Wireless Networking

Expert knowledge means success

Contents

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

Introduction

Wireless networking refers to the technology that enables multiple computers to communicate without data cabling. It offers an affordable, tidy and flexible solution to the requirement to network multiple systems.

Wireless networks are not just for laptop users. The emergence of wireless standards and reducing hardware and software costs has allowed the technology to be brought to a broader marketplace. Wireless solutions are now used widely in business, schools and homes as well as in more complex situations such as warehousing or point-of-sale handheld equipment.

Why Wireless?

A wireless network can work on its own or can be used to allow an existing network to grow without the need to run extra data cabling. Today's typical network may have an existing wired network, with an Internet connection and additional wireless clients. In this scenario, all the wired and wireless clients can be configured to communicate with both the Internet and other PCs, and with laptops or PDAs in the network.

Resource Sharing

The explosion of the Internet has created a new demand for computers to be networked to allow Internet connections to be shared. Similarly, as the use of IT by businesses has grown, so the demands for file and printer sharing have grown. These demands could be serviced by a wired network. However, in many cases the demand has developed since an original wired network was created, and an easier solution can be to add in a wireless component to the existing network.

Difficult Building Layouts

Wireless networks are particularly useful where unsuitable building layouts make it difficult to build a wired network. Schools are an obvious example of multiple buildings without inter-connecting data cabling that have a need to access shared data.

Temporary Networks

Where a temporary LAN is required, for example for an exhibition, or pilot IT development project, a wireless network can be created quickly and simply without the need for permanent cabling.

Mobile Workforce

Mobile staff operating from laptop computers have also helped to fuel the demand for wireless networking. These staff can operate from any desk at any office where the network is configured to accept their laptop as a network client.

Home Use

In the UK, more than 3.1 million people now work from home, and the number of households with multiple PCs for work, home and educational use is rising. Homeowners can create a wireless network to share printer and Internet access without running extra cabling around their home.

In the US, estimates suggest that over fifty million U.S. workers (about 40% of the working population) could work from home at least part of the time - yet in 2008, only 2.5 million employees (not including the self-employed) considered their home their primary place of business. Occasional telecommuters— those who work remotely (though not necessarily at home) —totalled 17.2 million in 2008.[1]

Wireless Standards

Wireless networking uses the 802.11 Radio Frequency Wireless Networking standard as produced by the Institute of Electrical and Electronic Engineers (IEEE). The various "flavours" of this standard currently in use include 802.11b. 802.11a and 802.11g. The most common of these is the 802.11b.

Wireless Equipment

All equipment used in a wireless network must adhere to the same network standard.

The following products will be required:

- all laptop wireless network clients will require a wireless PCMCIA (now rarely provided) or USB based network card, or have an inbuilt wireless capability e.g. Intel Centrino;
- all desktop wireless network clients will require a USB based network card or an internal PCI wireless network card; and
- an access point to connect the wireless clients to the network.

Access Points

Wireless networks can be used to link network clients to an access point which functions as a hub for all the systems connected to it. Alternatively, they can link systems in a peer-to-peer fashion without an access point. It is more common and more secure to connect using an access point, and it is this option that we will be addressing in this publication.

An access point allows the wireless network clients to access the network. There is a wide choice of access points available depending on the network solution required. An access point must support the same wireless network standard used by the network cards in the clients. Some access points support multiple standards.

Access points may be dedicated hardware access points or may be software access points that run on a computer with a wireless network card installed. Software access points offer greater flexibility in access to different network types and in the number of connections available. They often include additional features such as web caching and content filtering.

Some access points are designed for "wireless only" networks; others include Ethernet switch ports to allow wired clients to be connected to the network. They may also include firewall and broadband router functions.

The number of client connections is limited by the access point chosen. Multiple access points (extension points) can be used to increase the number of client connections or extend the operating range of a network. Extension points are not defined in the wireless standard, and advice should be sought when considering their use.

Siting an Access Point

The key points to remember when siting an access point for optimum performance are:

- network clients should be as close as practical to the access point;
- network clients should be in line of sight of the access point wherever possible; and
- there should be no other equipment operating within the same frequency band.

Adherence to these points would provide the ideal environment for a wireless network. The practical reality is often different. One of the benefits of a wireless network is the ability to use a client in different locations which may be out of line of sight, some distance away from the access point.

Range

An access point should be sited centrally to all wireless network clients. The further a client is from the access point, the weaker the signal strength will be. Typical indoor ranges are quoted as 100 to 150 feet where there is line of sight between an access point and a network client.

Some manufacturers provide external aerials to boost signal strength where required.

Interference

Equipment that works at high frequencies is susceptible to interference. Wireless networks operate in the 2.4GHz spectrum, along with cordless phones and wireless speaker systems. Consequently, all these systems may interfere with each other. For example, answering a cordless phone next to a PC could cause the PC to lose connectivity with the access point.

Obstacles

The higher a network frequency, the more any obstacles will affect its range. Solid walls and ceilings will greatly impede radio transmissions. Siting an access point as high as possible will maximise the performance available.

Wireless Connectivity - IP Addressing

Modern networks are based on the TCP/IP protocol. All devices on a TCP/IP network must have an IP address, an identifier unique to that network. The wireless network uses the IP address to determine which system a user wishes to access.

Internet addressing

A network requires a router of some form to allow it to connect to the Internet. This may be discrete hardware or software or may be integrated into another device, for example a hardware access point. A router will have two IP addresses: a local LAN address that is used locally by the other systems in the network and a separate Internet IP address that needs to be unique on the Internet.

Security

Wireless networks expose systems to additional security risks not associated with wired networks. Unwelcome users, equipped with a wireless PC and PDA can potentially connect with a wireless network and bypass any firewall software installed. Using a properly secured access point rather than peer-to-peer wireless networking provides greater security.

The following steps should be considered as part of any wireless network security plan.

Changing default settings

Access points come with default settings and it is up to the user to change the settings to implement their own security. Any default passwords should be changed and recorded securely.

Disabling DHCP

The Dynamic Host Configuration Protocol (DHCP) function of an access point is used in allocating IP addresses to any requesting client. This in itself can be a security risk. If security is an important issue, it may be better to disable the DHCP and manually configure IP addresses instead. Keep a record of the IP addresses you assign as duplicate addresses can cause your network to fail.

Disabling SSID broadcast

An access point will broadcast its Service Set identifier (SSID) to all clients within range. Again, it may be better to disable the SSID broadcast and manually configure each wireless client with the SSID name. An obscure SSID name should be chosen, so that it cannot be easily guessed. Be aware that the SSID is embedded in every data packet header unencrypted and can therefore be easily read by a determined hacker.

Enabling MAC address filtering

Each network card has a unique code called a Media Access Control (MAC) address, which is assigned by the IEEE and is guaranteed to be unique for every network device in the world. If MAC address filtering is enabled, only clients with a MAC address configured on the access point will be able to access the network. However, MAC addresses can be manipulated in software, and cloning facilities do exist for legitimate uses.

Implementing encryption

Most access points and wireless network cards support the Wired Equivalent Privacy (WEP) standard which can be used to encrypt wireless traffic before transmission. However, WEP is not fully secure. An alternative is to purchase equipment that supports the emerging Wi-fi Protected Access (WPA) encryption standard. Application level encryption such as Windows NTFS could also be used to add security to data transmissions.

Wireless Security – The Reality

Survey results announced by RSA Security in January 2004 found that 66% of the networks surveyed use the encryption system built-in to the wi-fi standard to help them prevent unauthorised access. Many are more secure than last year too and have the basic Wired Equivalent Privacy (WEP) system turned on. This scrambles signals to make it harder to use a wi-fi network without permission. It found that many other networks are protected with other techniques that stop people outside a business using the net or getting access to internal networks.

But, despite the good news, RSA said that many firms were still not doing the basics to ensure that they were protected. About a quarter of the networks surveyed, almost 300 wi-fi access points, were poorly protected

Findings from a Survey by RSA Security January 2004

Configuring the Network

Configuring a wireless network can be complex. It is a job best left to a professional IT Services Company.

Configuring the Access Point

Different manufacturers have different configuration methods for their access points, with some using wizards. A new password and Service Set identifier (SSID) should be configured for security reasons. The same SSID must be referenced from the network cards to enable the cards to communicate with the access point.

If the access point includes broadband router functionality, the ISP settings should be configured.

Configuring the Wireless Network Cards

Today, wireless network cards should come with software drivers and configuration utilities that must be installed on all clients running current versions of Windows. The latest versions of Windows have built-in support for wireless networking that allows it to “discover” available wireless networks without the need for installing additional client software.

An IP address (in the range specified for the access point) must be configured for each network client.

Configuring the Network

Once all the wireless network clients can communicate with the access point, the IP addressing strategy for the network as a whole needs to be determined.

The easiest method is to configure one system as a Dynamic Host Configuration Protocol (DHCP) server and all other systems to obtain an IP address automatically. The DHCP server will then allocate IP address, subnet mask, default gateway and DNS server information to all the network clients.

Network client IP addressing

Configuring the clients is achieved by setting the option “obtain an IP address automatically” from the Properties section of Internet Protocol (TCP/IP) on the Properties section of the wireless network card.

DHCP server

There are often a number of options to choose from when selecting a suitable system to act as a DHCP server. Care must be taken to avoid IP addressing conflicts.

The access point could be used as the DHCP server, where the range of IP addresses is suitable for your network. However, the automatic assignment of IP addresses by the DHCP function can pose a security risk. It may be better to disable the DHCP function of the access point where an alternative method of assigning addresses is available. If DHCP is enabled, ensure that other security measures are in place.

If you have Internet Connection Sharing (ICS) on your network, the system running ICS will be automatically configured as a DHCP server. In this case, the DHCP server cannot be disabled, but it does not have to be used. Network clients can be manually configured to access the Internet via the ICS system.

However, the IP addressing is implemented, addressing conflicts may occur if multiple DHCP servers are running on the same network.

Configuring File and Printer Sharing

Windows XP and 2000 automatically support file and printer sharing. On Windows 98 and ME systems, it will be necessary to install and enable “File and Printer Sharing” on the systems hosting the data, and to install “Client for Microsoft Networks” on the systems wishing to access the data.

Wireless Networking Tips

- Future-proof your wireless network by buying 802.11g products. These offer a real-world data throughput of around 22Mbps (54Mbps theoretical) compared to around 6Mbps (11Mbps theoretical) for 802.11b.
- Improve security by using Wi-Fi Protected Access (WPA0 encryption instead of the flawed Wired Equivalency Protocol (WEP). WPA is used on new Wi-Fi equipment, but recent purchases can often be upgraded by downloading new driver software.
- Make sure you also upgrade Windows to support WPA. Search for article 815485 at http://support.microsoft.com for an overview and download the WPA Client using article 826942.
- Careful placement of wireless access points can dramatically improve the signal and connection speed. The worst reception is directly below one – in the basement of a house, for example. Keep the access point in clear sight if possible and not hidden behind other objects.
- Protect your data in a public hotspot by preventing people connecting to your laptop. Go to the Windows XP Control Panel and click on Network Connections. From here you can disable ‘peer-to-peer’ mode.

Source: PC Pro, August 2004

Improving the performance of your wireless network

1. Position your wireless router (or wireless access point) in a central location.

When possible, place your wireless router in a central location in your home. If your wireless router is against an outside wall of your home, the signal will be weak on the other side of your home. Don't worry if you can't move your wireless router, because there are many other ways to improve your connection.

2. Move the router off the floor and away from walls and metal objects (such as metal file cabinets). Metal, walls, and floors will interfere with your router's wireless signals. The closer your router is to these obstructions, the more severe the interference, and the weaker your connection will be.

3. Replace your router's antenna.

The antennas supplied with your router are designed to be omni-directional, meaning they broadcast in all directions around the router. If your router is near an outside wall, half of the wireless signals will be sent outside your home, and much of your router's power will be wasted. Most routers don't allow you to increase the power output, but you can make better use of the power. Upgrade to a hi-gain antenna that focuses the wireless signals only one direction. You can aim the signal in the direction you need it most.

4. Replace your computer's wireless network adapter.

Wireless network signals must be sent both to and from your computer. Sometimes, your router can broadcast strongly enough to reach your computer, but your computer can't send signals back to your router. To improve this, replace your laptop's PC card-based wireless network adapter with a USB network adapter that uses an external antenna. Laptops with built-in wireless typically have excellent antennas and don't need to have their network adapters upgraded.

5.Add a wireless repeater.

Wireless repeaters extend your wireless network range without requiring you to add any wiring. Just place the wireless repeater halfway between your wireless access point and your computer, and you'll get an instant boost to your wireless signal strength.

6. Change your wireless channel.

Wireless routers can broadcast on several different channels, similar to the way radio stations use different channels. Just like you'll sometimes hear interference on one radio station while another is perfectly clear, sometimes one wireless channel is clearer than others. Try changing your wireless router's channel through your router's configuration page to see if your signal strength improves. You don't need to change your computer's configuration, because it'll automatically detect the new channel.

7. Reduce wireless interference.

If you have cordless phones or other wireless electronics in your home, your computer might not be able to "hear" your router over the noise from the other wireless devices. To quiet the noise, avoid wireless electronics that use the 2.4GHz frequency. Instead, look for cordless phones that use the 5.8GHz or 900MHz frequencies.

8. Update your firmware or your network adapter driver.

Router and network adaptor manufacturers regularly make free improvements to their products. Sometimes, these improvements increase performance. To get the latest firmware updates for your router or network adapter visit the manufacturer's Web site.

9. Pick equipment from a single vendor.

You often get better performance if you pick a router and network adapter from the same vendor. Some vendors offer a performance boost of up to twice the performance when you choose their hardware: e.g. Linksys has the SpeedBooster technology, and D-Link has the 108G enhancement.

10. Upgrade 802.11b devices to 802.11g.

802.11b is the most common type of wireless network, but 802.11g is about five times faster. 802.11g is backward-compatible with 802.11b, so you can still use any 802.11b equipment that you have. If you're using 802.11b and you're unhappy with the performance, consider replacing your router and network adapters with 802.11g-compatible equipment.

Source: Microsoft

Wi-Fi Hotspots

Wi-Fi Hotspots are generally used in public places to allow a wireless enabled device such as a laptop to access the internet and use e-mail. According to BroadGroup research, the UK is the most wireless enabled country in Europe.

Wi-Fi hotspots offer a range of access packages aimed at both business and personal users. The hotspot will be automatically detected by a wireless enabled device after which a consumer can select to subscribe for a defined period of time, at a typical cost of £3 to £5 an hour. In many locations, such as in Starbucks, access is free.

BT Openzone provides wireless at over 3,000 locations for £5 a month (plus VAT).

T-Mobile hotspots are widely available across the US – see: https://content.hotspot.t-mobile.com/AssetProcess.asp?asset=com.default.main.001

If a Wi-Fi hotspot is not available, a 3G data card can be used in a laptop to connect through the 3G phone network to the internet.

VoWiFi – Using Phones over Wireless Networks

Mobile phones and the Internet have changed our way of life and now, with current technology — mobile phones that use wireless broadband (VoWiFi) to access the internet and make voice calls over it — a further quantum leap in how we do things and communicate with others is set to happen.

These mobiles, using voice-over- internet protocol can bypass the telcos' dedicated voice switching systems if the person they are calling is on a similar system. The bandwidth requirements of Voice-over-IP are negligible compared to the average throughput on a commercial WiFi network. If you have serious phone bills, a need for international voice communication while on the road, and the willingness to experiment, voice over WiFi might be for just right for you.

For example, you will be able to talk to your contacts over the internet without having to pick up a receiver and dial. The only pre-requisite will be a Voice-over-IP enabled router.

It has been predicted that voice will be the killer application of WiFi networks.

A word about Bluetooth

Bluetooth is a specification designed for the use of low-power radio communications. It supports simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, mice, printers, keyboards and wireless headsets over short distances, typically up to 10 metres. Higher ranges can be supported with higher specification equipment. As with Wireless Networking, it has both security and interoperability issues.

Bluetooth is much slower than Wireless Networking - typically up to 1Mbps - is more limited in range and supports many fewer devices. Its slow speed makes it unsuitable as the technology for an entire wireless office, but it can be useful for connecting PDAs or laptops to a network. It can also be used to connect a laptop, mouse, mobile phone and printer to create a Wireless Personal Area Network.

Recommended Reading

- Wireless Home Networking for Dummies by W. Bruce, published by John Wiley & Sons Inc, ISBN: 0764539108;
- The Wireless Networking Starter Kit by Adam Engst and Glenn Fleishman, published by Peachpit Press, ISBN: 0321174089;
- Wireless Networking Made Easy: Everything You Need to Know to Build Your Own Pans, Lans, and Wans by Russell Shaw, published by AMACOM, ISBN: 0814471757;
- Absolute Beginner's Guide to Wi-Fi Wireless Networking by Harold Davis, published by Que, ISBN: 0789731150;

- Complete Wireless Home Networking by Paul Heltzel, published by Prentice Hall PTR, ISBN: 0131461532;
- Deploying Secure 802.11 Wireless Networks with Microsoft Windows by Joseph Davies, published by Microsoft Press, ISBN: 0735619395;
- Wireless Local-area Network Fundamentals by Pejman Roshan and Jonathan Leary, published by Cisco Press, ISBN: 1587050773;

Product Manufacturers

The following manufacturers provide products in all of the four 802.11g ranges: Short-Range, Short-Range Centrino, Medium-Range and Long Range:

U.S. Robotics: www.usr.com
Asus: www.asus.com
D-Link: www.dlink.com
Belkin: www.belkin.com/
Linksys: http://home.cisco.com/en-eu/home?referrer=www.linksysbycisco.com

Wireless Industry Associations

- CTIA - Cellular Telecommunications Industry Association www.ctia.org
- GSM Association - Responsible for the development, deployment and evolution of the Global System for Mobile Communication (GSM) standard for digital wireless communications and for the promotion of the GSM platform. www.gsma.com/home/
- PCIA - Personal Communications Industry Association www.pcia.com
- Wireless Networks Online - A source for professionals in the wireless communications industry, providing information on wireless infrastructure, test equipment, mobile switching center, bluetooth, satellite communications and more. www.wirelessnetworksonline.com
- International Telecommunications Union - The ITU is an international organization which coordinates global telecom networks and services. www.itu.int
- WiFi Alliance - Their mission is to certify interoperability of Wi-Fi (IEEE 802.11) products and to promote Wi-Fi as the global wireless LAN standard across all market segments. www.wirelessethernet.org www.wi-fi.org
- WLANA Wireless LAN Association www.wirelesspedia.com/show/company/Wireless_LAN_Association/68.html

Glossary of Wireless Terms

- Asymmetric Digital Subscriber Line (ADSL): A common method of accessing the Internet using digital signals over phone lines.
- Access Point (AP): An access point connects the wireless network clients to a wired network. It transmits and receives WLAN radio signals. Access points may be dedicated hardware access points or maybe software access points that run on a computer with a wireless network card installed. They may incorporate a router or other facilities.
- Bluetooth: A short-range wireless protocol that provides 1Mbps data transfer rates at a range up to 10 metres. Typically used for mobile phones and PDAs.
- Broadband: High speed Internet access, typically up to 10-50 times faster than a dial-up connection.
- Centrino: Intel PC processor incorporating wireless facilities.
- Dynamic Host Configuration Protocol (DHCP): The DHCP function automatically allocates IP addresses to any requesting client.
- Encryption: The conversion of data into another form so that it must be decoded by a decryption device.
- Firewall: Hardware or software that prevents unauthorised access to a network from an external source.
- Hotspot: A location that offers wireless Internet access.
- IP Address: All devices on a TCP/IP network must have an IP address: an identifier unique to that network. The wireless network uses the IP address to determine which device a user wishes to access.
- Local Area Network (LAN): A group of local devices connected together in a network.
- Media Access Control (MAC): A MAC address is a unique identifier, which is assigned by the IEEE and is guaranteed to be unique for every network device in the world.

- **Network Address Translation (NAT):** A method of maintaining a set of IP addresses for internal use and another set for external use, for security purposes.
- **Peripheral Component Interconnect card (PCI):** A network card for a desktop PC.
- **Personal Computer Memory Card International Association card (PCMCIA):** A network card for a laptop.
- **Router:** A hardware or software device that routes data according to its address. It may incorporate security features.
- **Service Set Identifier (SSID):** A unique identifier for a wireless network. All wireless devices on the network must use the same SSID.
- **Transmission Control Protocol/Internet Protocol (TCP/IP):** An industry standard protocol used for sending data over the Internet.
- **Wardriving:** This refers to the identifying of unsecured wireless networks, originally conducted by attempting to access a network from within its connectivity range (albeit outside a building).
- **Wired Equivalent Privacy (WEP):** Currently the most common encryption protocol used for secure transactions on the web. It scrambles wireless network traffic, uses a shared, secret key and 128-bit encryption. It is not fully secure and is gradually being replaced by WPA.
- **Whitecap:** A similar technology to 802.11b, with the improved quality of service needed for streaming multimedia. Whitecap 2 is expected to be compatible with the 802.11 protocols.
- **Wireless Fidelity (Wi-Fi):** A term referring to the group of industry standards for wireless communication, i.e. the 802.11 protocols.
- **Wireless LAN (WLAN):** A Wireless LAN connects multiple devices without data cabling. It often connects to an existing wired local area network.
- **Wi-Fi Protected Access (WPA):** This encryption protocol supports authentication and stronger encryption than WEP. WPA2 will be a 256-bit encryption solution with support for Advanced Encryption Standard.
- **802.11a:** 802.11a is an IEEE standard for wireless networking that provides 54Mbps data transfer rates at a range of approximately 45 metres. It uses the 5GHz frequency range.
- **802.11b:** 802.11b is an IEEE standard for wireless networking that provides 11-22Mbps data transfer rates at a range of approximately 90 metres. It uses the 2.5GHz frequency range. It is a low-cost solution, used for wireless communication via Ethernet, and is typically found in home networks.
- **802.11g:** 802.11g is an IEEE standard for wireless networking that provides 44-100Mbps data transfer rates at a range of approximately 90 metres. It also uses the 2.5GHz frequency range.

Further Information

This guide is for general interest - it is always essential to take advice on specific issues. We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

Important Notice

© Copyright 2019, Martin Pollins, All Rights Reserved

This publication is published by Bizezia Limited. It is protected by copyright law and reproduction in whole or in part without the publisher's written permission is strictly prohibited. The publisher may be contacted at info@bizezia.com

Some images in this publication are taken from Creative Commons – such images may be subject to copyright. Creative Commons is a non-profit organisation that enables the sharing and use of creativity and knowledge through free legal tools.

Articles and information contained herein are published without responsibility by us, the publisher or any contributing author for any loss howsoever occurring as a consequence of any action which you take, or action which you choose not to take, as a result of this publication or any view expressed herein. Whilst it is believed that the information contained in this publication is correct at the time of publication, it is not a substitute for obtaining specific professional advice and no representation or warranty, expressed or implied, is made as to its accuracy or completeness.

The information is relevant within the United Kingdom. These disclaimers and exclusions are governed by and construed in accordance with English Law.

Publication issued or updated on:
25 January 2012

Ref: 662

Reference:

[1] Source: http://en.wikipedia.org/wiki/Telecommuting