WIRELESS NETWORKING

NETWORK SETUP & CONFIGURATION

Mr. Paul Creed III, Adjunct II Instructor
Kent State University
Amy Hissom
Thursday, May 8, 2008

The following research is a compilation of information based on a number of different sources. Each source is listed at the end of the section it is contained in.

What Is Wireless Networking?

Wireless networks utilize radio waves and/or microwaves to maintain communication channels between computers. Wireless networking is a more modern alternative to wired networking that relies on copper and/or fiber optic cabling between network devices. A wireless network offers advantages and disadvantages compared to a wired network. Advantages of wireless include mobility and elimination of unsightly cables. Disadvantages of wireless include the potential for radio interference due to weather, other wireless devices, or obstructions like walls. Wireless is rapidly gaining in popularity for both home and business networking. Wireless technology continues to improve, and the cost of wireless products continues to decrease. Popular wireless local area networking (WLAN) products conform to the 802.11 "Wi-Fi" standards. The gear a person needs to build wireless networks include network adapters (NICs), access points (APs), and routers. ***(Source: Montana)***

Benefits of Wireless

Wireless offers tangible benefits over traditional wired networking. Ever tried to quickly look up a recipe on the Net while cooking in the kitchen? Do the kids need a networked computer in their bedroom for school projects? Have you dreamed of sending email, instant messaging, or playing games while relaxing on your outdoor patio? These are just some of the things wireless can do for you. The following benefits apply to both wired and wireless networking in homes.

Network file sharing between computers gives you more flexibility than using floppy drives or Zip drives. Not only can you share photos, music files, and documents, you can also use a home network to save copies of all of your important data on a different computer. Backups are one of the most critical yet overlooked tasks in home networking. Once a home network is in place, it's easy to then set up all of the computers to share a single printer. No longer will you need to bounce from one system or another just to print out an email message. Other computer peripherals can be shared similarly such as network scanners, Web cams, and CD burners. Using a home network, multiple family members can access the Internet simultaneously without having to pay an ISP for multiple accounts. You will notice the Internet connection slows down when several people share it, but broadband Internet can handle the extra load with little trouble.

Sharing dial-up Internet connections works, too. Painfully slow sometimes, you will still appreciate having shared dial-up on those occasions you really need it. Many popular home computer games support LAN mode where friends and family can play together, if they have their computers networked. Voices over IP (VoIP) services allow you to make and receive phone calls through your home network across the Internet, saving you money. Newer home entertainment products such as digital video recorders (DVRs) and video game consoles now support either wired or wireless home networking. Having these products integrated into your network enables online Internet gaming, video sharing and other advanced features.

Although you can realize these same benefits with a wired home network, you should carefully consider building a wireless home network instead, for computer mobility, no unsightly wires, and the fact that wireless is the future. Notebook computers and other portable devices are

much affordable than they were a few years ago. With a mobile computer and wireless home network, you aren't chained to a network cord and can work on the couch, on your porch, or wherever in the house is most convenient at the moment. Businesses can afford to lay cable under their floors or inside walls. But most of us don't have the time or inclination to fuss with this in our home. Unless you own one of the few newer homes pre-wired with network cable, you'll save substantial time and energy avoiding the cabling mess and going wireless. Wireless technology is clearly the future of networking. In building a wireless home network, you'll learn about the technology and be able to teach your friends and relatives. You'll also be better prepared for future advances in network technology coming in the future. ***(Source: How to Build a Wireless Home Network)***

Wireless Technology Standards

Because there are multiple technology standards for wireless networking, it pays to do your homework before buying any equipment. The most common wireless technology standards include the following:

- **802.11b**: The first widely used wireless networking technology, known as 802.11b (more commonly called Wi-Fi), first debuted almost a decade ago, but is still in use.
- **802.11g**: In 2003, a follow-on version called 802.11g appeared offering greater performance (that is, speed and range) and remains today's most common wireless networking technology.
- **802.11n:** Another improved standard called 802.11n is currently under development and is scheduled to be complete in 2009. But even though the 802.11n standard has yet to be

finalized, you can still buy products based on the draft 802.11n standard, which you will be able to upgrade later to the final standard.

All of the Wi-Fi variants (802.11b, g and n products) use the same 2.4 GHz radio frequency, and as a result are designed to be compatible with each other, so you can usually use devices based on the different standards within the same wireless network. The catch is that doing so often requires special configuration to accommodate the earlier devices, which in turn can reduce the overall performance of the network. In an ideal scenario you'll want all your wireless devices, the access point, and all wireless-capable computers to be using the same technology standard and to be from the same vendor whenever possible.

(Source: Webopedia)

Threats to Wireless Network Security

Unauthorized users accessing your network and eaves dropping your internal network communications by connecting with your wireless LAN (WLAN) is just one of the threats of a wireless network. There are a variety of threats posed by insecure or improperly secured WLAN's which include Rogue WLAN's, spoofing internal communications, and theft of network resources.

Since wireless routers are relatively inexpensive, ambitious users may plug unauthorized equipment into the network whether it is officially sanctioned or not. These are called rogue wireless networks and may be insecure which in turn can pose a risk to the network at large. An attack from outside of the network can usually be identified as such. If an attacker can connect with your WLAN, they can spoof communications that appear to come from internal domains.

Users are much more likely to trust and act on spoofed internal communications. Even if an intruder does not attack your computers or compromise your data, they may connect to your WLAN and hijack your network bandwidth to surf the Web. They can leverage the higher bandwidth found on most enterprise networks to download music and video clips, using your precious network resources and impacting network performance for your legitimate users.

Understanding Threats and How to Protect Your Network against Them

Segmenting your WLAN from the rest of your network will help to protect the internal network from any issues or attacks on the wireless network. To protect the wireless network itself, there are other steps you can take such as wireless encryption and user authentication. These will ensure unauthorized users do not intrude on your WLAN and that your wireless data can not be intercepted. Encrypting wireless data is one of the ways to ensure that unauthorized users don't eavesdrop on your wireless network. WEP (wired equivalent privacy), which is the original encryption method, was found to be fundamentally flawed. To restrict access, it relies on a shared key or password. Anyone who knows the WEP key can join the wireless network.

It won't take long for an attacker to access a WEP-encrypted wireless network since there are tools available that can crack a WEP key in minutes. The reason a WEP key can be cracked in minutes is because there was no mechanism built in to WEP to automatically change the key. WEP is insufficient for protecting an enterprise network, but it is better than not using any encryption at all. WPA (Wi-Fi Protect Access) is the next generation of encryption. It is designed to leverage an 802.1X-compliant authentication server, but it can also be run similar to WEP in PSK (Pre-Shared Key) mode. The main improvement from WEP to WPA is the use of TKIP (Temporal Key Integrity Protocol), which dynamically changes the key to prevent the sort

of cracking techniques used to break WEP encryption. Even WPA was a band-aid approach though. WPA was an attempt by wireless hardware and software vendors to implement sufficient protection while waiting for the official 802.11i standard. WPA2 is the most current form of encryption. This encryption provides even more complex and secure mechanisms including CCMP, which is based on the AES encryption algorithm. Your WLAN should be set up with at least WPA encryption, and preferably WPA2 encryption to protect wireless data from being intercepted and to prevent unauthorized access to your wireless network.

WPA can interface with 802.1X or RADIUS authentication servers to provide a more secure method of controlling access to the WLAN besides just encrypting wireless data. Where WEP, or WPA in PSK mode, allows virtually anonymous access to anyone who has the correct key or password, 802.1X or RADIUS authentication requires users to have valid username and password credentials or a valid certificate to log into the wireless network.

Requiring authentication to the WLAN provides increased security by restricting access, but it also provides logging and a forensic trail to investigate if anything suspicious goes on. While a wireless network based on a shared key might log MAC or IP addresses, that information is not very useful when it comes to determining the root cause of a problem. The increased confidentiality and integrity provided are also recommended, if not required, for many security compliance mandates.

With WPA / WPA2 and an 802.1X or RADIUS authentication server, organizations can leverage a variety of authentication protocols, such as Kerberos, MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), or TLS (Transport Layer Security), and use an

array of credential authentication methods such as usernames / passwords, certificates, biometric authentication, or one-time passwords.

Wireless networks can increase efficiency, improve productivity and make networking more cost effective, but if they are not properly implemented they can also be the Achilles heel of your network security and expose your entire organization to compromise. Take the time to understand the risks, and how to secure your wireless network so that your organization can leverage the convenience of wireless connectivity without creating an opportunity for a security breach. ***(Source: Secure Your Wireless Network)***

How to Set Up a Wireless Home Network

1. Connect Your Wireless Router

Turn off your cable modem and your wired PC. Unplug the Ethernet cable from your cable modem and plug it into one of the four LAN ports on the back of the wireless router. The other end of the cable should remain connected to your PC. Connect a second Ethernet cable between your modem's Ethernet port and the wireless router's WAN port. (The WAN port is separate from the four grouped LAN ports.) Turn on the modem and wait for the status lights to indicate that it's connected to your service provider. This may take up to a minute. Plug in the router. The status lights will blink as it goes through its own diagnostics; this may also take up to a minute. Boot up your wired PC.

2. Configure Your Router

Refer to the router's printed quick-start guide, launch your Web browser, and type in the address indicated in the guide. Follow the on-screen setup wizard, which should guide you step by step through the process. Enable your router's security functions. The options will be WEP and

WPA. (See page 88 for more information on enabling WPA.) Both will ask you to enter a key. Depending on your router's manufacturer, you may need to go to Advanced Settings to handle this step and the next two. Change the default administrator's password, which is often known to hackers. Change the SSID—the name you give your wireless network. Again, hackers know many of the default SSIDs and can use them to join your network.

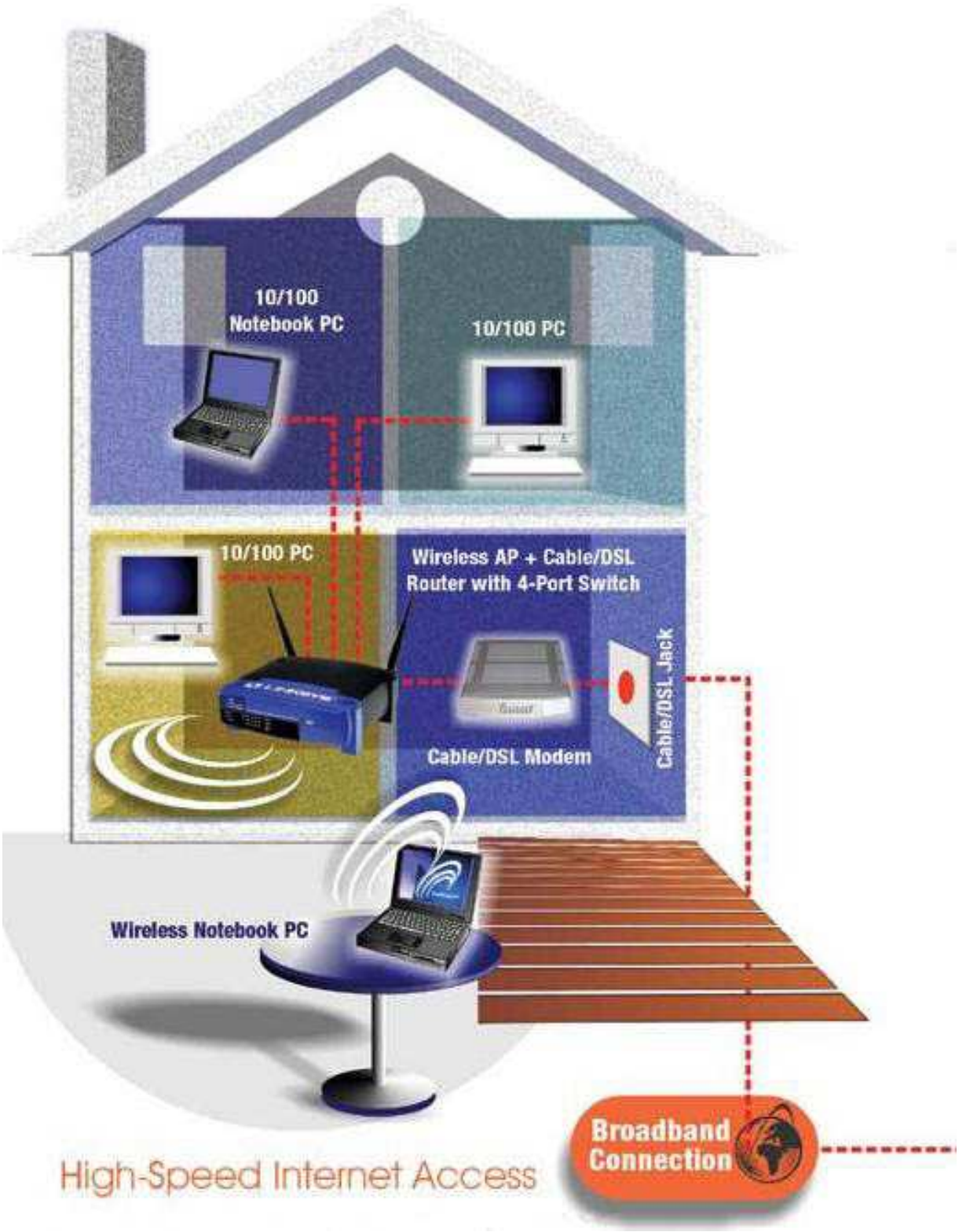
3. Install a Wireless PCI Card in a Desktop PC

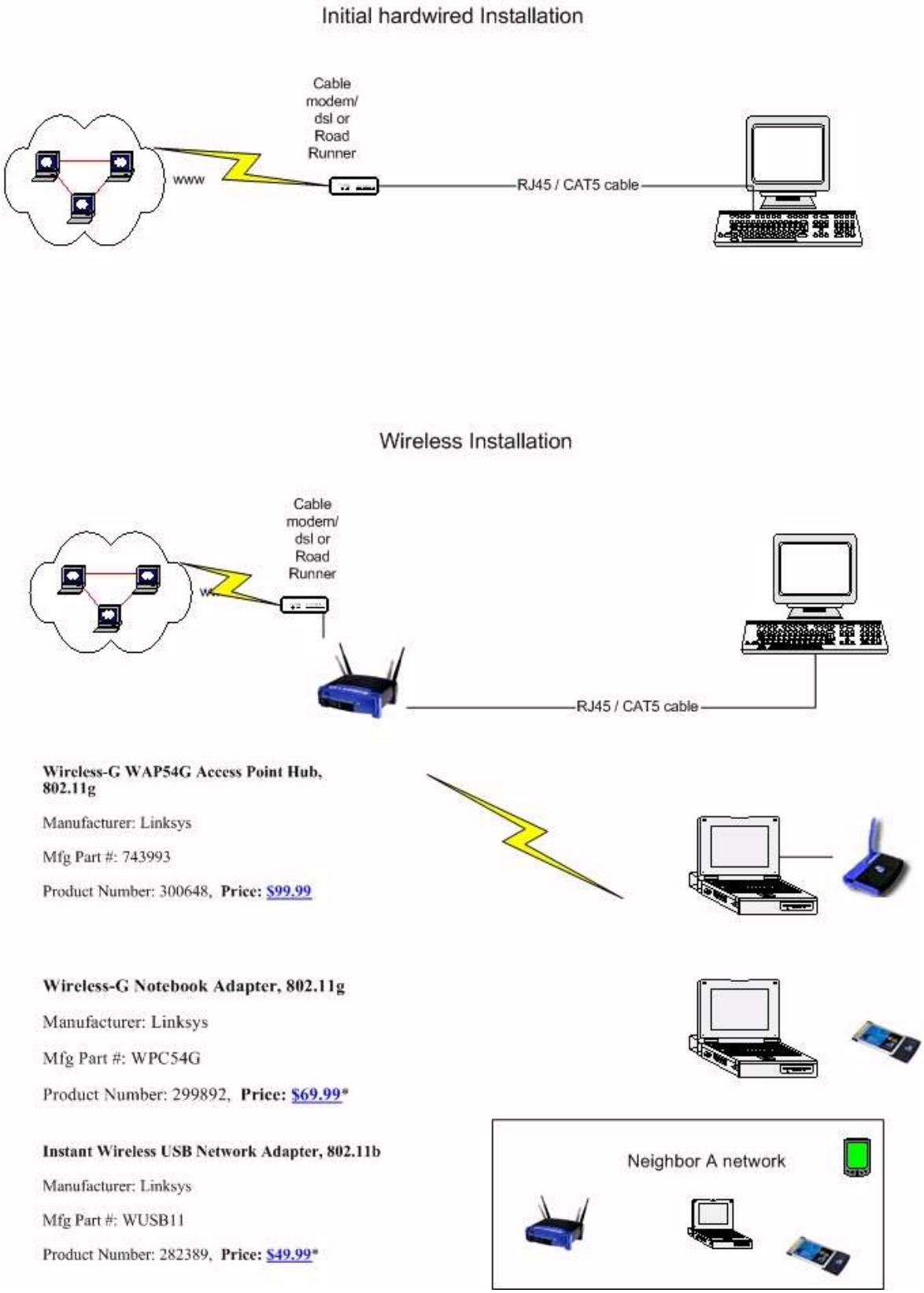
Refer to the card manufacturer's quick-start guide. If necessary, run the software installation program. Shut down the PC. Remove the cover. Locate an available PCI slot and remove the corresponding slot cover from the back of the PC. Carefully route the antenna through the open slot in the back of the PC, insert the card in the slot, and secure it. Replace the cover. Turn on the PC. It should recognize and enable the new hardware. Go to the Control Panel, select Network, select Wireless Networking connection. Click on Properties. Click on Wireless Networking tab. Select the wireless networking name (see step 2e above). Click on Configure. Adjust your security settings to match those on your wireless router.

4. Install a Wireless PC Card in a Notebook Pc

Many notebooks have built-in wireless cards. If yours doesn't, follow these instructions. Follow steps "a" and "b" in number 3. Plug your wireless PC Card into an available slot on the side of your notebook. Follow steps "f" and "g" in number 3.

(Source: PC Magazine)


10/100
Notebook PC
10/100 PC
10/100 PC
Wireless AP + Cable/DSL
Router with 4-Port Switch
Cable/DSL Jack
Cable/DSL Modem
Wireless Notebook PC
Broadband
Connection
High-Speed Internet Access



(Source: PBS Free Tips and Tricks and Tech Info)

Bibliography

Your Guide to Wireless Networking, Bradley Mitchell; *About.com*; Retrieved: March 29, 2008

Secure Your Wireless Network; From Tony Bradley, CISSP-ISSAP, Your Guide to Internet / Network Security, http://netsecurity.about.com/od/secureyourwifinetwork/a/securewifi.htm, Retrieved on April 29, 2008

Montana Internet Help and Tools; Blackfoot Telecommunications Group, Glossary of Terms: https://www.blackfoot.com/montana-communications.php#w, Retrieved on March 25, 2008.

How to Build a Wireless Home Network – Tutorial; Bradley Mitchell; *http://compnetworking.about.com/cs/wirelessproducts/a/howtobuildwlan.htm*; Retrieved: March 29, 2008

Webopedia: The #1 Online Encyclopedia Dedicated to Computer Technology, How Wireless Networks Work; http://www.webopedia.com/DidYouKnow/Computer_Science/2008/wireless_networks_explained.asp, Retrieved on April 29, 2008

PBS Free Tips and Tricks and Tech Info; http://www.pbshawaii.com/Wirelessathome.jpg, Retrieved on April 29, 2008

PC Magazine; How to Set Up a Wireless Home Network, http://www.pcmag.com/article2/0,2817,1277381,00.asp; Retrieved on April 29, 2008