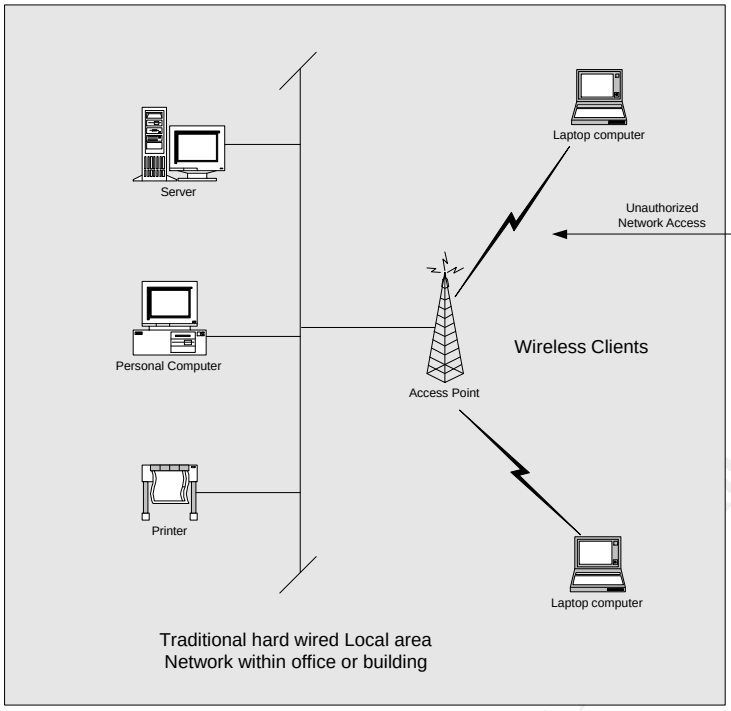
GIAC / GSEC

Submitted 4/20/04

Abstract

This paper started out as a reference guide for users at my place of employment to secure their wireless LANs. After researching wireless security, and seeing that it is not the most secure platform out of the box, I decided to create a step by step guide for users to be able to secure their wireless networks at home. I had an eight page document that was basically screen shots with brief descriptions of how to lock down a Linksys wireless router and a wireless Linksys network interface card. A friend of mine reviewed the document and asked what all of the settings really meant. After hearing that, I thought that this would be a great paper to build upon and answer some of these questions for myself as well as others who were making these changes without really knowing why they were doing them.

There are currently a lot of worries about wireless security. Standard networks at home or at work are based on physical connectivity. There is a network interface card that plugs into a personal computer that has a network cable plugged into it. You plug the other end into a hub or switch and you are on the LAN. You then configure DHCP or get a static IP address and you are ready to go. With wireless there is no physical connection. Wireless access points are really radio transmitters. They use radio waves that can go through walls and buildings. This makes connecting to a local network in your home or place of employment very versatile. You don't need all of those cables laying on the floor or hanging out of the walls. The downside is that connecting to your network as an intruder is a lot easier. Security considerations now have to be taken to prevent unauthorized access to your network and data. So if you do not take precautions, passers by with the right equipment and tools can hijack a connection onto your LAN and off they go. The diagram on the next page shows a traditional hard-wired LAN with PCs, printers and a hub or switch. It also shows the access point, which is the radio transmitter receiving and transmitting data to and from your wireless devices in your facility. Although, on the right there is an intruder listening and eavesdropping onto your LAN without your permission. To prevent this act, wireless vendors have implemented different levels of security which I will try to show over the next few pages.



The following pages detail the changes necessary to secure a wireless network access point and the wireless end nodes that are connected to it. The example network equipment used to create this document were the Linksys Wireless Router model number BEFW11S4, (2.4GHz 802.11b, running code version 1.44) and a Linksys Wireless PC laptop card, model number WPC11 version 3 running code version 1.04.02.00. Although this document uses the previously identified Linksys equipment as an illustration example, these security principles remain the same with any wireless access equipment, and should be implemented if the equipment supports them.

To start securing these devices, there are three sections that need to be addressed. The first section will describe the SSID (Service Set Identifier) parameter. Secondly, we will talk about MAC address filtering and then, we will go into WEP (Wired Equivalent Privacy) and the encryption features that this will enable. The last section that we will talk about is the next generation security for wireless, WPA (Wi-Fi Protected Access) and 802.11i. Hopefully this will address any security questions that you might have related to 802.11 wireless home networks.

SSID (Service Set Identifier)

The SSID (Service Set Identifier) is the first parameter that gets talked about when wireless LAN security is discussed. This is a 1 to 32 alphanumeric character string that is used to identify membership to an access point (AP) in a wireless local area network (WLAN). An access point (AP) is a wireless device, also known as a base station, which will accept wireless communications from wireless devices such as a laptop with a wireless network interface card (NIC). The AP acts as the link between the wireless network and the hard-wired local area network. All wireless devices that want to communicate on the WLAN need to have their SSID set to the same string as the AP. This string, SSID, is also referred to as the network name. On the next page is a table that lists the default SSID names that some of the well known wireless vendors ship their products with. The wireless router (access point) has its SSID set to some alphanumeric name. The wireless clients can have their SSID set manually or automatically by leaving it blank. If your client is not going to set its SSID, you can try to access the AP as long as the AP is still broadcasting its SSID. By default, the AP will broadcast the SSID in clear text in the packet header of every wireless packet. Most wireless vendors allow the network administrators to disable the "broadcast SSID" feature. If we are to secure this WLAN, we will want to disable the SSID broadcast feature on the AP. By disabling this feature, we will force all clients to have their SSID manually set to the same as the AP. This will prevent eavesdroppers from attaching to our network and surfing the web from our AP or gleaning any confidential information that might be communicating over our WLAN. The use of a packet sniffer, or wireless hacker tools such as AirSnort (http://airsnort.shmoo.com/) or Netstumbler (http://www.netstumber.com/) can be used to decode clear text data and even allow the security parameters, that we are putting in place, to become ineffective. Once we implement WEP (Wired Equivalent Privacy), we will have set up basic encryption, but it is crackable by the hacker community. Next generation wireless standards will include much more secure ciphers that will make it much harder for hackers to crack. The next few pages will show examples of how to set your SSID and disable the "broadcast SSID" feature on your WLAN.

Vendor Default SSIDs - Table A-1[1]

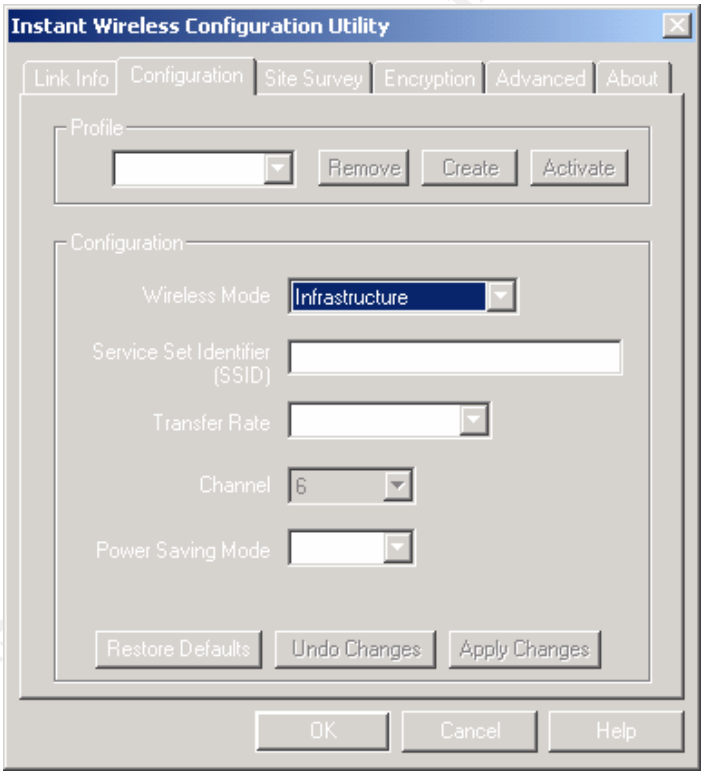
Vendor	Default SSID	Vendor	Default SSID
Cisco	tsunami	Compaq	Compaq
3Com	101 or comcomcom	Dlink	WLAN
Netgear	Wireless	Linksys	linksys

[1] URL - **http://www.cirt.net/cgi-bin/ssids.pl**

Securing the Access Point

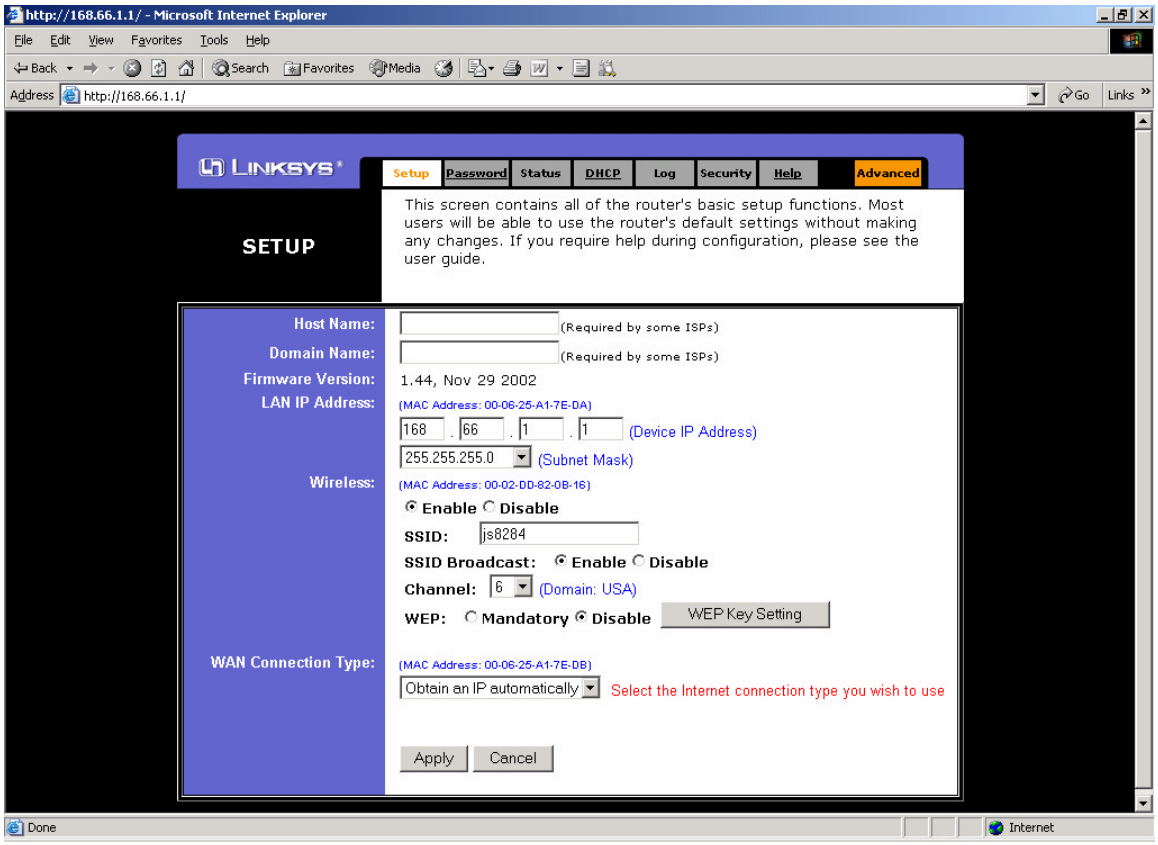
The SSID (Service Set Identifier)

Start by changing the SSID (Service Set Identifier) from the factory default to something more secure. Use of a random password generator using the maximum allowable characters for the SSID string is recommended, however for this example we will change it to js8284 (it is best to use a combination of letters and numbers since it will be harder to crack). It is also highly recommended to change this parameter at regular intervals for added security. ***One more important point to make is that you will need a PC to browse into the IP address of the wireless router prior to making any changes. If you try to make the changes to the router from your wireless PC card, you will lose connection as soon as you make the changes.***



Setting the SSID on the Wireless Card- Figure 1.

Go to your PC's Wireless Configuration Utility and select the **Configuration** tab. Set the SSID to **js8284** or any secret passphrase that you select, and make note of it, since you will need to match this up with the SSID on the router. Then hit the **Apply Changes** button, then **OK.** See Figure 1. above for detail.



Setting the SSID on the Wireless Router- Figure 2.

Now using the PC that is connected to the router, browse into the router and log on. On the **Setup** tab, set the SSID on the router to **js8284** or whatever you used as the SSID on the wireless card and hit **Apply**. By doing this you have made the first step in preventing people from accessing your wireless network and surfing the web on your broadband connection. See Figure 2.above.

The next step is even easier, and prevents hackers who might be scanning your neighborhood, from cracking your SSID and hijacking your network. This is done by making a change on your router. On the screen above, locate the **SSID Broadcast Enable/Disable** Radio buttons, and change the setting from enable to **disable**. At this point I would recommend that you verify that you can still connect to the network and surf the web. If you cannot, do not proceed and review the settings. If it still does not work, reboot your laptop or device that has the wireless network card. If it still does not work, reboot your wireless router. If all looks good, you're ready to go and you have set up enough basic security to get you going. If you want to set a higher level of security, proceed to the MAC address filtering section of our document.

MAC Address Filtering

Every device that connects to a network has a unique hardware address called a MAC address (Media Access Control). This address is a 48-bit address expressed as 12 hexadecimal digits. This 12 digit hex number can be broken down even further into two fields. The first part of the MAC is a 24 bit vendor code[2]. This identifies what vendor has made this particular network device. This manufacturer code is called the Organizational Unique Identifier (OUI). A few examples of different vendor MAC addresses are:

3Com 00-10-4b-6e-6e-1b (This is the MAC address and is a 3Com)

Linksys 00-06-25-a1-7e-da (This is the MAC address of my Linksys AP)

Cisco 00-00-0c-24-32-67 (This is a MAC address of a Cisco device)

The underlined digits in the above MAC addresses are the vendor codes. You can lookup these vendor codes at the following web site http://standards.ieee.org/regauth/oui/index.shtml[3]. The last 24 bits in the MAC address is the serial number of the network interface card.

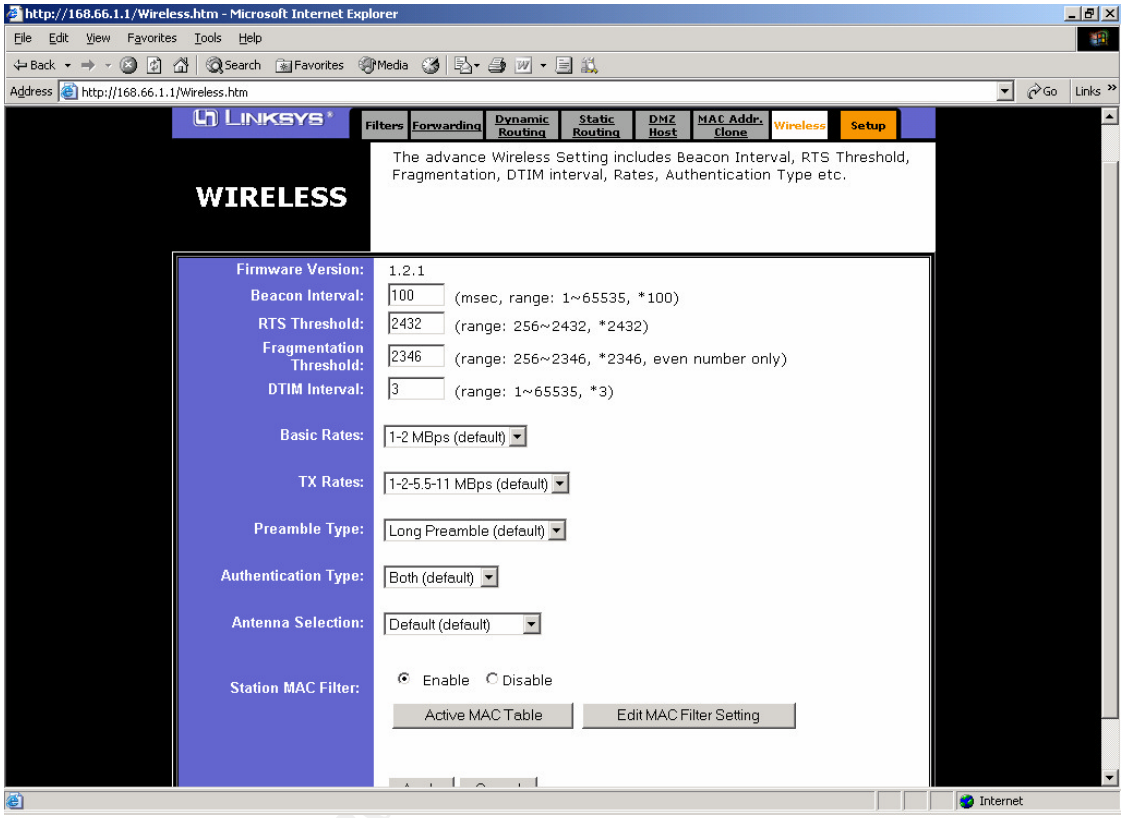
So, we can identify our Access Points by the SSID, but how can we uniquely identify our wireless clients. We can identify them by their unique MAC address. So, by creating a list of unique MAC addresses we can restrict what PCs can connect to the AP. This is called MAC address filtering. If a PC with an unknown MAC address tries to connect, he will not be able to associate with the AP and thus will not be allowed to connect. This feature along with the previous SSID lockdown provides a great way to start securing your wireless network. MAC address filtering is easy to do on small networks, but does not scale well if you have to maintain a large network. This will turn into a network management nightmare. If one of your clients ever replaces a network card, you will have to reprogram the filter table. Since this document is directed at smaller wireless LANs, it should be easy to implement. The next few pages will document the steps that are needed to identify and implement MAC address filtering.

Setting Up Static MAC Address Filtering

[2] Cisco Press p43

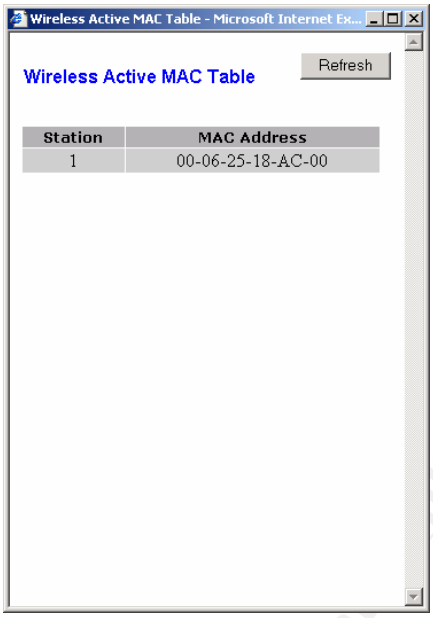
[3] http://standards.ieee.org/regauth/oui/index.shtml

This step will secure your network even more. Here we will allow only specific wireless network cards to connect the wireless router. This is done by setting your MAC address into the wireless router MAC address filter table.



Setting MAC address filtering on the Wireless Router - Figure 6.

Using your web browser, connect to the router and log in. Click the orange **Advanced** tab in the upper right hand corner. Next, select the **Wireless** tab. Near the bottom of the screen locate the **Station MAC Filter Enable/Disable** radio buttons and select **Enable**. This will activate the filter table. Click on the **Active MAC Table** box and proceed to the next page. The MAC address in the box labeled Station 1 is the only wireless device connected to the AP.



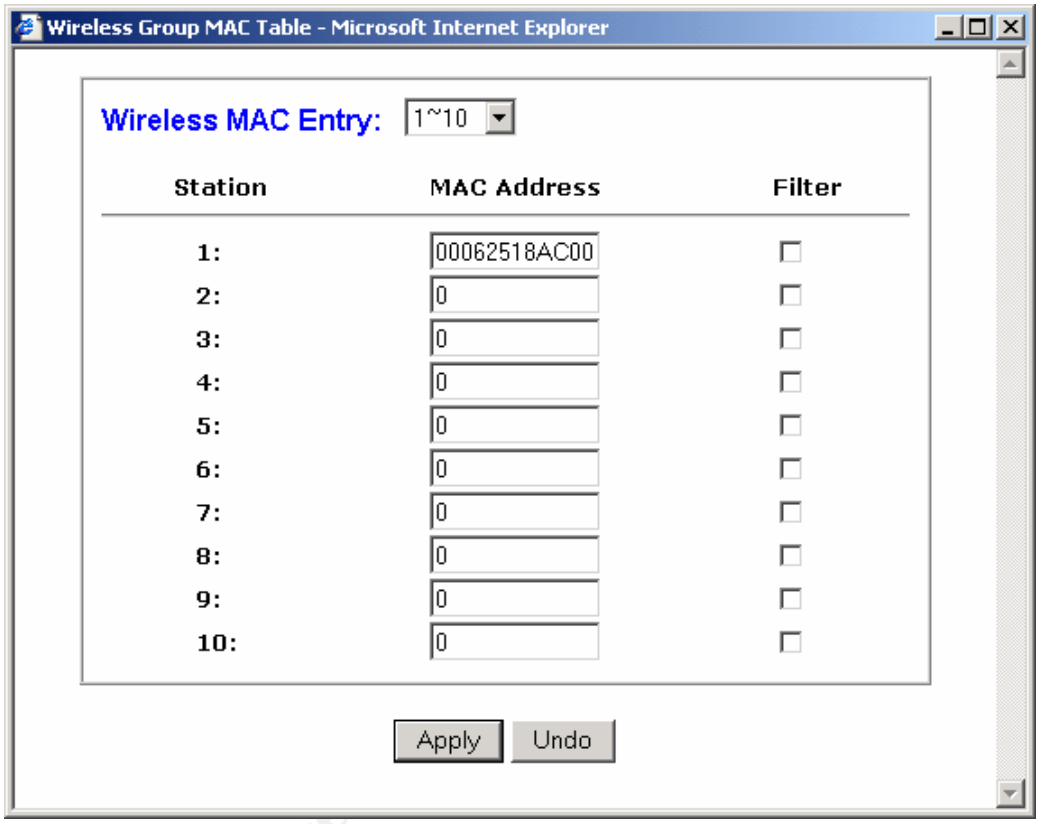
Determining Your MAC address on the Wireless Router - Figure 7.

Record the MAC address in the above screenshot; this is your MAC address. If you see more than one MAC address in the screen, either you have someone else in your household with a wireless card, or someone else is using your wireless router to surf the web. If you want to verify the MAC address of your PC, execute the following command from a command prompt (c:\>**ipconfig/all**). View the screenshot below. Look for the line labeled Physical Address. In this example it is **00-06-25-18-AC-00.**

```
C:\>ipconfig/all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : lappy-k8mcjcu4i
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Broadcast
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : ne2.client2.attbi.com

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : ne2.client2.attbi.com
        Description . . . . . . . . . . . : Instant Wireless Network PC Card V3.
0
        Physical Address. . . . . . . . . : 00-06-25-18-AC-00
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 168.66.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 168.66.1.1
        DHCP Server . . . . . . . . . . . : 168.66.1.1
        DNS Servers . . . . . . . . . . . : 63.240.76.19
                                            204.127.198.19
        Lease Obtained. . . . . . . . . . : Monday, March 08, 2004 7:27:31 PM
        Lease Expires . . . . . . . . . . : Tuesday, March 09, 2004 7:27:31 PM
```

Verifying Your MAC Address From Your PC - Figure 8.

Close out this previous window after recording the MAC address. Click on the box that says **Edit MAC Filter Settings** in **Figure 6**. In the box beside Station 1 enter the MAC address that we previously recorded. Enter the number without the dashes in the address as below, then click **Apply**.



Entering Your MAC Address into the Filter Table - Figure 9.

Click **Apply** in the next window and you are done. You should see the wireless card reset and reconnect. At this point you should try to surf the web to verify that you have completed this whole process successfully. If you have problems reboot the PC or the router and try again. The next section in this document will go into encryption. It will explain 802.11 encryption and then give examples of how to configure WEP on your Access Point and your wireless network interface card.

Wired Equivalent Privacy (WEP)

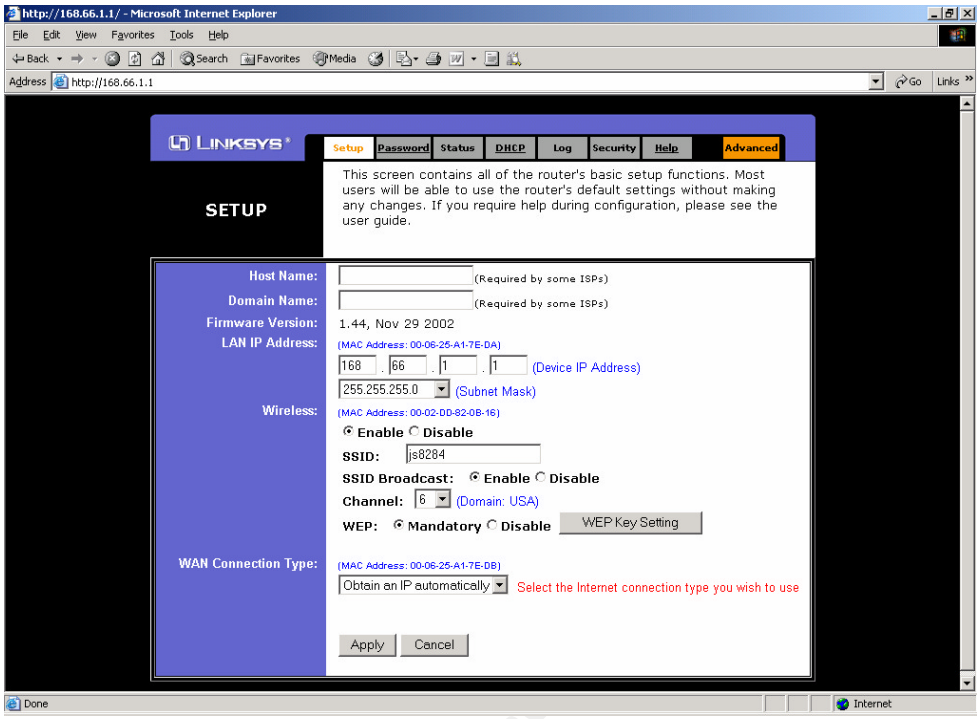
802.11 wireless has implemented a security protocol called WEP (Wired Equivalent Privacy). All members of the wireless network use WEP to encrypt and decrypt communications between their wireless client and the AP. It basically turns clear text data into secret code. WEP makes use of RC4 (Ron's Code 4 Pseudo Random Number Generator) symmetric stream cipher using an encryption key[4]. In 802.11 networks using WEP, you can use 64 or 128 bit keys, which you will see later when you create the encryption keys. The key can be broken down into two pieces. There is a 24 bit Initialization Vector (IV) and a secret key. If you have a 64 bit key, it consists of a 24 bit IV and a 40 bit secret key. If you have a 128 bit key, it has the same size 24 bit IV, but has a 104 bit secret key. RC4 combines a 40-bit or a 104-bit WEP key with a 24 bit random IV. The result is encrypted data. There are many concerns about the size of the IV, 24 bits. Using 24 bits as a value will give you 16 million possible values for the IV[5]. This may seem like a large number, but in computer terms it is not that large or difficult to crack. Another problem is that the IV is sent in clear text in the header of the 802.11 packet. This makes it easy to intercept. Once you have the IV, you can get hacker tools that will allow you to break the WEP data. The best way to beat this is to change the keys often. Next generation security will fix this problem as we will see. So for now, we should at least implement WEP, along with changing the SSID, disabling SSID broadcasting, and static MAC filtering to get us to the first phase of wireless security. There may be many holes in WEP, but it was a good start, and since out of the box wireless is wide open, this is a good start. Next we will proceed to the WEP configuration of the Linksys devices.

Configuring Wired Equivalent Privacy (WEP)

---

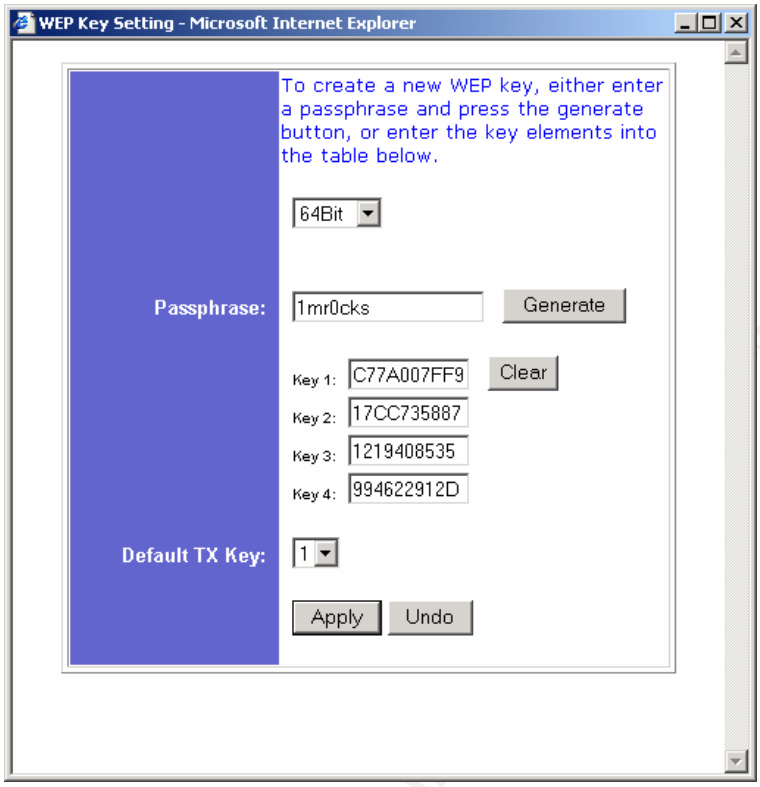
[4] **http://www.dell.com/downloads/global/vectors/wireless_security.pdf**

[5] **http://www.nwfusion.com/research/2002/0909wepprimer.html**



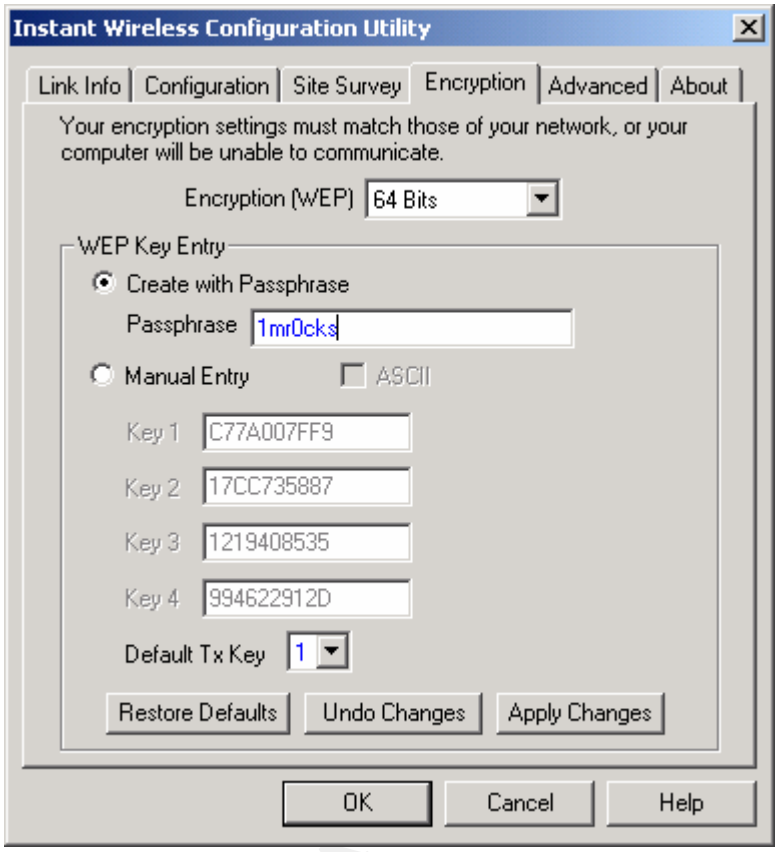
Setting the WEP Encryption on the Wireless Router - Figure 3.

In this section, we will have to determine whether you want to use 64 bit or 128 bit encryption. The higher the encryption the better, but if you have a slower PC you might want to back off to 64 bit. You will also need to provide a WEP passphrase which is used to generate your encryption keys. First, on the **Setup** tab of the screenshot above, locate the **WEP: Mandatory/Disable** radio buttons. Enable the **Mandatory** button. Next, select the **WEP Key Setting** button just to the right. A new WEP Key Settings menu will open up. Proceed to next page.



Setting the WEP Keys on the Wireless Router - Figure 4.

Here we will set up the encryption level, the passphrase, and generate the keys. In the example, I will be using **64 bit** encryption since I have a slower PC. I will set a hard-to-crack passphrase of **1mr0cks** and then click **Generate**. You will see the four keys populate in the fields. Click **Apply** to turn on encryption. See Figure 4. above. We will now have to match up these changes to the wireless interface card, so proceed to the next page.



Setting the WEP on the Wireless Card – Figure 5.

Now we have to match up the encryption setting on the wireless card to match the router settings we just made. Start up the Instant Wireless Configuration Utility and select the **Encryption** tab. Click the pulldown beside the **Encryption (WEP)** and select your encryption method. The one that I selected in the previous section was **64 bit**, so that is what I will select. Now you need to set the passphrase which matches the settings you previously made on the router, **1mr0cks** is what we selected. Click on **Apply Changes** and hit **OK**.

You should see your wireless PC card reset and reconnect. At this point, make sure that you can connect to the network and surf the web. If you have successfully browsed the web, you have now succeeded in setting up encryption and locking down your wireless LAN. At this point you have successfully prevented your SSID from being broadcast, changed the default SSID, instituted MAC address filtering and started to encrypt your data between your PC and the AP. At the current time, this is the best we can do. Remember to change your SSID often along with changing your WEP key as frequent intervals. The next section will talk about the next generation in wireless security.

WPA and 802.11i Encryption

WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) is the next level of securing wireless communications. It is an industry supported version of encryption that is being used as an interim solution until 802.11i is ready. WPA uses the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, including using dynamic keys. Using TKIP is expected to keep security rolling ahead until 802.11i is ready later this year. WPA is supposed to eliminate the two main problems with WEP, authentication and encryption. WPA will also to be an easy upgrade for users since it is usually just a firmware upgrade. This will most likely involve a chip replacement which is fairly easy. If you are in the market for new Wireless hardware, look for devices that are WPA enabled. Linksys offers WPA in its 802.11g WRT54G wireless router. Linksys also plans to have firmware upgrades available for 802.11b routers such as the one in this exercise. Make sure that all of your devices are WPA enabled before implementing this in your environment.

WPA uses TKIP to take care of the weaknesses in WEP encryption, while still using RC4 as a stream cipher. TKIP will force keys to be exchanged and redistributed more often and on a scheduled interval. This will make it more difficult for a hacker to decrypt your keys and break into your network. With WPA, "wireless clients begin with a 128 bit shared secret, referred to as a temporal key (TK). The client's MAC address is mixed with the TK to produce a phase 1 key. The phase 1 key is then mixed with an initialization vector (IV) to develop per-packet keys. Each key is used with RC4 to encrypt one data packet"[6]. This is supposed to take care of the weakness in the RC4 key used in WEP since the keys are rotated regularly. The IV has also been increased from 24-bits in WEP to 48-bits in WPA. This will increase the chance of the key being repeated and thus it makes it more difficult for a hacker to break your encryption.

For authentication, WPA uses a combination of server based, 802.1x, and EAP (Extensible Authentication Protocol). The 802.1x port based authentication works as follows. Initially a wireless user (called a supplicant) authenticates to the wireless LAN via the AP (called the Authenticator). The AP will not allow the user to connect to the network until access has been granted by an authentication server such as RADIUS or LDAP. The AP, using WPA sends the user credentials encrypted to the authentication server. The authentication server verifies the user and his rights and sends the information to the AP. The AP allows user access and assigns him encryption keys. Now the wireless client has gained network access. "WPA is also capable of operating in

[6] http://www.isp-planet.com/fixed_wireless/technology/2002/better_than_wep.html

what's known as "pre-shared key mode" if no external authentication server is available, such as in homes and small offices"[7].

This newer security protocol, WPA, for wireless is much improved over the somewhat easily crackable WEP. It is, however, just an interim solution until 802.11i is ready for prime-time. 802.11i is scheduled to be ready for the release in 2004, but we will see.

802.11i (Next Generation Wireless Security)

802.11i is an overhaul to the first generation security in WEP. WPA is a subset of 802.11i, which has a lot of the functionality of 802.11i. It will also address the weaknesses that WEP has in encryption and authentication, just as WPA did. 802.11i will include features such as 802.11x port-based authentication, TKIP (Temporal Key Integrity Protocol) key exchange and Advanced Encryption Standard (AES) encryption. AES will replace RC4 as the encryption scheme. It will also include a new security standard called Robust Security Standard (RSN). RSN will require new hardware for both the client wireless device and the Access Point. The much more advanced levels of encryption used will need more horsepower on both the client and the AP to support new functionality. The 802.11i task force has also setup a transitional standard called Transitional Security Network (TSN). This standard will allow older WEP systems and newer RSN systems to operate in parallel on the same Wireless LAN[8]. If you have the resources available, it is suggested to upgrade your WLAN to 802.11i once it has been formally released. This will guarantee that you are operating at the most secure level available at this time. Reality dictates that this will be a phased-in implementation which will allow a migration to the newer levels of security rather than a forklift upgrade. Since 802.11i is not yet released, WPA is the best choice currently available and it can be achieved at a reasonable cost, due to the fact that it is just a firmware upgrade. I hope that this document offers some valuable information for people who have similar concerns as I. Again, this started out as a quick reference guide for my wireless home users and evolved into the document before you. I hope that you will gain as much knowledge from document as I have gained in creating it. Thank You…

References

[7] http://www.wi-fiplanet.com/tutorials/article.php/2148721

[8] http://dailywireless.org/modules.php?name=News&file=article&sid=2347&src=rss09

1 - No Author Specified, “Default Wireless Configurations”

URL - **http://www.cirt.net/cgi-bin/ssids.pl**

2 – Cisco Systems Press, edited by Laura Chappell. Introduction to Cisco Router Configuration. Macmillan Technical Publishing. 1999. p43

3 – No Author Specified. “IEEE OUI and Company id Assignments”. April, 2004. URL: **http://standards.ieee.org/regauth/oui/index.shtml**

4 – Dell Computer. “Wireless Security in 802.11 (Wi-Fi) Networks”. Jan, 2003. URL:
http://www.dell.com/downloads/global/vectors/wireless_security.pdf

5 – iLAbs Wireless Security Team. “What’s Wrong With WEP?”. Sept, 2002. URL:
http://www.nwfusion.com/research/2002/0909wepprimer.html

6 – Phifer, Lisa. “Better Than WEP”. Feb, 2002. URL:

http://www.isp-planet.com/fixed_wireless/technology/2002/better_than_wep.html

7 – Geier, Jim. “WPA Security Enhancements”. Mar. 2003. URL:
http://www.wi-fiplanet.com/tutorials/article.php/2148721

8 – No Author Specified. “Planning for 802.11i”. Apr, 2004. URL:
http://dailywireless.org/modules.php?name=News&file=article&sid=2347&src=rss09

9 - ***Please note that all of the screenshot above were generated via my Microsoft Internet Explorer browser version 6.0. The screens depicted as Linksys screenshots were obtained via my browser connecting into my Linksys wireless router. All of the actual pages in the screenshot were created by Linksys and used as actual examples for my users. I did not create the pages, I only edited the content. Linksys is credited with designing the web-enabled front-end for the web browser.***