digit
May 2005

Fast Track to WIRELESS NETWORKING

- **Wireless** Home Networking
- Planning A **Home Network**
- Setting Up **Access Points**
- Using A **Wireless Network**
- Threats To **WLANs**
- **FAQs** And **Troubleshooting**
- **Glossary**

Jasubhai DIGITAL MEDIA

YOUR HANDY GUIDE TO EVERYDAY TECHNOLOGY

Fast Track to Wireless Networking

By Team Digit

Credits

The People Behind This Book

EDITORIAL
Sachin Kalbag Editor
Aditya Kuber Coordinating Editor
Robert Sovereign-Smith Writer and Copy Editor
Aliasgar Pardawala Writer
Ram Mohan Rao Copy Editor

DESIGN AND LAYOUT
Jayan K Narayanan Lead Designer
Harsho Mohan Chattoraj Illustrator
Vijay Padaya Layout Artist
Sivalal S Layout Artist

May 2005
Free with Digit. Not to be sold separately. If you have paid separately for this book, please e-mail the editor at **editor@thinkdigit.com** along with details of location of purchase, for appropriate action.

Go Wirefree!

Today we use myriad devices that could merit the term 'wireless'—mobile phones, cordless phones, radio equipment, and such. When it comes to information technology, however, 'wireless' generally means trhe ability to create a network *sans* wires.

Networking is key to our computing experience, and the Internet is the biggest network of all. What good is a computer if you can't connect to your Local Area Network or the Internet? Less than one per cent of the computers in the world are standalone machines that lack the ability to connect to others.

Technology advancement has seen the definition of a PC shift from 'Personal Computer' to 'Portable Computer'. The new breed of laptops are no longer the signature of the higher echelons of management. Today, sales executives and even delivery personnel have mobile devices such as laptops and PDAs to increase effeciency.

With technology becoming more and more portable, networking had to catch up, and thus we have wireless networking, which is fast becoming the solution of the future. This book will cover wireless technologies and devices in order to give you in-depth knowledge, and also to help you set up your own wireless solutions.

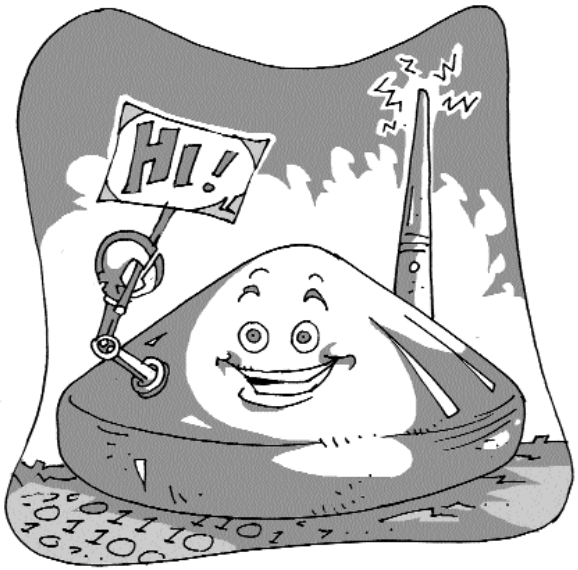
The first chapter introduces you to the technologies that power the solutions. The second guides you through the identification of the correct solution for your needs, and then you will learn how to set up your solution in the third chapter.

Chapters four and five show you how you can best use your setup, and how you can prevent unauthorised use from outsiders. These chapters span everything from the coolest wireless gadgets to the tools you need to protect them from hackers.

Chapter six will answer any questions you have about wireless devices, help you troubleshoot problems, and also identify resources that can prove really handy. The Glossary and Bibliography demystify all the jargon you may come across when dealing with wireless technologies, and identify books and resources you should consider in order to take your learning about wireless to the next level. We've also included several whitepapers, should you want to explore the subject in even further detail.

Contents

Wireless: The Basics



Wireless technology has pervaded our lives—mobile phones, cordless phones, and infrared remote control devices are just a few examples of the wireless devices we use. This book will steer clear of consumer electronics and mass communication devices, which use infrared, cellular and satellite transmission technologies, and stick to the definition of wireless in Information Technology (IT): "To establish communication without the use of cables or wires, where data distribution occurs through an unguided medium such as the atmosphere, by using radio wave technologies."

Wireless devices can be used both by businesses and individuals. This book will focus on the individual, and address our personal needs and possible deployments of wireless. The most basic use for wireless is to set up a Wireless Local Area Network (WLAN) or Personal Area Network (PAN) at home. This can be achieved by using wireless technologies and protocols such as Wi-Fi and Bluetooth.

1.1 Wireless Home Networking

An access point—one of the most important building blocks of a Wi-Fi network

Today, many of us own more than one IT device such as a desktop, a laptop, a PDA or a cell phone. Our personal and professional data is often scattered between these devices, and obviously we need to have all our data available to us all of the time. The solution to this is wireless networking.

Wireless networking can help us connect various wireless-enabled devices together, and as a result, improve our computing experience. Whether it's just connecting your PC and laptop to each other, sharing an internet connection between multiple PCs, or even making sure that you can sit anywhere within your house with a wireless device and have access to your networked devices and the Internet, wireless is the easiest way to go.

A wireless PCMCIA card for a laptop. These are credit-card sized devices

The term 'Wireless Home Networking' is something that has just begun to make sense. Until a few years ago, wireless networking was something that brought to mind a swanky corporate office with money to splurge on 'extras' such as wireless technologies. Today, wireless devices and peripherals are universal, and don't cost an arm and a leg. Most laptop owners already have wireless-capable hardware; all PDAs and cell phones available today are either wireless-enabled or wireless-capable. Using such devices, one can easily set up a Local Area Network (LAN), or a PAN at home.

Before we get into how you can identify the solution you need (Chapter 2), or how to go about installing it (Chapter 3), you should know what technologies and protocols are available, and how they work.

1.2 From a To g And b-yond

The most common wireless technology is called Wi-Fi—short for Wireless Fidelity. This is actually a combination of different protocols that use the IEEE 802.11 specification standard. So, what is the IEEE 802.11 standard? In order to simplify things, detailed definitions are listed below.

IEEE

The Institute of Electrical and Electronics Engineers (IEEE) was formed on January 1, 1963, by way of a merger between the American Institute of Electrical Engineers (AIEE) and the Institute of Radio Engineers (IRE), both leaders in their respective fields.

The IEEE publishes 30 per cent of the world's literature relating to computer science, electrical and electronics engineering. The group has developed almost a thousand industry standards. Visit www.ieee.org for more information. For this book, we are only interested in a particular group of the IEEE.

802

IEEE 802 is a collection of networking standards that were designed or researched to run LANs and Metropolitan Area Networks (MANs). They are maintained by a specific committee called the LAN/MAN Standards Committee (LMSC). This committee oversees the functioning of smaller research groups. It is one of those groups—Group 11 to be precise—that we are getting to.

Group 11 (802.11)

A working group of the LMSC researched and developed the IEEE 802.11 WLAN standard, which is popularly called Wi-Fi today. This family of wireless standards currently includes four major wireless modulation techniques that all run on the same protocol, all developed by the IEEE 802.11 group. The standards are 802.11a, 802.11b, 802.11g, and 802.11n. The very first wireless standard was released in 1997, and was simply termed 802.11. It offered theoretical speeds of 1 Mbps and 2 Mbps, and operated at the 2.4 GHz

radio frequency (RF). It died out almost as soon as it was implemented, due to the lack of a standard specification for operation, which resulted in devices from different manufacturers not being interoperable. It was soon replaced by the 802.11b standard.

802.11b

This was the first amendment to the original wireless standard introduced by the working group 11 of the IEEE 802 committee. It was released in 1999, and offered an improved theoretical data transfer rate of 11 Mbps. This standard also operated in the 2.4 GHz RF spectrum, and offers ranges of up to 8 km. The 802.11b standard was the first wireless standard to gain popularity with the masses. Since it operated on the same protocol and frequency as the original standard, manufacturers has few modifications to make in the then manufacturing technique in order to make devices 802.11b-capable. While this protocol was being developed, another task force (a group within the 802.11 working group) was developing the 802.11a protocol.

802.11a

This standard, too, was released in 1999, but products that supported it only started appearing at the end of the year 2000. The main reason for this was that 802.11a operates on the 5 GHz RF spectrum, and so manufacturing processes had to be altered, which most vendors were averse to—802.11b was catching on just fine and spinning sustainable revenue. The best thing about the 802.11a standard was the increased theoretical throughput speeds of up to 54 Mbps. 802.11a and 802.11b devices are not interoperable, unless used in conjunction with dual-mode hardware that supported both protocols. Using the 5 GHz frequency almost multiplied the theoretical throughput by a factor of five, but it also significantly reduced the range, mainly due to the additional susceptibility of 802.11a signals being absorbed by obstacles. The need arose for a standard that offered the bandwidth of 802.11a and the range of 802.11b.

802.11g

After further research, in mid 2003, the 802.11g protocol was released. This protocol was fully backward-compatible with 802.11b, mainly because it used the same 2.4 GHz RF spectrum, and also offers 54 Mbps theoretical throughput, like the 802.11a standard. The drawback of this backward-compatibility is the fact that an entire network can be slowed down to a fraction of 802.11g's supported throughput speed, just by introducing an older 802.11b device into it. 802.11g offers lower ranges than 802.11b, but makes up for this in terms of actual data throughput limits over short distances.

An 802.11g PCI wireless card

802.11n

This standard was approved for research in early 2004, and results are expected somewhere in 2006. The 802.11n standard will offer a throughput of 100 Mbps, and will have a higher range than the previous standards. Task group 16 of IEEE 802 is working on something even more exciting, though.

802.16

Popularly called WiMAX (Worldwide Interoperability for Microwave Access), this standard is developed by working group 16 of the wireless committee. It is a standard that will complement current Wi-Fi setups and is solely a MAN technology. It can con-

An 802.11g Linksys wireless broadband router

nect existing Wi-Fi LANs to the Internet by offering shared theoretical throughput rates of 70 Mbps over a range of up to 50 km. WiMAX is touted as the answer to cheap broadband access across the world, especially in rural areas. Because of its long range, the costs of expensive cabling will be negated, and so connecting even the remotest of villages will become possible.

All these standards and more come under the wide umbrella of 'Wireless'; however, we will only concern ourselves here with the IEEE 802.11a, 802.11b and 802.11g standards when referring to Wi-Fi—because these are the most cost-effective and accepted standards. Also, this book only attempts to help you bring wireless into your personal life, and not to plan wireless solutions for towns, cities or nations.

On the personal or home front, there are a few more technologies that deserve mention when talking about home networking.

1.3 Bluetooth, HPNA and HomePlug

Bluetooth

Bluetooth supposedly got its name from the Danish King Harald Blåtand, which translates to 'Harold Bluetooth' in English. It is a

low-cost, short-range wireless networking standard that enables you to establish PANs. The earlier 1.2 version offered speeds of about 700 Kbps, but the current 2.0 version offers speeds of up to 2.1 Mbps. Bluetooth 2.0 operates on the 5 GHz frequency (2.4 GHz for the original Bluetooth standard), and has a range of just 10 metres (33 feet). In terms of home networking, Bluetooth has nothing much to offer. However, when looking for a cheap and neat alternative to the messy wires that connect various immobile devices together, such as a printer and scanner connecting to a PC, Bluetooth is the answer.

Bluetooth is mainly used in mobile devices such as cell phones, PDAs and laptops as a means of short-range data transfer, such as when syncing the PDA with a PC or laptop, or using a Bluetooth headset with your mobile phone, so that you never have to take the phone out of your pocket to answer a call. Though the speeds offered are a fraction of what Wi-Fi has to offer, the significantly lower power consumption of Bluetooth chips more than makes up for it. The fact that battery technologies for mobile devices are lagging far behind all other technologies in the same field has helped Bluetooth gain a stranglehold on the mobile device market—after all, what good is a Wi-Fi cell phone that transfers data at speeds in excess of 20 Mbps, but whose battery lasts only 5 minutes?

In the near future, Bluetooth 2.0 should soon become the solution to the clumsy and cluttered wires that connect our devices, such as keyboards and mice to PCs, and printers or scanners in small LANs. Already, you can use most new phones with Bluetooth to connect to laptops and PDAs in order to connect to the Internet.

Home networking doesn't necessarily have to be wireless, as the next two technologies will prove.

HPNA

Short for Home Phoneline Networking Alliance, this solution is based on the assumption that you have a phone line in your house. Most modern houses have internal phone wiring with outlets in

every room. HPNA uses this existing wiring to connect devices to form a LAN. The beauty of this solution is that there is no need for the phone line to be connected or alive: the networking happens using the existing building's wiring. Even if your phone line is alive, this networking solution does not interfere with your standard telephone frequencies, and thus will never interrupt inbound or outbound voice or data calls.

A snap-in wireless card for a PDA

HPNA operates at a frequency much higher than voice or analogue signals, so you always have the use of your phone as is normal. HPNA can connect up to 50 devices, and offers a throughput of 1 Mbps to each device.

The hitch here is that you need to buy HPNA-compatible devices and connectors before you can go about setting up your LAN. Devices can be as much as 1,000 feet apart, and in offices, as much as 10,000 feet apart on different floors of the same building.

HomePlug

Every device in our home needs to be powered. HomePlug does away with excessive wires for everything, as the networking is done using your home's power sockets. This standard can ensure that you always have a broadband connection to the Internet for every device that is connected to a power outlet. HomePlug works by superimposing an analogue data signal onto the standard 50 or 60 Hz AC signals.

The standard is capable of network transmission of 14 Mbps

and over large areas. Though not a mobile technology per se, HomePlug seems to be a good investment for individuals who have a wide range of gadgets that need networking. This will also help reduce the need for wires.

Home Networking

We have thus far explained all the home networking techniques that exist today. If you cannot make up your mind as to what solution is right for you, stay with us until Chapters 2 and 3, which will help you decide on a solution and also on the hardware that will power it.

What's The Plan?

Now that you have the hang of the basics, it's time to get your hands dirty and actually do something—network a few computers wirelessly. It's not as difficult as it seems. In fact, it's hardly more complicated than networking computers using wires. There are a couple of complexities, of course, such as where to place Access Points and so on. But these are easily overcome if you have your plans in place. This chapter will guide you through precisely that—how to plan your wireless network, including what you need to purchase, where to place devices, and how to secure your network.

2.1: Planning a Wireless Home Network

The Basics

Planning is the name of the game. Spend quality time planning for the best performance of the wireless network you intend to set up in your home.

Since we are talking about linking two or more PCs wirelessly, you will need to first make the list of the Wi-fi equipment that you will be needing.

Wireless hardware available in the market usually comes with documentation that explains in detail how to get it up and running. It will therefore help if certain issues are cleared beforehand. These issues will depend on what kind of systems you are going to connect. Is it going to be two PCs, a Mac and a PC, or is there a wireless printer involved as well?

What kind of speed you expect out of your wireless network? Are your data transfers going to involve accesses to files and folders, or are you planning to stream movies and music stored on one machine to the other? The amount of data transfer will play an important role in deciding what type (a, b or g) of Wireless LAN you will need for seamless data transfer.

A WLAN Access Point

You will also need to take into consideration how you will connect to the Net. Is it going to be a dial-up connection, a connection provided by the local cable*wallah,* or DSL? Also, how will you share the connection?

Finally, plan well for security, since a wireless network is an open network and if not secured, anyone with the right tools can easily get access to your content.

The Site Survey

A site survey doesn't mean you have to scan the entire neighbourhood with expensive gadgets. What it means is, choose the right location for your Wi-Fi equipment such as the access point, and if possible your PCs, so that there is a minimum of hindrance to the flow of radio signals. There are a few factors that can affect the performance of the network such as a thick wall, electrical equipment in the vicinity, and so on.

Therefore, before starting to nail the access point into a wall, make sure the location is right. This involves a little implementation of the trial and error method, as you will need to place the access point at different locations to see what location gives the best data transfer results and seamless connectivity. To do this, it is advisable to rent a Wi-Fi-enabled laptop and check the signal strength at various locations in your home that you get from an access point placed at a certain location.

Change the location of the access point if you are not getting acceptable signal strength in almost every corner of your home. If you are living in a house that is something like a ground plus one or two, than chances are that you will need more than one access point for continuous connectivity. You can also plan to place the access point near the window, in order to do away with the second access point, but that will not help much—signal strength will drop once you move away from

A wireless broadband router

the window on another floor. This will also make your network more inviting to external entities.

The second access point will have to be configured in repeater mode, which means it will work as a range extender, and therefore will need connectivity with the main access point. Therefore, the placement of second access point will have to be such that it is within the range of first access point.

Equipment Planning

Equipment planning can be done only when you are clear as to how many PCs are going to be connected, and what your data throughput requirements are. What kind of equipment is required will also need you to take into consideration the kind of hardware you will be connecting. For example, a PC will need a PCI Wi-Fi card, whereas a laptop will need a PCMCIA-based Wi-fi card (if it is not already Wi-fi-enabled).

If you are going to use a dial-up connection to connect to the Internet, you will not need a wireless router, but if you are going to connect to the Internet using a cable connection or a DSL line, a wireless broadband router is your best option.

A router will let you plug the cable coming in from the service provider directly to it, bypassing the PC completely. This helps in placement of both the PC and the broadband router, because you don't have to run long cables coming all the way to the PC. This is especially true if you are staying in a ground plus one house or a duplex flat, where

A 4-port switch

you don't just have to deal with distances, but also need to factor in floors. Routers also normally come with a 4-port switch, which can come in handy in the future.

If you are going to connect, say, two systems, of which one is a desktop and the other is a laptop, and you will connect to the Internet using a dial-up account, then you need

1. A PCI wireless card supporting 802.11b/g

2. A PCMCIA wireless card if the laptop is not Centrino-based, or not Wi-Fi-ready supporting 802.11b/g

3. An Access Point supporting 802.11b/g

4. An RJ-45 network cable for connecting the access point to the desktop PC. (This cable is bundled with most of access points available in the market.)

If you are going to use DSL or cable internet with one desktop and laptop connected wirelessly, and you want to share the Internet connection on both, then you will need

1. A PCI wireless card supporting 8022.11b/g

2. A PCMCIA wireless card if the laptop is not Centrino-based, or not Wi-Fi ready supporting 802.11b/g

3. A wireless router with either a cable modem or a DSL modem inbuilt

If you are going to connect two systems that are not far away from each other, like two desktop PCs with fixed locations, then the Ad-Hoc mode is a very cost-effective solution. For this, you will need two wireless cards, and no access point or wireless router.

2.2: Choosing the Right Equipment

A cable with RJ45 connectors at both ends

If you are planning to connect two PCs placed in different rooms, you have two options. The first is to connect them in Infrastructure mode using an Access Point. The Access Point or Base Station will act as a trans-receiver for both the PCs. The other option is to connect the PCs in Ad-Hoc mode, where you do not need an Access Point. Here, the radio cards will connect directly with each other. Performance with Ad-Hoc mode is not going to be as good as with an Access Point as the distance increases and there are more hindrances between the two wireless cards.

You need to choose from various standards available in the market depending on the data throughput you need. If you are going to stream a movie, then 802.11g, which supports 54 Mbps throughput speed, will be required. However, if you are planning on just sharing files and folders and listen to MP3s, then the older, slower and now cheaper 802.11b hardware supporting 11Mbps is sufficient.

Installation

Once you have figured out what equipment you need, and have bought all the requisite hardware, you need to know how to go about installing your wireless network.

From hardware to software, it's all just a matter of following some simple steps and remembering a few simple rules. Read on to find out how to get your wireless network up and running.

3.1: Setting Up Wireless Access Points

We will consider two scenarios for configuring an Access Point. The first is where you just have a plain-Jane Access Point. The other is where the Access Point has a wireless broadband router with either cable or DSL or dial-up modem built in.

Connecting Two PCs Using An Access point

To connect two PCs wirelessly using a simple Access Point will need you to connect the Access Point to one of the system directly where you have the Internet connection coming in. This PC should have a Network Interface Card (NIC). The other machine should have wireless PCI adapter. An RJ45 cable is provided with some of the available Access Points.

Follow the steps as below to get an Access Point up and running:

1. Switch off the PC and connect the RJ45 cable to the Network Interface Card of the PC.

2. Connect the other side to the LAN port of the Access Point.

3. Power up the Access Point and make sure the LED indicates that everything is normal, as mentioned in the manual.

4. Now power up the PC and get the LAN on the same IP range as the Access Point is. The default IP address of the Access Point will be mentioned in the quick setup guide on the CD. A typical IP is 192.168.1.1 and a the corresponding subnet mask would be 255.255.255.0. If this is the IP of the Access Point, then give the LAN an IP something like 192.168.1.2, up to 254.

5. Once the TCP/IP settings are configured, it is time to ping the Access Point to check whether everything is working properly.

6. To ping, click Start > Run, and in the dialog box, type in “ping <IP address of Access Point>”

7. If the ping commands works successfully, launch your browser and type in “http://<IP address of Access Point>”, for example, http://192.168.1.1, in your browser address bar, and press [Enter].

8. This will let you access the Web server of the Access Point, which has an inbuilt utility that will let you configure the Access Point according to your need. From here, you can change the SSID, IP/Subnet mask and enable or disable wireless security.

9. Do the necessary changes, and that's it. The Access Point is configured.

Now, go to the other system, which has a PCI Wi-Fi card plugged in to it, and make the following changes.

1. Switch off the system and plug in the PCI wireless card. Now turn on the system and let the card get detected by the system. Install the necessary device drivers and the configuration utility provided with the card. Restart the system to complete the installation process.

2. Now launch Control Panel and go to 'Network connections'. The window that opens will display ‘Wireless Network Connections’. Right-click it, and click properties.

3. Now scroll down to the TCP/IP connection, and click once on it to highlight it, and then click properties. This will open the TCP/IP dialog box. Here, you need to assign an IP to the wireless card with the first three metrics, which in our case is 192.168.1. This should remain the same, and the last one can be any number between 0 and 254—but not the same as the one already assigned to the Access Point and the first system’s LAN card.

4. Click OK to close the dialog box, which will bring you back to the Wireless Network connection properties. Again, here, click OK, and that’s it.

This is all the settings that are needed to get two PCs to connect wirelessly using a simple Access Point. Share a folder on the master system where the Access Point is connected, and try to access it from the client system—it should work.

Connecting Two PCs Using A Wireless Router

Wireless routers are Access Points that have the Internet port for a DSL or cable modem connection, and in most cases, also has a 4-port switch. A wireless router is useful only when you have DSL or cable Internet at home, or if you are planning to connect one of the PCs or network printers to one of the ports on the switch. However, if you have DSL or cable Internet, a wireless router is the best solution as it doesn't require you to connect it directly to the PC to share the Internet connection, or files and folders on another PC. Here is how you will have to go about getting it running.

1. Connect the incoming DSL or cable connector, which is an RJ45 cable, to the Internet port of the router.

2. Power up the wireless router and observe whether all the LEDs are behaving in the exact manner as mentioned in the manual. If not, try resetting it.

3. Now go to the first system, with the wireless card plugged in. Get the wireless card on the same IP range as the router is. You can learn about the router IP from the manual.

4. Once the wireless card is configured, try to ping the IP address of the router and see whether the response is positive. You can also try to search for the available network, either by using the wireless card's utility, or by right-clicking the network icon in the system tray and clicking 'View available Network'. This will show you the active wireless network available.

5. Once you get your router detected by the wireless card, launch your browser and type in your router IP address in the following manner: http://<IP address of router>. Press [Enter].

6.This will launch the configuration utility of the router. But to enter this utility you will have to provide a username and password, which again, is provided in the manual.

7.The first thing you should do now is change the login and password to something really difficult, which no-one can guess. Also change the security setting to at least 128-bit if you are going to access your bank account and other sensitive information.

8.You can and must change the IP address to something else, as the default IP is easily traceable, and known to most Wi-Fi users. If possible, restrict DHCP (Dynamic Host Control Protocol) to very few numbers. For example, if you are going to connect just one more system wirelessly, than restrict the start and end IP to accommodate just one machine. Change this later if you have to add one more system.

3.2: Setting Up Wireless Networking (Windows + Mac)

Configuring the Client

The adapter card will have to be installed on the client PC, since we're going to connect the client machine to the Access Point configured on the LAN.

Here are the steps to follow in order to configure the client PC and the laptop.

1.Power down the system and remove the side cover. Locate a free PCI slot if you are going to use a PCI Wi-fi card. Secure it tightly, screw it in, and attach the detachable antenna to the card.

2.Power up the system. The PC will detect the card and ask for the drivers. Install the drivers as mentioned in the manual and restart the system if need be.

3.You'll see a small icon sitting in the system tray once the drivers are properly installed and the hardware properly detected. Double-click the adapter card configuration icon in the system tray. This will launch the configuration utility.

4.Here, you don't have to do anything, as most of the settings, including SSID and the encryption key, are automatically picked up by the adapter card. Select the Ad Hoc mode if connecting to the other PC or laptop configured in Ad Hoc mode. Give an SSID different from the one assigned to the other wireless card.

5.Check the signal strength available at the place the wireless desktop or laptop is placed by double-clicking the utility in the taskbar.

Setting Up Ad-Hoc Mode

Ad-Mod or Peer-to-Peer mode as it is commonly known is very easy to set up. It has multiple advantages: you can quickly create a network between notebooks that are Wi-Fi enabled, and share small files during a meeting. It doesn't need an Access Point, as one of the notebooks can be turned into a soft Access Point, and the rest can connect to each other through it. Here is the stepwise explanation of how to turn a Wi-Fi enabled notebook into a soft AP, and to configure the rest to connect to it. We will use Windows to get the network up and running.

1.To set up the soft AP, click Start > Connect To > Wireless Network Connection. This will open up the Wireless Network Connection Dialog box. Here, click Properties; a new dialog box will open, from where we need to assign various settings.

2.In this dialog box, under the 'General' tab, scroll to 'Internet Protocol (TCP/IP)' and select it. Now click 'Properties', which will take you to the next dialog box where we assign the IP. Just assign the IP and click on the subnet mask once—it will appear automatically.

3.Close this dialog box and then click the second tab—'Wireless Network'. Here, at the bottom, click 'Add', which will launch another dialog box where we need to assign a name for Network Name (SSID). Check 'WEP' and 'Key provided automatically' for the rest to seamlessly connect to this AP. Press OK once through with these settings. Now click 'Refresh' in the 'Wireless Network' dialog box, and the network name will appear in the 'available networks' area.

4.Configure the client systems that will connect to the soft AP, and eventually to other client systems through it. For this, go to the 'Network properties' dialog box and assign an IP in the same range. For example, if you assigned 192.168.1.1, assign 192.168.1.2 and so on to the other client systems. Now click on 'Subnet mask', and it appears automatically.

5.Right-click on the network icon in the system tray. This will launch a dialog box that will display the name of the soft AP. Check 'Allow me to connect to the selected network'. This will highlight the Connect button at the bottom. Just click it, and you should be able to connect to the other machines.

Repeat the exercise with the other client machines, and you will be able to connect each to the other, all without an Access Point.

3.3: Sharing An Internet Connection

If you are going to use wireless router with a DSL or cable modem inuilt, you will not have to use any third party tool like SyGate. Here we take a look at both scenarios—a normal Access Point and a cable or DSL wireless router.

Sharing An Internet Connection Using A Wireless Router

To share an Internet connection between two or more systems using a wireless router, you will need some information handy,

like PPPoE (Point to Point Protocol over Ethernet), your user name and password which is provided by the ISP, subnet mask, default gateway, and so on.

When you log in to the Web server of the router, you will be asked to give this information. If the broadband router asks for any additional information, you will have to get it from your ISP. Once you have provided all the necessary information, use the test button to check whether you are able to connect to the Internet.

Sharing An Internet Connection Using An Access Point

When you have plugged a simple Access point to your PC with a dial-up connection to connect to the internet, you will have to use third-party software to share internet. We will take the example of SyGate, which is a widely used Internet sharing program. Internet connection software needs to be installed on both the server and the client. Once you are through with the installation on the server—where the dial-up modem and Access Point is connected—and the client system (where the PCI wireless card is connected), the rest of the installation is straightforward.

For the setup mentioned above, leave 'Use Single NIC mode' option unchecked. SyGate will show the appropriate connections in 'Direct Internet/ISP Connections', as well as '1' In 'Local Area Network Connection'. The 'Direct Internet/ISP Connections' would have a 'Local Area Connection' if you have more than one LAN card or dial-up connection. To share a dial-up connection, you would first have to set up one in Windows, and then add it in SyGate.

Now select the LAN card that connects your PC to the Access Point in '1' within 'Local Area Network Connection'.

Once the above step is complete, your configuration is done. But there are further settings to look at, for better optimisation of Internet bandwidth and system resources.

Dial-On-Demand and Auto Disconnect are two settings that

will help you keep your dial-up costs to a minimum. If Dial-On-Demand is enabled, then each time a user wants to access the Internet, one of the connections will be activated depending upon precedence.

Auto-disconnect will keep a tab on no-activity periods, and disconnect the call. If you wish, you can configure the software to set up additional connections if bandwidth exceeds a certain threshold, by enabling and specifying the threshold level for 'Connect additional line if...'

In the options section, 'Enable Internet Sharing At startup', 'Enable Activity Log', 'Enable Bandwidth Management' and 'Enable DNS forwarding' are recommended. Finally, if you have set up your network with a static IP for each PC, untick the 'Enable Address Server (DHCP)' option. If you've manually assigned IPs to each machine, you don't need a DHCP server.

You can modify some of the advanced settings for DHCP server or DNS forwarding by clicking on 'Advanced' in the configuration window. If DHCP Server is enabled, you can specify the IP range that should be used while allocating IPs. This setting is also available with the configure utility of the Access Point. If DNS Forwarding is enabled, you need to specify one or more DNS server addresses for forwarding to work. Here, you can either use the DNS server your ISP has provided, use the ISP's helpline, or look up the documentation. Alternatively, you can use some of the most commonly used ones, such as those of VSNL—202.54.1.18 and 202.54.1.30. You need not specify any settings if you want to host a DNS server yourself.

The server-side setup, configuration and optimisation ends here. Now, you need to configure the clients to be able to use the server. On all machines that should have Internet connectivity, specify the gateway as the IP of the Internet server you just set up.

In Windows XP, go to Start > Control Panel > Network

Connections. Here, right-click the local area connection, and click Properties. In Properties, click 'Internet Protocol (TCP/IP)' from the list, and then again click Properties. Now specify the Default Gateway IP as that of the server IP. Go to Start > Settings > Control Panel > Network. Here, click on 'TCP/IP', and click Properties. Go to the Gateway tab, and specify the server's IP.

Using A Wireless Network

In this chapter, we will take a look at the uses for the different types of networks that we spoke of in the earlier chapters. If you are looking for reasons why you should consider Wi-Fi as a solution, this is the chapter that will make up your mind for you...

4.1 Putting Your Wireless Home Network To Work

Now that you have set up your wireless Home network, you need to get to know the various uses for it.

Sharing

The most basic use for any network is file sharing. Wireless networks are no different. If you have multiple computers around the house or home office, you can create shared folders and have files accessible between, say, your desktop and your laptop.

Even More Sharing

If you have a friend who also happens to be a neighbour, or vice versa, you can set up a wireless link, which will let you share files without spending a paisa on Internet bills. This will also help you save the costs of having to burn CDs and share data with your friends.

Internet

Perhaps the most basic function of any network setup today is to share Internet connectivity. Using an access point, or even an ad-hoc connection between a desktop and a laptop, you can enable the laptop to have Internet connectivity anywhere in the house. This eliminates the hassles of wiring up the house to have multiple LAN plug points. Now, if you want to sit in the balcony on a starry night and surf the Internet, or access that file you downloaded to your desktop while sitting in the garden, you can!

Peripherals

Where do you keep your printer? How about your scanner? If these questions sound insane, or if you answered, "Next to the computer, Duh!", welcome to the wireless world. Who says everything related to computers has to be located in one place? This is perhaps why most people have such an ugly computer setup.

One of the worst limitations of wires is the inability to get any distance between connected peripherals. However, with wireless-enabled peripherals, you can place your printer near the cabinet you keep paper in, the scanner near the wall unit that contains your picture albums, and your computer near the window. OK, so maybe that's a little far fetched, but what if you don't have a PC, and only use your laptop, even at home? Isn't it painful to have to connect those wires every time you want to print or scan something?

Entertainment

Just as with peripherals, the gadgets that constitute your home entertainment setup are also bound into place by the wires that

connect them. Wireless can be a couch potato's saviour. As every movie buff will tell you, the worst parts of watching movies at home, is right before and right after. That's when we have to walk towards the TV, stoop down and insert or eject the CDs or DVDs. Though this sounds like it could make it into the Guinness Book for laziness, wouldn't it be nice if your DVD player sat on a table within arm's reach, instead of 6 to 10 feet away either under or on top of the TV?

As you have probably figured out by now, the uses of wireless are only governed by your imagination. The hardest thing to do, though, is learn to 'think' wireless. The most common mistake people make is to buy wireless equipment, set it up, and then leave the device placement the way it was when it was wired. Why connect your printer wirelessly, if you still plan on keeping it on the same trolley that houses your PC?

4.2 Bluetooth Networks

Wireless networking doesn't only come in the 'Wi-Fi' flavour. For a Personal Area Network, Bluetooth is the best solution. The most common misinterpretation of that people make of the term 'Network', is to think that it only involves PCs.

Even when you connect your Bluetooth-enable phone to a Bluetooth headset, it is a form of networking at work. Bluetooth networks can let you connect your PDA and cell phone to your PC, your PDA to your cell phone, and even let you have a completely wireless mouse, joystick and keyboard.

It can also be the perfect solution to sharing Internet access between your mobile phone, PDA and your PC. With Bluetooth, you could set up your PDA to connect and use the home printer as well.

4.3 Wireless Away From Home

When travelling, you have to carry spare batteries, chargers, carry cases for all your mobile devices. The last thing you need is to have to carry and take care of data connector wires as well.

When on the road, nothing beats being wireless-enabled. Why unpack and boot up your laptop when you can send that short quick e-mail off in a flash using your PDA and mobile phone.

When staying at hotels around the world, you would have to be very lucky today, to find rooms with LAN connectors. Wireless has become the Internet access solution of choice that hotels and restaurants across the globe offer their patrons.

You also don't want to have to hook up a cradle, connect it to your laptop and sync your PDA everyday, just tapping on the sync icon and letting them connect wirelessly is just too right a solution to ignore.

4.4 Wireless Entertainment

This is where wireless starts to make a lot more sense. Most of us know the benefits of wireless networking, and are quite aware of how to use it. Even if we aren't, there is tons of help available via the Net and books. But who says something that's useful and practical can't also be used to have fun?

In today's fast paced world, we often miss out on opportunities to have fun. As work hours get longer, and people start working more and more at home, free time is rare. Anything that's rare automatically earns "precious" status, and that's exactly what entertainment has become to the majority. Whether it's

watching a movie with your friends or family, or flipping through picture albums, reliving the "good old days"-when you had time to spare, and time to care, or just listening to your favourite MP3s, it is all important. Even a ritual UT2004 frag match with friends in the neighbourhood is a great stress-buster, as is a game of Microsoft Hearts against your family. Though the possibilities are limitless, we'll stick to those who like to be entertained in their living rooms.

The TV

The idiot box has evolved into a powerful and innovative entertainment and informative tool. The choices of channels and programmes are mind-blowing, and the technologies are advancing rapidly in order to attempt to provide you with near-real, true-to-life image and sound quality. Whether it's "true-flat TVs" or "cinema-screen TVs", or perhaps the choice between medium-sized Plasma TVs and huge CRTs, the choices can even get confusing at times.

However, the TV is merely the window to your entertainment, quite like a PC monitor, which is merely the visual element of a whole system of components. Just as your computing experience relies on the hardware under the hood, your entertainment relies on the gadgets that connect to your TV.

Using the right combination of gadgets, you can have an entertainment centre with no visible wires at all. As described in Chapter 4.1, you can also have the freedom to place your gadgets or devices as and where you please. You can even have the freedom of hiding away gadgets so no one sees them. Some of the gadgets you should be considering are listed in Chapter 4.5.

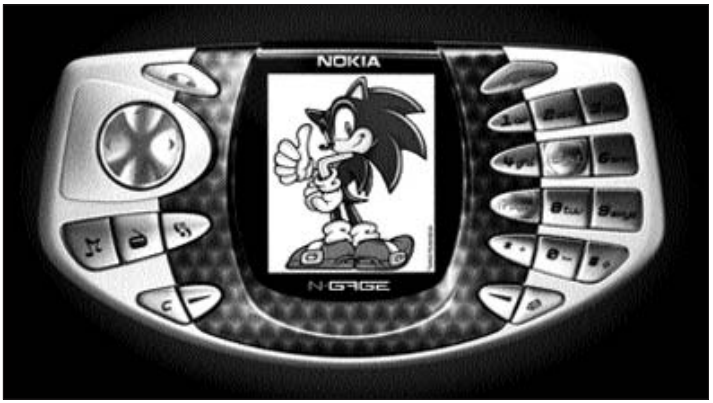
Gaming

Gaming is huge multi-billion dollar industry, and millions of people are using gaming more and more as a means of entertainment. There's just something about the fantasy world of gaming which appeals to our senses, much like the surreal world of movies.

Wireless can play a huge role in enhancing your gaming experience, as well as provide opportunities where none existed before. The simplest example is where you have a neighbour who is as into gaming as you, but neither of you has the requisite bandwidth that multiplayer games demand. Though a wired LAN would also give you the same connectivity, a Wireless LAN (W-LAN) setup removes the hassles and costs of running wires across rooftops and seeking permission from building associations, etc. With a wireless card in each computer, you can set up a W-LAN in a matter of minutes.

Of course, many people today are also using other wireless protocols such as Bluetooth to play multi-player games on their cell phones. Perhaps the most popular gamer-cell phone today is the Nokia n-Gage (see picture below).

You can also set up advanced networks using some of the gadgets shown in the next part.



The N-Gage has taken multiplayer gaming from the PC and brought it to mobiles

4.5 Cool Wireless Gadgets

Ever since wireless started catching on, every manufacturer has been hard at work integrating the technology into their offerings. The race to your home is on, and it's brutal. This, as it turns out, works to your benefit, as the gadgets become more useful and less expensive. Let's take a look at some of the gadgets that are available to you, either right here in India, through online shopping sites, or via that sweet relative coming in from the US.

HP's Digital Media Receiver

This digital Wi-Fi enabled receiver can stream movies, pictures and music from your PC and play it back on your home entertainment centre. You can even print pictures with the press of a button, provided you have a printer connected to your PC of course.

The Media Receiver also scans other networked computers for images and music, so you can enjoy everything that's available on your computer, or others.

It supports MP3, WMA, PLS, RMP and M3U audio formats, and JPG, GIF, BMP and PNG image formats. It also offers composite

HP's Digital Media Receiver

Video, S-Video and RCA outputs, so that you can connect it to any television set or audio player in the house.

A special feature is its ability to connect to other Digital Media Receivers in the vicinity using a W-LAN, and access shared files. It uses the 802.11b wireless protocol to connect.

GoVideo Wireless Media Receiver + DVD Player

This is another wireless media receiver that will let you stream media from your PC to your TV. With its easy-to-use menu interface it is a must have for those with entertainment fetishes.

It features 802.11g connectivity, which lets it connect easily to your Wireless Home Network, as well as an Ethernet connector, so people with standard wired LANs don't felt left out. The player can play DVD, VCD, DVD-RW, DVD+RW, Audio CDs, MP3 CDs, and Picture CDs.

It also boasts of an inbuilt Dolby Digital Surround Sound decoder, and an upgradeable firmware chip, which ensures future compatibility. It supports MPEG1, MPEG2 and MPEG4 videos as well as JPG, TIFF, PSD, PCT and BMP images. It can connect to your TV using either S-Video, Component Video, or Composite Video outputs.

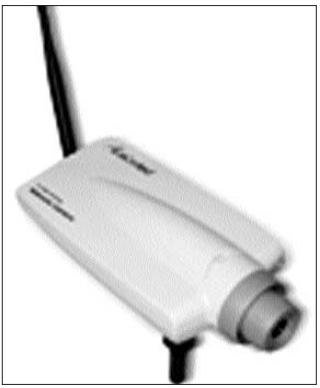
GoVideo's Wireless Media Receiver

The audio offering is about as good as it gets—it supports MP3 and WMA, and has various audio output connectors, including 6 Channel Discreet Surround Sound (RCA) or a simple stereo RCA output, Coaxial/Optical Digital Audio outputs and two headphone outputs on the front panel.

This player can also connect to your LAN or W-LAN and other Universal Plug and Play (UPnP) devices.

Actiontec 54 Mbps Wireless Network Camera

Video monitoring and surveillance just became easier with the release of the Actiontec 54 Mpbs Wireless Network Camera. Imagine being able to view what's going on in or around your home from virtually any location in the world. Now you can keep an eye on your children or monitor the safety of your home - all by opening a web browser and watching live streaming video. If you would rather watch it later, the Actiontec 54 Mbps Wireless Network Camera offers multiple recording and alert options. The possibilities are endless,and video surveillance just couldn't be easier or more convenient with the Actiontec 54 Mbps Wireless Network Camera.



Actiontec's Wireless Network Camera

hugms

hugms is a device designed for sending someone you care about a hug using your mobile phone. once hugms is connected to your mobile phone all you have to do is send it the phone number of the person you want to hug, and then squeeze. Sensors inside the device read how long and how hard you squeezed, and format a text message based on your hug.

Show your loved ones how much you care, with hugms

A long squeeze on hugms will produce a text message like:
'hhhhhhuuuuuuuuuuggggggg'
A short and hard squeeze will result in:
'hhHHUUUUug'

Nabaztag

Nabaztag is a WiFi rabbit designed by Violet (a company focused on the design of products and services based on calm and emotional technologies). This rabbit can access the Internet. The most interesting part is that the colors change depending on various parameters: the weather, car traffic or reception of e-mails. There is also different sounds as well as ear movement modified by those variables! It can also communicate with other rabbits located elsewhere, thanks to a coded language

The Nabaztag Wi-Fi rabbit

you can create—such as a specific posiiton of the ear to show that you are busy!

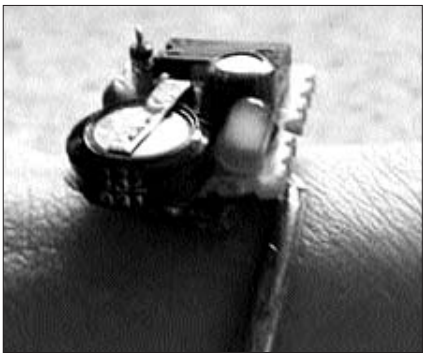
Bluetooth Rearview Mirror

LG showed off a prototype Bluetooth-enabled rearview mirror at this years 3GSM World Congress exhibition, in Cannes. The idea is pretty straightforward: pair up the mirror with your phone, using Bluetooth, and caller ID information is displayed as you drive. The mirror also functions as a hands-free speaker-phone, whic is great, because you don't want to go about searching for a cell phone when you are driving. It also boasts of a battery life of 150 hours standby and a talk-time of 7 hours. You should note, hoever, that talking on a cell phone while driving has been equated to drunk driving.

The LG Bluetooth Mirror

Prototype Wi-Fi Detector Ring

Looking at the prototype image, this ring looks a little ugly and ridiculous, but gadget freaks are less likely to care for looks, they willl be too busy sallivating over its 'coolness'. However, future models will have a bit more care put into the physical design and layout.



The Wi-Fi detector ring

The maximum detection range is a lit-

tle under 40 feet, with line-of-sight, of course—nothing exciting yet, but this can be improved upon—its antenna and the lack of a sensitive tunnel diode are the main reson for its short range. Besides, it's not supposed to connect to a WLAN, it only detects the presence of one.

Next-Gen Wi-Fi Detector

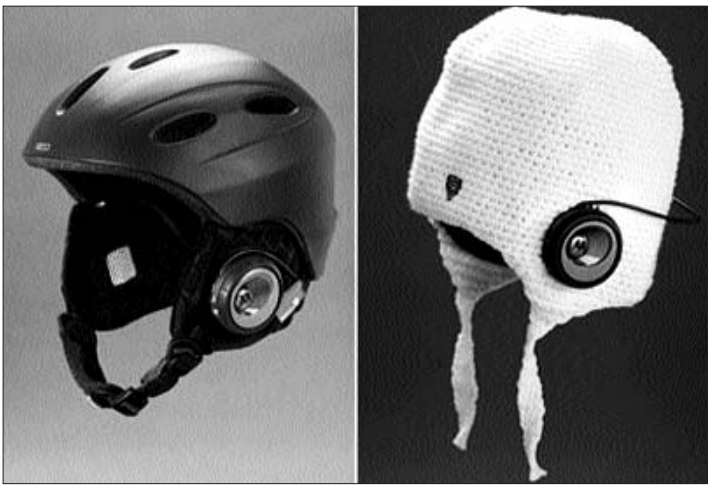
This gadget from Smart ID Technology, better known as the "WiFi Trekker," represents the latest generation of Smart's low cost 802.11 detectors.

The LG Bluetooth Mirror

The Trekker can auto-scan for networks—just press the button a couple of times, and when a network is discovered, the Trekker lights up and buzzes.

Motorola and Burton's Bluetooth Helmet and Beanies

Motorola's new Bluetooth helmets and beanies are co-designed with snowboard gear maker Burton. They are meant to work with



Motorola's bluetooth-enabled helmet and beanie

a new Bluetooth jacket, also developed for Burton.

Motorola also recently unveiled a new line of Bluetooth headphone and audio dongles, allowing you to dump audio from any device with a miniJack to wireless headphones.

D-Link DGL-4300 Gaming Router

The D-Link DGL-4300, proclaims to be the first 'gaming router', and is designed to optimise Ethernet traffic for a better gaming experience.

The D-Link DGL-4300

Though it sounds ridiculous at first (why would gaming need its own router?), it starts to make a little more sense once you understand how it works.

The router gives priority to gaming packets, so even though it allows huge file transfers, it sets them as background processes. D-link calls this intelligent packet processing engine technology 'GameFuel'.

The Egg

The Egg, designed by students Jennifer Bove, Thomas Stovicek and Nicholas Zambetti, is a wireless device that can communicate last-minute rescheduling of your appointments with other Egg owners.


The Egg that reschedules appointments

As time passes, and your appointment draws near, the light inside the Egg starts to dim. You can reschedule your plans with your friends by

shaking your egg, turnning it upside down—the light becomes brighter. When this happens The Egg knows you are going to be late, and informs other Eggs that you will be late.

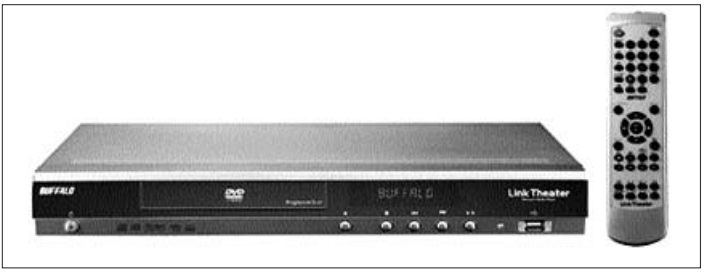
USB WiFi card

All new laptops seem to come with inbuilt Wi-Fi these days, but if you've got an older PC that you would like to add WiFi to, and you don't have a PCMCIA slot free, BenQ has an 802.11b card that pops into any available USB port.

A USB Wi-Fi card that Wi-Fi-enables anything with a USB port

Buffalo Technology's LinkTheater PC-P3WG/DVD 54Mbit/s Wireless Media Player with DVD

This networked DVD player can stream audio and video files from your Wi-Fi-enabled PC. The LinkTheater also has a USB 2.0 port, and will let you plug in an external hard drive, so just fill that drive with tons of movies and MP3s, and stream the media anywhere. What's even cooler is that it supports XviD, DivX, DivX HD, WMV, and WMV HD video files.



Buffalo Technology's LinkTheatre PC-P3WG Wireless Media Player

Siemens' Wearable Communication Badge

Siemens' new wearable communications device is a *Star Trek* style communication device that uses Bluetooth technology to connect to a central home communications server. It sends voice commands that the server translates into software commands that you can use to control your house.

The speech recognition technology doesn't need to be trained to understand your voice—a big advantage. It claims to understand over 30,000 words and predefined commands 'out-of-the-box'. You can control various functions of your digital home, such as using the house intercom system, opening doors and windows, and answering or dialling calls hands-free. It's a pity they couldn't make the lapel controller a little cooler looking. If you're looking to awe your friends with gadgets, this is one you should consider buying.

Siemen's Wearable Bluetooth-enabled Communication Badge

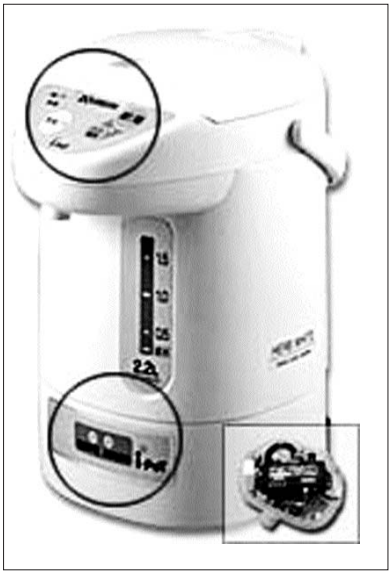
On/off Wireless Light Switch

This on/off switch, designed by Tobias Wong, is a wireless, metal-plate wall switch that can be placed anywhere in your house. All you need do is attache the remote component to a light bulb fixture or appliance, and you can switch it on or off using this switch.

With a range of 100 ft, and a price of about Rs 5,000, it's not exactly a solution for all the devices and electrical fixtures in your house, but if you set it up in your living room, you are sure to be able to make a conversation piece out of it.

iPot: Internet-Enabled Hotpot

A Japanese company, Zojirushi Corporation, has developed the first Internet-enabled 'Hotpot'. The iPot monitors its usage statistics and then sends the data out wirelessly, informing others about your tea drinking habits. Why anyone would want to do this is beyond us, but one theory that's ciculating the Net seems to make a little sense: perhaps the i-Pot could be used to keep an eye on an elderly grandmother or grandfather—grandparents with regular tea drinking habits could be gifted one of these, and if the usage drops, or stops, you could set the i-Pot to contact you. Obviously, this would send you rushing over to make sure all was well, and check why grandma or grandpa missed their daily dose of tea or caffeine. Makes sense, right?



The iPot: making hot water wirelessly

Just make sure to tell your grandparents to inform you if they leave town, or you are in for some worry!

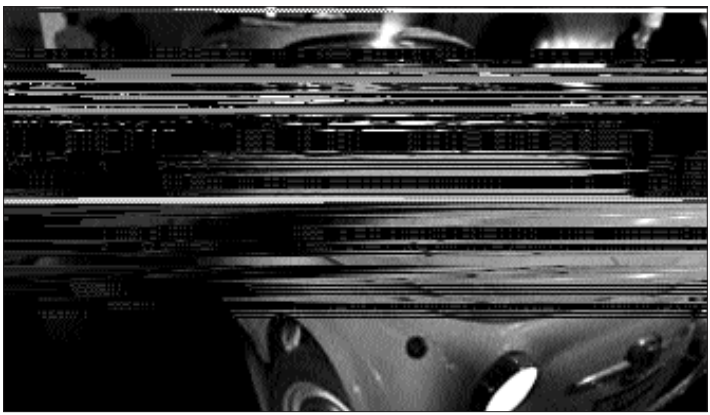
A Vintage Car With A Digital Twist

This vintage Fiat is not really a gadget anyone can go out and buy, but is a decent indicator of what you can build, or have built, if you have the time, money and enthusiasm for all things geeky.

In order to get into this car to open, you need to send your password to it by SMS; the car then starts flashing its lights and send a reply with something along the lines of "Good evening, welcome back! I'm thirsty, I'm out of fuel...". This makes life a lot more interesting than looking at a fuel gauge.

The car has TV cameras to monitor the passengers and its rear view mirrors are made up of screens that can be written on—just scrawl a message on the windows and instruct the car to send it as an e-mail! The car also has its own Web site, and automatically uploads images and messages taken or written inside it.

It is also capable of downloading MP3s from a prototype fuel pump with an inbuilt jukebox. When parked, it can broadcast images and movies from inside the car using a device installed between its headlights. Read more about the car at **http://www.interaction-ivrea.it/en/gallery/lamia500/index.asp**



The Vintage Fiat that has an inbuilt wireless communications network

The WIP-6050M, Samsung's WiFi phone

A standalone WiFi phone might seem pointless, especially when we have already seen cellular phones that come with inbuilt 802.11b, but Samsung's WIP-6050M is sleek enough to change your mind. It is 802.11g compatible, has a 65k color LCD screen, and a user interface that will remind people of Samsung's cell phones interface—not necessarily a good thing.

Samsung's WIP-6050M WiFi Phone

LTB's FreeZone WiFi headphones

These cool Wi-Fi headphones are compatible with PCs that have either 802.11b or 802.11g wireless networking cards, or any wireless audio source. Called FreeZone, the headphones will make any user with a wireless-enabled PC squeal with delight.

LTB's FreeZone WiFi headphones

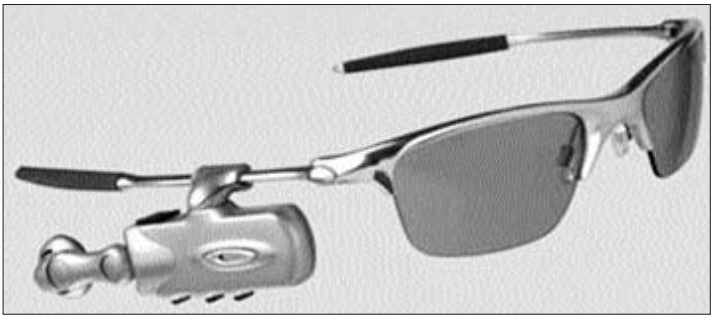
Future models will have true 5.1 surround sound capability, and

offer crystal clear audio. These headphones will be a delight to use while watching movies or gaming, and will ensure that you never disturb a soul at home.

World's First Bluetooth Sunglasses: Oakley RAZRWire

There's only so much your ears can take! With earrings, earphones and even spectacles and sun glasses depending on your ears to hold them up, it's about time people started making devices that are less of a earful.

Oakley, the designer eyeware giant, and Motorola, communications giant, have collaborated to produce a gadget that's as useful as it is trendy. The Oakley RAZRWire is simply a pair of Oakley's with an attached Bluetooth ear piece—courtesy Motorola. Now you can talk hands free on your mobile phone and look cool all the while. Don't expect them to be very affordable though, especially when going by Oakley's normal prices.



The Oakley RAZRWire: Wireless at its coolest

Sonos Digital Music System

The Sonos unit is a Wi-Fi distribution system that are also amplifiers, with speaker and line outs on the back of the unit. On the back of the unit there is also a four-port Ethernet switch, in case you want to use a wired LAN. It can connect with up to 16 computers, and also connect to other units wirelessly.

You can choose to listen to a song in all the rooms in your house, or in a particular room. You can also play multiple different songs in multiple rooms, so everyone has their choice of music playing. The Sonos can also stream Internet radio stations, or you can just plug in an audio device such as your stereo system into the audio input.

With 50 watts or power per channel and a weight of just under 5 kilos, this aluminium gadget is light and mobile.

The funky looking handheld controller (shown below) is great to use after you install the supplied Sonos Desktop software and link all your music together. The controls will remind you of an iPod, and its 3.5-inch LCD makes it a snap to browse through even the largest MP3 lists. You can also sort your collection by Artist, Album, Genre, Track Name, Composer, or even Playlist. The controllers Li-Ion battery is supposed to have a life of almost a week and takes only two hours to recharge. At an introductory price of about Rs 50,000, this device is for serious audiophiles that want to bring wireless technologies into their audio experience.

The Sonos Digital Music System's handheld controller

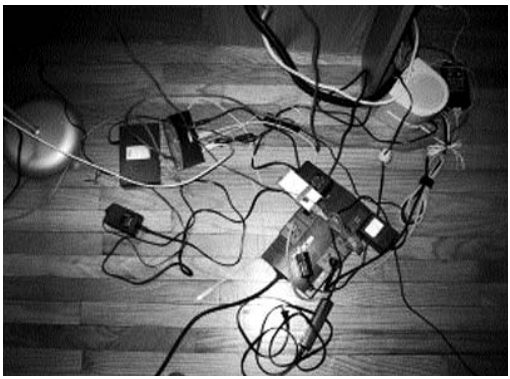
Security

In this chapter, we will list out some of the known vulnerabilities to WLANs, and also give you a look at the security software that can help overcome these vulnerabilities.

How can anything that broadcasts everything sent or received through the air be secure?

This is perhaps a question that each and everyone of us has thought at some point or another. And the truth is, Wireless LANs (WLANs) are a lot less secure than their wired counterparts. Perhaps WLANs are not the best solution for the paranoid, but then again, neither is the Internet. The mother of all networks, the Internet, has become the single biggest threat to the security and privacy of the millions that use it, yet the number of people using it is increasing by millions every year. The only safe computer is one that isn't networked at all, and has no Internet connection, but who wants that?

It's obvious that every good thing comes with its price, and WLANs are no different. Yes your data is more at risk than those on a regular wired LAN; yes your computer can be hacked into using your wireless card; however, bypassing the security that you can set up for your WLAN is something only a professional hacker could do, and chances are, if a professional hacker wants to get into your computer that badly, he probably already has access-WLAN or not.



In this chapter, we will list out some of the known vulnerabilities to WLANs, and also give you a look at the security software that can help overcome these vulnerabilities.

5.1 Threats To WLANs

WLANs are vulnerable in various ways, and all the vulnerabilities can be classified into two types:

1. Unauthorised Access Threats
2. Denial of Authorised Access

The first is perhaps the most deadly, as this involves threats from hackers and viruses, in an attempt to get into your network and access your data. The second type is more or less like a Denial of Service (DoS) attack, where functionality of your network may be affected by some other device, either intentionally or unintentionally.

Here we will focus more on threats of the first type, as they are more of a security risk and are perpetrated by malicious users or software.

Default SSIDs

Every wireless access point manufacturer has known and well publicised Service Set Identifiers (SSIDs). All access points ship with their default SSIDs, which a user is expected to change when they set up their WLAN. Quite often, home users set up their WLAN by powering up everything, setting the type of connection to ad-hoc, which is default, and then are overjoyed by the fact that a connection is established immediately. There are no more checks done, and the network is left the way it is, for fear of changing a setting and finding that clients cannot connect. This is perhaps the most common mistake that people make, and leave their WLAN open for absolutely anyone to access.

The very first thing you need to do when configuring your access point is to change the SSID to something only authorised users of your WLAN will know.

Use Uncommon SSIDs

The second biggest mistake people make is to use their first names or surnames as their SSID. Think of an SSID like your ATM bank card PIN, or your email address password, this will help you create a decently un-guessable SSID.

Those setting up multiple networks, with more than one SSID need to take care to not set simple SSIDs and not use a simple variation of a single SSID. Security experts have often found homes and small offices using their names and company names as their SSID. Moreover, people have used the simplest variation of SSIDs over different floors. You need to think like a network intruder would: If a company is called XYZ Pvt. Ltd., and has offices on the third, fourth and fifth floor, the very first guesses of an unauthorised user would be "XYZ", "XYZ3", "XYZ4" and "XYZ5". Though this sounds silly in hindsight, many of us have been caught making this very simple mistake which puts our entire network at risk.

Don't Broadcast SSIDs

Wireless access points can be configured to stop broadcasting SSIDs, as is usually the case. This will help ensure that unauthorised users in the vicinity do not detect your SSID by default.

Of course, there are tools available that will still hack your SSID from the signals that are transmitted in your network, but turning off the broadcast of your SSID will stop novice hackers or rogue wireless devices from accessing your network.

Use IP/MAC Access Control

If your network consists of only a few devices, make sure to set your access point to limit access to only those devices. You can do this when configuring the access point. Either set it to acknowledge only a given IP, or range of IPs, or set it to allow access to only the specified MAC addresses. Each wireless device will have a card that has a unique MAC address. Find this address from your device and enter it into the access point's list of allowed devices.

Though even these can be spoofed by the most ingenious of hackers, you are probably never going to encounter one-unless you happen to work for the government, or are an employee of a huge multinational company. The safest option is to set restricted access only to the specified MAC addresses, as these are much harder to spoof.

Access Point Placement

It's amazing how many people take what is printed on boxes literally. Just because your access point says that it covers a radius of 200 feet doesn't mean that the signal abruptly ceases to exist at that point!

For a home, you most likely aren't going to need an access point in the first place, but in a small office that could be considerably bigger than your home, you might add one in just to keep the signal strength healthy for all your users. However, placing an access point near a window, door or outer boundary wall is not advisable. Since most access points are omni-directional, their signal extends beyond the physical perimeter of your home or office. This means that someone sitting outside your house or office in a car, or a neighbouring building could potentially access your WLAN.

The best way to prevent this is to make sure access points are located towards the centre of your home or office, and you should use a laptop or mobile device to investigate how far out, in all directions your signal extends. A good warning sign that your network extends a little too far out of your perimeter is strangers repeatedly sitting in cars or at neighbouring bus stops, with laptops, chuckling to themselves.

WEP

Wired Equivalent Protocol (WEP) is an encryption standard for 802.11b networks. It was introduced a long ago, and even though it was found to contain severe security flaws, continues to be in use today by somewhat outdated equipment.

When buying Wi-Fi equipment and peripherals, make sure that all of them support more robust security and encryption techniques than WEP such as WPA.

Client Infections

The very reason you install a Wi-Fi network may be its downfall, mobility. The problem with a WLAN is that its clients are mobile. Laptops, especially, can cause much damage to your LAN as they are carried about to locations across the city, country or even the world. These laptops are used by executives and management personnel to connect to other WLANs, in airports, coffee bars, hotels, etc., and can easily pick up viruses and worms. When they return

to your network, they can spread these worms through the network and infect other machines, which in turn will breach any security practices you may have in place.

The only way to combat this is to impress upon your users the importance of keeping their client PCs updated with the latest antivirus definitions and security patches. Even in your home network, you need to be careful to update all computers with the latest security fixes, or else you could end up transmitting a virus from home to computers on your office network.

War Driving

War Driving is a term used to describe a hacker that literally drives up outside a building that has a WLAN and attempts to access the network using his or her hacking tools. Some of these tools are available freely on the Net, and do not even require a hacker's level of knowledge to use. So, just about anyone armed with the right (or wrong!) tools can gain access to your network if it isn't configured properly. The solution to this is to have better access point placement, as described earlier in the same section.

Threat Outcomes

If a hacker gained access to your Wi-Fi-enabled computer, or your WLAN, there could be a multitude of outcomes, depending on what the attacker wants.

Internet Usage: More often than not, people who gain unauthorised entry to a WLAN will use your Internet connection. This gives them free Internet access, and shields them from being traced on the Net-much like what an anonymiser service does. Though this may not sound as bad, it is in fact worse than you can imagine. Most people's activities online are governed by whether or not they feel secure about their identity being hidden. A user who gains unauthorised access to your network knows that all his activities can only be traced back to you, and thus may use your network to download warez, surf illegal pornography Web sites, or send spam and worms out on to the Internet. Depending on which

laws he breaks, you find yourself getting into serious trouble for things that you did not do.

Information: Most of us are paranoid about our personal information. Most of us don't even like giving out our real e-mail addresses, so someone gaining access to files that you think are private and secure is somewhat of a nightmare come true. An attacker can also gain access to cookies stored on your computer, and also any confidential material such as office documents and trade secrets that are stored on your laptop or desktop. Your online purchases via credit card transactions or Internet banking details and passwords may be accessed by the attacker. If you find yourself poorer by a few thousands all of a sudden, or find that you bought the gadgets you always wanted to have by credit card, you know where to start looking.

File Damage: Some attackers are just malevolent, and have no interest in anything but damaging your computer. These are generally one-off attacks and result with most of your files going missing or being changed. For example, you may find all your word documents deleted, or all text replaced with something along the lines of "MUHAHAHAHAHAHA! You were hacked by Da Hax-Master."

DoS/DDoS: Your Internet connection may be used to launch Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks on the Internet. Hackers use the Wardriving technique to find vulnerable WLANs and then infect the computers with worms or Trojans that they can control via the Internet. These worms or Trojans lie dormant waiting for a signal from the hacker. When a hacker wants to target another computer, he may use your computer to hack into another, or just launch a huge DDoS attack against his victim, using your computer and thousands of others similar to yours which are online at that moment.

5.2 Must-have Security Tools

In order to combat the threats to your WLAN, there are a few software tools you should keep handy. Some of these are designed to keep hackers out using encryption and passwords, and other security measures, while others are tools that hackers would use, and which you can use as well to check your network for vulnerabilities.

The Hacker's Tools

NetStumbler

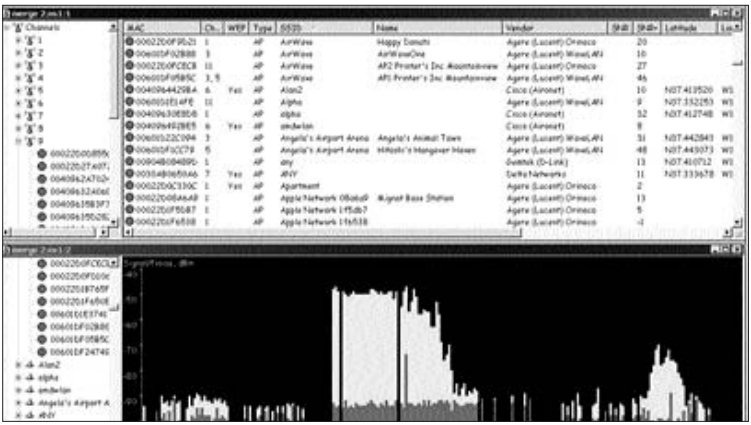
This is a tool that hackers would use in order to view details about your network. NetStumbler can search for and locate all available wireless devices within range. It displays available access points, their SSIDs, the channels they operate on, what type of encryption and security in place, and the signal strength at the current location. The tool can also connect to GPS technologies to map and display the exact geographic location of the access points.

You can put NetStumbler to work for you by using your laptop and circling your home to see how far your signal extends. You can also use it to test the security of your wireless security solutions.

NetStumbler is "beggarware", software developed by programmers that request a donation for the use of their products, though this donation is completely voluntary.

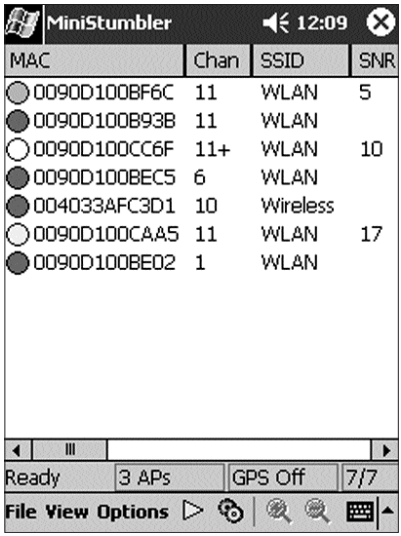
MiniStumbler

Another tool created by the developers of NetStumbler,



Net Stumbler can connect to GPS technologis to map and display geographic location of the access points

MiniStumbler can be used on devices running PocketPC 3 and PocketPC 2002 operating systems. The functionality is the same as NetStumbler, and the uses similar. You can get both NetStumbler and MiniStumbler at www.net-stumbler.com.

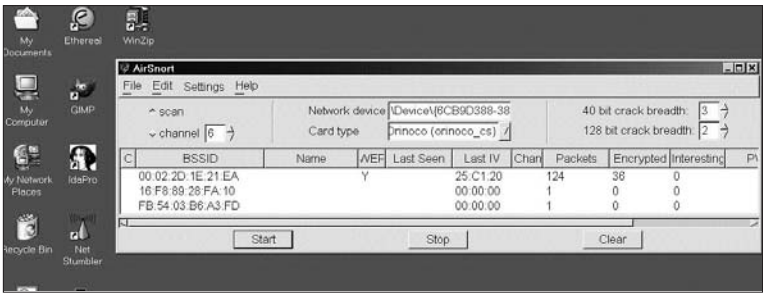


AirSnort

This is a WLAN tool that cracks WEP encryption. It sits as an invisible client on a network and "collects" packets and analyses them. Once it has gathered sufficient packets, it analyses them and attempts to decrypt the WEP code for the network. AirSnort eventually figures out the WEP key and lets the rogue client connect to the network as an authorised client. This tool can also be used to check the security of your WLAN and also to retrieve lost WLAN passwords. Get it from www.airsnort.com.

SSID Sniff

This is a tool that is dedicated to finding a wireless network's SSID. It is available at **www.bastard.net**.



RedFang

This was a proof of concept tool that could find non-discoverable Bluetooth devices by using brute force to find the last six bytes of a devices address. This tool was developed by @stake (**www.atstake.com**). The company has since been acquired by Symantec, the AntiVirus bigwigs, on 8 October, 2004. The original RedFang tool is still making its rounds on the Internet, though on sites that we would rather not name, because of their illegal or pornographic content or sponsors. This information is provided to you so that you are aware that even your Bluetooth devices are not really safe, even if your device is NOT set to discoverable mode.

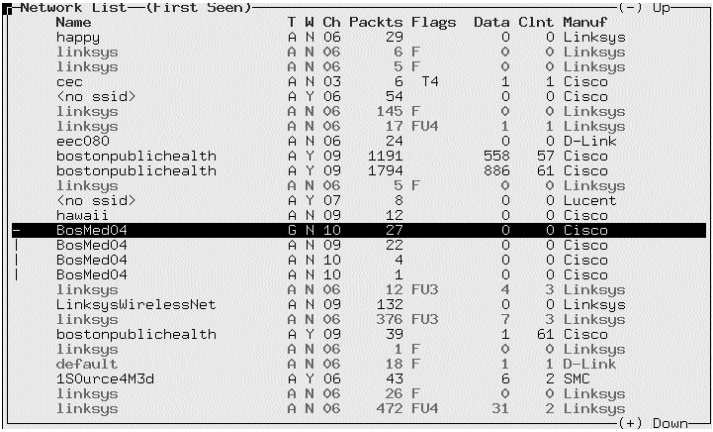
BTScanner

Available for download at **http://www.zone-h.org**, BTScanner is a tool that lets you scan for Bluetooth devices in your vicinity and provide you with as much information about them as possible without actually pairing with the devices. This tools allows you to make educated guesses about the type of device that BTScanner finds information about.

Network Admin's Tools

FakeAP

While most tools attempt to hide and cloak your access points, FakeAP goes in quite the opposite direction. It is generally used as a **honeypot***, to catch would be hackers in the act, or analyse the tools they use. The tool uses the concept that the best place to hide is in a crowd, and literally creates thousands of fake access points (thus the name FakeAP). If your network consists of two or three access points, using FakeAP will drive would-be hackers crazy when they try and intrude upon your network. Unless they have plain dumb luck, the chances of a hacker finding the actual access points, hidden amongst the thousands of fake ones, is remote at best. The developers describe their tool as "Times Square on New Year's eve", and you can read more about it, or download the free tool from **www.blackalchemy.to**.



Kismet

The default wireless network administration tool, with good reason, Kismet works with any wireless card (802.11a/b/g) that supports raw packet monitoring mode. It can be used as an Intrusion Detection System (IDS), an invisible network detector, as well as a packet sniffer. It is available at http://www.kismetwireless.net/.

Snort

The self-proclaimed "heavyweight champion of intrusion prevention", Snort is a popular open source network intrusion prevention system. It is capable of real-time traffic analysis as well as packet logging. It can be used to detect many types of probes and attacks, such as SMB probes, OS fingerprinting, stealth port scans, buffer overflow attacks and much, much more. The clincher is its real-time alerting capabilities, which make it a network administrators favourite IDS tool.

*According to online encyclopedia, Wikipedia, “A honeypot is a trap set to detect or deflect attempts at unauthorised use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network, but which is actually isolated and protected, and which seems to contain information that would be of value to attackers.”

WIDS

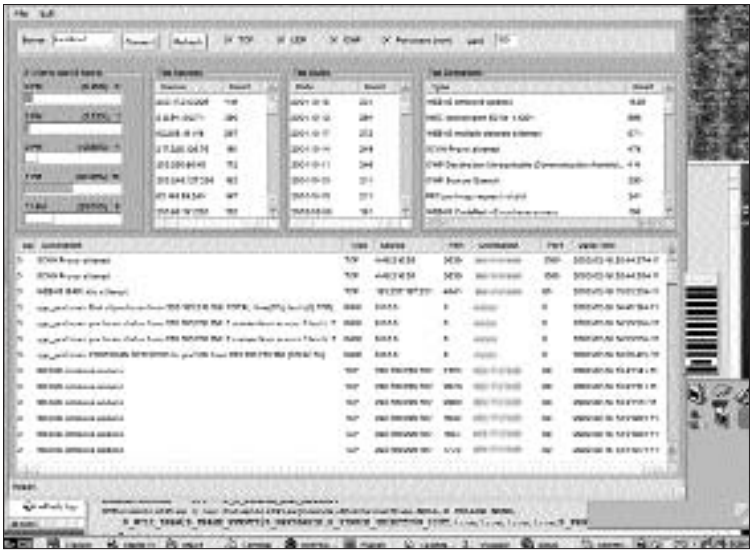
Short for Wireless Intrusion Detection System, WIDS can be used by wireless network administrators as a honeypot. Download it from **http://packetstorm.linuxsecurity.com.**

Wellenreiter

This is a GTK/Perl program that helps you discover and audit 802.11b wireless networks. The inbuilt statistics engine gives you common parameters provided by wireless drivers, and lets you view details about the consistency and signal strength of a network. It can also be used to detect nearby access points, networks, and ad-hoc cards. It is also capable of brute force cracking the eSSID of low-traffic networks. It can be used by network administrators or users as an IDS. Read more about this tool at **http://www.remote-exploit.org**.

WIDZ 1.8

This is an Intrusion Detection System for the IEEE 802.11 family of protocols. It guards access points and monitors local frequencies

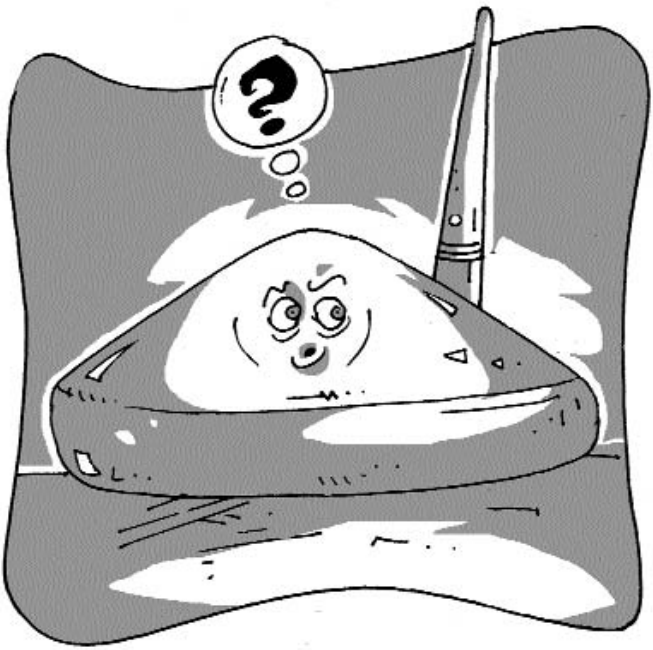


Widz is an Intrusion Detection System for the 802.11 family of protocols

for potentially malevolent activity. It detects scans, association floods, and bogus or rogue APs, and can be easily integrated to work with other WLAN monitoring tools such as Snort.

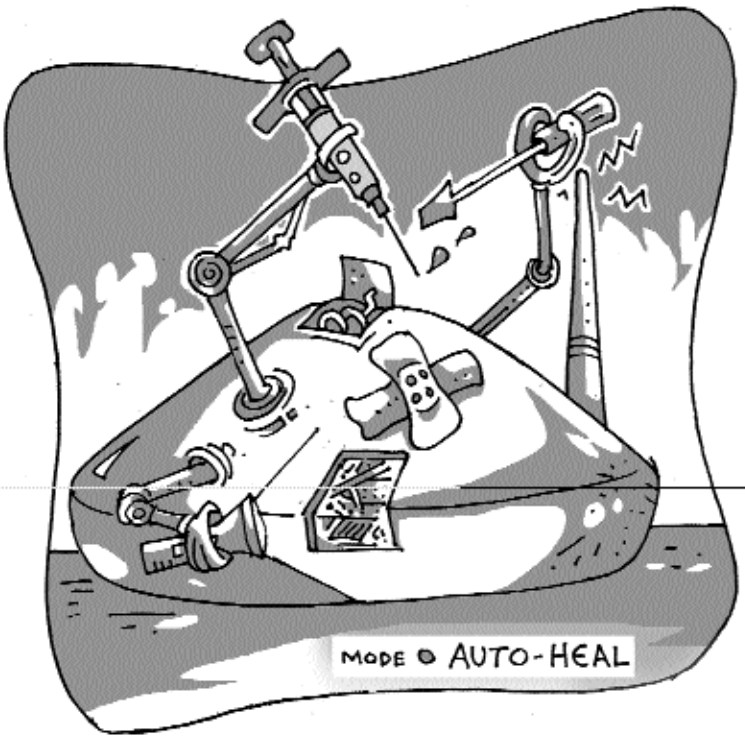
Download the tool from **http://packetstorm.linuxsecurity. com**.

Wireless Knowledge



There are always a million Dos and Don'ts for everything tech, and situations you can't seem to get yourself out of, or questions you have been dying to ask; wireless networks and devices are no different. This chapter will try to answer any questions and solve any problems that you may encounter while setting up or using your Wi-Fi network.

6.1 FAQs And Troubleshooting



What is an Access Point?

An access point (also known as a base station) is a wireless server that connects clients to an internal network. They are wireless LAN/WAN transceivers that act as a centre point of an all-wireless network, or as a connection point between wireless and wired networks.

Does an antenna affect wireless LAN security?

Yes. The wrong kind of antenna could extend the wireless network beyond the physical perimeter of your home or office. Choose the

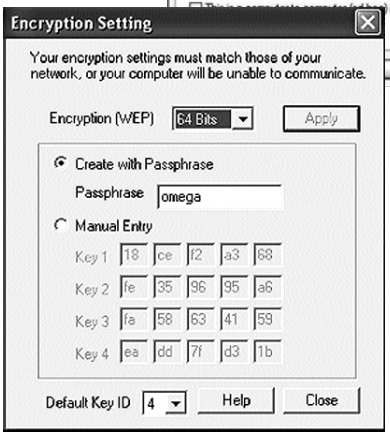
right type of antenna, and place it in a location such that you get optimum coverage inside your physical perimeter, and minimum "leakage" of signal out side the perimeter.

What is an Insertion attack?

When a hacker or attacker attempts to add a client or access point to an existing network, it is called an insertion attack. More often than not, employees of a company are to blame: they install a base station on their own, do not configure or secure it properly, and this becomes a security hazard, as security on a WLAN is only as strong as the weakest point.

Can I encrypt the SSID using WEP?

No. The Wired Equivalent Privacy (WEP) encryption standard only encrypts data packets, and not any of the management packets. Since the SSID is sent out in these management packets, namely the beacon and probe management packets, it is not encrypted even if WEP is turned on. The SSID goes over the air in clear text, making it easy for an intruder to get hold of. You are better off turning SSID broadcasts off, and forcing your clients to do a network search when they boot up.



What is this "Jamming" I hear about?

Jamming is sort of a Denial of Service (DoS) attack against your wireless network. It can be achieved in many ways by an attacker. The easiest method is to send out a much stronger signal than your access point, using the same SSID and channel of the 2.4 GHz frequency that your network uses. This will confuse all your wireless clients, and end up reducing your network bandwidth, or even killing your network. Use one of the tools mentioned in Chapter 5 to survey your premises and find out whether there are any rogue devices in the vicinity. If there are, change your SSID, channel settings and WEP key immediately.

Why do I get such a low network bandwidth?

Before setting up your network you should run an amateur site survey using the tools mentioned in the previous chapter, Security, of this book. Not only do they help improve your access point placement, they also inform you of any rogue devices or interfering devices in the vicinity. If you place your access point or wireless device too close to a microwave or cordless phone that runs on the 2.4 GHz frequency, be prepared to have a lot of interference, and perhaps even network data loss. Make sure to keep other devices that run at frequencies greater than 2 GHz as far away as possible from your wireless access points and clients.

What are the real-life data transfer speeds I can expect from a WLAN?

The 802.11b standard offers a theoretical data transfer speed of 11 Mbps (that's in bits, not bytes), and the 802.11g standard boasts of theoretical speeds of up to 54 Mbps. Though this is still very slow when compared to the 100 Mbps bandwidth offered by standard Ethernet, it would still be sufficient for most users. Of course, just as we never really get 100 Mbps on a wired LAN, you will never get the rated theoretical speeds on a WLAN either. Expect to see speeds of a maximum of 5 Mbps for 802.11b and 20 Mbps for a 802.11g network.

I have 802.11g compatible equipment, but I still don't get more that 3 or 4 Mbps transfer speeds. Why is that?

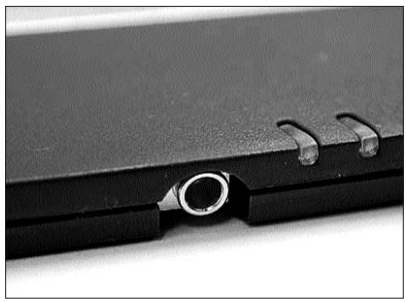
Unfortunately, though devices of the 802.11b and 802.11g standards can co-exist in the same network, you are bound to see a huge drop in performance when a slower 802.11b devices connects to your network. The hardware is designed to shift into slower modes when interacting with a slower device. Thus, introducing an 802.11b device into a network of 802.11g devices, is in effect the same as running an 802.11b network.

Will being near a WLAN for a prolonged period of time give me brain cancer, like with mobiles?

Not unless you stick your head into a fileserver cabinet that has multiple wireless cards, and keep your head in there for a decade or two. Though, the laws of probability dictate that stressing over such things might get to you first. A wireless card or access point emits the same signals as your microwave oven and cell phone, but the signals are about a 100 to 1,000 times weaker. Moreover, wireless devices emit signals irregularly, only when data is transferred, while cell phones emit signals, and thus radiation, constantly, so long as they're powered on. These signals increase in strength when you receive or make a call. So in short, you are about a 100 to 1,000 times safer being exposed to wireless devices than you are with your cell phone.

My laptop has a weak wireless card, and I have to be really close to an access point to get a signal. How do I increase its range?

If your laptop's wireless card has the option to attach an external antenna, you should do that. You can tell whether this option is available to you by looking for a jack similar to a headphone or microphone jack. If your laptop does not support this antenna extension, you can always add a USB wireless network adapter with a decent external antenna.



You should also go through the available configuration options for your laptop's wireless card, as some of them give you the option of increasing the transmission power of the card. Remember that certain laptop models reduce the power sent to peripherals when running in their battery savings mode, the best way to tell is by noticing whether the range seems to improve when you start charging the laptop.

Can I use Wi-Fi to join existing wired LANs?

Yes, you can use multiple access points running in bridging mode to bridge connections between various wired LANs. However, since wireless access points run a lot slower than their wired counterparts, the access speeds from one LAN to another might not be up to the mark. Unless using a hardware switch or router is forbidden or impossible, you should not attempt to bridge two wired LAN networks using this solution.

Why does everyone recommend Wi-Fi, and then warn you about the possible security flaws?

Wireless has given us a solution to problems that could not be fixed earlier. Wireless can also save a lot of money, by doing away with cabling costs, and the need to fill out a hundred forms, while standing in a never-ending queue inside a government office, in order to get permission to dig up a road to lay your cables. It's the same reason most of us use the Windows operating system; we are all more at threat when using Windows than any other OS, but its ease of use and simplicity has us hooked.

What is ad-hoc mode, and is it advisable to use it?

Devices running in ad-hoc mode can connect to each other directly, without needing to connect to an access point. All devices running in ad-hoc mode can discover each other and communicate with each other to form an unorganised network. The limitation here is that all the devices must share the same SSID and operate on the same Wi-Fi channel. The disadvantages of such networks is that the performance takes a hit as the number of devices increases, and there is no way to properly manage, and thus protect, the users of such a network.

Ad-hoc networks have one huge disadvantage as well: they cannot connect to a wired LAN to access the Internet, and to make this possible, you would have to invest extra in a dedicated hardware or software-based gateway to bridge the wired and wireless networks.

What can a wireless network do for me?

A wireless network can let you do the following:

1. Connect all your devices together without any signs of ugly wires
2. Share files easily between devices
3. Share an Internet connection easily
4. Set up a multiplayer gaming network
5. Carry your mobile devices around your house, the way they were meant to be, and not worry about losing connectivity to your LAN
6. Show off to your friends, as having a wireless network is the in-thing today

My clients can't connect to my access point; what's wrong?

1. Make sure the SSIDs are exactly the same, as SSIDs are case sensitive as well.
2. Make sure the access point is configured properly. In some cases there may be a checkbox that says something like "Enable access point", which needs to be checked before the access point becomes accessible.
3. Make sure all devices are set to use the same Wi-Fi channel, generally 6 or 11.

4. If you have turned on the access list, make sure that the clients' IP addresses and MAC addresses match those in the access points list.

5. Check for disturbances caused by other devices such as microwaves or cordless phones that work on the 2.4 GHz frequency.

6. Make sure your clients are as close as possible to the access point when configuring them. Obstructions such as walls could block the signal.

7. Make sure all the cards connected to the computers have the correct drivers loaded and are enabled.

8. If you have enabled WEP, as you should, turn it off and see if the clients connect. If they do, you have a network strength problem.

9. Change the position of the access point's antenna and try to get a better signal.

10. If you are having signal strength problems, consider getting a better antenna-the default 4 dBi antenna can be upgraded to as much as 24 dBi. You could also consider getting a directional antenna, which would concentrate the signal in one direction.

11. Update the OS on the clients. Windows XP SP2, for example, comes with better Wi-Fi support and inbuilt support for WPA.

Any advice for first timers?

Yes, tons! We'll take this opportunity to give you a set of more comprehensive troubleshooting tips than the short list above:

Though manufacturers have put a lot of effort into making WLAN setups easy and quick, there are times when a few hiccups

will have you tearing your hair out.

The most common connectivity problem occurs with one access point and one client device. For this you should use the checklist in the answer above to solve your problem.

When the network is a little bigger, and you have, say, four access points connecting 12 client machines, and some connect fine while others don't, you begin to feel the throbbing of the veins in your temple. The first step is to calm down and start thinking logically again. Ask yourself a simple question, "Is there a pattern here?".

What you need to do is visualise the layout of your mansion (you would need one to have this many access points and client PCs) or office. If all the computers that can't seem to connect, or are getting miserable network speeds, are located in the same overall geographical area, then you know the access point that they're supposed to be connecting to is to blame. The first thing to do is to make sure it's switched on! Sure this sounds silly, but you won't believe the number of network administrators who have kicked themselves repeatedly in the backside because they didn't think of checking such a basic problem. If it's all powered up and tells you via its LEDs that it's ready and rearing to go, you can bet it's probably a simple configuration error. Check the SSID! A little typo or misplaced capital letter can cause you much pain.

The next step is to look for other devices that might cause interference in the particular area of the building where the problem occurs, such as an evil giant microwave, or a powerful cordless phone that someone thought looked good placed on top of your access point!

No? All right then, try pinging the access point from a wireless client. If it pings, but you cannot connect to it from a wired client, go and check that the Ethernet cable is plugged in properly, think of yourself wearing a "Kick Me" sign for the rest of the week, that ought to give you the energy to go back and check the cable.

If it refuses to ping, but uses its LEDs to claim that it's online and functioning properly, reset it a couple of times and try pinging it about 10 minutes after it comes online again, from both wireless and wired clients. If that fails, either you can check and recheck its configuration settings, and compare them to the setting of a working access point, or you could use a sledge hammer to finally see what the insides of an access point look like, unless it's still under warranty, of course.

This scenario is rare though, as most often it is a bad configuration job that spoils the day.

If the wired LAN can communicate with the access point, but the wireless devices refuse to do so, you need to first test signal strengths. You can use NetStumbler, one of the utilities mentioned in the previous chapter, Security, to do this. If the signal strength is bad, check the access point's antenna, and move it about to look for improvements; consider changing the antenna if this does not work. If the signal strength is good, and still the wireless clients refuse to connect, try changing the channel on which the access point operates, and make the same change for one of the wireless clients that couldn't connect earlier. If this let's the client connect, you have an interference problem. If not, change the channel back to the original value and check the SSID once again.

The next step is to check and recheck the WEP configuration. Make sure that all the WEP settings on the access point and the test client are identical-the encryption level (40, 64 or 128-bit). Try changing the WEP settings on both the access point and the wireless test client and see if that helps.

The next step is to check for a mismatched configuration of DHCP. If your client is set to use a static IP and your access point set to let clients connect and assign IPs using DHCP, the client will not be able to ping the access point (as in our example problem here). So make sure that both, client and access point, are set to use either DHCP or fixed IPs. Some access points have an inbuilt

DHCP server, if this is so with your access point, make sure you disable it and force the access point to assign IPs that it obtains from your wired LAN's DHCP server.

By now you've either solved the problem or are looking at the insides of your access point. If all the above solutions fail, please have a service engineer look at the device, or send it back to the company you purchased it from.

More things to remember

In case you are using an access list, where IPs are fixed, and only a given list of IPs or MAC addresses are allowed to connect to the network, make sure to enter this "white list" on all the access point in your network, or else you will find that some clients, when moved, are not able to access the network anymore.

If you have a network with more than one access point, and both have the ability to assign IPs using inbuilt DHCP, and both work on an identical address range such as, say, 192.168.0.XXX, pretty soon your network will get clogged with duplicate IPs. The moral of the story? Never be afraid to manually configure your devices, or you might end up in more trouble than you bargained for. In this scenario, you should set each access point a fixed and non-overlapping IP limit that they are allowed to assign to clients. This can be done while first configuring the access point itself.

6.2 Devices That Can Connect To A WLAN

Laptops / Notebooks

The most common reason for having a wireless network is the fact that an increasing number of people are buying laptops that already have Wi-Fi cards inbuilt into them. People buy laptops for mobility. If you are always on the move, a laptop is the only solution you have in order to be able to carry your work around with you.

Desktop PCs

A common misconception people have is that wireless networks are only meant for laptop owners. However, this shouldn't deter people with desktops from setting up a wireless LAN, as you will see from the list below of other devices that can be connected wirelessly.

Printers

The most common shared device in a home or office is a printer. No longer do you need to connect a printer directly to a PC, as standalone printers that connect directly to a network have been around for sometime. Now, even wireless printers have become the norm, and there's no need to connect it to a wire, just find a

suitable nook, near a power supply, in your home or office, and your printer is ready to do what it does best.

Entertainment Streamer*

This is a relatively new breed of device which streams the movies, music and pictures stored on your PC to your big screen TV (or small screen, doesn't matter). This gadget is useful for those who have a PC located in the bedroom, but spend family time in the living room-with an entertainment streamer, you never need to watch movies one at a time, sitting at your PC, or be too embarrassed to show your friends your vacation album, because the PC is in the bedroom and the bedroom is a mess! These Wi-Fi enabled media servers bring the power of your PC to the living room, or to any television or music system in the house.

Wi-Fi Enabled File Severs*

Sony will soon come out with a file server that has an inbuilt access point and a 20 GB hard drive. All you need to do is set it up and let your network users start copying files to and from the Wi-Fi file server. Devices like this will become more common in the coming year, and prices will fall. You can soon have an always-available backup storage drive that can be hidden away out of sight. And since it's also an access point, it increases the wireless coverage within your house or office.

PDAs*

With PDAs becoming Wi-Fi friendly, you can connect to your WLAN while using your little PDA and surf the Net and check your e-mail. This will do away with the need to carry laptops around with us all the time. As of now, you can buy a Wi-Fi card that fits

into your PDA, converting it into a wireless device.

Digital Cameras*

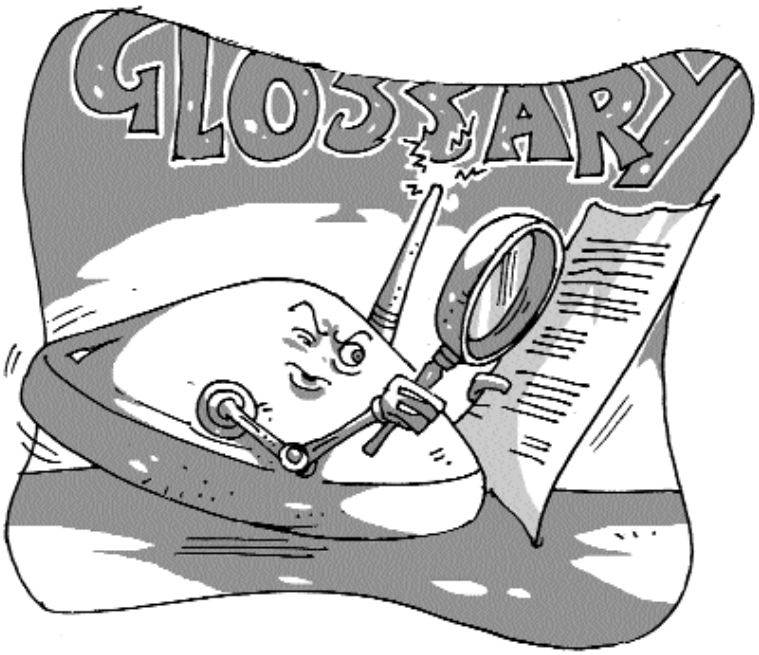
Manufacturers have already started launching digital cameras that are Wi-Fi enabled and can connect to a wireless network to store their pictures in a shared folder, or e-mail the pictures to a desired e-mail address.

Enablers*

Prototypes of Wi-Fi enablers are available, which will take any device that we can connect to a PCs USB port and convert it into a wireless device. The "enablers" will connect to gadgets such as digital cameras, PDAs, etc., via the same cable you use to connect them to your PC, and make these devices available on, or able to connect to, the WLAN. Once such enablers come into the market, any and everything that you connect to your computer today using wires, you will be able to connect wirelessly tomorrow.

* Details on the above mentioned products are available in Chapter 4.

Glossary



When reading about Wi-Fi, it is very easy to get a little confused with all the terminology, and also the numbering system for different wireless standards.

Not only will this Glossary explain any jargon you come across when reading this book, it will also serve as a handy guide to understanding some technologies that you are bound to encounter in the near future.

100BaseT
A synonym for the Fast Ethernet networking standard. The '100' here refers to the maximum data transfer rate of 100 Mbps over twisted-pair wiring.

10BaseT
A synonym for the Ethernet networking standard. The '10' here refers to the maximum data transfer rate of 10 Mbps over twisted-pair wiring.

3DES
The three-DES data encryption standard. This is a three-step data encryption algorithm that evolved from DES. 3DES provides greater security than DES because it encrypts, decrypts, and then again encrypts the data, thus using three keys instead of one. The size of a 3DES key is also three times larger—168 bits, as against the 56 bits for DES.

802.11
A set of IEEE standards for data transmission over wireless LANs (WLANs). The specifications within 802.11 include 802.11, 802.11a, 802.11b, and 802.11g. All these use the Ethernet protocol. 802.11 describes a WLAN that operates in the 2.4 GHz range and provides a data transmission rate of 1 Mbps or 2 Mbps using spread-spectrum technology.

802.11a
This describes a WLAN that operates in the 5 GHz range, and provides a data throughput of up to 54 Mbps. It uses orthogonal frequency division multiplexing (OFDM) technology. The 5 GHz range is less crowded with devices than the 2.4 GHz range, so there is less risk of interference.

802.11b
The most widespread WLAN standard. It describes a WLAN that operates in the 2.4 GHz range with a data throughput of up to 11 Mbps using spread-spectrum technology. This specification

was also known as Wi-Fi, but 'Wi-Fi' now encompasses newer standards such as 802.11a and 802.11g.

The 2.4GHz range is already crowded with microwave ovens, cell phones, PDAs, Bluetooth, and other devices, so signal interference is a risk.

802.11g

This describes a WLAN that operates in the 2.4 GHz frequency range. Over short distances, it provides a data throughput of up to 54 Mbps using orthogonal frequency division multiplexing (OFDM) technology.

The 2.4 GHz range is already crowded with microwave ovens, cell phones, PDAs, Bluetooth, and other devices, so signal interference is a risk.

802.1x

A security standard for wired and wireless LANs. It encapsulates EAP processes into Ethernet packets instead of using the protocol's native PPP (Point-to-Point Protocol) environment, thus reducing some network overhead. It also puts the bulk of the processing burden upon the client and the authentication server (such as a RADIUS server), letting the 'authenticator' middleman simply pass the packets back and forth. Because the authenticator does so little, its role can be performed by a device with minimal processing power, such as an access point on a wireless network.

Access Point

Wirelessly networked devices usually connect to a wired LAN through a hardware device called an access point. Multiple access points set up in various locations let users roam from, say, their seats to a conference room to another cubicle, while staying connected.

An access point can also refer to one of the capabilities offered by a gateway or other networking device.

Ad-hoc Mode

Also known as peer-to-peer mode or IBSS. Ad-hoc mode lets wirelessly networked devices communicate directly, without going through an access point or other intermediary.

Adapter

An adapter is a device that connects to your computer and adds a capability or feature. The most common example is a circuit board, such as a graphics card or an NIC, that installs into an expansion slot on a computer's motherboard. Such an add-on board is also known as an expansion board. The SmartCard reader you plug into a USB port to download photos from your digital camera, or the cradle you use to synchronise your PDA with your desktop, can also be called adapters.

AES

Advanced Encryption Standard. AES is a data encryption scheme that beats both DES and 3DES by using three different key sizes—128-bit, 192-bit, and 256-bit, but with only one encryption step to encrypt data in 128-bit blocks. It is based upon the Rijndael algorithm created by Joan Daemen and Vincent Rijmen of Belgium. AES was adopted by the US government in 2002 as the encryption standard for protecting sensitive but unclassified electronic data. With the arrival of AES, the US officially phased out DES except for in legacy systems.

Antenna Gain

This refers to an antenna's transmission power as a ratio of its output (send) signal strength to its input (receive) signal strength. Antenna gain is usually expressed in dBi - the higher the dBi, the stronger the antenna.

Bandwidth

Refers to data-carrying capacity on a transmission path—how much and how fast data flows. It can apply to network connections, system buses, or any 'pipe' through which data flows. Bandwidth is usually measured in bits or bytes per second. Low-

bandwidth, such as dial-up modem, connections provide rates in the range of 56 Kbps, while high-bandwidth, or broadband, connections deliver more information at a much faster speed, making possible, for example, full-screen, full-motion video.

Beacon
In wireless networking, a beacon is a packet sent by a connected device to inform other devices of its presence and readiness.

Beacon interval
When a wirelessly networked device sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. Network managers can adjust the beacon interval, usually measured in milliseconds (ms), or its equivalent, kilomicroseconds (Kmsec).

Bluetooth
A wireless computing and telecommunications specification that defines how mobile personal computing devices work with each other and with regular computer and phone systems, within a close range. It uses the 2.4 GHz band at 720 Kbps within a 30-foot range. This technology is used with Personal Area Networks (PANs), as opposed to LANs.

BSS
Basic Service Set. When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID
The unique identifier for an access point in a BSS network. Also see SSID.

Cable
A broadband transmission technology using coaxial cable or

fibre-optic lines. It was first used for TV, and is now also being used for Internet access. Cable can transfer data downstream to a computer at speeds as fast as 27Mbps, much faster than DSL can. The actual speed a user gets, however, depends on variables including the modem's throughput capability, the maximum throughput per user that the cable service sets, and the number of other users sharing a neighbourhood connection at any time.

CDMA

Code Division Multiple Access. CDMA is a digital spread-spectrum modulation technique used mainly with personal communications devices such as mobile phones. CDMA digitises a conversation, and tags it with a special frequency code. The data is then scattered across the frequency band in a pseudo-random pattern. In order to reconstruct the signal, the receiving device is instructed to decipher only the data corresponding to a particular code.

Client

The 'customer' side of a client/server setup. When you log on to a server, the word client can refer to you, to your computer, or to the software running on your computer. For example, to download something from an FTP site, you use FTP client software; the FTP site runs FTP server software.

Decibel or dB

A logarithmic ratio that indicates the relative strength of a device's electric or acoustic signal to that of another. It can be used by itself, but is often paired with a specific unit of measure, such as a milliwatt (dBm) or an isotropic antenna (dBi). The higher a device's decibel rating, the more powerful its signal.

dBi

Decibels compared to an isotropic antenna. An antenna's gain is often measured in decibel strength compared to an isotropic antenna, a theoretical, perfect antenna whose range is 360 degrees in all directions. The higher the dBi, the stronger the antenna.

dBm
Decibels compared to one milliwatt. A wireless networking device's transmitting and receiving powers are often measured in decibel strength compared to one milliwatt of power. The higher the dBm, the greater the device's transmitting or receiving power.

DES
Data Encryption Standard. DES is an encryption method originally developed by IBM in the 1970s. Certified by the US government for the transmission of any data that is not classified top-secret, DES uses an algorithm for private-key encryption, in which the sender uses the same private key to send the message that the recipient uses to decode it.

The key consists of 56 bits of data, which are transformed and combined with each 64-bit block of the data to be sent. DES is fairly weak with only one iteration, and repeating it using slightly different keys can provide excellent security.

DHCP
Domain Host Control Protocol. DHCP is a protocol for dynamically assigning IP addresses to networked computers. With DHCP, a computer can automatically be given a unique IP address each time it connects to a network, making IP address management easier for network administrators. When a computer logs on to the network, the DHCP server selects an IP address from a master list and assigns it to the system.

Dipole Antenna
A type of antenna commonly used with wireless networking devices. It has a signal range of 360 degrees horizontally and 75 degrees vertically. It works best in offices, away from exterior walls where signals could leak out.

Directional Antenna
Defines several types of antennas that redirect the signal received from a transmitter to enhance its strength in a certain direction, unlike an omni-directional antenna.

DMZ
Demilitarised Zone. Originally, this term defined a closely monitored no-man's land placed between rival nations, for example, the buffer zone established between North and South Korea after the Korean Conflict in the 1950s. Networking has co-opted the term and used it to refer to an unprotected subnet connected to a local network but outside the peripheries of a firewall. A DMZ allows you to protect certain computers behind a firewall while allowing one or more other computers full exposure to other networks. A DMZ is often used for servers or gaming computers that require full access to the Internet in order to function properly.

DNS
Domain Name System. The DNS is the international network of Internet domain name servers, names, and addresses that lets you locate other computers on the Internet. When you send an e-mail, or point a browser to an Internet domain, a DNS server looks up the domain and finds its associated IP addresses, which routers use to identify the domain's server, and make a connection.

DSL
Digital Subscriber Line. Digital subscriber lines carry data at high speeds over standard telephone wires. DSL supports download speeds ranging from 384 Kbps to 1.5 Mbps (the near-unattainable maximum is 8 Mbps), depending on the quality of the lines and the distance one's connection stretches from the telecom operator's switching station. The term xDSL refers to the many variations of DSL, such as ADSL and HDSL.

DSSS
Direct Sequence Spread Spectrum. DSSS is a spread spectrum radio technology. The sender alters, or modulates, the signal by spreading it over a wider frequency, generating what seems like signal noise to everyone except the receiver, who knows how to return the signal to its original form, that is, by demodulating it.

DTIM
Delivery Traffic Indication Message. A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

DTIM Interval
A DTIM interval, also known as a Data Beacon Rate, is the frequency at which an AP's beacon will include a DTIM. This is usually measured in milliseconds, or its equivalent, kilomicroseconds (Kmsec).

Dual-band Radio
A radio device is dual-band if it can send and receive signals from two frequencies—in the case of wireless networking, both the 2.4 GHz and 5 GHz bands.

Dynamic DNS
The DNS would quickly run out of IP addresses if every Web-browsing computer user in the world were assigned a permanent one. Dynamic DNS is the system by which ISPs or companies are assigned a pool of IP addresses that they can assign to any user only for the time needed, so the same IP addresses can be used repeatedly for different people in different sessions.

EAP
Extensible Authentication Protocol. When you log on to the Internet, it's most likely that you are establishing a Point-toPoint Protocol *(see PPP)* connection via a remote access server. The password, key, or other device you use to prove that you are authorised to do so is controlled via PPP's Link Control Protocol (LCP). LCP is somewhat inflexible, however, because it has to specify an authentication device early in the process. EAP lets the system gather more information from the user before deciding which authenticator to use. It is called extensible because it allows more authenticator types than LCP did, such as passwords, public keys, or biometrics.

EAP-MD5
Extensible Authentication Protocol-Message Digest 5. EAP-MD5 is an EAP security algorithm developed by Rivest-Shamir-Adleman (RSA) Security that uses a 128-bit generated number string, or hash, to verify the authenticity of a data communication.

EAP-TLS
Extensible Authentication Protocol-Transport Layer Security. This high-security version of EAP requires authentication from both the client and the server. If one of them fails to offer the appropriate authenticator, the connection is terminated.

Encryption
The process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (data encryption standard) are two of the most popular public-key encryption schemes.

ESS
Extended Service Set. This is the collective term for two or more Basic Service Sets *(see BSS)* that use the same switch in a LAN.

ESSID
Extended Service Set Identifier. An ESSID is the unique identifier for an ESS. Also see SSID.

Ethernet
A standard for connecting computers in a local-area network (LAN). Ethernet is also called 10BaseT, which denotes a peak transmission speed of 10Mbps using copper twisted-pair cable.

Fast Ethernet
Also known as 100BaseT, Fast Ethernet is an upgraded standard for connecting computers in a LAN. Fast Ethernet works just like regular Ethernet (also known as 10BaseT), except that it can transfer data at a maximum rate of 100 Mbps instead of 10 Mbps.

FHSS
Frequency Hopping Spread Spectrum. A type of spread spectrum radio technology where the sender and receiver 'hop' together from one frequency to another to avoid detection or jamming.

Firewall
A system that prevents unauthorised users from logging in to a private network, usually one that's connected to the Internet. It can also be used to keep users inside the firewall from accessing computers outside the firewall. A firewall could be a dedicated computer equipped with security measures such as a dial-back feature, a software-based protection, or a combination of both. The firewall screens incoming server requests to make sure they come from authorised sources.

Fragment
In networking, a packet whose size exceeds the bandwidth of the network is broken into smaller pieces called fragments.

Fragmentation Length
In a network, the maximum size or length of a fragment is determined by the protocol used to transport the data.

FTP
File Transfer Protocol. This protocol is used to copy files between computers, usually between a client and an archive site. It's a bit on the slow side, doesn't support compression, and uses cryptic Unix command parameters. But you can download shareware or freeware applications that shield you from the complexities of Unix, and you can also connect to FTP sites using a Web browser.

Gateway
A combination of a software program and a piece of hardware that passes data between networks. You typically encounter a gateway when you log on to an Internet site or when you send e-mail to someone who uses a e-mail system different from the one that you do. In wireless networking, gateways can also serve as security and authentication devices, access points, and more.

HomePlug
A home-networking standard where devices connect using cables plugged into regular AC outlets, removing the need for running physical cables or configuring a wireless network. The maximum throughput is 14 Mbps.

Hot spot
In wireless networking, a hot spot is a specific part of an access point's range in which the general public can walk up and use the network. The service may be available either free or for a fee, and the hot spot's range is usually short to control the physical proximity of the user. In some parts of the world, it is called a cool spot.

Hub
A piece of networking hardware that serves as a central connection point for multiple PCs or other devices, usually on a wired or wireless Ethernet network. A passive hub simply transmits data from any of its connected devices to the rest of the network. An active, or manageable, hub can also monitor network traffic and configure its ports.

IEEE
Institute of Electrical and Electronics Engineers. Pronounced 'eye-triple-E', this non-profit US engineering organisation develops, promotes, and reviews standards within the electronics and computer science industries.

Infrastructure Mode

When a wireless network functions in infrastructure mode, every user communicates with the network and other users through an access point; this is the typical way that corporate WLANs work. An alternative is ad-hoc mode, but users would have to switch to infrastructure mode to access a network's printers and servers.

Internet Connection Sharing

Also known as ICS, this is a Windows XP function that lets home or small-office users with networked computers share one Internet connection. One computer with an Internet connection serves as the ICS host for all the computers.

Intranet

An intranet is a restricted-access network that works like the Web but isn't on it. Usually owned and managed by a corporation, an intranet enables a company to share its resources with its employees without confidential information being made available to everyone with Internet access.

IP Address

Internet Protocol address. This address is a 32-bit, unique string of numbers that identifies a computer, printer, or another device on the Internet. The IP address consists of a quartet of numbers separated by periods. Each number can be anything from 0 to 255, for example, 128.128.130.4. An IP address can be either static, meaning it never changes, or dynamic, meaning the address is assigned randomly to a computer for only as long as the Internet session lasts. Dynamic IP addresses are commonly used in large corporations and online services for efficiency.

ISM Band

The 2.4 GHz frequency spectrum is also known as the ISM band. ISM is not actually synonymous with 2.4 GHz, however, it stands for Industrial, Scientific, and Medical, the non-commercial uses

for which the 2.4 GHz band and other frequencies were once reserved by the ITU-T.

Isotropic Antenna

A theoretical, ideal antenna whose signal range is 360 degrees in all directions. It is used as a baseline for measuring a real antenna's signal strength, in dBi, where the 'i' stands for 'isotropic antenna'.

ITU-T

International Telecommunications Union-Telecommunication. The newer name for the international committee CCITT, ITU-T has a long way to go until it's as well-known as its older counterpart.

LAN

Local Area Network. A local-area network is a short-distance network used to link a group of computers together, usually within a building. Ethernet is the most commonly used type of LAN. A piece of hardware called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network.

MAC address

Media Access Control address. Each device connected to an Ethernet network has a unique numeric identifier called a MAC address, which is used for data transmission and security functions. For instance, the MAC address lets other devices on the network find each other, and it accompanies each data packet to identify its sender.

MAC filtering

MAC filtering is like using a guest list to restrict entry to a party. A network checks a device's MAC address against a database to see if it's authorised to access the network.

Mbps

Megabits per second. A megabit is roughly a million bits of data. This abbreviation is used to describe data transmission speeds,

such as the rate at which information travels over the Internet. Several factors can influence how quickly data travels, including modem speed, bandwidth capacity, and Internet traffic levels.

Modem
An external box or internal circuitry that converts computer data into sound-range signals that can be transmitted over phone lines. First used to send telegrams, early modems alternated between two different tones. This is called modulation, and the process of modulating, and demodulating at the receiving end, gave the modem its name. These days, modems transmit data with lots of different tones, signals, and complex mathematical processing, so 'modem' is a bit of a misnomer.

NAT
Network Address Translation. NAT solves both security and efficiency issues surrounding Internet use by letting a network at, say, a company, use its own pool of IP addresses for internal communications and another pool of addresses for external communications. This method hides internal IP addresses from hackers. In addition, because NAT lets the same IP addresses be used internally by multiple companies, it reduces the demand for globally unique, static IP addresses.

NIC
Network Interface Card; an adapter inside a computer that lets the computer connect to a network via a wired or wireless transmission medium.

OFDM
Orthogonal Frequency Division Multiplexing. A wireless transmission technique that splits a signal into smaller signals that are then transmitted at different frequencies simultaneously. It's the method employed for wireless transmissions that use the IEEE 802.11a and 802.11g specifications.

Omnidirectional antenna

This is like a dipole antenna because it radiates its signal 360 degrees horizontally; however, its signal is flatter than a dipole's, allowing for higher gain.

Packet

While it may seem as though you send or receive a continuous stream of data every time you use the Internet, actually, it's more efficient to break up the transmission into pieces called packets. These packets contain information about which computer sent the data and where the data is going. If a packet runs into a problem during its trip, it can attempt to find another route. When all the packets reach where they're going, the recipient computer puts them together again. Modems generally send packets of around 64 characters along with some extras for error checking. When downloading files using a protocol such as Xmodem, however, the packets are larger. And when using Internet protocols such as TCP/IP, the packets are larger still—around 1,500 characters.

PAN

Personal Area Network. A PAN is distinct from a LAN because it's a casual, close-proximity network where connections are made on the fly and temporarily. Meeting attendees, for example, can connect their Bluetooth-enabled notebook computers to share data across a conference room table, but they break the connection once the meeting is over. See also WPAN.

PC Card

A credit card-size peripheral that plugs into a special slot on portable computers (and some desktop models). The card may add RAM, a modem or network adapters, a hard drive, or another device. These PC Cards conform to several standards set by the Personal Computer Memory Card International Association (PCMCIA), and were originally called PCMCIA Cards.

The original Type I PC Card is 3.3 mm thick, a format used mainly to add RAM. Type II cards are thicker—5mm—and often

are used for modems and NICs (though they're also used for RAM). Type III cards are much thicker—10.5mm—and often are used for hard disks and radio devices. A PC Card slot on a computer is usually designated by the thickest card it can accommodate. A Type II PC Card slot, for instance, can take a Type I PC Card as well as a Type II (and it might be called a Type I/II), but it cannot fit a Type III.

PCI

Peripheral Component Interconnect. If you have a Pentium system, it's extremely likely that it runs a self-configuring PC local bus called PCI. Designed by Intel, PCI has gained wide acceptance—even by Apple, in its PowerPC series.

PCMCIA

Personal Computer Memory Card International Association. This acronym stands for the name of a trade association founded in 1989 to establish standards for expansion cards for portable computers. Based in Sunnyvale, California, the PCMCIA's specifications for the PC Card enabled the computer industry to manufacture credit-card-size removable cards to add RAM, modems, network adapters, hard disks, and even radio devices such as pagers and global positioning systems to portable computers. Many people call PC Cards by the longer name 'PCMCIA cards'. The association has trademarked the term PC Card, however, which is therefore the preferred usage.

Ping

When submarine crews wanted to determine the distance of an object from themselves, they'd send a sonar ping and wait to hear the echo. In the computer world, 'ping' is a program that 'bounces' a request—in other words, sends a packet—over the Internet to another computer to see if the remote computer is still responding. If the ping returns, the remote computer is still connected. Some people think 'ping' stands for 'Packet Internet Groper', but according to the inventor of Ping, that is a secondary acronym.

Port

In networking, a server's various functions, such as managing FTP traffic or maintaining the DNS list, are each assigned a virtual address called a port. Any requests for that function are sent to the port address. Some common functions are assigned standard port numbers by the IANA (Internet Assigned Numbers Authority); for instance, DNS traffic is always routed to port 53.

Port Forwarding

This lets a computer external to a secured network access a computer on the network through the mapping of a port on the network's firewall to a port on a specified computer. This allows a firewall to block certain connections using certain port and protocol combinations while permitting predetermined port connections on specified computers.

PPP

Point-to-Point Protocol. PPP is the Internet standard for serial communications. Newer and better than its predecessor, Serial Line Internet Protocol (SLIP), PPP defines how your modem connection exchanges data packets with other systems on the Internet.

PPTP

Point-to-Point Tunnelling Protocol. PPTP is a protocol developed by a number of companies, including Microsoft, that allows secure transmission of data in TCP/IP packets. PPTP and similar protocols are used to carry secure communications over Virtual Private Networks that use public phone lines.

Protocol

Because so many different types of computers and operating systems connect via modems or other connections, they have to follow communications standards called protocols. The Internet is a heterogeneous collection of networked computers and is full of different protocols, including PPP, TCP/IP, SLIP, and FTP.

Proxy server
A system that caches items from other servers to speed up access. On the Web, a proxy first attempts to find data locally, and if it's not there, it fetches it from the remote server where the data resides.

QoS
Quality of Service. QoS can be used to describe any number of ways in which a network provider guarantees a service's performance, such as an average or minimum throughput rate.

RADIUS
Remote Authentication Dial-In User Service. The RADIUS is a server database used by an ISP to authenticate users who are trying to log on to the service. It can also track network usage.

RJ-11
Registered Jack 11. This is the standard telephone connector—a tab snaps into the socket and has to be pressed to remove the connector from the wall or your phone. An ordinary phone circuit uses two wires. The RJ-11 jack has room for up to four wires.

RJ-45
Registered Jack 45. RJ-45 connectors look a bit like standard phone connectors (RJ-11) but are twice as wide, with eight wires. RJ-45s are used for hooking up computers to LANs or for phones with lots of lines.

Router
As the name indicates, this piece of hardware routes data from one local area network to another or to a phone line's long-distance line. Routers also act as traffic cops, allowing only authorised machines to transmit data into the local network so that private information can remain secure. In addition, routers handle errors, keep network usage statistics, and handle security issues.

RTS
Request To Send. An RTS is a message sent by a networked device to its access point, seeking permission to send a data packet. See also RTS threshold.

RTS Threshold
Request To Send threshold. The RTS threshold specifies the packet size of an RTS transmission. This helps control traffic flow through an access point, especially one with many clients.

Server
The 'business' end of a client/server setup, a server is usually a computer that provides the information, files, Web pages, and other services to the client that logs on to it. The word server is also used to describe the software and operating system designed to run server hardware.

SLIP
Serial Line Internet Protocol; a standard for connecting to the Internet with a modem over a phone line. It has serious trouble with noisy dial-up lines and other error-prone connections.

Spread spectrum
A wireless communications technology that scatters data transmissions across the available frequency band in a pseudorandom pattern. Spreading the data across the frequency spectrum greatly increases the bandwidth (the amount of data that can be transmitted at one time), and it also makes the signal resistant to noise, interference, and snooping. Spread-spectrum modulation schemes are commonly used with personal communications devices such as digital cellular phones, as well as with WLANs and cable modems. See FHSS, DSSS, and CDMA for examples of spread-spectrum techniques.

SSID
Service Set Identifier. Every wireless network or network subset, such as a BSS, ESS, or IBSS, has a unique identifier called an SSID

(and may be called a BSSID, ESSID, and so on, depending on what it is identifying). Every device connected to that part of the network uses the same SSID to identify itself as part of the family, so to speak, when it wants to gain access to the network or verify the origin of a data packet it's sending over the network. Using SSID carries some security risk, however, because it can be detected by wardrivers and used to gain unauthorised access. Some network administrators, therefore, disable SSID.

SSL

Secure Sockets Layer, an Internet protocol that uses public-key and secret-key encryption to secure data sent from one server to another. It was developed by Netscape Communications to safeguard commercial transactions taking place over the otherwise insecure Internet.

Static IP address

See IP address.

Switch

A device in a network that selects the path that a data packet will take to its next destination. The switch opens and closes the electrical circuit to determine whether—and where—data will flow. On the Internet, the switch sits at the point that connects one network to another network.

TCP/IP

Transmission Control Protocol/Internet Protocol. TCP/IP is the method by which data is sent across the Internet. These two protocols were developed by the US military to allow computers to talk to each other over long-distance networks. IP determines how the data is formatted into smaller chunks called data packets and ensures that those packets are addressed correctly to reach the right destination. TCP is responsible for establishing a connection between the client computer and the server and actually transmitting the data packets. TCP/IP forms the basis of the Internet, and is built into every common modern operating

system, including all flavours of Unix, the Mac OS, and the latest versions of Windows.

Throughput

A general term used when defining how much data is going how quickly over a particular transport medium, such as a wireless network or a phone line. When your modem says it can transfer data at a rate of 56 Kbps, for instance, it is describing its maximum throughput level.

Twisted Pair

Telephone companies commonly run twisted pairs of copper wires to each customer household. The pairs consist of two insulated copper wires twisted into a spiral pattern. Although originally designed for plain old telephone service (POTS), these wires can carry data as well as voice. New services such as ISDN and ADSL also use twisted-pair copper connections.

UPnP

Universal Plug and Play. Universal Plug and Play is a networking architecture developed by a consortium of companies to ensure easy connectivity between products from different vendors. UPnP devices should be able to connect to a network automatically, handling identification and other processes on the fly. The standards developed by the UPnP Forum are media, platform, and device-independent.

UWB

Ultra Wide Band. An emerging wireless technology that sends signals in extremely short pulses over a wide swath of the radio frequency spectrum. The technology has numerous advantages. Because the power required to send these pulses is very low, the signal can pass through doors and other obstacles, such as the ground, that would reflect a higher-powered signal; also, UWB devices don't need a lot of juice to operate. The brevity of each signal pulse, measured in billions per second, is very hard to detect, giving it some intrinsic security.

And because the signal is spread over such a wide bandwidth, the risk of interference is low. This technology is also used for ground-penetrating radar devices.

Virtual Server
The part of a server that functions as if it were a separate, dedicated server. Each virtual server can run its own operating system and applications and even be networked with other virtual servers on the same machine. Web hosting companies use virtual servers to house multiple clients' Web sites on one server, for instance.

VPN
Virtual Private Network. A private network of computers that's at least partially connected by public phone lines. A good example would be a private office LAN that allows users to log in remotely over the Internet (an open, public system). VPNs use encryption and secure protocols such as PPTP to ensure that data transmissions are not intercepted by unauthorised parties.

WAN
Wide-Area Network. Take two LANs, hook them together, and you have a WAN. Wide-area networks can be made up of interconnected smaller networks spread throughout a building, a state, or the entire globe. The Internet could be considered a WAN. A wireless WAN is called a WWAN.

Warchalking
The unauthorised act of physically marking the locations of wireless access points (APs) that are available for free network access, such as those at a coffee house or an airport, or an office AP with a leaky signal. The word 'chalking' derives from the informal system of markings used by vagabonds to indicate places where one might get a meal or a place to sleep. See also wardriving.

Wardriving
The unauthorised act of seeking out and mapping wireless access points (APs) that are available for free network access, such as those at a coffee house or an airport, or an office AP with a leaky signal. This is the new, wireless version of war dialling, in which hackers would dial hundreds of numbers to find an open modem so that they could gain access to a company's network. See also warchalking.

WECA
Wireless Ethernet Compatibility Alliance. This is the former name of the Wi-Fi Alliance of vendors promoting 802.11 wireless networking standards and compatibility.

WEP
Wired Equivalent Privacy. All 802.11b (Wi-Fi) networks use WEP as their basic security protocol. WEP secures data transmissions using 64-bit or 128-bit encryption; however, it does not offer complete security, and is usually used in conjunction with other security measures such as EAP.

Wi-Fi
Wireless Fidelity. Wi-Fi originally referred to the 802.11b specification for wireless LANs, but it is now used to describe any of the 802.11 wireless networking specifications.

Wireless Bridging
A networking bridge is used to connect two or more separate networks. A wireless bridge functions the same way but can be used in situations in which running a wire or cable would be impractical or prohibitively expensive, such as creating a 10-mile point-to-point link.

Wireless Channel
Different networking technologies divide up their allocated spectrum in different ways. One can sometimes improve the performance of your network and avoid interference on the band by

moving your network to a different non-overlapping channel available to the devices. 802.11b and 802.11g devices have three non-overlapping channels. 802.11a devices have eight non-overlapping channels.

WLAN
Wireless Local-Area Network; a wirelessly connected LAN, such as an 802.11 network.

WPA
Wi-Fi protected access. WPA is a specification for improving the security of Wi-Fi networks, replacing the weaker WEP for current and future 802.11 standards. It uses 802.1x and EAP to restrict network access, and it uses its own encryption, called Temporal Key Integrity Protocol (TKIP), to secure data during transmission.

WPAN
Wireless Personal Area Network. A WPAN is specifically a PAN that uses wireless connections, but because all current PAN technologies, such as Bluetooth, are wireless, you can consider the terms synonymous.

Xmodem
A protocol for transferring files during direct dial-up communications. Developed in 1977, Xmodem does basic error checking to ensure that information isn't lost or corrupted during transfer; it sends data in 128-byte blocks. Xmodem has undergone a couple of enhancements: Xmodem CRC uses a more reliable error-correction scheme, and Xmodem-1K transfers data faster by sending it in 1,024-byte blocks.

Whitepapers

In the pages thus far, you have, hopefully, learned a considerable bit about everything wireless—how to set up a wireless network, network terminology, and so on. In this section, we present material that, while not essential knowledge for beginners, goes a little deeper into the subject. There are three papers dealing in some way or the other with security; one on taking control of your IT assets with Wi-Fi-based asset tracking; and a paper with a different take on the advanced issues of spectra, regulation, licensing and so on.

The Five Deadly Dangers of Unsecured Wireless Networks

How Hackers Use Open Wi-Fi Networks To Access Your Information And How You Can Stop Them

The Benefits Of Wireless Networks

It seems these days that wireless networks are everywhere. With Wi-Fi capabilities built into most new laptop computers, and with relatively inexpensive network adapter cards, Wi-Fi is within reach of most PC users.

The freedom and benefits of an un-tethered connection to your network are very compelling:

- Create your network when wiring isn't practical. Many office and warehouse spaces find it very difficult or impossible to lay wire for networking. Wi-Fi is a cost-effective and convenient alternative to a wired network.

- Expand your network with no additional wiring costs. This is especially beneficial in home offices that aren't pre-wired for Ethernet, or for small businesses that are rapidly expanding, or frequently reconfiguring their office layouts.

- Information at your fingertips anywhere you work. The ability to to access your e-mail, the Internet, and network-based applications in a conference room or another office gives you additional degrees of productivity and convenience.

- Doctors can carry patient records on a laptop or tablet PC to each exam room and stay connected all the time.

- Lawyers can bring their laptops into depositions and conferences and fact check or access networked data instantly.

- Project members can collaborate in team meetings each with

instant information available across the wireless network to accelerate decisions with immediately available information.

- Wireless at home means delivers the ability to work anywhere in the house, or deck. The ability to be around your family when you're catching up on e-mails is truly convenient.

Beware The Dark Side

Despite the benefits, there is a dark side to wireless. Without the proper security measures in place, your business and personal information can easily be retrieved over the wireless network. With a $100 directional antenna and free software available on the internet, hackers can access your network traffic and PC data from as far as a mile away.

In June 2004, a worldwide "war drive" event among the hacker community uncovered over 230,000 wireless networks and posted their positions on the Internet. A startling 61.6 per cent of all the networks they surveyed had no security whatsoever, and the majority of the other networks had the weakest form of security that can be cracked in under 15 minutes.

There are a number of fallacies associated with wireless security. Many users believe (or want to believe) that they are secure because they don't see anyone around them that they consider dangerous. This article discusses the common misconceptions of wireless, the 5 deadly dangers of open wireless networks, and the specific steps you can take to enjoy the benefits of wireless without compromising your network and confidential data in the hands of hackers.

The Common Fallacies Of Wireless Network Security

No one wants to get into my network, and if they get a free ride on the internet who cares?

Unfortunately, we live in a world where crimes and vandalism is commonplace, even more so when the crime can go undetected. Many hackers or disgruntled employees are merely

looking to compromise someone's systems whether or not there are huge payoffs—these vandals break in simply because they can. Through your open network, and intentional hacker can destroy the network and every PC on the network. Imagine the cost to your organization if a hacker launches a virus directly into your network or re-initializes the hard drives on every PC they could access.

I don't have any important information that anyone would want to access. Many people believe that their electronic information is not at risk or of little value to anyone who sees it. This is dangerous thinking. With simple sniffing software, every packet of data you send or receive over the wireless network can be read and stored to disk. Most users don't realize that when they access their e-mail from a POP3 account over wireless, their e-mail account username and password are readable over the air. Imagine the access to personal and confidential information a hacker can have after capturing your e-mail password and having unrestricted access to your e-mail account for months on end without being detected.

There's no one within 300 feet of my building, and wireless can't reach beyond that point. Many users falsely believe that they are secure because none of their neighbors are within 300 feet of their home or office. In fact, with a $100 directional antenna hackers can access your network traffic and PC data from as far as a mile away, making it very difficult to pinpoint the hacker at all. Another common hacker trick is to leave an unmonitored PC in their car, hotel room, or other temporary location. The PC can be connected to an antenna pointing at your office or home and collects gigabytes of network traffic for offline analysis after the PC is retrieved. It is nearly impossible to detect a hacker listening to your network.

If I put in a wireless network, no one else will find it. Did you know there is a website that lists almost 2 million unprotected wireless networks? War driving is the practice of finding

and logging wireless networks. With a high-powered antenna, GPS, and a laptop, war drivers can detect and plot your network on a global grid. These war drivers then file the location of your network into a permanent database on the web. Once an unsecured network is found by these war drivers, anyone can pinpoint the exact location of you network (complete with road maps) on the internet. Go to www.wigle.net to see if your network is already one of the 1,881,793 Wi-Fi networks that have been logged already.

MAC address filtering can do the job. MAC address filtering is dangerous because it provides a false sense of security to the unsuspecting. Many wireless access points and routers allow MAC address filtering—a low level check on the MAC address or identifier of your wireless interface—to determine if a particular PC should be allowed access on the network. There are 2 significant problems with MAC address filtering. First, it doesn't prevent passive attacks. A hacker can still capture and listen to your network traffic without ever being seen. And second, if hackers want access to your network, they need only listen for a valid MAC address, and change the MAC address on their PC to match a valid address. This can be done in less than a minute.

WEP Security is good enough. WEP (Wired Equivalent Privacy) uses common 60 or 108 bit key shared among all of the devices on the network to encrypt the wireless data. Unfortunately, WEP is a very weak form of security. Hackers can access tools freely available on the internet like WEPcrack, Aircrack, and Airsnort that can crack a WEP key in as little as 15 minutes. Once the WEP key is cracked, the network traffic instantly turns into clear text—making it easy for the hacker to treat the network like any open network.

The Five Deadly Dangers Of Unsecured Wireless Networks

Once hackers have access to your network, they can readily capture personal and business information. There are two types of attacks. Passive attacks, where the hacker captures your network

traffic, are almost impossible to detect because the hacker never joins your network. They can sit silently with their antenna tuned into your network and capture gigabytes of network traffic for off-line analysis at a later time. Active attacks, where the hacker joins the network, can be the most devastating because they can launch active attacks into the network and onto your devices on the network.

There are five attacks that hackers can very easily and readily perform on your wireless network with very little effort or expense. The first two are passive attacks, and the last three are active attacks. But make no mistake—all these attacks can be deadly.

Deadly Attack #1: Account And Password Capture

There are several applications that send your account and passwords in clear text over the network. For example, every time a POP3 mail account checks for new e-mail, the account name and password are in the clear as part of the data transfer. Anyone sniffing the network traffic can easily get your e-mail account information. Once they have that information, they can access your e-mail account at their leisure, monitoring for personal information without leaving a trace. From there, any confidential information they can get from your account just escalates their attack.

Deadly Attack #2: E-mail, IM And Web Site Traffic Capture

It is very easy to monitor and capture all of the e-mail traffic sent over an unsecured wireless network. Since most e-mail is sent in clear-text, and instant messaging is sent in HTML, it's very simple to capture the traffic and mine the traffic offline for any "interesting" information at a later time. By monitoring your wireless traffic, all of the HTML data can be captured and reconstituted as web pages on the hackers PC to see exactly what web sites and content you are surfing over the wireless network.

Deadly Attack #3: Accessing Data On Your PC

Let's face it, it's pretty easy to turn File Sharing on, and then forget to turn it off when you attach to an Open Network. Once File

Sharing has been left on or the personal firewall is misconfigured, a hacker can readily access you PC and hard drive across the wireless network. Firewalls are also easy to misconfigure or turn off, and forget to turn back on. With older versions of Windows (NT, W2K), if improperly configured, it's easy prey for a hacker to get in over the network, log-in as a null session and take over your platform.

Deadly Attack #4: Access To The Corporate Network

If your wireless network is connected to a corporate network through a site-to-site VPN, an open wireless network punches a hole through the network, and opens up both sides of the VPN to anyone attaching to the network. Another threat is with improperly configured client VPNs which can be more easily compromised to provide the hacker access through the VPN.

Deadly Attack #5: Spam And Virus Launching Over The Wireless Network

Unsecured Networks provide are an ideal launch point from which hackers can launch spam and virus attacks because it is very difficult to track the source back to them. From a distance, the spammer can launch the spam (from your e-mail account if he sniffed your e-mail account info) without repudiation. When the ISP or FBI tracks down the violator, the trail points to your network, and possibly your e-mail account. The liabilities to the owner of the unsecured network are still newly contended battlegrounds for the lawyers.

Best Practices To Secure Your Wireless Network

The good news is that simple tools are available to properly secure your wireless network and avoid the dangers discussed above.

The Wi-Fi Alliance designated WPA (Wi-Fi Protected Access) as the recommended security practices for consumer and business networks. WPA comes in two forms: WPA-PSK, which offers a lower-level security for consumers, and WPA-Enterprise, which

offers a higher level of security for enterprises. Solutions like LucidLink Wireless security delivers enterprise level security with the consumer-level simplicity that can be easily and quickly deployed in home offices, small offices, and medium businesses.

WPA-PSK (Pre-Shared Key): WPA-PSK provides a relatively secure solution for consumer networks. If you're technically competent, and feel comfortable configuring the security parameters of your wireless access point or router, you can configure your wireless network to support WPA-PSK. By entering a common 64 digit hexadecimal key into every device on the network you can properly encrypt all network traffic to and from the access point.

WPA-PSK has fixed many of the problems associated with pre-shared keys used in WEP. While it is quite awkward to properly enter a 64 digit hexadecimal key into each device on the network, if done carefully, it can provide strong encryption of network traffic and ward off hackers.

One of the common complaints with WPA-PSK, however, is that it uses a common key across all of the devices and PCs on the network. If you, an employee, or your child innocently shares this key with anyone, the integrity of the network can be compromised. If any person leaves an organization or needs to be denied access to the network, every PC on the network needs to be reprogrammed with a new 64 digit pre-shared key. The need to re-key every device on the network if a single user is removed can become a heavy burden to maintaining a small business network.

WPA-Enterprise uses the same type of network security used by enterprises and ISP over the last decade to protect access to wired networks. Unlike WPA-PSK, each user accessing the network is given unique credentials. These credentials may be in the form of passwords, electronic certificates, or in the case of LucidLink, automatically configured security credentials.

For a user to access the network, they provide the unique credentials, which are verified by a designated PC providing access management using a security protocol called 802.1X. When the server acknowledges the user as having valid credentials, the user is given access to the network and given a new encryption key every time they enter the network. The encryption key is used to encrypt and secure the network traffic between the user's PC and the network access point. Without proper credentials, the user is denied access.

One of the benefits of WPA-Enterprise is that it offers a much higher level of manageability. User access can be controlled on a user-by-user basis. A user can be removed from the network without re-keying every device on the network.

Take Control of Your IT Assets with Wi-Fi-Based Asset Tracking

PanGo Networks, Inc. March 2005

Introduction

The headlines scream "Missing PC Held Trove of Secrets" and "Laptop Containing Top Secret Data Stolen." In these cases, sensitive government information is potentially lost or stolen. Less publicized, but much more frequent, are lapses in the corporate world where use of mobile computing devices presents protection and asset utilization challenges. While information technology (IT) departments must be sensitive to "Big Brother" and other privacy concerns, some control of mobile devices is essential in the information age. As a result of this need, organizations are taking enterprise asset management more seriously than ever. Computing and IT equipment often contain sensitive and valuable information, yet these assets are seldom properly protected against indiscriminate access, loss or theft. To help take control of their assets, IT professionals are turning toward Radio Frequency Identification (RFID) technologies that offer real time asset-tracking capabilities, enabling them to clamp down on loose security and asset management practices that leave open the risk of having valuable corporate information fall into the wrong hands.

Asset-tracking solutions are now available that allow companies to leverage RFID capabilities that already exist in their 802.11 wireless (Wi-Fi) network, thereby eliminating the need for an additional proprietary RFID network infrastructure. With asset-tracking systems in place, companies can strengthen IT asset security while better utilizing human and capital resources. Given recent advancements in active RFID, it is a question of when, not if, real-time enterprise asset-tracking capabilities become common practice.

This white paper will identify the potential for Wi-Fi-based IT asset tracking in the enterprise. In particular, it will explore how

Wi-Fi-based asset-tracking solutions can help organizations achieve rapid return on investment (ROI) by leveraging their 802.11 wireless network for more than just data connectivity. It reviews the key organizational, business process and technological factors that contribute to the rapid deployment of 802.11 WLAN infrastructures within the enterprise arena to enhance visibility, deliver bottom line financial benefits and effectively address recent federal guidelines for better IT asset management.

WLAN Drivers In The Enterprise

Numerous factors are contributing to the rapid deployment of 802.11 WLANs in the enterprise, including organizational and business process requirements, government and industry standards and new technological developments. These include the increased demand for mobile information access by personnel, as well as the maturation of 802.11 standards and the proliferation of 802.11-enabled devices.

The following are seven key drivers for the rapid deployment of 802.11 WLANs in enterprise IT environments:

1. Intrinsically high levels of mobile staff who demand access to the same information whether they are mobile or at their workstations.

2. Strong benefits for customer service and organizational efficiency through more timely and accurate information access.

3. Maturation of the 802.11 family of standards to provide high speed (802.11a/g), secure (802.11i) and reliable networks offering good quality of service (802.11e/k).

4. Data security guidelines that are driving the need for strong security measures such as those specified by the latest 802.11i standards.

5. Proliferation of 802.11 enabled devices including note-

book/tablet computers, Personal Digital Assistants (PDAs), voice over Internet protocol (VoIP) phones and other Wi-Fi enabled equipment as organizations and individuals recognize their flexibility and value.

6. Economies of scale are rapidly driving down price points for Wi-Fi equipment, which will continue to decrease as annual shipments of 802.11 radios grow from 70+ million units in 2004 to 125+ million units in 2008 (*Source: IDC*). For example, an 802.11 NIC can be purchased for less than $25, a low-end Access Point (AP) for less than $60 and a full-featured enterprise class AP for about $500. Clearly, 802.11 is becoming the wireless equivalent of the wired Ethernet.

7. The ability to add new services such as "location awareness" to the standard 802.11 infrastructure. This will deliver additional ROI by enabling active RFID capabilities such as tracking of people and assets, and delivery of location-aware content to devices such as PDAs and tablet computers. Providing enterprises extended visibility into their mission-critical assets can drive significant cost savings and efficiencies.

Considering the drivers outlined above, most organizations are now rapidly replacing various point wireless solutions with a single wireless network based on 802.11 technologies to provide their mobile workforce un-tethered access to both voice and data services. As enterprises commence these deployments, they are realizing that their existing 802.11 infrastructure can also be used to solve one of their biggest headaches-locating valuable assets.

The Emergence Of Location-Aware Applications

Keeping track of valuable equipment across large facilities with hundreds or thousands of IT assets (i.e., servers, notebooks, PC's, PDA's, software) used by thousands of employees is a daunting task. Some estimates claim that more than 2,000 computers are

lost or stolen each day. More than 90 percent of the 300,000 notebooks stolen each year go unrecovered. Lost is not only the hardware and data, but also the owner's time spent obtaining and configuring a replacement. In addition, government regulations like Sarbanes-Oxley are guiding organizations towards more timely and accurate accounting for valuable assets, better asset management and control. As a result, IT administrators are making the security of mobile computers and high value IT assets a priority.

"Laptop theft poses a major risk when it comes to compromising corporate data, and it will only get worse with the increase in the use of handheld devices," said Chris Christiansen, an analyst at International Data Corporation in Framingham, MA. "People are walking around carrying corporate passwords, internal phone lists, memos and details on proprietary projects that could cause damage if such information were to fall into the wrong hands." Obviously, theft of IT assets is only one of the issues faced by IT managers. Another common theme is asset mismanagement, i.e., "Where did that thing go?" Servers and other IT equipment are regularly disconnected, moved for service or switched from one rack or IT closet to another. When the equipment needs to be returned to its original location, searching a data center to track down the missing asset can take hours or even days.

While expensive laptops used to be the target of thieves looking for quick cash, the primary aim today is the information on the device, NOT the device itself. Personal digital assistants (PDA's), servers and software systems are at high risk. A recent article by Ephraim Schwartz in InfoWorld entitled "RFID for Asset Tracking," wrote "...suppose a particular machine has customer Social Security numbers on it. You'll want to know where that box is at all times."

Location-aware applications can address the needs of the IT administrators for greater asset security, staff efficiency and

improved customer service. Application Organizational Needs and Benefits IT Asset Management Automate asset inventory and maximize asset utilization; drive improvements in overall IT workflow and efficiency with real-time data and floor map views of resources so workers can quickly find what they need when they need it.

IT Asset Security Prevent loss and theft of valuable equipment and monitor, in real-time, the location of equipment containing sensitive and valuable information; receive alerts when assets move into and out of areas of interest.

Staff Productivity Optimize workflow and improve efficiency by quickly locating mobile IT equipment (i.e., notebooks, handhelds, monitors, projectors, printers, etc.). IT Asset Maintenance Locate assets for break/fix and preventative maintenance, and understand usage patterns to drive the appropriate asset and staff allocation. Recently emerging from companies such as PanGo Networks are software-only location-aware solutions and active RFID asset-tracking applications operating on standard 802.11 WLAN infrastructures.

These software-only Wi-Fi-based active RFID applications bring to enterprise environments the ability to:

1. Track IT equipment affixed with 802.11-based active RFID tags
2. Identify the location of devices that incorporate 802.11 Network Interface Cards (NICs) such as PCs and PDAs; and
3. Integrate location information into asset management and workflow systems.

The process of implementing 802.11-based RFID for asset tracking begins by conducting an initial survey of the environment that captures RF fingerprints (based on signal strength readings) at various important places throughout the facility or campus. The principle is that a unique RF fingerprint can be

established at each of these locations. These RF fingerprints are then stored in a database and used later at runtime to match the currently observed RF environment to the previously stored data. Using pattern-matching and a series of advanced locationing algorithms, the system can then determine the current location—with reliable "room level" accuracy (approximately 3 meters)—of a device or person with either the 802.11 NIC or an 802.11 asset tag. Location information is used by 802.11 active RFID asset tracking systems to display the current location of different types of equipment as well as enable users to search for specific assets.

These newer approaches offer advantages over traditional active RFID technologies. First, they use the existing 802.11 WLAN infrastructure which offers significant cost reduction in terms of initial installation and on-going operation/maintenance. Wireless asset-tracking capabilities have traditionally been the domain of specialized Real Time Tracking Systems (RTLS) that require their own dedicated, proprietary network infrastructure. These single-purpose tracking networks-due to their hardware-intensive deployment-have proven to be costly to purchase, install, implement and maintain. Wi-Fi-based Enterprise Asset Visibility solutions leverage an organization's existing Wi-Fi infrastructure, and eliminate the need for specialized radio receivers, access points, antennas and wiring. By deploying on the existing Wi-Fi network, using software-only location architectures, the newer generation of Enterprise Asset Visibility solutions dramatically lowers the total cost of ownership and opens up new possibilities by combining services together. Second, they enable opportunities to deliver exciting new applications that combine voice, data and location awareness which can improve efficiency and customer service. In sum, these new approaches represent a superior, more efficient and cost-effective alternative to first-generation RFID technology that require enterprises to deploy separate, single-purpose networks of proprietary readers, cabling and tags in order to provide location/tracking capabilities.

Summary

Wi-Fi-based active RFID offers unparalleled cost savings and vastly improved security and asset visibility. What many companies may not realize is that they already have an RFID infrastructure installed-their off-the-shelf WLAN. The inherent mobility of corporate environments and growing demand for increased security coupled with the maturity of 802.11 WLAN technologies is driving a rapid deployment of 802.11

WLAN infrastructures in major organizations with a high volume of IT assets. Capabilities including real-time IT asset tracking can be deployed in a cost-effective manner by leveraging a single shared infrastructure, the 802.11 wireless network. Real-time asset-tracking solutions such as those offered by PanGo Networks can precisely respond to the increasingly growing demands of CIO's and IT asset managers to enhance business processes. As a result, corporations have the means to maximize system performance, and to in turn realize lower costs by boosting the efficiency of their network resources.

Your Wireless LAN is Exposed: Weaknesses and Solutions to WLAN Vulnerabilities

By Kevin Beaver, CISSP (Certified Information System Security Professionals)

Top Reasons SMBs Need to be Concerned about WLAN Security

1. Default WLAN configurations can be easily exploited for malicious purposes.

2. Limited IT budgets and support resources can put information at greater risk.

3. Most networks do contain information that a hacker would want including confidential customer information and intellectual property.

4. Hackers can use a WLAN as a launching pad for virus, spam, and other attacks—creating unwanted liability issues.

5. Someone can compromise a vulnerable WLAN very quickly by sitting in the parking lot of the office building or even by simply driving by in a car.

6. A security breach equals lost time and resources both of which, in turn, equal money.

7. Word about security breaches can spread very quickly to customers and competitors.

8. Increasing government regulations and business partner requirements are making information security a basic business requirement.

WLANs offer connectivity options and convenience never

thought possible, especially given their relatively low cost. For this reason a growing number of small to medium-sized businesses (SMBs) such as accounting firms, doctor's offices, and law firms are relying on wireless LANs (WLANs) to connect computers and expand their networks. However, as with any new technology, there are always disadvantages that must be considered as part of the overall picture. With WLANs, the downside that stands out the most is the technology's inherent information security vulnerabilities. Why is information security such a big deal?

For starters, many people believe that their electronic information is not at risk. This is simply not true. Most hackers are not "professionals" but rather teenagers and young adults who are looking to break in just because they can. They download a selection of hacking programs that are alarmingly easy to use. All they're looking for is somewhere to use them. Remember, most hackers aren't targeting you any more than a thief targets your house. They are only looking for a target of convenience. Once they find a WLAN they can crack, they do so, not knowing is most cases whose system they're breaking into. They are merely looking for systems to compromise whether or not there are huge tangible payoffs.

There's also the issue of disgruntled employees. In this case, you are the desired target. But regardless of intent, your business relies on computers more and more to keep up with the times and stay competitive. This means an increasing amount of information is being processed and stored electronically and, therefore, is in turn made vulnerable to outside attacks. Insecure WLAN usage is making this problem bigger than ever before.

Another information security misconception is that once the cost of firewalls, anti-virus software, and other security solutions are introduced—however small they may be—those costs will far outweigh the need for information security. In addition to the monetary aspect, many people believe that the time, effort, and

expertise required to secure their systems makes it simply not worth it. This is hardly the case, especially for smaller organizations. In fact, a more effective recipe for information security success in SMBs is to spend less on unnecessary high-end security solutions and more on lower-cost technologies and educating employees on the various information security issues to be aware of when conducting business.

When using WLAN technology, it has become increasingly easier for hackers and other malicious users to hide their identity given that the physical boundaries of traditional wired networks are not present to serve as a layer of protection. This makes the art of hacking more appealing and therefore more prevalent. As if malicious hackers, spammers, and virus attacks aren't enough to encourage SMBs to take information security seriously, government entities throughout the U.S. and the world are forcing businesses-no matter how small-to adequately secure their information in the name of personal privacy and protecting corporate information. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) that affects the healthcare industry and the Gramm-Leach-Bliley Act (GLBA) that impacts the financial industry require strict information security controls for organizations in their respective industries as well as any organization that works with these entities as a business partner.

This can include accountants, consultants, lawyers, financial advisors, and more-expanding the requirements for solid information security practices throughout practically every industry. The bottom line is that computers, networks, and the Internet are now more complex than ever.

These complexities are introducing new security weaknesses that are being exploited in more ways-especially in the new realm of wireless computing. Regardless of the size of the organization or the network, information security principles are here to stay and will only become more demanding as we move further into the information age.

The Ultimate Irony

It used to be the case that hacking required a great deal of skill, and that technical hurdle limited the risk of being hacked.

Today, it's no secret that WLANs are extremely easy to hack. In fact, until recently it was far easier to hack into a network than it was to protect it. Part of the problem is that WLAN technology is relatively new and highly complex. Because WLANs historically don't have the same physical protection of wired LANs, many businesses have made the conscious decision to forego the many benefits of going wireless rather than deal with the security and complexity issues involved. What has contributed to the security vulnerabilities associated with WLANs is the fact that most wireless devices—access points (APs), network interface cards (NICs), and computers—are very insecure by default.

Hackers, malicious employees, and virus writers know this and are capitalizing on it. WLAN components are very inexpensive to buy at the local discount electronics or office supply store and are very simple to install—so they are very appealing to SMB employees for home and office use. Making matters worse, the lower-cost WLAN devices tend to have fewer security controls enabled or available by default compared to the controls built into their higher-end enterprise counterparts. All of the threats covered so far concern known vulnerabilities, but what you don't know can indeed hurt you. How many of your employees are connecting to the office network via dial-up or a virtual private network (VPN)?

This can pose serious risks for any employees that have an unprotected WLAN setup at home. Anyone who is able to compromise the home WLAN can often gain access to the office network to which the employee is connected.

There are various ways that WLANs can be compromised. This includes someone walking by an office building with a laptop or wireless PDA (an act called war walking), someone sitting in the

parking lot of the building or simply driving by (war driving), and even someone flying over the building in a plane (war flying). And you can't even trust line-of-sight as a requirement for compromise as hackers, using inexpensive antennas, can tap into your network from over a mile away.

These attackers can capture network traffic, place viruses or other Trojan horse hacker tools on local computers, and even send spam out to the Internet through the unprotected WLAN. So, how do the bad guys take advantage of unprotected WLANs? It's very simple-they exploit various well-known vulnerabilities that make WLANs susceptible to attack.

Protecting against vulnerabilities is not simple. Rather than just making one or two simple configuration changes, there are literally dozens of changes—often very technical in nature—that must be made to WLAN devices to harden them from most of these attacks.

Increasing WLAN Security for Small Businesses © Interlink Networks, Inc.

Abstract

With the rapid adoption of WLAN technology and the growing pool of network vulnerabilities, small business IT managers and leaders have had to plan for additional security in order to support a mobile environment. Preparation comes with significant challenges. In addition to a multitude of confusing acronyms and multi-proprietary Wi-Fi protocol choices in the 802.11 security landscape, current security products do not adequately address the needs of the small business community. Solutions are expensive and entail a complex set-up process and specialized knowledge beyond the scope of many small business IT organizations. Compared to the security infrastructure typical of a large enterprise, small businesses have been "forced to settle for security that is flimsy at best" or defer deploying it altogether.

These factors lend to the belief that security and simplicity cannot co-exist in the same network security solution. Interlink Networks has created a technology that now makes this possible. This white paper addresses small business IT consultants, IT management generalists, early adopters and influencers, and security-conscious small business leaders. The document details how traditional solutions have failed to offer a specialized security resource for the small business market. First, it analyzes the WLAN market and its impact on the small business seeking to improve business efficiencies. Then it defines unique requirements essential to small businesses when investing in a security solution, further examining WLAN security challenges and traditional solutions. Finally it introduces a software solution developed by Interlink Networks that specifically addresses small business requirements for WLAN security issues. The document concludes that although small business practitioners have become increasingly sophisticated in their use of electronic information and their knowledge of computer-related vulnerabilities, they should not be required to invest in costly infra-

structure improvements or act as security experts in order to benefit from enterprise-class WLAN security.

WLAN Market Environment

Market Predictions

Despite the slow economy and weak spending on IT equipment, WLAN technology continues to gain a sure foothold and prove an unqualified success in the networking market. Worldwide consumer spending on WLAN hardware is projected to grow nearly 40%, reaching $3.2 billion in 2006. The market is naturally segmenting between home personal networking, small to medium-sized businesses (SMBs) and large enterprises. SMBs are expected to constitute more than one-third of the WLAN market value by 2006.

Market Drivers

Since their initial emergence on the market in 1990, WLANs have become significantly more affordable, faster and better in performance. Primary market drivers for the popularity of WLANs, and thereby the attraction for small businesses who seek to improve business efficiencies in a vast array of processes, include:

- Lower costs
- WLAN NICs and access points (APs) are available at $49 - $99
- 802.11b prices are plummeting with the arrival of 802.11g
- Embedded WLAN capabilities
- WLAN-friendly capabilities in notebooks such as Intel's Centrino

Mobile Technology

- o Simplicity
- o delivery of Microsoft's XP Professional, improving overall wireless experience
- o Faster speeds
- o availability of 802.11g products
- o Global expansion
- o growth of public WLAN hotspot infrastructures

Despite the increasing popularity of WLANs, market growth is still hampered by issues of complexity, interoperability and security vulnerabilities.

Market Inhibitors—Roadblocks To Adoption

The reality of Wi-Fi today is that it requires technical competency, presents an inconsistent user experience and is not secure out-of-the-box. Typical Wi-Fi security and configuration challenges include a number of factors:

- o Choosing WEP security means:
- o security is enabled by default—it is necessary for the user to manually configure a card or AP
- o users must be able to wade through a wide variety of confusing WEP terminology
- o users encounter multiple processes in order to generate or enter keys, i.e. SSID (Service Set Identifier), pass phrase, or personally created hexadecimal keys. Users must also understand hexadecimal or ASCII (American Standard Code for Information Interchange) keys

- o should the wireless link break, it is imperative for users to correctly enable WEP in order to establish reconnection between devices

- o Choosing VPN (virtual private network) security means:

- o users must deal with the difficulty of selecting and configuring add-on software

- o failure occurs and the VPN does not function properly if the AP is acting as a router or if "dual NAT" (Network Address Translation) is present

- o Risk impacting network speed

- o Choosing RADIUS (Remote Authentication Dial-In User Service) security means:

- o Configuring and managing the RADIUS server requires specialized technical competence

- o overall, a misfit in price point, complexity and maintenance requirements—this solution is compatible with the larger enterprise with significant IT staff

The above Wi-Fi security options require a sequence of complex steps and knowledge that generally serve the large enterprise market and are not suitable for the small business.

Understanding Small Business WLAN Requirements

Wireless LAN technology is now a viable option for small and midsize businesses. Lower costs and solid performance make wireless LANs a networking answer.

- Gartner Research

Wi-Fi has promised wireless mobility, quick connection, and anytime, anywhere use. The small business user seeks to buy solutions

with convenience, simple configuration, and—most elusive of all—security by default. Today's solutions force a choice between security and ease-of-use. Small businesses demand a security solution for wireless networked offices and/or employees that includes:

- Ease-of-use (including initial installation, configuration and deployment across both large and small networks)
- Reliable connectivity—associating with an AP
- Flexibility on a small business budget; and
- Knowledge of who is on the network and confidentiality of network communications to protect valuable data

In order to reap the benefits of a WLAN implementation, businesses of any size or type are faced with investing in a security solution that protects their network and ensures that critical business functions stay up and running. However, network security has typically relied on how much money a company is willing to invest, what degree of difficulty IT management is ready to accept, and how secure it wishes its network to be. This presents a problem for the small business that is not willing to treat security as an option but has limited IT support and budget to meet their security requirements. Security should be an integrated part of the wireless network and users should be confident that set-up and configuration are no more difficult or time-consuming than standard Microsoft XP "anti" applications. Once the security solution is installed, the small business must be able to safely assume that the WLAN is secure and private.

Should Small Businesses Be Concerned About WLAN Security?

Through 2005, 40 percent of SMBs that manage their own network security and use the Internet for more than e-mail will experience a successful Internet attack, and more than half of them won't know they were attacked.
- Gartner Research

Businesses are never too small to be the target of a hacker. The reality is that small businesses are attacked because of all too common vulnerabilities:

o Lack of IT resources

o WLAN may present a larger threat because it:

o involves broadcast data

o requires specialized knowledge

o depends on current equipment

o Security is often turned off

It's not personal, but—where there's a security hole in your server, a hacker will locate it, exploit it and set up residence to launch Denial of Service attacks or distribute spam through mail relays. This can be a serious challenge for a small business that has limited or no dedicated IT resources to defend potential hacker openings. Here are some points for a small business to consider when examining whether it has a false sense of security or is in truth leaving easy opportunities for network attack or invasion.

Lack Of Security Infrastructure

Is the organization typically governed by a dedicated IT resource? Or is security sometimes viewed as an option? Small businesses, especially those that are wireless, are particularly vulnerable to unwanted system entry due to lack of resources and security expertise.

Considering The Cost Of Business

What's at stake if the network is attacked? Information or orders are lost? Customers are exposed? Reputation is marred? Network vulnerabilities leave a business at risk of lost data, revenue, and

customers. Productivity level decreases and legal liability increases. A stolen IP address alone could be fatal for a small high-tech company. To address network security, many small businesses have mitigated their risks by relying on the basics of marginal security with WEP in off-the-shelf solutions. Due to well-known cryptographic weaknesses, WEP is no longer a viable option. Today, WPA 802.1X/EAP is regarded as the most secure alternative for securing Wi-Fi connections.

What's A Small Business To Do?

WEP is not an adequate solution for even the smallest businesses like accounting, attorneys-at-law, and healthcare firms that handle sensitive client and financial data. Even a VPN solution is not foolproof. Although it strengthens WEP security, it does not protect the wireless link. Nor is it easy to configure. The current working WLAN security standard, WPA, requires choosing 802.1X authentication. Although the preferred mode of security, not every business—particularly small businesses—are capable of deploying the RADIUS server necessary to track users and their log-ins. For the small enterprise, this solution may be more complex and costly than necessary.

So, what's the alternative?

The alternative to a RADIUS solution is a WPA upgrade in combination with PSK—using PSK in place of 802.1X. However, the problems with PSK involve:

- o Scalability and Manageability
- o difficulties adding/deleting users
- o no support for guest access
- o does not provide individual user authentication so if values chosen are obvious; a user is left open to a dictionary attack.

Various security researchers fault PSK for the WPA security snag. Though WPA remains cryptographically secure, the PSK method makes it susceptible to passive monitoring and diction-

ary attack—"so the consumer-implementation of WPA is subject to the same kinds of shortcomings that afflicted the weak and broken WEP system." Is WPA the Right Fit for the Small Business?

Included in WPA are 802.1X mechanisms for authentication, key management and other capabilities to address widely publicized security and privacy concerns. WPA undoubtedly improves wireless security and is well designed for the enterprise. However the complexity of AP configuration and deployment as well as RADIUS implementation makes WPA seem an inappropriate solution for the small business network.

Thinking Different About Wireless
By Kevin Werbach

Open Spectrum Defined

Most wireless frequency bands are licensed, meaning that the government gives an entity such as a radio broadcaster or the military the exclusive right to transmit on those frequencies. That license comes with restrictions on geography, power output, technical characteristics and/or service offerings. Transmission in the band by any other party is prohibited as "harmful interference." This regime is considered necessary because the alternative would be a "tragedy of the commons": a chaotic cacophony in which no one could communicate reliably.

The tragedy of the commons idea resonates with our intuitions. After all, too many sheep grazing in the same meadow will use up all the grass. Too many cars on a highway at the same time will cause traffic jams and collisions. Why should spectrum be any different?

Spectrum is different. It is different because it is inherently non-physical, and because technologies developed in recent years make it practical to avoid the tragedy of the commons. What these technologies have in common is that they allow more than one user to occupy the same range of frequencies at the same time, obviating the need for exclusive licensing.

"Open spectrum" is an umbrella term for such approaches. As used here, open spectrum includes established unlicensed wireless technologies such as WiFi. It would be a mistake, however, to conclude that the existence of WiFi proves no further action is needed to facilitate open spectrum. WiFi was designed for short-range data communication and the limitations of current spectrum rules. It therefore still requires wired "backhaul" connections to the public Internet. Moreover, current unlicensed bands and technical standards are not optimized for efficient spectrum sharing. Enlightened policies will allow the emergence of open spectrum systems that are self-contained, and can handle a

range of services and environments. A true open spectrum environment would allow the same degree of openness, flexibility, and scalability for communication that the Internet itself promotes for applications and content.

There are two ways to implement open spectrum technologies. The first is to designate specific bands for unlicensed devices, with general rules to foster coexistence among users. This is the approach that allowed WiFi to flourish in the 2.4 GHz and 5 GHz bands. The second mechanism is to "underlay" unlicensed technologies in existing bands, without disturbing licensed uses. This approach, epitomized by the ultra-wideband technology the FCC authorized earlier this year, effectively manufactures new capacity by increasing spectrum efficiency. Underlay can be achieved either by using an extremely weak signal or by employing agile radios able to identify and move around competing transmissions.

Both unlicensed bands and underlay have their place. Eventually, underlay approaches will be more significant, because they can work across the entire spectrum rather than requiring the creation of designated "parks." Someday, if underlay is successful enough, we may not need licensed bands at all, but that day is well in the future. The important point today is to allow both unlicensed bands and underlay to develop based on technological capabilities and market demand. That involves four steps: removing limitations in existing rules, creating additional unlicensed bands, establishing rules to facilitate additional forms of underlay, and funding research into next-generation technologies.

By Land Or By Sea

Open spectrum is actually a simple concept. It requires no flights of fancy about the laws of physics. It sounds strange because, as the examples above suggest, we are accustomed to thinking of the radio spectrum as a scarce physical entity, like land. Charts showing the partitioning of the spectrum and auctions for geo-

graphically defined rights to slices of the airwaves reinforce the physicality of spectrum. We can't see or touch the radio spectrum, so we envision it as something solid and familiar.

This is a mirage. There is no "aether" over which wireless signals travel; there are only the signals themselves, transmitters and receivers. What we call "spectrum" is simply a convenient way to describe the electromagnetic carrying capacity for the signals. Moreover, the spectrum isn't nearly as congested as we imagine. Run a spectrum analyzer across the range of usable radio frequencies, and the vast majority of what you'll here is silence. Even in bands licensed for popular applications such as cellular telephones and broadcast television, most frequencies are unused most of the time in any given location. This is the case because historical spectrum allocations assume dumb devices that have a hard time distinguishing among signals, thus requiring wide bands with large separation.

With today's technology, the better metaphor for wireless is not land, but oceans. Boats traverse the seas. There is a risk those boats will collide with one another. The oceans, however, are huge relative to the volume of shipping traffic, and the pilots of each boat will maneuver to avoid any impending collision (i.e. ships "look and listen" before setting course). To ensure safe navigation, we have general rules defining shipping lanes, and a combination of laws and etiquette defining how boats should behave relative to one another. A regulatory regime that parceled out the oceans to different companies, so as to facilitate safe shipping, would be overkill. It would sharply reduce the number of boats that could use the seas simultaneously, raising prices in the process.

The same is true with spectrum. Allowing users to share spectrum, subject to rules that ensure they do so efficiently, would be far more effective than turning more spectrum over to private owners.

The Crowded Room

If the idea that many users can coexist in the same spectrum sounds counter-intuitive, another analogy should help. Wireless communication in the radio-frequency spectrum is fundamentally similar to wireless communication in the acoustic spectrum, otherwise known as speech.

Imagine a group of people in a room. Experience tells us that everyone can carry on a conversation with his or her neighbor simultaneously, even with music playing the background, so long as people speak at a normal volume. If someone starts yelling, he or she will drown out other speakers, who will be forced to speak louder themselves in order to be heard. Eventually, some portion of the room simply won't be able to communicate over the background noise, and each additional person who starts yelling will reduce the total number of conversations.

We could call that a "tragedy of the commons." We could enact laws giving only some individuals the right to speak during defined times, ensuring they can shout as loud as they want without interference. But that would clearly be an unnecessary solution with significant negative consequences.

Think back to the situation where everyone is speaking in a normal tone of voice. What allows so many conversations to occur simultaneously is that the people talking are modulating their communications in an appropriate way, and the people listening are able to distinguish one conversation from another. It's the intelligence at the ends of the conversation, not the integrity of the signal, that allows for more efficient communication. The same is true in the radio frequencies. Intelligent devices can distinguish among more simultaneous transmissions than simple ones. The more sophisticated and agile the system, the more the overall carrying capacity of the spectrum increases.

One might protest that the speaking analogy breaks down

when people want to communicate across the room. Here too, there is no reason many conversations can't occur simultaneously. By listening carefully, people can pick out individual speakers. Moreover, imagine that the people in the room could pass messages back and forth on pieces of paper. By cooperating to relay the communications, they would significantly increase the number of conversations, especially over long distances. Relaying and other cooperative techniques can serve the same function in the wireless world.

As this analogy points out, the term "interference" is problematic. Radio waves at the relevant frequencies do not bounce off one another. They pass through each other cleanly, like the intersecting ripples from two stones thrown into a pond. The overlapping signals simply make it harder for a receiver to distinguish one from another.

"Interference" is thus highly contingent on real-world factors. Again, this shouldn't be surprising. Put two television sets next to one another, and you may get a sharp picture on one but a fuzzy image on the other. The difference is that one set has a better tuner. Do we register "interference" when it shows up on one set, or both? Should the most poorly designed set define the requirements for everyone else? What if there is no set in the room but a hypothetical set with certain characteristics might experience a degraded picture there? Under current spectrum policy, such hypothetical "interference" prevents frequency sharing.

Whatever rules we set will influence behavior. If "interference" is defined with reference to a dumb receiver, vendors will try to save money and make receivers as dumb as possible. If, on the other hand, manufacturers have no guarantee of spectrum exclusivity, they will have the opposite incentive. They will build devices robust enough to deal with a variety of situations, bounded by the overall technical rules for use of the spectrum band. Those building transmitters or delivering services over the spec-

trum will face similar incentives depending on the way the rules are defined. The point is not that the most unrestricted environment is always the best. It's that our current system, without justification, assumes an exclusive licensing regime is the only viable answer.

Technologies Of Wireless Freedom

There are three primary techniques for magnifying the efficiency of wireless devices in a shared environment: spread spectrum, cooperative networking and software-defined radio. These can all be used in licensed bands, though they reach their full potential in an unlicensed environment.

Spread Spectrum

In a spread-spectrum system, wireless communications are digitized and chopped up into pieces, which are spread across a range of frequencies. If the receiver knows where to look, it can piece the message back together on the other end. Spread spectrum means that an individual frequency only carries a small part of each communication, so it's only occupied for a tiny slice of time. In the unlikely event that another message is occupying that slot, only that small portion of the signal must be re-sent. Spread spectrum was invented in the 1940s, and has been used extensively for military and other applications that require robustness and resistance to jamming or eavesdropping (because only the receiver knows how the signal is spread across the range of frequencies). Many mobile phone services use spread-spectrum today to improve efficiency within licensed bands, but the technique is even more powerful when used for underlay or in unlicensed bands.

Software-Defined Radio

Every radio can be tuned to pick up a certain range of frequencies, and it takes some amount of time to change the tuning. Traditionally, these characteristics are fixed in the radio hardware. Thus, for example, the same radio can't pick up both FM radio and mobile phone transmissions, or both 2.4 Ghz and 5

Ghz wireless LAN signals. Software-defined radios, by contrast, can tune dynamically over a wider range of frequencies. A software-defined radio can receive or transmit different kinds of wireless transmissions automatically. If it is a so-called "agile radio," it could adapt to the local environment and seek out open frequencies to communicate. Even in licensed bands, most of the spectrum is empty most of the time. Agile radios could take advantage of that empty space, moving out of the way when another transmission appears.

All of these areas are the subject of extensive academic research and corporate R&D. Nonetheless, the licensed spectrum model has been the dominant paradigm for so long that there is a surprising amount we simply don't know about how radios work. For example, we don't know as a theoretical matter what the maximum capacity is of a geographically defined system filled with randomly distributed radios.

We do know that many of our intuitions are wrong. Research has shown that many factors we believe should decrease the capacity of a system-adding more transmitters, creating more alternative paths for signals to travel, or putting receivers in motion, for example-can actually increase capacity. This occurs because the more data a smart receiver has about the surrounding environment, the better it can do in distinguishing the desired signal.

The commercial viability of any system using these techniques will depend on business conditions. That is one reason government policies should advance both designated unlicensed bands and underlay approaches that coexist in licensed bands. Under any scenario, though, open spectrum is not a fantasy, but a concept based on proven techniques. It is time for our policies to catch up with the state of technology.

The Myth Of Scarcity

To take advantage of the fantastic potential of open spectrum, we

must change our spectrum policies. With a few exceptions, existing laws and regulations are rooted in historical anachronisms.

Since the passage of the Federal Radio Act in 1927 and the Communication Act in 1934, virtually everything about wireless has changed. What began as a technology for ship-to-shore communication became the foundation of the radio, broadcast television, satellite and cellular telephone industries, as well as supporting private radio services, public safety communications, military communications, wireless data networking and a host of other applications. The amount of spectrum considered usable has increased dramatically, as more sophisticated devices have been developed. Analog services are giving way to digital, allowing for additional features and efficiency.

Everything has changed except for one very important thing: We still regulate the radio spectrum based on the technology of the 1920s.

Spectrum licensing arose in the 1920s because of a historical phenomenon. Radio receivers of the period were primitive. They couldn't distinguish well between different transmissions, so the only way for multiple users to share the spectrum was to divide it up. In 1912, nearby ships hadn't responded to the Titanic's distress calls, prompting calls for regulation. By licensing spectrum to broadcasters, with wide separation between bands, the government could ensure that receivers could identify which signal was which. The exclusive licensing model was almost certainly the right approach when it was developed. It has been in place for so long, during which there has been so much commercial innovation in use of the wireless spectrum, that we take it for granted. When you think about it, though, our approach to spectrum is the exception rather than the rule. We shrug at intense government regulation of communications over the airwaves that would be unconstitutional in other media. After all, wireless communication is speech. Under the First Amendment, the government faces a high burden in justifying any law that

defines who may communicate and who may not. Yet Congress and the FCC routinely determine who may broadcast on certain frequencies, and they regularly shut down those, such as "pirate" radio broadcasters, who fail to observe those rules.

The rationale for limiting speech over the airwaves is that there is no alternative. Spectrum is scarce, so the argument goes, so either some may speak or none will be able to get their message across amid the cacophony of interfering voices. As discussed above, though, that scarcity is not an immutable property of a physical spectrum resource. It's a historically and technologically contingent judgment. Needless to say, much has changed since the 1920s. And indeed, there has been a major shift in the government's approach to spectrum assignment. Auctions have replaced outright grants, competitive hearings, and lotteries as the tool of choice. Beginning with Ronald Coase's seminal 1959 article, "The Federal Communications Commission," economists have argued persuasively that competitive bidding is the most efficient way to assign scarce licenses among competing users. Starting with the personal communications service (PCS) auctions of 1994, the FCC has raised over $30 billion for the US Treasury and delivered substantial new spectrum to the marketplace in this manner.

Most of the debates around spectrum policy today involve variations of the auction idea. Some parties advocate secondary markets or moving from licenses to fee simple ownership, while others propose combining auctions with annual lease fees after the initial license period. These debates, intense though they may be, occur within the safe confines of the dominant exclusive licensing paradigm. If we have decided to license wireless frequencies, there are important questions about how best to do so. But why take licensing for granted?

A Spectrum Commons

Capacity-magnifying techniques such as spread spectrum, cooperative networking and software-defined radio make it possible

to see spectrum as something other than a physical resource to be licensed. Portions of the radio spectrum could instead be treated as a commons. A commons, like the air we breathe and the language we speak, is a shared, renewable resource. It is open to all. It is not completely free or inexhaustible, but it can seem that way if individuals follow rules to prevent over-grazing. A commons is entirely compatible with competitive capitalism. The key is that the marketplace occurs among users of the commons; the commons itself cannot be bought or sold. We have no trouble accepting the automobile and trucking industries, even though they depend on public roads and highways that are free to use and maintained by the government. And we accept that even though anyone can drive on the highway, everyone has to observe speed limits, seatbelt laws, and other safety rules. Those public roads even coexist with private toll roads, but we don't think that privatizing all the roads would improve the quality of transportation in the US.

A spectrum commons works just like the highways. Government defines the scope of the common resource and sets limited rules to facilitate efficient use. That means setting aside unlicensed frequencies, adopting rules to facilitate new "underlay commons," setting power limits or other technical standards, and responding to any breakdowns.

The beauty of a spectrum commons is that is creates the right incentives. Exclusive licensing and propertization create spectrum monopolies, which seek to maximize the rents they can collect. Forcing licensees to buy spectrum at auction ensures it goes to those who value it highly, but it forces the winner to recoup its up-front investment, biasing the way it makes use of the spectrum. As noted above, exclusive licensing also encourages receiver manufacturers to make their devices as dumb as possible, while a spectrum commons has the opposite effect. In a commons environment, companies can respond to marketplace demands by tailoring new services, since the costs of entry are minimal.

Open Spectrum In The Real World: The WiFi Explosion

Arguments about the benefits of open spectrum have in the past been largely theoretical. Techniques such as spread-spectrum were widely employed, but primarily in licensed bands or in military applications. Academic research showed the benefits of a spectrum commons. Without mass-market commercial examples, though, few were convinced the idea could fly in the real world.

Such real-world validation arrived in the form of WiFi and related wireless local area network (LAN) technologies. WiFi is a marketing and certification term promulgated by the Wireless Ethernet Compatibility Alliance, an industry trade group. It refers to the 802.11b and 802.11a wireless Ethernet standards defined by the Institute for Electrical and Electronic Engineers (IEEE). 802.11b, which was the first to take off commercially, operates in the 2.4 GHz Industrial, Scientific and Medical (ISM) band and delivers data speeds up to 11 megabits per second. 802.11a operates in the 5 GHz U-NII band and offers connections up to 54 megabits per second. Standards work in this area is ongoing, with proposed standards including 802.11g, which delivers higher-speed connections in the 2.4 GHz band, and 802.11e, which adds quality-of-service mechanisms to support high-quality voice and video delivery. The IEEE issued the final 802.11b standard in September 1999. The first mass-market commercial implementation, Apple's AirPort technology, went on the market that year. Since then, the market has grown rapidly, with expected sales of some 10 million PC/laptop adapter cards this year. Vendors such as Cisco, Linksys, D-Link, Netgear and Proxim are doing a brisk business selling access points for home networks, adding value to residential broadband connections. On the enterprise side, wireless LAN deployments doubled last year, with more than one million access points now in use in 700,000 companies, according to the Yankee Group. Cahners In-Stat sees the WiFi hardware market generating over $5 billion in 2005, and that doesn't even include service revenues.

WiFi Applications

Though WiFi was originally developed for corporate LANs, it has garnered attention for two applications: hotspots and community access points. Hotspots are wireless access points deployed in high-traffic locations such as hotels, airports, and cafes. Typically, the facilities owner contracts with a company that installs the necessary equipment and Internet connection, with the revenue split between them. Sometimes the service provider keeps all the revenue, with the facilities owner benefiting from additional traffic the access point generates. End-users usually pay a per-minute or monthly access fee to connect to the Internet through the hotspot.

Over 4,000 hotspots have been deployed in the US, as well as in Europe and Asia. Most major hotel chains have announced plans to deploy WiFi hotspots, as have major US airports. The most prominent hotspot arrangement is MobileStar's deployment in Starbucks coffee houses around the country. MobileStar filed for bankruptcy, but its assets were purchased by VoiceStream and its hotspots are now supported under its T-Mobile brand. T-Mobile and Hewlett Packard recently announced that WiFi will be available in 2,000 Starbucks by the end of 2002. Community access points are similar to hotspots, but they are made freely available to anyone in the area. Typically, community access points are established by individuals or groups such as BAWUG in the San Francisco Bay Area, NYCWireless in New York City, or Personal Telco in Portland, Oregon. Many hook without permission into corporate networks or home broadband connections. An increasing number, however, are funded by governments, universities, and non-profits who see a benefit in providing widespread wireless Internet access. Athens, Georgia offers free WiFi connectivity throughout its downtown area, funded by the University of Georgia, while Intel sponsors free WiFi connections in Manhattan's Bryant Park. Hotspots and community access points have generated significant media attention, and for good reason. However, they are only one element of a WiFi market that includes several other major applications.

Campus Networking

Major corporations are deploying WiFi networks across their corporate campuses to provide ubiquitous connectivity for their employees; universities are doing the same for their students and faculty. Unlike the consumer access points, these deployments typically have beefed up security and reliability. WiFi is one of the few remaining growth areas in the depressed data networking sector, a fact not lost on vendors such as Cisco. Leading information technology services companies such as IBM have developed expertise integrating and installing these corporate networks.

Industrial Applications

Manufacturers such as Boeing are using WiFi to network their factories and warehouses. Such environments don't lend themselves to wired connections. The ability to track inventory and access internal corporate documents from anywhere can generate substantial cost savings and efficiency benefits for these companies, who take advantage of the maturity and low cost of WiFi equipment thanks to its consumer applications.

Virtual ISPs

Several companies are linking together the scattered hotspots through roaming arrangements, creating nationwide virtual networks. Examples include Boingo, Joltage, Wayport, and NetNearU. Some of these companies encourage individuals and small businesses to establish new access points, offering to share revenues from wireless access with them. A New York Times report earlier this year stated that several major technology and communications companies including Intel, Microsoft and Cingular Wireless were evaluating creating a nationwide WiFi roaming network, known as Project Rainbow. All this activity has taken place in an already-crowded unlicensed band, without any protection against interference from other users. WiFi is an existence proof for the validity of the open spectrum argument.

Other Unlicensed Technologies

WiFi is not alone. Several other unlicensed wireless data technologies are either commercially available or nearly so. Each has technical characteristics that lend themselves to particular market opportunities, though there are many areas of potential overlap. The beauty of an unlicensed environment is that hardware vendors and service providers need not go through a gatekeeper such as a cellular carrier to gain access to spectrum. If the technology works, and there is a market for it, the equipment can simply be deployed.

802.11 Variants

WiFi is a particular protocol designed for local-area network applications. Several companies are trying to marry the cost economies of standards-based 2.4 GHz radios with proprietary software and hardware to support additional capabilities. There are also competing standards to WiFi, including HomeRF and the European HyperLAN2, but these have generally lost out to WiFi in market adoption and will likely fade away.

Ultra-Wideband

As described above, ultra-wideband (UWB) systems use such low power that they can underlay beneath existing licensed spectrum bands. Because of the power limitations, current UWB implementations have limited range, but they offer significant capacity. Vendors such as Time Domain and XTreme Spectrum are building chipsets to deliver 100 Mbps or more over short distances. After a long and bitter fight, the FCC authorized UWB underlay for the first time in February. The FCC's initial rules put strict limits on UWB systems, but the Commission committed to reviewing and potentially loosening the restrictions if interference fears do not materialize.

Bluetooth And Other Personal Area Network Technologies

WiFi works in a local area, but many wireless applications need only a range of a few feet. Personal-area networking (PAN) encompasses situations such as transmitting between a mobile phone

and a headset, sending data between a phone and a personal digital assistant, and printing from a laptop to a printer in the same room. For these scenarios, WiFi may be overkill in terms of power requirements and chip costs. Bluetooth is an unlicensed ad hoc 2.4 GHz standard for such applications. It has been slow to roll out, leading to speculation it would lose to WiFi. However, it now looks as though Bluetooth will find a niche, primarily replacing wires in short-range situations.

Unlicensed Metropolitan-Area Networking

At the other extreme from PANs are metropolitan-area networks (MANs), which cover entire neighborhoods or cities, though often designed primarily for business connections. The IEEE is developing standards, 802.16, for wireless MANs using the 10 GHz - 66 GHz spectrum. Though these are initially targeted at licensed spectrum, the same concepts could be applied in an unlicensed environment. Motorola offers a proprietary unlicensed system called Canopy that is designed for the metropolitan area. Canopy, or some variant of it, might become the basis for the 802.16 standard in unlicensed bands.

Lessons Of WiFi

The success of WiFi shows that spectrum sharing works in the real world. Without heavy-handed control by government or by service providers who have incentives to maximize only their own welfare, an entire industry has emerged. That industry has developed with no legal protections against competing uses. Despite repeated warnings of a "meltdown," only isolated anecdotal cases of congestion among WiFi users have been reported. Companies such as Intel and Microsoft are devoting substantial resources to these technologies, which they would be unlikely to do if they were seriously concerned about a tragedy of the commons.

Moreover, wireless LAN technology is evolving and diversifying rapidly. Vendors are beginning to deliver hybrid 802.11a/b chipsets, and devices that add software intelligence to WiFi are coming on the market. Innovation in the WiFi world follows the

computer industry curve of Moore's Law, because it is based on improvements in hardware. WiFi devices become cheaper and more sophisticated every year, just like personal computers (but unlike most telecommunications services). They are standards-based components sold in a competitive market, at volumes that allow for economies of scale. Those new devices become part of the network as soon as users purchase and install them. Capital investment is spread among users, rather than shouldered upfront by a network operator. By contrast, 3G services can only be deployed after service providers build and upgrade expansive network infrastructure and proprietary hardware.

Limitations in WiFi devices are being addressed through market forces. For example, first-generation WiFi equipment has a relatively weak built-in security mechanism known as Wireless Equivalent Privacy (WEP). For users concerned about security, such as enterprises, third parties and hardware vendors quickly developed supplemental security solutions that integrated with standards-based WiFi deployments. Meanwhile, an enhanced security standard, 802.1x, was recently ratified by the IEEE.

A key to the success of WiFi is that it uses a different business model than traditional telecommunications and broadband services. Because the network grows incrementally with every new access point and every device capable of receiving WiFi signals, there is no need for incentives to convince a monopoly service provider to build out expensive infrastructure. No one needs to predict what the killer applications of the technology will be, because users will find them on their own. With a licensed service, the network operator must invest in delivering services in the hope that customers will pay enough to recoup that investment. With WiFi, services grow bottom-up through market forces.

There are many things WiFi cannot do. For example, as a short-range LAN technology, it can't provide universal coverage over a large area, and it isn't designed for mobile scenarios such

as connecting from a car. For these applications, WiFi gracefully coexists with licensed services. Vendors such as Nokia are building equipment that supports both WiFi and licensed wide-area cellular services, allowing users to switch automatically to the best network for their current needs. Licensed mobile operators are beginning to enter the WiFi hotspot business, including T-Mobile, Sweden's Telia, and Japan's NTT DoCoMo.

Open Spectrum And The Last-Mile Bottleneck

Unlicensed technologies could play an important role in residential broadband adoption. Today, incumbent cable and local telephone companies dominate the residential broadband market with cable modem and digital subscriber line (DSL) services. These companies control the two primary wires into homes. To deploy high-speed services, they must upgrade their networks, which requires significant investment. Most incumbent service providers now charge $45 to $50 per month for broadband connections. They frequently place significant limitations on the services, including highly asymmetric bandwidth, prohibitions on home servers, prohibitions on virtual private network connections, and limits on streaming video usage.

The operators claim these restrictions are necessary for their broadband offerings to be economically viable, even though equivalent services in other countries are priced significantly lower. Though subscribership is increasing and new technologies are reducing the costs of broadband infrastructure, many companies have actually increased their prices during the past year, as competition dried up.

The fundamental problems in the residential broadband market are the same as in wireless. Service providers must build expensive networks and define the services for which they think users will pay, then charge high rates to recover their costs. Most cable modem and DSL providers market their services as providing faster Web surfing than dial-up access.

Many end-users simply don't find this compelling, especially at $50 per month. Unlike the open WiFi market, there is no room for innovators to roll out new service offerings or better technology, because everything must go through the network owner.

As noted above, standard WiFi technology provides only short-range connections, to a range of approximately 300 feet. This is insufficient for most residential broadband deployments. To deliver broadband to a home, the home must connect to a high-speed Internet trunk, which can be shared among many customers. Having a fast WiFi connection in a house doesn't substitute for DSL or a cable modem, because the wired connection is still necessary to reach the public Internet.

Despite these limitations, there are several approaches that could allow unlicensed wireless devices to deliver last-mile broadband service. Companies such as Nokia (with its Rooftop system), MeshNetworks and SkyPilot have created systems that use a meshed architecture. In other words, rather than connecting to a central hub, each device can send information to every other device it can see. Information can be routed through the network using many different paths, depending on capacity, line of sight, and other characteristics. The mesh approach gets around limitations that hobbled previous fixed-wireless systems in the last mile. Other companies such as Etherlinx and Motorola have created proprietary technologies on top of WiFi radios to allow significantly increased range in traditional point-to-multipoint deployments. Motorola claims its Canopy technology can serve up to 1,200 subscribers from a single access point at a range of up to two miles, operating in the unlicensed 5 GHz band. Unlicensed wireless connections could also serve as "tails" at the end of existing phone, cable, or fiber infrastructure in residential neighborhoods.

All these configurations have their limitations. As with any wireless service, connection quality depends on physical geography and the local spectral environment. As a result, it's

unlikely unlicensed technologies would represent the majority of broadband connections in the near future. Even if they take a small share of the market, however, wireless last-mile systems would foster significant competition and innovation. Wired broadband providers would have to improve their offerings or lower costs to compete.

Demand Pull

Unlicensed wireless technologies will impact the broadband market even if they aren't used as the primary connection method. Large numbers of WiFi access points are being deployed for home networking. Users install these devices in their homes to share broadband connections among several computers, share peripherals such as printers, or give themselves untethered Internet access anywhere in their house.

Digital consumer electronics devices are beginning to incorporate WiFi connections as well. For example, Moxi Digital, which recently merged with Digeo, a company funded by Microsoft co-founder Paul Allen, incorporates an 802.11a transmitter in its personal media center. This allows the Moxi box to stream high-quality audio video among TVs and stereos throughout a house. Intel is spearheading a standards effort to allow WiFi to interoperate with FireWire (IEEE 1394), a wired standard popular for digital media applications.

As home networks and related devices proliferate, they will create a "pull" for broadband applications. WiFi hardware is becoming sufficiently cheap for hardware manufacturers to include it without significant effects on device prices. As users buy laptops and consumer electronics hardware with high-speed wireless connections built in, they will find new uses for it, such as sending music files from their computer to their stereo system, or sharing pictures downloaded from the Web. Many of these applications will benefit from broadband connections into the home. Wireless devices will therefore stimulate broadband demand even when the last-mile connection is wired.

Policy Recommendations

Open spectrum is not inevitable. Technologies now available or under development will lay the groundwork for a radically more open and more efficient wireless environment, but without the right policy framework, those technologies may never see the light of day. WiFi, exciting though it may be, cannot simply evolve into the full realization of open spectrum. If the US wants to enjoy the benefits of open spectrum, it must take steps to facilitate it.

First, Do No Harm

Despite the promise of open spectrum, there are many threats to the continued growth of unlicensed wireless. Open spectrum profoundly threatens the status quo. It represents a new form of potential competition for existing wireless services, and for wired services as well. Moreover, it runs counter to conventional assumptions about which policies are truly market-based. Absent a clear understanding of open spectrum's implications, policy-makers may take actions that would prevent it from reaching its potential. The FCC and Congress must ensure that the following threats from incumbent industries do not undermine the future potential of unlicensed technologies:

- **Requests For Regulatory Protection**

Sirius Satellite Radio filed a petition with the FCC earlier this year seeking restrictions on WiFi based on trumped-up concerns about interference with its adjacent licensed satellite transmissions. Though Sirius hadn't even launched its service and the potential for interference was minimal, it wanted significant limitations and new device requirements placed on the thriving WiFi industry. The Sirius petition was withdrawn after it provoked serious objections. Nonetheless, it gives a sense of how licensed users could seek to hamstring unlicensed alternatives. Wireless operators facing new competition from unlicensed devices may similarly rely on scare tactics and legal maneuvers to prevent unlicensed services from encroaching on their markets.

❍ Spectrum "Propertization"

If the FCC were to give spectrum licensees full ownership rights, it would significantly decrease the likelihood that spectrum would be available for unlicensed uses. Companies that pay for control over frequencies will want to recoup their investments, which means excluding competing users. Even if "band managers" could operate toll-gated frequencies for unlicensed use, the transaction costs involved would be substantial. Worst of all, propertization is a one-way street. Once spectrum becomes private property, converting some of it to unlicensed "parks" or even eliminating restrictions on band sharing could require costly eminent domain proceedings. Giving spectrum licensees greater flexibility or opportunities to engage in secondary market transactions may make sense, but the step from there to further propertization would have significant negative consequences.

❍ Backhaul Discrimination

Unlicensed wireless data devices must at some point connect into the public Internet. For traditional point-to-multipoint systems such as WiFi, an access point serves as the local hub and connects to a wired data connection such as a T-1 line to deliver traffic to the Internet. Bringing data from a local point of presence to a central aggregation point is known as "backhaul." It typically involves facilities of incumbent local exchange carriers, because their networks span virtually every city. Because of the lack of competition, backhaul is expensive. Moreover, if telephone companies see unlicensed wireless devices as competitive, they may seek to prevent them from connecting into their networks. An advantage of meshed networks and systems that combine short-range unlicensed "tails" with long-range unlicensed "backbones" is that they cut down on the need for wired backhaul connections. Until such alternatives are widely available, the government should reject rule changes that would make it easier for telephone companies to discriminate in provision of wireless backhaul, and should police against anti-competitive behavior.

❍ Affirmative Steps

At the same time, policymakers should take affirmative steps to facilitate open spectrum. Most current unlicensed wireless services, including WiFi, operate in the 2.4 GHz and 5 GHz unlicensed bands. These bands are relatively narrow, at high frequencies that limit their propagation, and subject to many established competing uses. Though unlicensed devices can coexist in seemingly crowded spectrum, their ability to do so is not absolute. Moreover, WiFi's software protocols don't have the adaptive and cooperative characteristics of truly scalable unlicensed networks. Current FCC rules have done a reasonable job of setting conditions that allow for innovation and market growth, but more is needed.

The US government should follow a four-step program to make open spectrum a reality:

- ❍ Develop rules to foster more effective cooperation among unlicensed users
- ❍ Set aside more spectrum for unlicensed uses
- ❍ Eliminate restrictions on non-intrusive underlay techniques across licensed bands
- ❍ Promote experimentation and research in unlicensed wireless technology

All of the elements are important. WiFi, other unlicensed technologies in designated bands, and underlay are all part of the answer. Furthermore, the mix will change over time. Existing unlicensed bands are delivering value today. However, newer approaches designed from the ground up for open spectrum will be the long-term winners.

The only way to allow market forces to determine the best solutions is to give alternative approaches a chance. By announcing its intention to move forward with a comprehensive open

spectrum agenda, the US government would give investors and technologists the confidence to devote resources to new ventures that make open spectrum a reality.

1. Fostering Effective Cooperation

The first step is to enhance existing unlicensed bands, which were not designed with open spectrum in mind. The FCC should work with the private sector and the technical community to identify minimal requirements to facilitate efficient spectrum sharing. In the near term, this could include service rules for the 5 GHz band to allow for continued growth of wireless data networking applications. These should not pre-determine technology or applications, but could include general requirements such as mandating that devices be capable of two-way packet-switched communications. The FCC should also identify restrictions in its existing rules, such as outmoded prohibitions on repeaters, that could be removed to allow for greater spectrum sharing.

In the future, as it establishes new unlicensed bands and eliminates underlay restrictions, the FCC could define additional "rules of the road," either as requirements or as advisory "best practices." For example, companies could be encouraged to build devices that modulate their output based on actual conditions, or that repeat traffic for other users, allowing for meshed architectures.

Whatever rules are adopted should be developed in consultation with industry representatives and technical experts to ensure they do not over- or under-specify standards. Reasonable accommodations should be made for uses of spectrum other than data networking, including scientific activity such as radio astronomy. Different rules may apply to particular bands or techniques. Whatever decisions are made will need to be reviewed periodically as conditions evolve.

2. Expanded Unlicensed Spectrum

Improving existing unlicensed bands isn't enough. Most are so

narrow and congested that their utility for open spectrum is limited. Furthermore, the high frequency of the most prominent unlicensed bands limits signal propagation. Lower-frequency spectrum that penetrates weather, tree cover, and walls would provide significant advantages for services such as last-mile broadband connectivity.

The FCC should identify additional spectrum bands that can be designated for use as unlicensed "parks," with a particular focus on frequencies below 2 GHz where propagation is best. The FCC will need to consult with other relevant agencies such as the Department of Defense, Federal Aviation Administration, and Department of Commerce; technical and scientific organizations such as the National Academy of Sciences and Institute of Electrical and Electronics Engineers; and the private sector. Furthermore, the U.S. government should work through the World Radio Conference and other international fora to create global unlicensed bands wherever possible.

There are many possible sources for additional unlicensed spectrum. The 5 GHz unlicensed band could be expanded relatively easily, a move that would also help bring the U.S. allocation in line with other countries. Because of its limited propagation characteristics, however, 5 GHz should not be seen as a long-term solution. Creating unlicensed spectrum parks elsewhere would involve relocation or other accommodation of existing users. That is a process the Commission has engaged in repeatedly in the past.

3. Remove Constraints On Underlay

The FCC took a major step forward with its February approval of ultra-wideband. The Commission wisely rejected overblown fears about interference, relying on technical data and prudent restrictions on UWB deployment. However, the Commission's initial rules still put unnecessarily severe limits on where and how UWB can be used. Assuming that experience shows the fears about interference ungrounded, the FCC should loosen its restrictions without delay.

The FCC should look at other ways to facilitate underlay of unlicensed communications in existing spectrum bands. Underlay can be achieved either through weak signals or adaptive, agile receivers. As technology advances, the FCC could consider a rule allowing underlay in certain bands, so long as devices check the local environment before transmitting and vacate a frequency within a certain number of milliseconds if a licensed service appears there. Underlay could also be used as a transition mechanism in bands where there are limited numbers of incumbents. Those incumbents could be allowed to remain in the band, but without the current guarantees against interference.

4. Drive Technology Development And Adoption

The government should seek out additional mechanisms to encourage the development and deployment of unlicensed devices. These could include liberalizing rules for experimental licenses, funding research projects, and using government procurement power to drive adoption of WiFi or other technologies.

The Defense Advanced Research Projects Agency (DARPA) of the Department of Defense has a distinguished history of supporting cutting-edge research in data networking, including the packet-switching technology that led to the Internet. DARPA has long funded research into meshed wireless networking, ultra-wideband, and software-defined radio, because of their military applications. These efforts should be continued, and every effort made to ensure smooth transfer of the resulting technologies to civilian applications.

The FCC and other relevant agencies should review their rules to identify unnecessary restrictions that keep unlicensed devices out of existing programs. For example, the FCC doesn't allow the use of Schools and Libraries subsidies for unlicensed networking devices, because they do not involve a communications "service." Of course, government should not try to pick winners among competitors in the marketplace, but rather work

in tandem with the private sector to ensure innovative technologies can reach their potential.

Alongside these steps, the FCC and Congress should continue their broader efforts to foster investment and competition in communications. Open spectrum will flourish in a growing market.

A Near-Term Opportunity In 700 MHz

The forthcoming return of analog television spectrum provides an opportunity to put some of these policies into practice. Congress has directed the FCC to auction the 700 MHz spectrum now occupied by broadcast channels 60-69, though the auction has been delayed several times. Because of its propagation characteristics, the 700 MHz spectrum could make an excellent unlicensed wireless park, a scenario that simply could not be contemplated when the original plans for return of that spectrum were drawn up.

Congress should take advantage of the opportunity and designate some or all of the 700 MHz spectrum for unlicensed devices. As a transitional mechanism, the FCC could allow only underlay uses that do not intrude on incumbent licensees.

Conclusion

We are living under a faulty set of assumptions about spectrum. Licensing may have been the only viable approach in the 1920s, but it certainly isn't in the first years of the 21st century. We take it for granted that companies must pay for exclusive rights to spectrum, and that once they do, they must invest in significant infrastructure buildout to deliver services. We also take for granted a pervasive level of regulation on how spectrum is used, which would be intolerable for any other medium so connected to speech. We assume that market forces, if introduced into the wireless world at all, must be applied to choices among monopolists rather than free competition. We make these assumptions because we can't imagine the world being otherwise.

Open spectrum technologies forces us to rethink all of our assumptions about wireless communication. By making more efficient use of the spectrum we have, it can effectively remove the capacity constraints that limit current wireless voice and data services. By opening up space for innovation, it could lead to the development of new applications and services. It could provide an alternative pipe into the home for broadband connectivity. And it could allow many more speakers access to the public resource of the airwaves.

Today, we stand at a crucial point. Our policies could fritter away open spectrum's historic opportunity, either through inaction or harmful limits on new technologies. Or we could listen to what the market and technology are telling us. Computers have made wireless devices vastly smarter than they were in the past. It's time for our policies to become smarter as well.

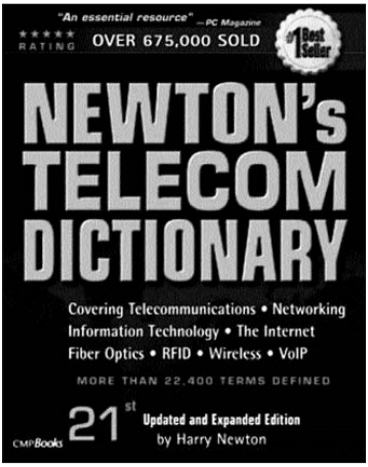
Kevin Werbach is a technology consultant, author, and founder of the Supernova Group. He has served as the Editor of Release 1.0: Esther Dyson's Monthly Report, and as Counsel for New Technology Policy at the Federal Communications Commission.

Wireless Knowledge

This book has attempted to take you from little or no knowledge to the level of an intermediate wireless user. However, there are plenty of other books and resources that will take you on your journey to further understanding wireless technologies.

We have compiled a whole load of titles that you should condsider reading for an indepth understanding of wireless technologies.

Newton's Telecom Dictionary, 21st Edition: Covering Telecommunications, Networking, Information Technology, The Internet, Fiber Optics, RFID, Wireless, and VoIP



Author: Harry Newton

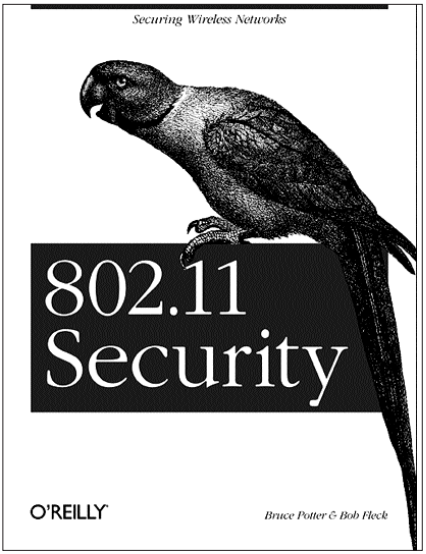
Perhaps the world's best-selling reference book on telecom, data communications, networking, computing and the Internet, this book has sold over 6.5 lakh copies. The 21st edition of Newton's Telecom Dictionary includes wireless, broadband, VoIP, RFID, and fibre optics terms.

This book is packed to the brim with over 22,000 definitions, and explains technical concepts in a language that everyone can understand. It's the perfect tool to use for training-give your employees a crash course in networking and telecommunications.

It contains four bonus sections such as Harry Newton's favourite money-saving tips for telecom, computing, and more. The book also attempts to give you an insight into how you should use your telecom budgets in a world where purse strings are tight. Also make sure to read the section on disaster recovery planning, to learn how to best protect your telecom and computing resources.

802.11 Security

Authors: Bruce Potter and Bob Fleck

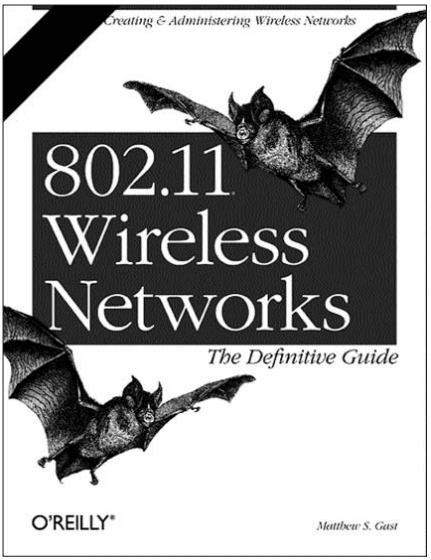


Beginning with a general introduction to 802.11b, this book dispels common myths about security, and gives you both theoretical and practical insights into the workings of wireless security. Once you have gone through the basics, you will be better able to understand the rest of the book, and think about how it may apply to your specific needs.

This book should never leave a network engineer's side, and in fact should also be carried about by wireless security personnel and systems engineers. This is a must read for anyone interested in deploying large 802.11b-based systems and networks.

802.11 Wireless Networks: The Definitive Guide: Creating and Administering Wireless Networks

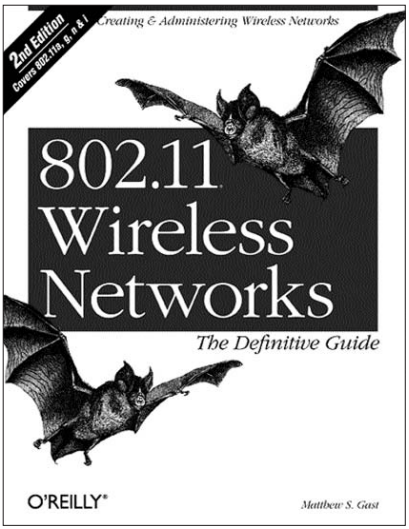
Author: Matthew Gast



Network administrators, architect, and security professionals need to understand the capabilities, limitations, and risks associated with integrating wireless LAN technology into current infrastructure. This practical guide provides all the information necessary to analyze and deploy wireless networks with confidence. It's the only source that offers a full spectrum view of 802.11, from the minute details of the specification, to deployment, monitoring, and troubleshooting.

802.11 Wireless Networks: The Definitive Guide, 2nd Edition

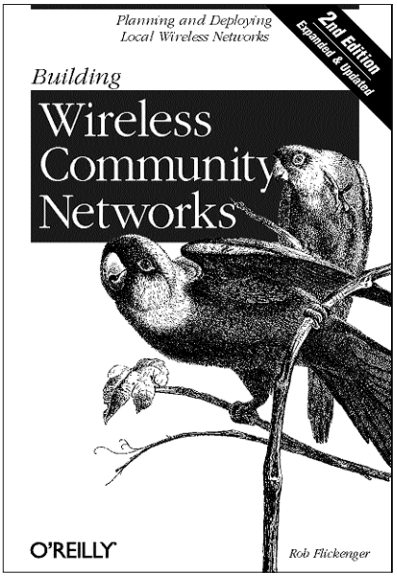
Author: Matthew Gast



If you want to deploy your own wireless network-either at home or at the office-you must first understand the capabilities and risks associated with the 802.11 protocols. 802.11 Wireless Networks: The Definitive Guide, 2nd Edition is the perfect place to start. This updated edition covers everything you need to know about integrating wireless technology into your current infrastructure.

Building Wireless Community Networks, 2nd Edition

Author: Rob Flickenger

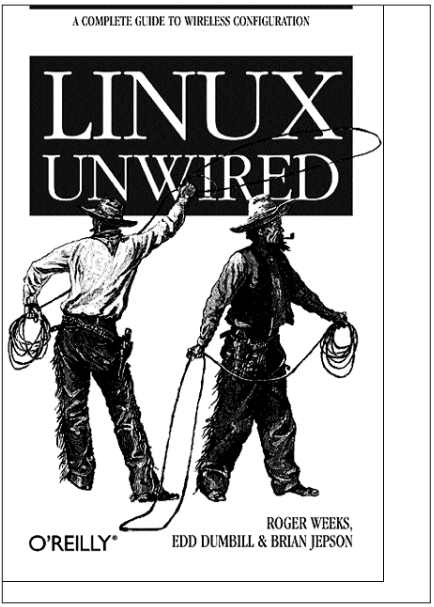


Building Wireless Community Networks is about getting people online using wireless technologies. The 802.11b standard, better known as Wi-Fi, makes it possible to network towns, schools, neighbourhoods, small business, and almost any kind of organisation. All that's required is a willingness to cooperate and share resources. The first edition of this book helped thousands of people engage in community net working activities. This revised and expanded edition adds coverage on new network monitoring tools and techniques, regulations affecting wireless deployment, and IP network administration, including DNS and IP Tunnelling.

Linux Unwired

Authors: Roger Weeks, Edd Dumbill and Brian Jepson

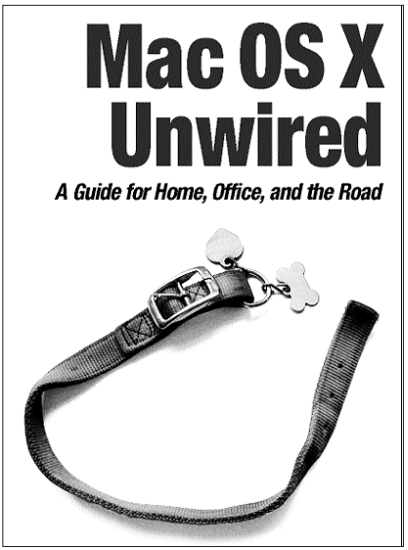
Linux Unwired is a comprehensive wireless information source for mobile Linux users. Whether you are considering Wi-Fi as a supplement or alternative to cable and DSL, using Bluetooth to network devices in your home or office, or want to use cellular data plans for anytime anywhere data access, this book will give you an indepth look at the wireless capabilities of Linux, and how to take advantage of them.



Mac OS X Unwired: A Guide for Home, Office, and the Road

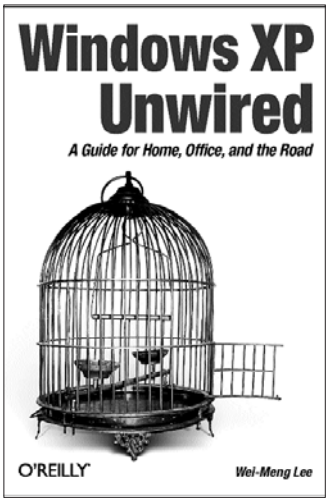
Authors: Tom Negrino, Dori Smith

Mac OS X Unwired is a one-stop wireless information source for technically savvy Mac users. If you are considering replacing your cable and DSL with wireless, or using wireless to network computers in your home, office, or on the road, this book will give you much needed insights into the wireless capabilities of Mac OS X, and how to best put it to use.



Windows XP Unwired: A Guide for Home, Office, and the Road

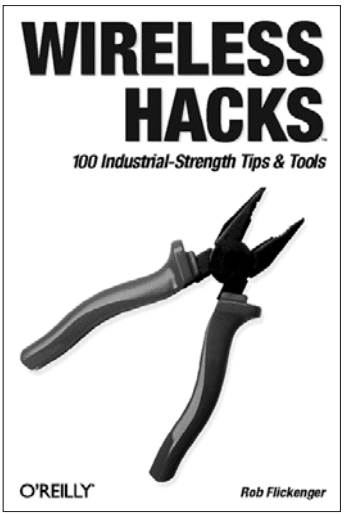
Author: Wei-Meng Lee



Windows XP Unwired provides a complete introduction to all the wireless technologies supported by Windows XP, including Wi-Fi (802.11b, a, and g), infra-red, Bluetooth, CDMA 2000, and GPRS. It's a one-stop wireless information source for technically savvy Windows XP users. This book will show you the full-spectrum view of wireless capabilities of Windows XP, and how to take advantage of them.

Wireless Hacks: 100 Industrial-Strength Tips & Tools

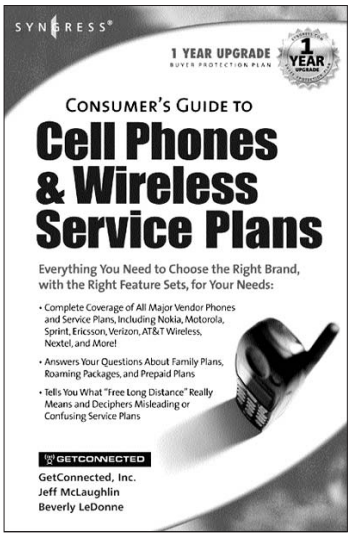
Author: Rob Flickenger



Written for the intermediate to advanced wireless user, the Wireless Hacks is full of direct, practical, ingenious solutions to real-world networking problems. Whether your wireless network needs to extend to the edge of your office, or even to the other end of town, this collection of non-obvious, practical techniques will show you how to get the job done.

Consumer's Guide to Cell Phones & Wireless Service

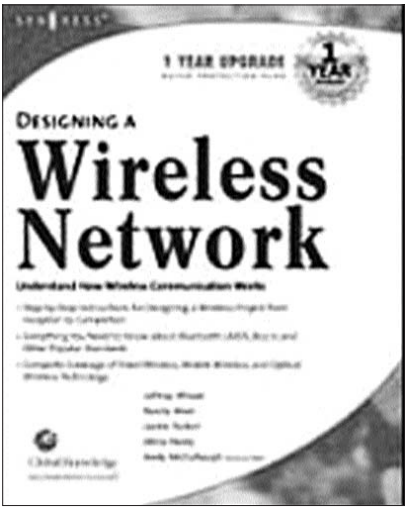
Authors: Jeff McLaughlin, WirelessAdvisor.com and Getconnected com



Consumers are spending between 50 and 500 per cent extra every month for services that keep them in touch, in tune, and informed. Why do people pay so much extra for long distance calls? The answer is simple; because there hasn't been a good way to determine the correct services based on the way you use your wireless phone. The Consumers Guide to Cell Phones & Wireless Service Plans will lead you through the maze of offerings based on how you should use your phone.

Designing a Wireless Network: Understand How Wireless Communication Works

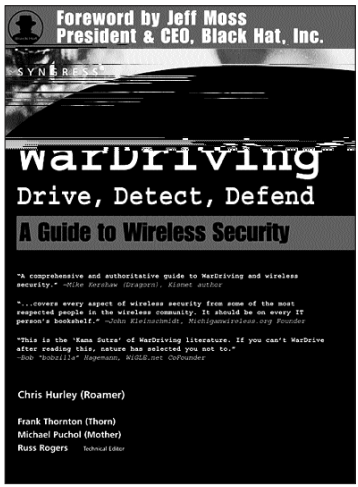
Author: Andy McCullough



Wireless network designs can be challenging to even the most experienced IT professionals, presenting unique obstacles. Your network requires the seamless and secure distribution of information, in spite of competing communication protocols, incompatible hardware platforms, and narrow bandwidths. This book is an introduction to developing efficient means of wireless transport in order to fully leverage your wireless solution.

WarDriving: Drive, Detect, Defend

Authors: Chris Hurley, Michael Puchol, Russ Rogers and Frank Thornton



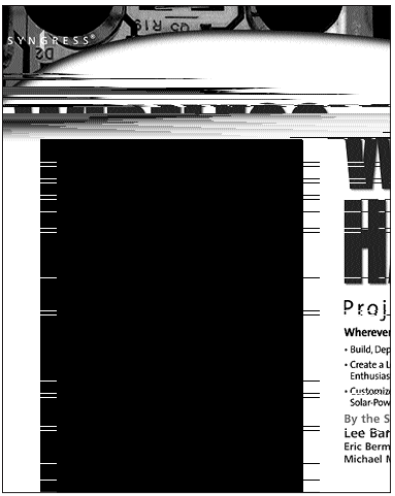
Wireless networks have become a way of life over the past two years. As more wireless networks are deployed, the need to secure them increases. This book educates users about wireless networks, and informs those who run the networks about the insecurities associated with WLANs.

In order to successfully WarDrive your own network to look for security, specific hardware and software tools are required. This book covers those tools, along with cost estimates and recommendations. Since there are hundreds of possible configurations that can be used for WarDriving, only some of the most popular ones are described to help readers decide what to buy for their own WarDriving setup.

Many of the tools that a WarDriver uses are the same tools that could be used by an attacker to gain unauthorised access to a wireless network. Since this is not the goal of a WarDriver, the methodology that users can use to ethically WarDrive is presented. In addition, complete coverage of WarDriving applications, such as NetStumbler, MiniStumbler; and Kismet, are covered.

Wireless Hacking

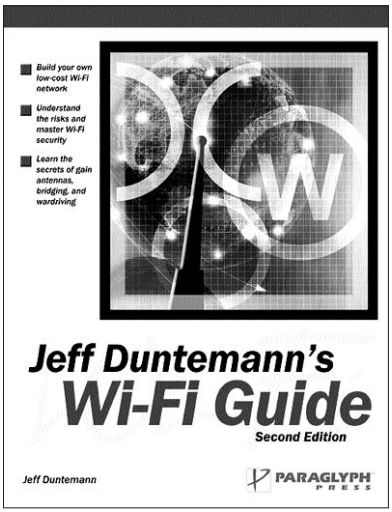
Authors: Lee Barken, Matt Fanady, Alan Koebrick, Michael Mee and Marc Palumbo; Foreword by Rob Flickenger



As the cost of wireless technology drops, the number of Wi-Fi users continues to grow. Millions of people have discovered the joy and delight of "cutting the cord." Many of those people are looking for ways to take the next step and try out some of the cutting edge techniques for building and deploying personalised Wi-Fi networks, both large and small. This book shows Wi-Fi enthusiasts and consumers how to do exactly that.

Jeff Duntemann's Wi-Fi Guide, Second Edition

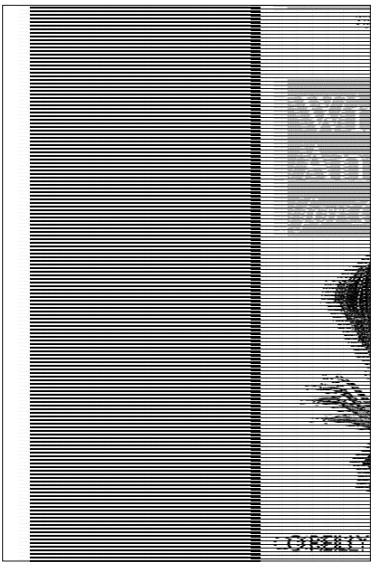
Author: Jeff Duntemann



This bestselling Wi-Fi guide provides everything Wi-Fi users need to design, build, protect, and extend Wi-Fi wireless networks! Jeff Duntemann provides practical techniques for setting up and using Wi-Fi gear and software. This second edition is expanded and brought fully up-to-date, covering more on setting up hotspots, community networking, security, Wireless Protected Access (WPA), new Wi-Fi standards (802.11g), and more.

Windows XP Annoyances for Geeks, 2nd Edition Tips, Secrets and Solutions

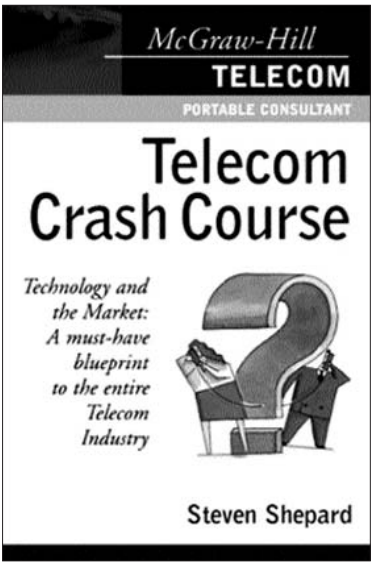
Author: David Karp



Offering dozens of on-target tips, workarounds, and warnings, Windows XP Annoyances for Geeks allows users to improve their overall experience with the popular XP operating system. And now, with this updated edition, users can also expect detailed coverage of the newly released Service Pack 2 (SP2) technology, which provides protection against viruses, hacker, and worms, and better support for wireless networking. It's the ultimate resource for the ever-expanding Windows XP market.

Telecom Crash Course

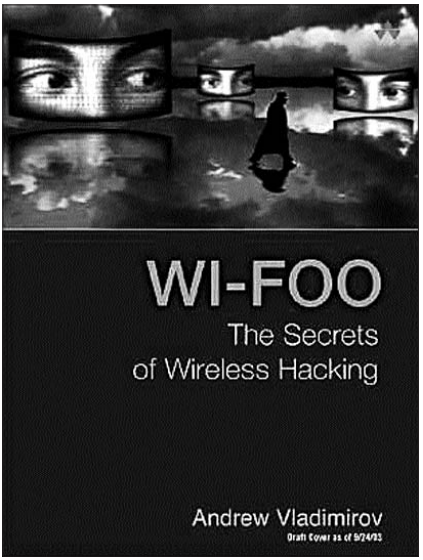
Author: Steven Shepard



Explore the vast telecom landscape, from standards and protocols to access and transport technologies. Far more than an acronym-studded quick fix, Telecom Crash Course is a true tutorial that offers you context, connections, and the wisdom to quickly grasp key technologies, including wireless Internet, optical networking, 3G, IP, protocol layer, PSTN, ATM, spread spectrum, GPRS, and SIP. Author Steven Shepard includes lively stories that deliver important points about the markets that drive the technologies. You get rigorous technical accuracy, with explanations of each technology's economic importance. Here's your chance to decipher the alphabet soup of telecom acronyms-not just what they stand for, but what they mean and how they can generate profits.

Wi-Foo

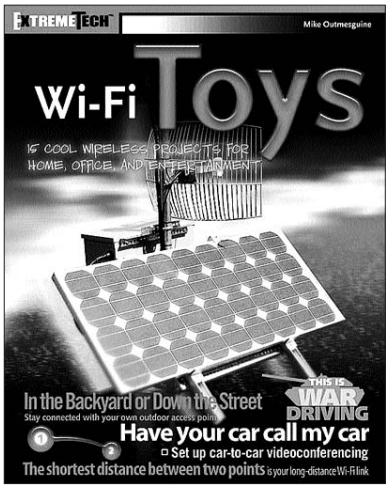
Authors: Andrew Vladimirov, Konstantin Gavrilenko and Andrei Mikhailovsky



There are plenty of wireless security books. This one's seriously hands-on. It was written by the leaders of one of the world's top wireless security auditing teams. Penetration testing is crucial to protecting yourself, and this book is the source for mastering it. But it doesn't just show you how to attack 802.11 networks, like many books do-it also shows your how to detect and defeat those attacks.

Wi-Fi Toys: 15 Cool Wireless Projects for Home, Office, and Entertainment (ExtremeTech Series)

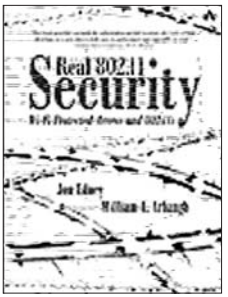
Author: Mike Outmesguine



Wireless is all about freedom, freedom from cables, cords, plugs, and limitations. So why be limited to readymade products? This book frees your imagination as it helps you create 15 exciting, individual projects using wireless technology. Each includes the necessary background, a list of materials, and step-by-step, illustrated instructions. Wardrive with Netstumbler and map your results. It's your freedom. Make the most of it.

Real 802.11 Security: Wi-Fi Protected Access and 802.11i

Authors: Jon Edney, William Arbaugh

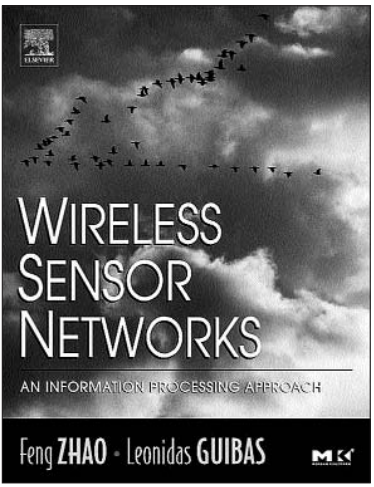


Real 802.11 Security addresses the theory, implementations, and reality concerning Wi-Fi Security. The first two sections introduce you to security issues in general, and how security works in Wi-Fi networks, delving into the various security protocols. In the third section of the book, practical real world issues and examples of attack tools are discussed.

This book describes new approaches to wireless LAN security, showing you how these approaches work and how they give maximum effect. They show you how to establish real security within your Wi-Fi LAN. Here is a book that provides you with an informed solution to your security dilemma.

Wireless Sensor Networks: An Information Processing Approach

Authors: Feng Zhao and Leonidas Guibas



Information processing in sensor networks is a rapidly emerging area of computer science and electrical engineering research. Because of advances in micro-sensors, wireless networking and embedded processing, ad hoc networks of sensors are becoming increasingly available for commercial, military, and homeland security applications. Examples include monitoring (e.g., traffic, habitat, security), industrail sensing and diagnostics (e.g., factory, appliances), infrastructures (i.e., power grid, water distribution, waste disposal) and battle awareness (e.g., multi-target tracking).

This book introduces practitioners to the fundamental issues and technology constraints concerning various aspects of sensor networks such as information organisation, querying, routing, and self-organisation using concrete examples and does so by using concrete examples from current research and implementation efforts.

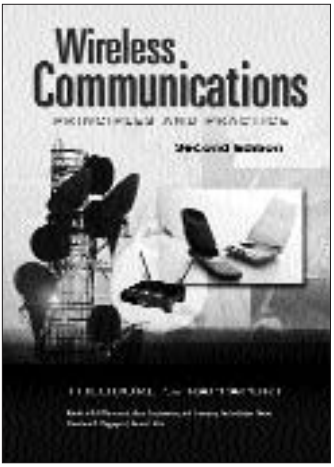
Complete Wireless Home Networking, Windows XP Edition

Author: Paul Heltzel

This guide offers advice on determining equipment needs and then provides instructions for each step of building a wireless network-installation, set-up, configuration, and troubleshooting. The explanations assume no previous experience with networking.

Wireless Communications: Principles and Practice

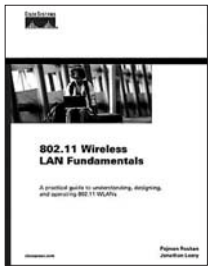
Author: Theodore Rappaport



Offering a wealth of practical information on the implementation realities of wireless communications, this book also contains up-to-date information on the major wireless communication standards from around the world. It covers every fundamental aspect of wireless communications, from cellular system design to networking, and even the world-wide standards.

802.11 Wireless LAN Fundamentals

Authors: Pejman Roahan and Jonathan Leary



802.11 Wireless LAN Fundamentals gives you the background and practical details you need to select, design, install, and run your own WLAN. This book begins with an overview of Ethernet technologies, 802.11 standards, and physical layer technologies, providing you with a frame of reference for the rest of the book. Subsequent chapters address challenges and solutions associated with security, mobility, and QoS. Radio frequency fundamentals are reviewed in detail, as are site-surveying methods. A series of case studies that highlight WLAN design considerations in various business environments helps place all the concepts covered in this book in the context of real-world applications.

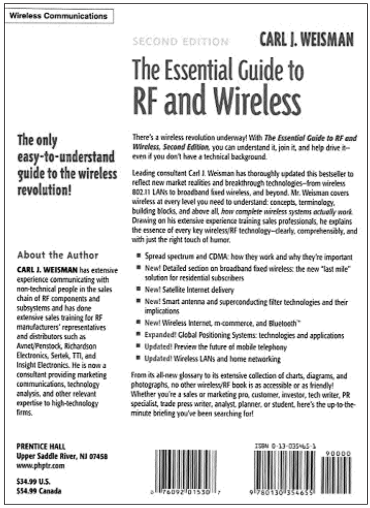
How Wireless Works

Author: Preston Gralla

How Wireless Works continues in the How It Works series tradition by explaining every aspect of wireless communications, from the remote control on your coffee table to the most sophisticated wireless Internet networks. As wireless technology proliferates, readers need to understand how wireless technologies work in order to make educated buying and business decisions related to wireless technologies. This book provides readers with a basic technical background on wireless technologies, including infrared, radio-frequency, power line, and PNA (wireless home networking.) The book explains the strengths and weaknesses of each technology, so you will understand which technology is best suited to a particular application. Where appropriate, it explains the differences between competing industry standards, so you can make an informed buying decision.

The Essential Guide to RF and Wireless

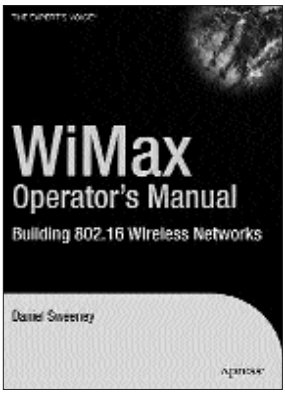
Author: Carl Weisman



This bestseller reflects new market realities and breakthrough technologies-from wireless 802.11 LANs to broadband fixed wireless, and beyond. The author covers wireless at every level you need to understand: concepts, terminology, building blocks, and above all, how complete wireless systems actually work. Drawing on his extensive experience training sales professionals, he explains the essence of every key wireless/RF technology-clearly, comprehensibly, and with just the right touch of humour. From its all-new glossary to its extensive collection of charts, diagrams, and photographs, no other wireless/RF book is as accessible or as friendly! Whether you're a sales or marketing pro, customer, investor, tech writer, PR specialist, trade press writer, analyst, planner, or student, here's the up-to-the-minute briefing you've been searching for!

WiMax Operator's Manual: Building 802.16 Wireless Networks

Author: Daniel Sweeney

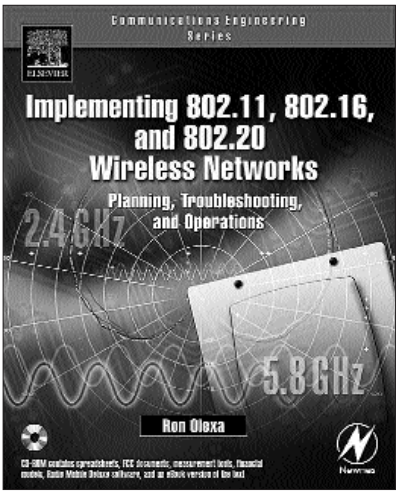


This book is aimed at someone making primary decisions as to the design and implementation of an 802.16 based wireless public network. This is a manual on how to architect and operate a service network offering broadband wireless last-mile access. The scope of the treatment includes all layers of the network and issues of management and administration. This operational handbook covers both the planning and construction, and the day to day operation, of a standards-based broadband wireless network. It explains the advantages of broadband wireless and where it constitutes a best solution, and it also discusses the unique difficulties, challenges, and limitations of broadband wireless.

It does not attempt to summarise all knowledge relating to digital radio services or public packet networks, but provides essentials for planning and running the networks and indicates what kinds of specialised services should be secured to ensure the success of the undertaking.

Implementing 802.11, 802.16, and 802.20 Wireless Networks: Planning, Troubleshooting, and Operations

Author: Ron Olexa



This is not another book about installing a home or "hobby" Wi-Fi system. Instead, this book shows you how to plan, design, install, and operate WLAN systems in businesses, institutions, and public settings such as libraries and hotels. This book is packed with serious information for serious professionals responsible for implementing robust, high performance WLANs covering areas as small as a coffee shop or as large as entire communities.

Ron Olexa provides a solid foundation in RF/wireless theory as it applies to WLANs. His detailed, thorough coverage of propagation at GHz frequencies helps you understand the mysteries of WLAN coverage (such as how it can change from season to season due to foliage). You'll also learn about antenna radiation patterns and gain so you can design your WLAN to have the coverage you need without causing interference to (or suffering interference from) other WLANs.

Wireless Communications & Networks

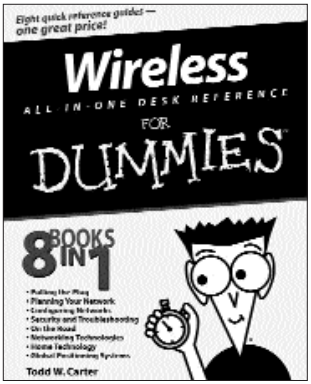
Author: William Stallings

William Stallings gives an up-to-date coverage of both wireless communications and wireless networks with new expanded coverage of Wi-Fi and WiMax. Designed for students and professionals, this text explores the key networking topics with a unique approach covering: technology and architecture, network design approaches, and types of networks and applications.

Wireless All-in-One Desk Reference for Dummies

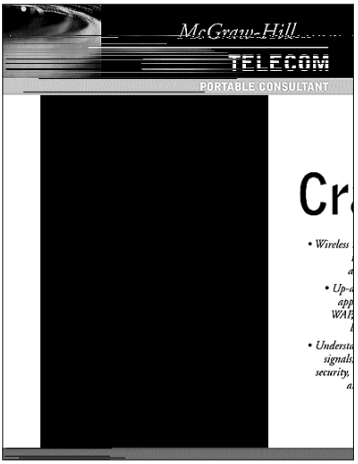
Author: Todd W. Carter

This definitive guide includes nine self-contained mini-books that show how to set up, configure, use, and maintain a wireless network for small offices and homes without the hassle of stringing cable or paying a network administrator.



Wireless Crash Course

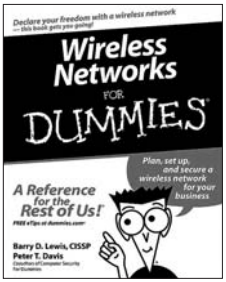
Author: Paul Bedell



Need a jargon-free explanation of how wireless telecommunications work, with an emphasis on the design and management of systems? You will find it in Paul Bedell's Wireless Crash Course. This guide provides everything you need to understand the basic working of wireless, its technology and markets. You get a crystal-clear introduction to basic concepts like radio frequency (RF), cell sites, and switching, and insight into issues such as site acquisition, tower selection and construction, design of the fixed network, and interconnection to the Public Switched Telephone Network. The author carefully delineates the complex regulatory processes that affect all wireless service providers. This A to Z treatment of every major feature of wireless explains both wireless Internet access (WAP, Bluetooth, wireless data, etc.) and wireless broadband access (LMDS, MMDS) and their prospects in the marketplace.

Wireless Networks for Dummies

Authors: Peter T. Davis, Barry Lewis and Barry D. Lewis



At last! Liberation from that office full of electronic spaghetti is only a few pages away! This fun and friendly guide shows you how to plan and set up a wireless network for your business, install users, provide security, and keep your network healthy. Explore sites, enable roaming, dodge war drivers, and celebrate your freedom!

Wireless Networks: First-Step

Author: Jim Geier

Wireless technology has the power to transform voice and data communication as we know it today. From cell phones and wireless laptops, to home wireless networks and outdoor wireless solutions, there's an exciting, new, and invisible world to discover.

Wireless Networks First-Step explains the basics of wireless networks in easy-to-grasp language that all of us can understand. This book takes you on a guided tour of the key concepts behind wireless communications. Whether you are looking to take your first step into a career in wireless networking, assessing the wireless options for your business, planning to install a wireless system at home, or are interested in gaining a conversational knowledge of the technology, this book is for you!

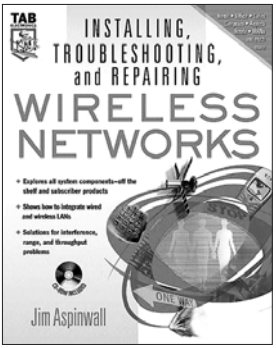
Absolute Beginner's Guide to Wi-Fi

Author: Harold Davis

Absolute Beginner's Guide to Wi-Fi Wireless Networking teaches you how to quickly get up to speed so you can surf at local hotspots, or while on the road. This book gives you the practical information you need to buy the right equipment, get your equipment working perfectly, and get the best deal with Wi-Fi providers. You will also learn how to set up a Wi-Fi network, avoid pitfalls, and save time and money so that you can easily set up a wireless network in your home or office. Rid yourself forever of that nasty mess of tangled wires running everywhere!

Installing, Troubleshooting, and Repairing Wireless Networks

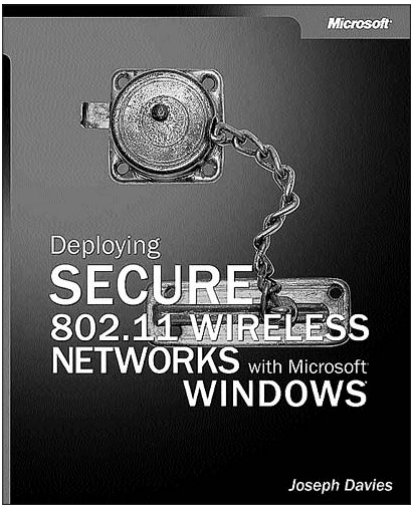
Author: Jim Aspinwall



With annual equipment sales projected to grow to more than $5 billion this year, wireless networking is clearly a technology whose time has come. But with many wireless networks expected to be created at both small offices and home offices, where can people charged with maintaining them get comprehensive information to help them do just that? The answer is McGraw-Hill's Installing, Troubleshooting, and Repairing Wireless Networks. Basic enough for the hobbyist-and yet still detailed enough for the IT professional. This book is the essential survival guide for keeping a wireless network up and running.

Deploying Secure 802.11 Wireless Networks with Microsoft Windows

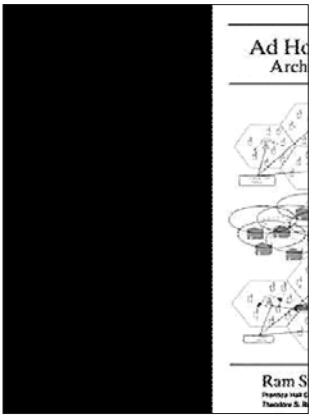
Author: Joseph Davies



Get in-depth technical guidance to help maximise security for wireless networking infrastructures for computers running Windows XP, Windows Server 2003, or Windows 2000. The book thoroughly details how to implement IEEE 802.11b wireless LAN networking, and its related authentication technologies for a Windows environment. You'll learn how to deploy solutions for corporate networks, public networks, and home/small business networks that employ the latest standards in wireless security technologies including Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), Protected EAP with Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2) and Wi-Fi Protected Access (WPA). The book also includes a detailed case study of wireless network deployment at Microsoft-sharing Windows-specific best practices from one of the largest wireless LAN deployments in the world.

Ad Hoc Wireless Networks: Architectures and Protocols

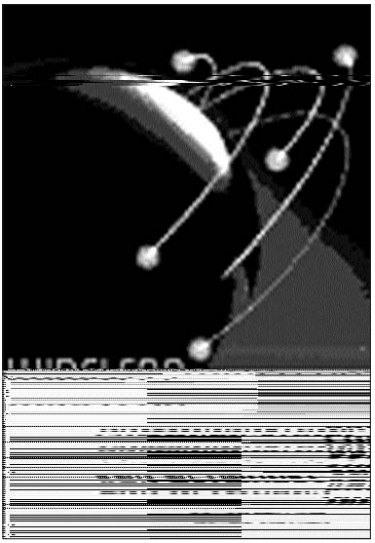
Authors: C. Siva Ram Murthy and B.S. Manoj



Ad Hoc Wireless Networks comprise mobile devices that use wireless transmission for communication. They can be set up anywhere and any time because they eliminate the complexities of infrastructure setup and central administration-and they have enormous commercial and military potential. Now, there's a book that addresses every major issue related to their design and performance. Ad Hoc Wireless Networks: Architectures and Protocols presents state-of-the-art techniques and solutions, and supports them with easy-to-understand examples. The book starts off with the fundamentals of wireless networking (wireless PANs, LANs, MANs, WANs, and wireless Internet) and goes on to address such current topics as Wi-Fi networks, optical wireless networks, and hybrid wireless architectures.

Wireless Communications and Networks

Author: William Stallings



This comprehensive, well-organised text covers wireless communication and networks, and the rapidly growing associated technologies-the most exciting areas in the overall communications field. It explores the key topics in the following general categories: technology and architecture, network type, design approaches, and applications. An emphasis on specific wireless standards reflects the importance of such standards in defining the available products and future research directions in this field.

The Wireless Networking Starter Kit

Authors: Engst Adam and Glenn Fleishman

Using illustrated step-by-step instructions, in-depth discussions, and tons of tips, they help you decide what to buy, show you how to configure wireless hardware and software, and explain the best techniques for managing your connections. Whether you're a novice or an experienced network administrator, you'll find the practical information you need about wireless networking.

The Book of WI-FI: Install, Configure, and Use 802.11b Wireless Networking

Author: John Ross

Introduces the 802.11b networking standard used by most wireless LANs, and offers advice on selecting the network adapters, base stations, and antennas needed to install a wireless network. The guide also addresses how to configure wireless connections for Windows, Macintosh, Linux, Unix, and PDAs, and how to protect wireless access points from unwanted intruders.

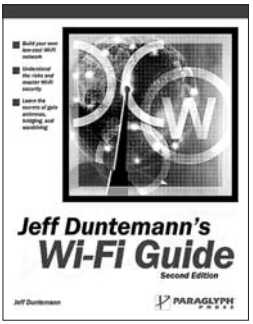
Build Your Own Wi-Fi Network

Authors: Shelly Brisbin and Glen Carty

Take advantage of the freedom and mobility of wireless networking with help from this easy-to-follow guide. Now you can surf the Web from the backyard, access your e-mail from a handheld device, share Internet connections, and save money, without messy wires or cables. This step-by-step photo-filled manual walks you through every stage of the process-from identifying and purchasing all the parts you need to get started to finding the right ISP and enhancing security. You'll also learn how to improve network performance and range by choosing the optimum access point location. Written in clear, straightforward language, this book will show you how to set up and maintain your own wireless network in no time.

Jeff Duntemann's Complete Wi-Fi Guide

Author: Jeff Duntemann



This practical guide explains wireless Ethernet (Wi-Fi) hardware for connecting computers without wires, sharing an Internet connection among family members, and sharing printers within a small office. The author offer advice on building a wireless network, installing client adapters, and choosing an antenna. The second edition adds a chapter on Wi-Fi protected access (WPA) technology.