Getting Started Guide to Wireless Networks

Mike Sharples, Ben Williams, Jeffrey Ting

Getting Started Guide to Wireless Networks

This guide is for IT managers responsible for running a network of computers and who are thinking about introducing a wireless network into the organisation. The document aims to look at the way wireless technology functions and it discusses a range of technical, physical and security considerations for deploying a wireless system.

THE UNIVERSITY
OF BIRMINGHAM

Microsoft®

Contents

What is a Wireless LAN?

A Wireless Local Area Network (WLAN) connects computers together through radio technology, giving the benefits of a wired network but without the costs of wiring cables to every computer. It also gives mobile devices, such as laptop or handheld computers, access to a local network and the Internet.

With wireless technology, you are able to access your e-mail, the Internet, and even your files and applications, anywhere you have access to a wireless network. You can stay connected in public places like airports, hotels and restaurants, wherever wireless access is available.

How Do Wireless Networks Work?

Wireless technology works in a similar way to a mobile phone system: radio waves, instead of wires, carry data from one point to another. Like a mobile phone network, there are limitations on where you can access the network. You must be within range of an access point (AP), the radio transceiver part of a wireless network that transmits data to your computer. However, unlike a mobile phone network, APs can be set up in organisations or homes, to link computers without line rental or connection charges.

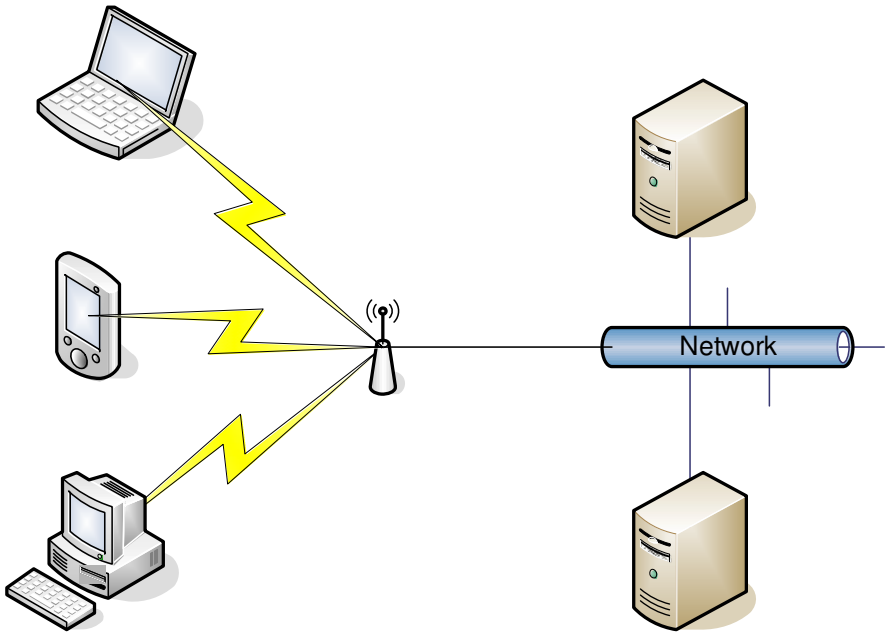

FIGURE 1: illustration of wireless network

Wireless Standards

802.11 is the original standard, established by Institute of Electrical and Electronics Engineers (IEEE) in 1997. It operates at a radio frequency of around 2.4GHz and provides for data rates of 1Mbps and 2Mbps. This standard is now largely obsolete, with little if any equipment still commercially available.

Most current wireless networks use the **802.11b** standard for transmission. Established in 1999 as the successor to the original 802.11 standard, it provides a range of up to 100 metres and a data rate of up to 11 Megabits/second. Its transmission frequency (2.4 GHz) does not require a licence, but that frequency band is also used by microwave ovens and other consumer devices, and this can interfere with the signal and lower the data rate.

The **802.11a** standard was established at the same time as 802.11b, but its adoption has been slower, because it requires more complex equipment and, until recently, it needed a licence for operation in the UK. This standard gives a higher data rate, of up to 54 megabits/second. It also uses a different coding scheme to transmit the data that has been specifically designed for use indoors.

The main drawback of 802.11a is that it uses a higher frequency for the transmission (5GHz) than 802.11b. For a given power, its range is shorter, which may mean installing more APs. Also, a computer with an 802.11a card cannot access a network using 802.11b APs. For compatibility, some recent APs offer support for both standards.

802.11g is a newer standard that gives the same speed as 802.11a and also has the advantage of being backward compatible with 802.11b. But the compatibility comes with a penalty: It operates on the same crowded frequency as 802.11b. Equipment for this standard is becoming more widespread and cheap, but earlier versions of products were not always compatible between different vendors.

The **802.11h** standard is being devised to meet requirements for using the 5GHz band in the European Union, and may replace 802.11a in Europe. It provides for a data rate of up to 54Mbps, dynamic channel selection and transmission power control.

Wireless Topologies

Wireless LANs can be as simple as connecting two computers with wireless network interface cards (NIC) to communicate directly with each other, or as complex as hundreds or thousands of computers with wireless NICs communicating through multiple APs which bridge network traffic to the wired Ethernet LAN.

Ad-Hoc Wireless Networks

Wireless communication directly between two machines is called an ad-hoc wireless network and is like a wireless version of a Windows peer-to-peer network. In an ad-hoc wireless network, the clients associate through use of a common network name or identifier. Once linked, they can share files and other resources exactly as they would in a wired peer-to-peer network.

The limitations of wireless peer-to-peer networking are the same as wired peer-to-peer networking: administrative problems and poor scalability. Though convenient to set up, they are difficult to manage when you have more than just a few nodes. Thus, ad-hoc networks should only be used for the smallest of networks where convenience is paramount and security is not an issue.

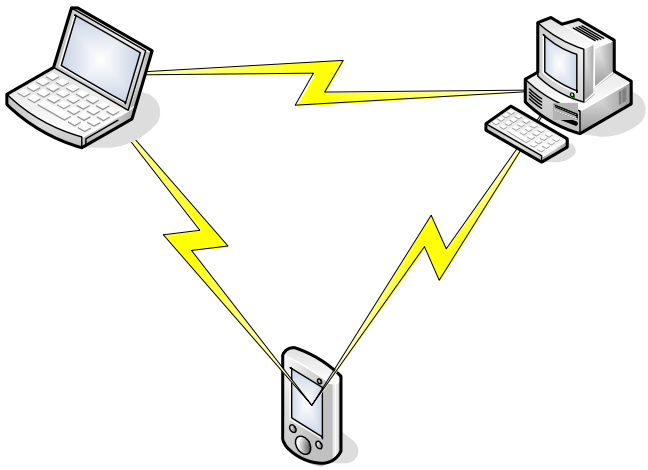

FIGURE 2: illustration of peer-to-peer

Basic and Extended Service Sets

The guide from here onwards will focus on larger, managed infrastructure topologies where multiple 802.11b client computers connect wirelessly through one or more APs to the wired network. In simplest setups, an AP forms an association with one or more wireless clients and acts as a bridge between them and the wired Ethernet network. This is referred to as a Basic Service Set, or BSS.

The further away a client is from the AP, the weaker the radio signal becomes and the data transfer rate drops, slowing down performance. In order to increase the range and coverage of the wireless network, more strategically placed APs must be added. This is referred to as an Extended Service Set (ESS), and is defined as two or more APs that connect to a specific wired Ethernet LAN and their associated wireless clients.

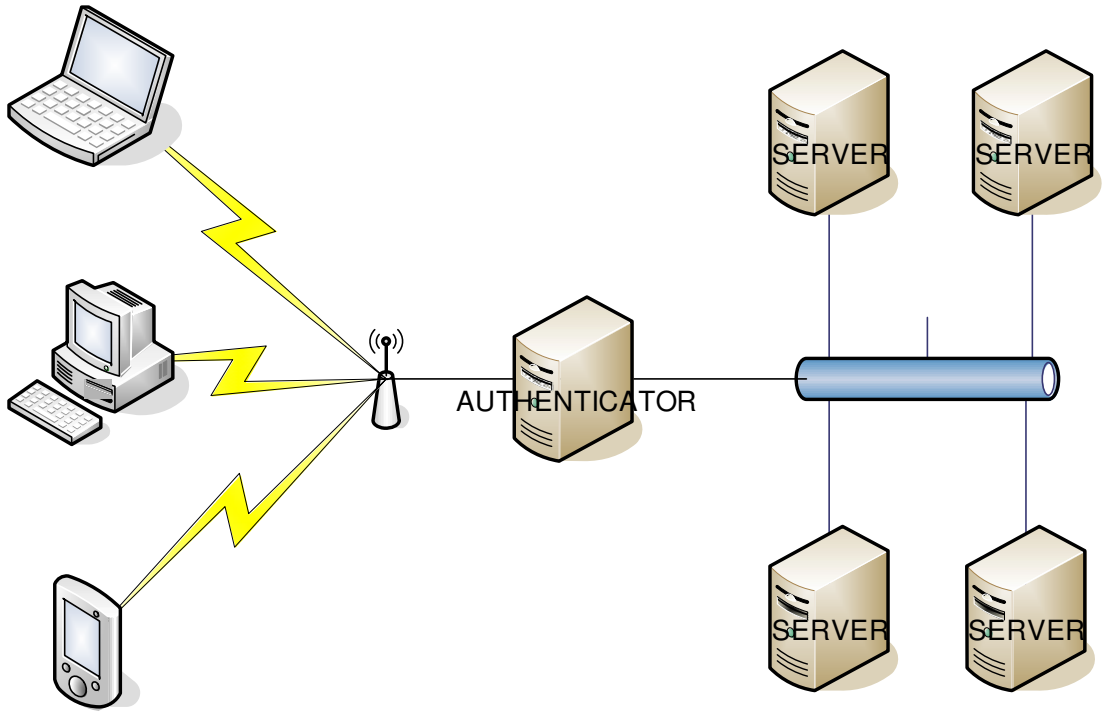

FIGURE 3: illustration of infrastructure mode

Planning Your Deployment

The first stage in a wireless implementation is to carry out a careful evaluation of the state of your current network and to look at what you hope to accomplish by the addition of wireless technology.

The options that need to be reviewed are very wide, and include the following:

- Which groups need access: everyone, staff only, visitors, etc?
- What network resources should each type of user be able to access?
- How many users require access in total, and how many are expected to be accessing the wireless points simultaneously?
- What are their bandwidth requirements?

You will also need to think about the physical nature of users' access to the wireless network. Will the users be moving around a lot? Or will they be mostly stationary?

Security

Security is a major consideration when looking at deploying a wireless solution. You should decide what level of security is needed and how you are going to authenticate clients both to the wireless network and to other network resources. Creating a wireless infrastructure with no security is equivalent to allowing anyone to access the wired network, and potentially, be able to browse the traffic on the network, use up valuable network resources as well as spoof their identify.

Management

Another important consideration is management. Most wireless products will support basic monitoring from a management computer using standard protocols such as Simple Network Management Protocol (SNMP), but there is still manual work involved in tasks such as firmware updates to APs, setting WEP keys, configuring MAC and IP addresses. Make sure you plan for, and allocate, proper resources for these tasks.

It is very important to ensure that the wireless network is not compromised by a rogue access point that is plugged into the wireless network. The security of a wireless infrastructure is only as strong as the weakest link. If a user decides to plug an access point into the wired network with no security then the network potentially becomes open and exposed to anyone who wants to access it. It is important to ensure that this is controlled by a strict policy and regular scans of the network. A procedure should be put in place to keep an updated list of valid AP names and periodically scrutinise the wireless network for AP names that do not appear on the list.

Advance Planning

It is important to have a well thought-out plan before you start deploying a wireless network. Wireless networks have the potential to affect many parts of your network infrastructure, so you should plan for any potentially negative interactions and resolve them before starting the implementation. For example, if you have a heterogeneous networking infrastructure using switches and routers from different suppliers, you will want to make sure that the wireless components you put in place will work properly with this environment. The only way to figure that out ahead of time is by running tests before getting too far into the process. We recommend that you adopt a phased approach to your implementation.

To explore the realities of this integration project, start with a test network, which should not be attached to your production network. It is critical to test new hardware and software in a pilot working environment before rolling it out to your production network.

Physical Planning

Survey the site

Once you know your anticipated number of users, their anticipated bandwidth consumption, and some idea of where they are and how they move around, you will need to match the wireless network requirements to the physical realities of your site. This is done through a site survey, which involves taking a look at the physical layout of your office space and determining optimal placement and density of APs to maximize client connectivity and bandwidth.

Before the site survey, it is useful to locate a set of building blueprints. If none are available, prepare a floor plan drawing that depicts the location of walls, walkways, etc.

Be sure to walk through the facility before performing any tests to verify the accuracy of the building plan. Note any potential barriers that may affect the propagation of radio signals, for example, metal racks, partitions, water tanks, and items that blueprints generally don't show.

Identify user areas

On the plans, mark the areas of fixed and mobile users. In addition to illustrating where mobile users may roam, indicate where they will not go. You might get by with fewer APs if you can limit the roaming areas.

Determine AP locations
Consider the location of wireless users and the estimated range of the wireless LAN equipment you will be using. Locate the APs to give adequate coverage throughout the user areas. Plan for some overlap of radio signal among adjacent APs, but keep in mind that the more distant APs will need to be far enough apart to allow them all to be assigned different channels without interference.

An important design goal is to ensure that users who are roaming from area to area have adequate coverage and bandwidth, while not over-installing APs, which can be expensive.

If you plan to have many users in a small area of space, you will quickly run into the 11Mbps throughput limitation of each AP. By situating APs so that their coverage areas overlap, you can provide aggregate throughput to clients in excess of 11Mbps. Each individual client will not experience an increase in speed beyond 11Mbps, but the total throughput of multiple clients will exceed 11Mbps, depending on the number of APs used.

Consider the mounting locations
Mounting locations could be vertical posts or metal supports above ceiling tiles. Be sure to select suitable locations for installing the AP, antenna, data cable, and power line.

If the APs are placed in hard-to-reach areas, make sure that they are connected to switched power circuits. This way, you can control the power supply to the APs at ground level, rather than having to climb up to it to flip the switch. Or for greater convenience, you can use Power-over-Ethernet (PoE), available in some models of APs, or as an add-on, which can supply DC power over the Ethernet cable, removing the need for a separate power supply.

Verify AP locations
This is when the real testing begins. Many wireless LAN vendors provide site survey tools that identify the associated AP, data rate, signal strength, and signal quality. You can load this software on a laptop or a handheld computer and test the coverage of each preliminary AP location.

Install an AP at each preliminary location, and monitor the site survey software readings by walking varying distances away from the AP. There is no need to connect the AP to the network because the tests only communicate with the AP itself; however, you will need mains power.

Take note of data rates and signal readings at different points as you move to the outer bounds of the AP coverage. When considering which APs are adjacent, it is important to remember that your site is 3-dimensional and that radio signals broadcast in a sphere. In a multi-floor facility, perform tests on the floor above and below the AP. Bear in mind that a poor signal quality reading more than likely indicates that RF

interference is affecting the wireless LAN. If possible, a spectrum analyzer should be brought in to investigate the interference, especially if there are no other indications of its source. Based on the results of the testing, you might need to reconsider the location of some APs and redo the affected tests.

Document your findings
Once you are satisfied that the planned location of APs will provide adequate coverage, identify on the plans the recommended mounting locations: the installers will need this information. Also, provide a log of signal readings and supported data rates near the outer range of each AP as a basis for future redesign efforts.

Signal Quality and Interference

Your site survey can identify conditions that cause deterioration in signal strength through path loss, multipath loss, or interference with other radio transmitters.

Path loss occurs when the signal strength between AP and the wireless client weakens with increasing distance. In short, the further away from the AP you are, the weaker the signal, and the lower the throughput becomes.

Obstacles and obstructions
Other things that affect path loss are ceilings, walls, or cubicles, and in particular, the materials used in their construction. For example, radio signals pass through brick or concrete with moderate difficulty, but not at all well through solid steel. Water absorbs a lot of radio signal, so watch out for water tanks or other obvious water storage locations.

Less obvious obstructions are plants and people, both of which can severely affect the wireless performance. If you are planning an outdoor wireless implementation, then do your site survey when plants are fully leaved (or allow for degradation if not) – otherwise come spring, you will find that your radio signals have degraded.

Dry outside walls can also cause path loss when wet from rain. To address these environmental factors, you will want to increase coverage and density of APs in affected areas.

Multipath loss occurs when radio signals arrive at the AP out of order because they followed multiple paths from the source to the destination, for example reflecting off walls. The result is multiple signals that are slightly out of alignment with one another, causing the radio equivalent of Moiré patterns. This causes additional work for the AP as it must rebuild the signals properly. Minimizing the number of objects that block or reflect the radio signal helps reduce multipath loss.

Antennae
Using diversity antennas reduces the amount of multipath loss. Diversity antennas contain two antenna elements at the base station. The antennas have a small physical distance between them that improves signal strength by cutting down the negative effects of multipath loss. Another strategy to increase signal strength is to use high-gain antennas.

One more option is to use unidirectional antennas to target areas of poor coverage. A unidirectional antenna has a single, well-defined direction of maximum gain, radiating most of its power in one direction.

Radio Interference
Radio signal interference happens when other devices operate in the same frequency range as 802.11b, and can cause a degradation of network performance. Cordless phones, microwave ovens, and Bluetooth networking devices all operate in the 2.4GHz range used by 802.11b. If they broadcast at the same time as a network device, they will interfere with the radio signal and corrupt the data packet, causing the network device to re-transmit, thus lowering the performance. Access points should be placed such that interference from other transmitters is minimized. This can be done by either moving APs further away from the source or by increasing the number of APs in the given area.

Crosstalk and channel selection

The 802.11b radio bandwidth is divided into 14 channels:

Channel	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

Various countries limit the use of these channels. For example, the U.S. only allows the use of channels 1 through 11. The U.K. can use channels 1 through 13, though the majority of the software for the equipment limit the channel selection to the 11 US channels.

By default, APs come configured to a specific channel. Adjacent APs should be set to different channels to minimize crosstalk between them. Crosstalk occurs when the signals from APs overlap and interfere with one another, reducing performance, as APs have to untangle the signals. Since each channel covers about 22 MHz of bandwidth, with the available channels, you are effectively only able to get 3 non-overlapping channels. A typical arrangement is to use non-overlapping channels 1, 6, and 11 such that adjacent APs are never on the same channel.

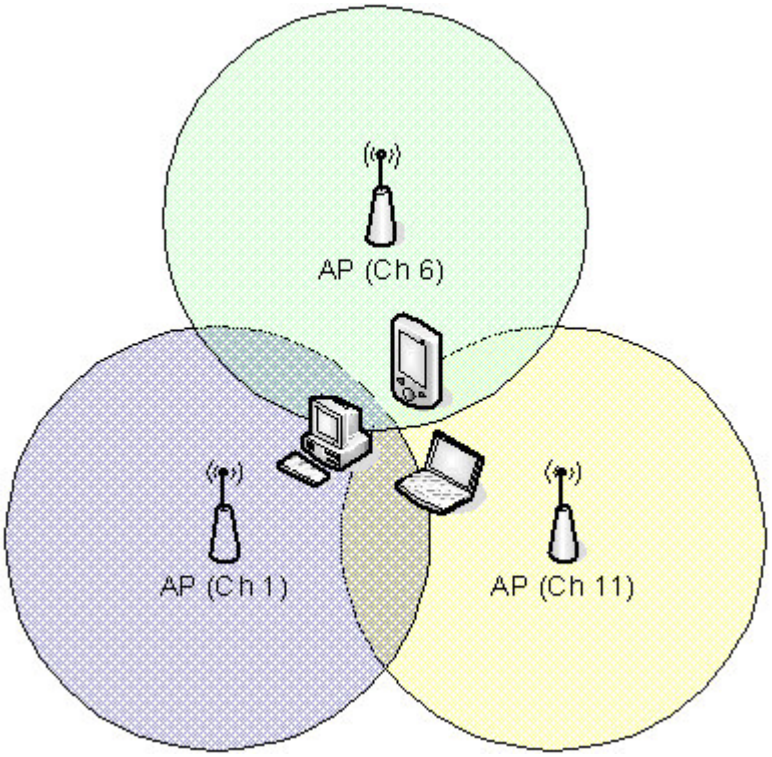

FIGURE 4: Crosstalk

Wireless Security

Ensuring adequate security should also be one of your main concerns. There are several security mechanisms built into the 802.11b standard, but these mechanisms provide only minimal security protection.

Disabling ESSID

The first security mechanism is the Extended Service Set ID (ESSID), which is an alphanumeric code that is entered into all APs and wireless clients that participate on the same wireless network. Different vendors provide their own default value for the ESSID. Changing the ESSID from its default value is a good first step towards improved security.

There is no significant reason to broadcast the ESSID, unless you want to set up a network for public access. By default, the APs will periodically broadcast the network name, which can be decoded by the wireless client software to give a list of available wireless networks. If this broadcast is disabled, hackers would either have to know the network name or have some kind of wireless packet capture software to derive this information.

The ESSID provides only rudimentary security and should not be used as the only method of securing your network.

Protection through access lists

The next layer of wireless security is the Access List. The access list is how you define the unique MAC addresses of the wireless network interface cards that you will allow to associate with your AP. An access list also creates management overhead, as you need to enter the MAC address of each card that needs access. If you want to update access lists, you'll have to do it manually, unless you use a tool provided by some vendors, which helps to automate the process. In a large network this may be unmanageable and the AP may not have the capacity to list all the devices approved for access.

Unfortunately, MAC addresses are easy to discover since they are transmitted in clear text. By configuring a wireless NIC with a known good MAC address that was captured out of the air, an attacker can gain access to the network.

WEP Encryption

Once a computer is granted access to the network, it is important to encrypt the data, since data transmitted in the clear can be captured. 802.11b provides an encryption mechanism known as WEP, or Wired-Equivalent Privacy. WEP uses either a 64-bit or a 128-bit encryption key and is generally disabled by default on APs. Not using WEP makes it

simpler to set up the network, but also means that hackers can use analyzers to 'sniff' network traffic and potentially compromise the network.

The difficulty with WEP lies with the management of the encryption keys. Without some sort of centralized way of managing and distributing keys seamlessly to both APs and clients, a change in any of the keys creates an administrative nightmare. Administrators will need to change the keys on all APs and clients in order to secure the environment properly. Although some vendors have their own proprietary software to deploy WEP keys to their APs, they are not compatible with each other, and are unable to manage WEP keys on most wireless clients.

This basic approach does improve security; however it does present some management issues and security drawbacks, particularly for larger deployments, which can be addressed through enhanced security options.

Enhancing Security through stronger Authentication & Encryption

Security of a wireless network can be improved through authentication of users and clients and enhancing the encryption of the wireless communications channel between the wireless client and fixed network.

RADIUS Server

If you need user-based authentication, you should set up a RADIUS (Remote Authentication Dial-in User Service) server. RADIUS has the advantage of being centrally managed, which is important for larger deployments. As well as authenticating wireless network clients and users, the RADIUS server can be used to authenticate clients and users of the VPN service, allowing you to authenticate multiple services from a single, centralized database, easing administrative overhead.

Components of a RADIUS Infrastructure

A RADIUS authentication, authorization, and accounting (AAA) infrastructure consists of the following components:

- Clients
- Access servers (RADIUS clients)
- RADIUS servers
- Authentication servers
- User account databases

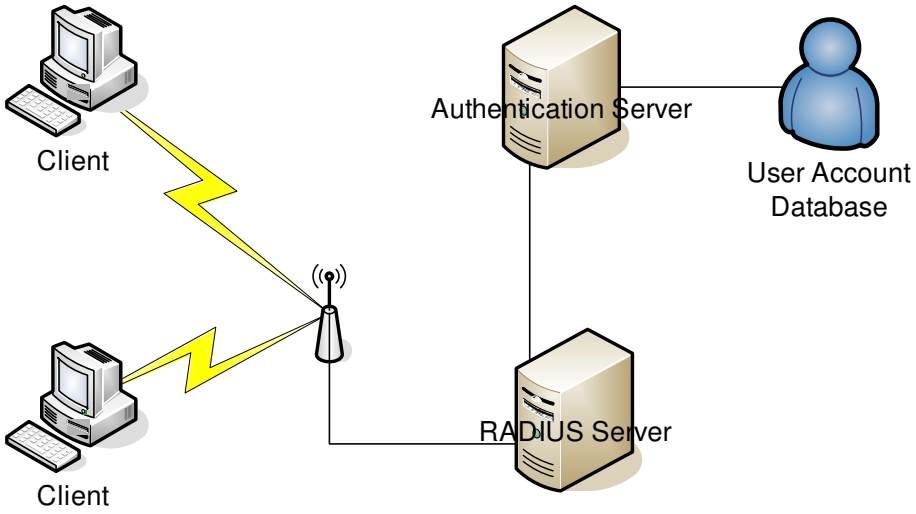

FIGURE 5: Components of a RADIUS infrastructure

Client Authentication

There are a number of client authentication options available. Client hardware-based authentication can be open, or based on a shared key between the AP and client, X.509 Public Key Certificates or a combination or certificates and shared keys.

IEEE 802.1X

IEEE 802.1X is a security standard featuring a port-based authentication framework and dynamic distribution of session keys for WEP encryption. Within this there are a number of options and a RADIUS server is required to support these.

802.1x with EAP

EAP is an 802.1x standard that allows developers to pass security authentication data between RADIUS, the AP, and the wireless client. EAP has a number of variants, including: EAP MD5, EAP-TLS (EAP-TLS), Lightweight EAP (LEAP), and Protected EAP (PEAP).

Extensible Authentication Protocol (EAP) – Transport Layer Security (TLS) uses X.509 certificates to mutually authenticate wireless clients and RADIUS servers using strong cryptographic means and generates encryption keys used to protect wireless traffic. This is one of the most popular and secure, EAP methods for use with 802.1X. It requires public key certificates on the client and RADIUS server.

Protected EAP (PEAP)

PEAP is designed to carry EAP types within a channel secured by TLS and requires a server based certificate. Passwords are used to enable the security channel between the server and the client. PEAP also dynamically generates keys for encrypting wireless traffic during the authentication process.

Virtual Private Networks (VPNs)

A VPN is a secure, private communication 'tunnel' between two or more devices across an open or public network, such as the Internet or a wireless network. Even though a VPN's data travels across the open network, it is secure because the data within the tunnel is encrypted.

VPNs are a great technology for remote access but can have limitations in a wireless network, an application it was not designed to support. For example, the VPN server can become a bottleneck, as all WLAN client access is channelled through the server. VPN devices traditionally service many low speed remote clients. This approach assumes that the VPN authentication method is secure, but many VPN implementations that rely on a pre-shared key authentication (a group password) share many of the security flaws of static WEP keys. Thus great care must be taken to ensure that all the VPN limitations and issues are understood before implementing a VPN as a security option for the WLAN.

Wi-Fi Protected Access (WPA)

WPA is a Wi-Fi standard that solves some of the concerns of WEP by utilizing Temporal Key Integrity Protocol (TKIP) to change the WEP key periodically. WPA upgrades for wireless network devices are generally available now from their respective vendors.

Wireless Network Management

The wireless network management marketplace is still quite immature. Tools to locate, implement, manage and monitor wireless networks are usually limited, proprietary solutions. However, some newer tools are promising greater scalability, ease and security in a cross-platform solution.

Most existing wireless network products ship with vendor-specific client and AP utilities. The client tools provide an interface to define ESSID, encryption keys, radio settings, and channels. Suppliers will often provide site survey tools of varying quality that can display signal strength and quality, data rate, or a host of other relevant information about the network's performance and efficiency. The AP tools are generally Web-based or command line-based, and provide the ability to configure APs individually, but often not collectively.

Running a Wireless Network

Once the wireless network equipment is in place, the task of running and maintaining the wireless network service becomes the focus. Depending on the choice of deployment, managing the system may be mainly automatic or very time consuming.

For security and management considerations, unless you are running a very small network with a handful of users, or an open public access network, you should register all wireless clients and users. You should collect and maintain such details as user contact, wireless client device types, MAC addresses, expected access hours, and expiration periods, particularly for temporary users, visitors, students and so on.

You should establish a policy and a set of procedures for allowing visitors and guests access onto your wireless network. This will involve registering their network devices, or loaning them wireless network interface cards, as well as controlling and managing their access rights on the internal LAN. It is recommended that if you have regular guests or visitors on the network, you have a firewall to control the wireless access into the internal LAN and limit it to internal users only.

If the deployed system is based on a shared key or open system concept then you should put in place a procedure of de-registering expired accounts to make sure users are not given access to the network beyond their validity periods.

WEP Key Changing

Unless WPA or dynamic re-keying features of 802.1x are being used, WEP keys should be regularly changed, and all APs and clients updated. This is non-trivial task for any network of all but the smallest size, and should be carefully planned and coordinated to ensure minimum downtime for the users.

There are concerns that unless planned and conducted very efficiently this form of administration could create big down time for large parts of the system and users may not be able to access network resources if they were unaware of the key change. The frequency of these stages should be planned to occur at regular intervals and advertised to users accordingly. One problem of managing a system in this manner is that there is no quick and efficient way to change all keys in the event of a security breach. In such an event, a firewall to block all access from wireless client would be the most expedient method.

What next?

Installing a wireless LAN is relatively straightforward, but configuring the system so that it is both secure and reliable can take time and skill. The aim of this Guide has been to give a broad introduction to the issues you need to consider, the common problems and a range of solutions. To go further you will need to select your equipment and software and then follow the manufacturers' installation guides and manuals. Specialist WLAN companies can give assistance in configuring and troubleshooting, or provide a full site survey and installation. The websites listed below give case studies of successful WLAN installation and also details of some recommended suppliers and consultants. The list is by no means complete, but equipment suppliers should be able to offer further recommendations.

Wireless Network Scenarios and Case Studies

For details and case studies of actual wireless network implementation and deployment, please go to

http://web.cetadl.bham.ac.uk/live/welcome.asp?id=86

http://www.microsoft.com/uk/education/wireless

Jeffrey Ting, IT Systems Manager, Educational Technology Research Group, University of Birmingham

Mike Sharples, Professor of Educational Technology, University of Birmingham

Ben Williams, Microsoft Consultant, Microsoft Ltd.

The authors cannot reply to queries relating to this Guide.

Glossary

The following is a list of some the terminology used when dealing with wireless networks:

There several generations of wireless networking technology.

802.11

The original standard was established in 1997. It operates at a radio frequency of around 2.4GHz and provides for data rates of 1Mbps and 2Mbps. This standard is now largely obsolete, with little if any equipment still commercially available.

802.11b

Most current wireless networks use the IEE 802.11b standard for transmission. Established in 1999, is provides a range of up to 100 metres and a data rate of up to 11 Megabits/second. Its transmission frequency (2.4 GHz) does not require a licence, but it is also used by microwave ovens and other consumer devices and this can interfere with the signal and lower the data rate.

802.11a

The 802.11a standard was established at the same time as 802.11b, but adoption has been slower, because it requires more complex equipment and, until recently, it needed a licence for operation in the UK. that gives a higher data rate, of up to 54 megabits/second. It also uses a different coding scheme to transmit the data, that has been specifically designed for use indoors.

The main drawback is that 802.11a uses a higher frequency for the transmission (5GHz) than 802.11b. For a given power its range is shorter, which may mean installing more access points. Also, a computer with an 802.11a card cannot access a network using an 802.11b base station. For compatibility, some recent base stations offer support for both standards.

802.11g

This is a newer standard that gives the same speed as 802.11a and also has the advantage of being backward compatible with 802.11b. But the compatibility comes with a penalty: it operates on the same crowded frequency as 802.11b. Equipment for this standard is becoming more widespread and cheap, but earlier versions of products were not always compatible between different vendors.

802.11h

The 802.11h standard is being devised to meet requirements for using the 5GHz band in the European Union, and may replace 802.11a in Europe. It provides for a data rate of up to 54Mbps, dynamic channel selection and transmission power control.

Bridge

A network device that physically connects two separate and distinct networks.

DHCP Server

Dynamic Host Configuration Protocol Server. A server that dynamically assigns hosts an IP address, and any additional information needed to properly communicate on a specific network.

Ethernet
A type of physical network that allows devices to communicate with each other.
Firewall
A server designated as a buffer between any connected public network and a private network to protect against unauthorised intrusions into the private network.
Host
Any device that is connected to a network.
IP
Internet Protocol. A set of protocols that allow hosts to communicate with each other regardless of location.
IP address
An identifier that hosts use to locate and communicate with one another. Typically an IP address is represented as: 147.188.128.3.
LAN
Local Area Network. Defines a type of network that is local in scope.
MAC address
Media Access Control address is your network interface card's unique hardware number. This allows network software to uniquely identify your computer on the network.
NAT
Network Address Translation. A mechanism for translating private IP addresses to public IP addresses, so that internal networked hosts can communicate to the public Internet. NAT is a basic form of firewalling, and NAT service is typically provided by a networked server.
NIC
Network Interface Card.
OSI Model
A 7-layer model which many networking terms and protocols are referenced against
PPPoE
Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.
Private address
An IP address from a set of reserved addresses used to communicate with other hosts on the same network.
Private network (or internal network)
Any network (Ethernet, wireless, or otherwise) that is protected from public access.
Public address
An IP address from a set of publicly available, globally routable IP addresses.

Public network
A network that is publicly accessible, generally a network with public IP addresses.
RADIUS server
Remote Authentication Dial-in User Service – used for remote user authentication and accounting.
RF
Radio frequency.
Server
A host computer providing a specific service, or services.
Spectrum analyzer
A device to display the signal strengths for a range of frequencies.
SNMP
Simple Network Management Protocol.
WAN
Wide Area Network. Defines a type of network that is global in scope.
Wi-Fi
Wi-Fi is a term that has been promoted by the Wi-Fi Alliance, a consortium of equipment vendors, to describe all 802.11-type devices. The Alliance provides a service to companies, to list their products as 'Wi-Fi certified.
Wireless Bridge
A component typically used to bridge a wireless network with an Ethernet network.
Wireless Network Access Point
Any device configuration that enables wireless access to a physical network.