**Wireless LAN Technology – IEEE 802.11**

**Introduction**

Wireless networking is causing a revolution in computing and Internet access. Wireless Local Area Networking (WLAN) frees users from the constraints of cables in the office or home environment. Ideal for notebook PC users wanting mobility and for desktop users requiring access to networks where the traditional wired method is impractical or prohibited such as in listed buildings or across public highways.

The arrival of the IEEE 802.11b Wi-Fi standards meant that most vendors could provide a low cost compatible solution for wireless communication over the local area, at speeds on a par with basic wired Ethernet technology. Prior to IEEE 802.11 brand x radio would not work with brand y access point. The WLAN standard continues to evolve to provide higher speeds, greater range and better security than the earlier systems.

Both radio and optical (laser or infrared light) transmission methods are used for the wireless connectivity of computer systems but radio systems are by far the most popular as they have greater range and don’t require line of sight.

Wireless versions of the *Network Interface Card* (NIC) are employed to transmit and receive the signals and *Access Points*, are used to concentrate and repeat these transmissions or bridge to wired network equipment such as hubs or switches, see Figure 1.

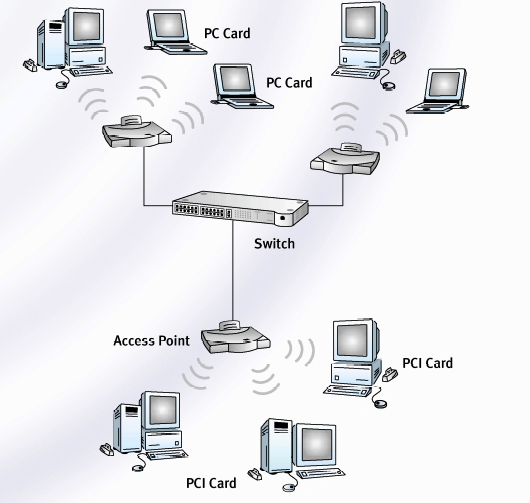


Figure 1 WLAN equipment

**Modes of Operation (Ad-hoc or Infrastructure)**

The main difference between a wireless NIC and a more traditional cabled NIC lies in the transmitter/receiver circuitry. In the case of radio frequency NICs, the transceiver performs the functions of a radio transceiver, and has an antenna attached. These may interact directly with other wireless nodes called **ad hoc** or peer to peer mode or may attach to a wired LAN via a wireless concentrator or access point called **infrastructure** mode to produce a hybrid network, see Figure2.

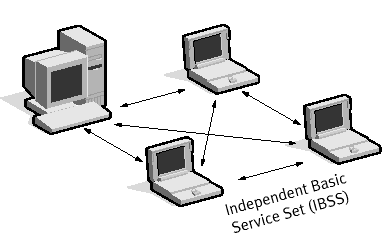
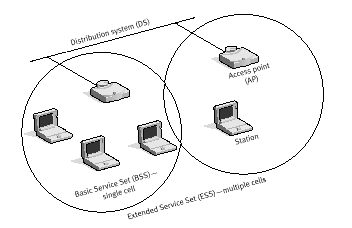
 

Figure 2 Ad Hoc mode Infrastructure mode

**WLAN Identification**

The IEEE 802.11 defines a network name or ***SSID*** (Service Set Identifier) to identify wireless nodes.

A ***BSSID*** (Basic Service Set Id)is the MAC address of the Access Point (AP) in an infrastructure mode BSS.

In an ***IBSS*** (Independent BSS)**,** the BSSID is a locally administered IEEE MAC address generated from a 48-bit random number.

An ***ESSID*** (Extended Service Set id) identifies devices on a particular ESS WLAN.

**Radio Systems**

Most Wireless Local Area Network systems employ Spread Spectrum Technologies (SST) radio technology. Standardised by the IEEE 802.11 committee to use the licence free 2.4GHz ***ISM*** (Industrial, Scientific and Medical) band having a range of about 100m in side buildings (dependent on construction methods and obstructions) and transmission rates from 1 to 54 Mbps at present depending on the version of IEEE 802.11 used (a or g). The actual data throughput will depend on the number of users sharing access points and the transmission environment.

The 5 GHz ***UNII*** band is also being used for higher speed 54Mbps data rates using the same access methods and is specified in IEEE 802.11a and h but has shorter range.



# Figure 3 narrow v spread spectrum bands

The spread spectrum transmission techniques used in WLANs, modulate signals over a broader range of frequencies than conventional narrow band radio systems. The result is a more robust signal, which is less susceptible to noise/crosstalk and provides added security against eavesdropping than narrow band systems, see Figure3.

Both Direct Sequence Spread spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) techniques are employed in standard WLAN equipment to enable multiple node access to the WLAN and permit roaming between access points.

Orthogonal Frequency Division Multiplexing is used by the higher speed technologies and when combined with convolution coding gives the most reliable wireless transmission systems.

**DSSS** spreads the signal across the whole bandwidth by ‘chipping’ – changing frequencies at a speed much higher than the signal bit rate using a repeated code sequence known as the chip code. It avoids excessive power concentration by spreading the signal across the frequency band such that each bit is mapped to a pattern of ‘chips’ by the transmitter and then mapped back again at the receiver. If the transmitter and receiver are using the same code sequence and are synchronised, they can establish a secure link and co-exist with other radio sources at the same frequency. In 802.11b low speed transmission each bit is XOREed with an 11bit Barker sequence. This adds redundancy to the transmission so that error correction can take place and allow lower level signals to be used.

**FHSS** spreads the signal by transmitting in short bursts on one frequency and then ‘hopping’ to another frequency for a short time and so on. The bandwidth is divided into a number of channels each capable of carrying data at the required rate. The transmitter ‘hops’ between channels in a random manner, but if the receiver knows the ‘hopping’ sequence in advance it can follow it.

The main advantage of FHSS is its ability to deal with noise/interference; if it hits interference in one channel it hops around it, and comes back later. The FHSS technique, however, cannot support high data rate with the limited channel bandwidth available and is only found in the earlier 802.11 equipment and Bluetooth PAN systems.

**OFDM** offers the highest data rates (up to 54Mbps) at the moment and maximum resistance to interference and corruption of the signals used in 802.11a and g equipment. OFDM achieves high data rate by squeezing a large number of sub channels into a given frequency band using sophisticated Digital Signal processing techniques and more efficient phase modulation methods such as Quadrative Amplitude Modulation (QAM).

The closely spaced small bandwidth sub carriers have a relatively low data rate but when transmitted in parallel high data rates are achieved. IEEE 802.11 a and g also employ convolution (error correcting) coding to minimise data loss due to narrow band interference. IEEE 802.11g was designed to be backwards compatible with 802.11b. Both work in the ISM band using the same channels but 802.11b can't hear 802.11g when it employs OFDM so the 802.11g equipment must use DSSS or to allow communication or DSSS-OFDM hybrid mode to ensure the 802.11b equipment can detect 802.11g transmissions.

**Range** IEEE 802.11b and g have greater range than 802.11a, but in all cases if interference grows, the distance over which the signal can be recovered falls for a particular data rate. To maintain range the speed may have to fall also.

*N.B. The latest WLAN non - standard MIMO equipment employ multiple aerial systems avoid to multi-path interference problems and boost signals to increased speed and rang.*

**IEEE 802.11 Wireless LAN standards and Wi-Fi**

Many vendors have offered proprietary wireless LAN systems, but now, fortunately, there is an industry standard (IEEE 802.11) that provides multi-vendor interoperability for both radio and IR networks. It covers both the data link and physical layers of the OSI model, see Figure 4.

Equipment with the Wi-Fi (Wireless Fidelity) logo is certified for multi vendor interoperability and avoids compatibility problems.

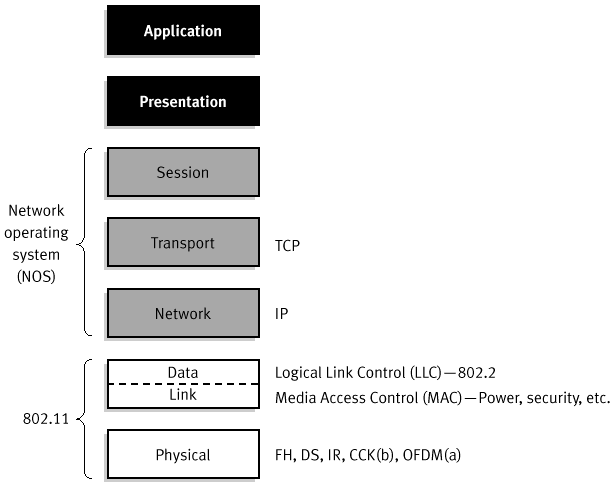
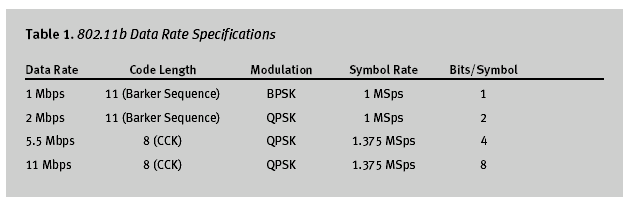
****

Figure 4 IEEE 802.11 and OSI

**Physical layer (PHY)**

Three physical layer protocols (PHYs) are specified, one for IR and three for radio (DSSS and FHSS and OFDM). Table1 gives details of the IEEE 802.11b signal and coding schemes used. Table2 summarises the development of IEEE 802.1l PHYs.



**IEEE 802.11b/g/a/n**

IEEE 802.11b WLAN is the most popular version at the moment. It employs radio signals in the 2.4GHz IMS band for communications between wireless NICs and access points at speeds of up to 11Mbps. Only the DSSS technique is used because the FHSS technique cannot support the high data rate with the limited channel bandwidth available.

Most new WLAN equipment supports the higher rateIEEE 802.11g standard, both b and g use the same ISM band so can coexist but speed will be limited to that of the slower device.

In the US the IEEE 802.11a standard operating at 54 Mbps in the 5GHz band is now widely used. IEEE 802.11a adoption was delayed in Europe because of concerns by regulatory body (ETSI) about channel allocation and power levels - 802.11h overcomes this concern.

Dual band (tri standard) equipment is available from some vendors. A new even higher speed standard is currently underdevelopment and is expected to be ratified next year as IEEE 802.11n.

Table 2 Various IEEE802.11 standards

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Standard** | **Ratified** | **Band GHz** | **Speed max)** | **Comments** |
| IEEE 802.11 \* | 1997 | 2.4 ISM  1MHz /ch FHSS  22MHz/ch DSSS | 2 | Original spec  FHSS or DSSS |
| IEEE 802.11b | 1999 | 2.4 ISM  22 MHz /ch | 11 | Enhanced PHY  DSSS only |
| IEEE 802.11a | 1999 | 5 UNII 1,2,3 | 54 | Popular in US  OFDM |
| IEEE 802.11g | 2003 | 2.4 ISM | 54 | Enhanced 11b  DSSS and OFDM |
| IEEE 802.11h | 2003 | 5 | 54 | Europe version of a  OFDM |
| IEEE 802.11n | 2009 | 2.4 and 5 | 300+ | Faster and longer range  MIMO |

*N.B. Another high speed WLAN, specified by ETSI, called Hyperlan 2 was seen as a competitor to IEEE 802.11a, but now looks unlikely to compete due to the great success of the IEEE standard.*

**Media Access Control (CSMA/CA)**

All the IEEE 802.11 technologies employ a MAC protocol similar to IEEE 802.3 (CSMA/CD) called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).



Figure 5 Basic CSMA/CA operation

CSMA/CD defines that a node should listen for a collision on a wired shared media following a transmission and back off for a period of time when a collision is detected. Collision detection is not possible in wireless LANs because of the “near-far” problem – i.e. a station can’t transmit and listen at the same time because the transmission drowns out the ability to hear the collisions.

CSMA/CA also called DCF (Distributed Coordination Function) on the other hand attempts to avoid collisions. It listens for the air to be free, and then waits for a predetermined time and if it is still free it transmits a packet and then waits for an acknowledgement (ACK) frame. If no ACK frame is received, the station assumes that a collision has occurred (or some other reason has caused the Access Point to not receive the packet or station not to receive the ACK), it then waits before trying again, see Figure 5.

**RTS/CTS Handshaking and Virtual Channel Sensing**

The ‘**hidden node**’ problem, which can result in collisions and degraded performance, may occur when nodes at opposite sides of an access point in infra structure mode or are out of range of each other in ad-hoc mode wish to communicate, see Figure 6. Here both A and B both want to communicate with C but are too far apart to detect each others transmissions and will cause a collision if they attempt to transmit at the same time.



Distance limits or obstacles may prevent each station detecting the others transmissions resulting in them both trying to use the access point at the same time. To solve this problem 802.11 specifies an optional RTS/CTS protocol at the MAC layer. When this feature is in use the stations transmit a RTS frame and then wait for the access point to reply with a CTS frame. Since all stations on the network can hear the access point, the CTS causes them to delay any intended transmissions, allowing the sending station to transmit data and receive a packet acknowledgement without any chance of collision.

Figure 7 shows the timeline diagram for RTS/CTS operation when A sends a frame of data to B and C asserts virtual channel busy flag (NAV) until the frame is transmitted. The time of NAV is set in the frame duration field according to size frame size. Care should also be taken when implementing RTS/CTS because the reduced collisions count may not improve utilization when the protocol overhead is taken into account.



RTS/CTS handshaking is set up on wireless nodes by specifying a frame size RTS threshold below which it is not used, i.e. only use it when it will improve performance.

*N.B. the CSMA/CA protocol is not as efficient as CSMA/CD because of the protocol overhead required for the ACK and RTS/CTS mechanisms.*

Another problem called ‘**exposed node**’ can cause degradation in performance in ad-hoc type networks in particular. When nodes mistakenly think a transmission will fail due to the proximity of another transmitting station even though the destination station is free to receive. For time bounded data such as voice or video the 802.11 MAC also supports a Master-Slave mode called Point Coordination Function (PCF) where the AP controls access by polling each station in turn to give permission to transmit. This guarantees a maximum latency figure needed by isochronous applications. Enhancements to the MAC protocol are now being developed by the IEEE 802.11e committee that add Quality of Service (QoS) to the coordination function to give better network utilisation by allowing time dependent data such as voice and video to have priority over other traffic.

**Association, Inter-Cell Communication and Roaming**

The process of connecting a node to an access point is called ‘Association’ This occurs when a node moves within range and tunes its radio channel to what the access point is set to.

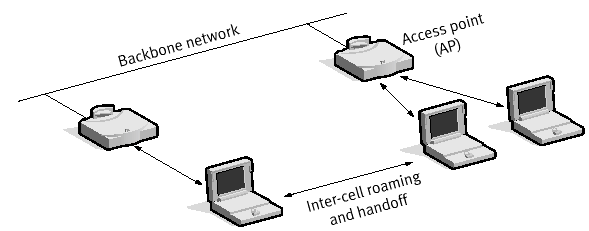


Figure 8 Inter-cell Communications and Roaming

Inter-cell communication of nodes connected to different access points by a distribution system or backbone network as in Figure 8 is accommodated by a frame structure which contain four MAC addresses. How these addresses are interpreted depends on the setting of the DS bits in the control field shown in figure 9. In the simplest case two addresses identify the source and target wireless nodes (DS=00) but in the most complex (DS=11) two additional intermediate addresses are needed. In the example shown in Figure 9, Addr1 is the destination node, Addr2 is source node, Addr3 is the local access point that forwards the frame to the destination access point Addr3.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| control | Duration | Addr 1 | Addr 2 | Addr 3 | Sequence | Addr 4 | data | checksum |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Version | Type | subtype | To DS | From DS | MF | retry | Pwr | more | W | O |

Figure 9 Frame format

Roaming, the ability of a mobile computer to move between access points is an important feature of larger WLANs. Roaming provides a continuous network service for mobile workers by a technique called ‘scanning’ and ‘re-association’

The wireless node assesses the received signal level from each access point within range and then resynchronises (adjusts channel settings) to the stronger as the user moves between service areas using either active or passive scanning. Active scanning employs four steps involving an interchange of frames: (1) node sends a probe frame, (2) all APs within range reply with a probe response, (3) node selects an AP by sending an association request and (4) the AP replies with an association response. In passive scanning the APs send out Beacon frames periodically and nodes wishing to change AP send back an association request. Beaconing is also used to awaken nodes in power save polling mode and advertise other access point services.

The process of dynamically associating and re-associating with access points allows network managers to set up WLANs with a very broad coverage by creating a series of overlapping cells as in Figure 10, but care must be taken to ensure that channels do not overlap.

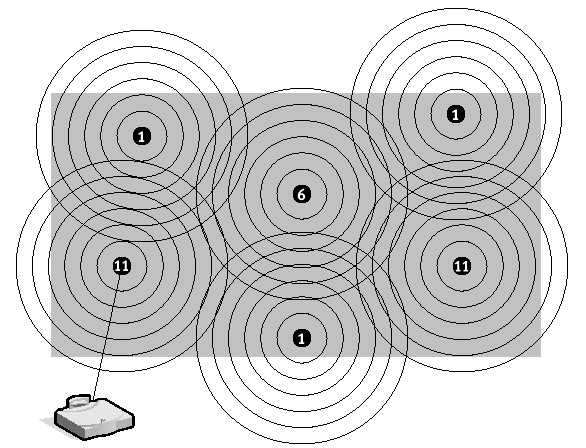


Figure 10 IEEE 802.11b DSSS cell overlap

N.B. In IEEE 802.11b *there are only three of the 14 channels that don’t overlap at all so these should be used if at all possible. If two partially overlapping channels are used they may cause interference for one another, leading to reduced bandwidth in the overlapping area. Not all channels are available in some regions.*

In large TCP/IP enterprise networks, however, moving between subnets can pose further problems because the IP configuration may need to change.

A DHCP server to re-allocate the IP address, default gateway etc. when moving between the wireless cells can do this or VPN tunnelling techniques can be employed as in Figure 11.

An alternative method, which also improves security, is to use VLAN techniques so that the IP configuration is maintained throughout the network.

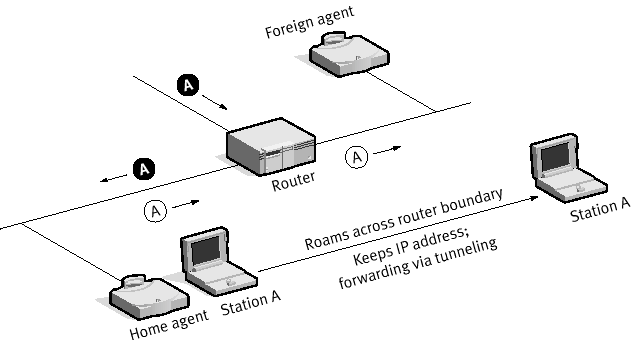
****

Figure 11 Mobile IP roaming

**Security issues with WLAN and IEEE 802.11i**

Security is a major concern in any wireless network because any computer or PDA equipped with a WLAN card can pick up the signals. Also the WEP (Wired or WiFi Equivalent Privacy) layer2 encryption method used by IEEE 802.11b is seen as insecure (easily cracked). There are, however many ways to make WLANs as secure as wired networks. See Appendix for 10 ways to improve wireless security.The more effective WPA (Wi-Fi Protected access) technology is now being used in by most IEEE 802.11g technology which is a subset of the new IEEE 802.11i standard designed to be used with the IEEE 802.1Xextensible authentication protocols to stronger data link encryption and than the fixed key method of WEP and improved access security. WPA2 provides authentication support via IEEE 802.1X and **PSK** (Pre Shared Keys) for the following applications:

**Personal Mode** is a term given to products tested to be interoperable in the PSK-only mode of operation for authentication. It requires manual configuration of a pre-shared key on the access point and clients. PSK authenticates users via a password, or identifying code, on both the client station and the access point. No authentication server is needed and Personal Mode is targeted to SOHO environments.

**Enterprise Mode** is a term given to products that are tested to be interoperable in both PSK and IEEE 802.1X/EAP modes of operation for authentication. When IEEE 802.1X is used, an authentication, authorization, and accounting (AAA) server (the RADIUS protocol for authentication and key management and centralized management of user credentials) is required. Enterprise Mode is targeted to enterprise environments, see Figure 12.

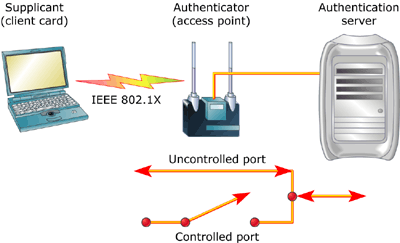


Figure 12

**Other Access Control methods**

Data link access control via the access point identifiers (SSIDs) offer some degree of protection against unauthorised access – if a station does not know this value then it is not allowed to associate. Turning off SSID broadcasting, which is on by default on some access points, is only a mild deterrent to hackers as packet sniffing will easily reveal the name of the access point when an authorised node transmits a frame.

Access control lists of MAC addresses can also be included in the Access Point used to restrict access to known users entered into a table, but again hackers can easily spoof (or clone) MAC addresses (pretend to be a valid user) to gain access.

If security is a major concern**,** however,users are being advised to implement higher layer authentication methods or use Virtual Private Network (VPN) or VLAN techniques. For mid to large networks WLAN switches can simplify administration and Enterprise Wireless gateways (EWGs) can ease the authentication and connectivity issues.

Extending Wired LANs and Public Access

Wireless networking works well as an extension to wired networks. Some wireless technologies extend wired networks by providing high-speed links between networks, whereas other wireless technologies extend traditional networks by giving mobile users easy access. This access can benefit people who work in environments that require mobility, such as hospitals, restaurants, warehouses, manufacturing plants, stock exchanges and for travellers at airports or rail stations.

There are 3 modes of operation defined for Access Points: Root, Bridge and Repeater. The latter two are intended to extend the range of WLANs or connect LANs together.

**Root APs** is connected to a wired distribution system such as Ethernet as in Figure 2 and provides wireless access to the network for wireless stations.

**Bridge APs** create a wireless distribution system (wireless bridge) between networks and typically do not allow association of wireless stations, see Figure 13. They are often used with directional aerials for mid to long range connection. Some APs can do both root and bridge functions. Wireless bridges provide wireless connectivity to remote Ethernet networks and are fully transparent to network protocol and applications. The wireless bridge connects a computer via an Ethernet cable, which is connected to a small transmitting antenna. This antenna sends signals to a larger antenna that is usually mounted on the roof of the building. From here, the signal is broadcast to a large receiving antenna where it can send the signal back down to the receiving end’s wireless bridge and so on.

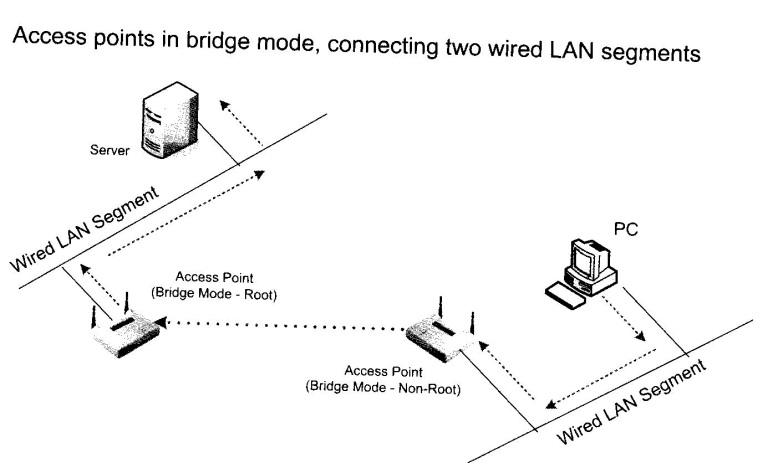


Figure 13

**Repeater APs** provide intermediate connectivity between Root APs and wireless stations that are out of range of the root AP, see Figure 14. It acts more like a bridge (rather than an Ethernet type repeater). Repeater use is not recommended since the APs must use the same channel and have 50% overlap giving limited range (they must have omni-directional aerials to service mobile clients) and poor performance.

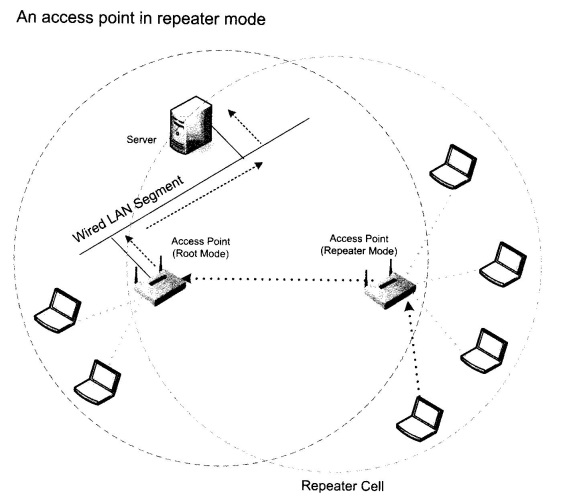


Figure 14

**Residential Gateways** Many broadband routers have built in APs to facilitate access to the internet via ADSL and cable connections, see Figure 15.

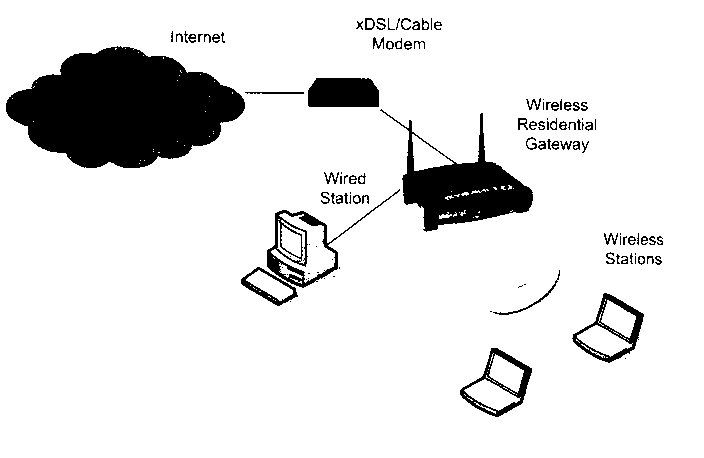


Figure 15

**Wireless Mesh Networks** are currently being developed to extend WLANs to cover larger areas such as towns and cities and provide a reliable wireless infrastructure, see Figure 16.

WLAN mesh routing protocols are required (still proprietary) to route data between the mesh routers such that if one fails others are ready to take over.

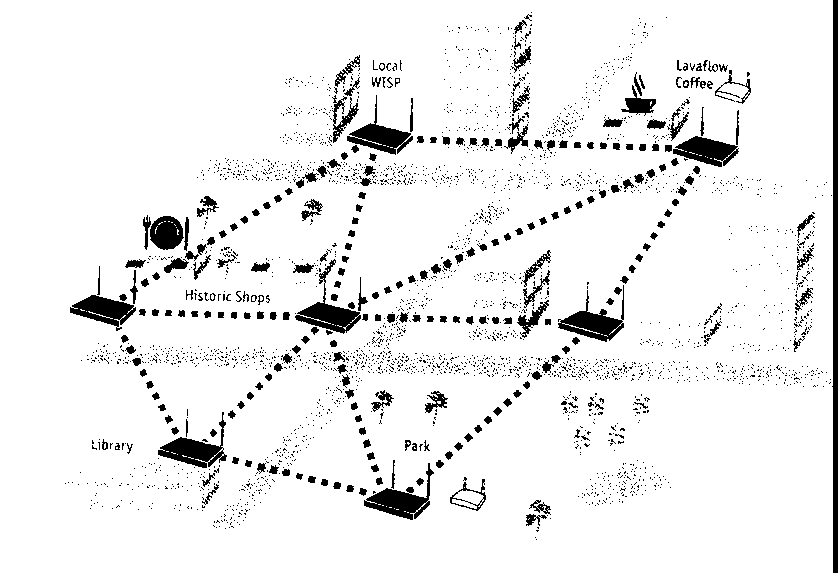


Figure 16

**Broadband Wireless** also called wireless local loop and **WiMax** is currently being developed to a provide a wireless alternative to wired services for Internet access and other WAN applications.. Standardised by the IEEE 802.16 committee, this technology currently provides fixed rather than mobile links with higher speed than IEEE 802.11 and full duplex operation. The mobile version IEEE 802.16e will be ratified soon and provide strong completion for WiFi and 3G mobile.3G mobile phone networks may also be used to link WLAN to the Internet to give more effective access. Some operators now offer 3G/WiFi services depending on location.

*N.B. The Radio Communications Agency (RCA) prohibited the commercial use of the ISM band until recently. Now operators like BT can provide IEEE802.11 WLAN services in public places - and charge for them. Broadband Internet access and Voice over IP services are two Wireless services now being offered by BT and other service providers*

**References**

*White paper on IEEE802.11b 3-COM*

*IEEE.org/getieee802.html*

*What-hackers.pdf*

*CWNA Official Study Guide Osbourne*

**AppendixA 10 ways to wireless security** **[Deb Shinder](mailto:mailroomuk@zdnet.com)** TechRepublic September 30, 2005

Wireless networking is easy to set up, and it's convenient, especially if you like to move around the house or office without your portable computer while staying connected. But because they use the airwaves, wireless communications are more vulnerable to interception and attack than a wired connection. Here are some tips for securing your wireless network.

**1. Use encryption**  
Encryption is the number one security measure, but many wireless access points (WAPs) don't have encryption enabled by default. Although most WAPs support the Wired Equivalent Privacy (WEP) protocol, it's not enabled by default. WEP has a number of security flaws, and a knowledgeable hacker can crack it, but it's better than no encryption at all. Be sure to set the WEP authentication method for "shared key" rather than "open system". The latter does not encrypt the data; it only authenticates the client. Change the WEP key frequently and use 128-bit WEP rather than 40-bit.

**2. Use strong encryption**  
Because of WEP's weaknesses, you should use the Wi-Fi Protected Access (WPA) protocol instead of WEP if possible. To use WPA, your WAP must support it (you may be able to add support to an older WAP with a firmware upgrade); your wireless network access cards (NICs) must support it (again, a firmware update may be necessary); and your wireless client software must support it. Windows XP Service Pack 2 installs the WPA client. SP1 machines can be updated to support WPA by installing the Windows WPA client with the Wireless Update Rollup Package — see this [page](http://support.microsoft.com/kb/826942/).%20) for more details. Another encryption option is to use IPsec, if your wireless router supports it.

**3. Change the default administrative password**  
Most manufacturers use the same default administrative password for all their wireless access points (or at least, all those of a particular model). Those default passwords are common knowledge among hackers, who can use them to change your WAP settings. The first thing you should do when you set up a WAP is change the default password to a strong password (eight characters or more in length, using a combination of alpha and numeric characters, not using words that are in the dictionary).

**4. Turn off SSID broadcasting**  
The Service Set Identifier (SSID) is the name of your wireless network. By default, most WAPs broadcast the SSID. This makes it easy for users to find the network, as it shows up on their list of available networks on their wireless client computers. If you turn off broadcasting, users will have to know the SSID to connect. Some folks will tell you that turning off SSID broadcasting is useless because a hacker can use packet sniffing software to capture the SSID even if broadcasting is turned off. That's true, but why make it easier for them? That's like saying burglars can buy lockpicks, so locking the door is useless. Turning off broadcasting won't deter a serious hacker, but it will protect from the casual "piggybacker" (for example, a next door neighbor who notices the new network and decides to try connecting "just for fun").

**5. Turn off the WAP when not in use**  
This one may seem simplistic, but few companies or individuals do it. If you have wireless users connecting only at certain times, there's no reason to run the wireless network all the time and provide an opportunity for intruders. You can turn off the access point when it's not in use — such as at night when everyone goes home and there is no need for anyone to connect wirelessly.

**6. Change the default SSID**  
Manufacturers provide a default SSID, often the equipment name (such as Linksys). The purpose of turning off SSID broadcasting was to prevent others from knowing the network name, but if you use the default name, it's not too difficult to guess. As mentioned, hackers can use tools to sniff the SSID, so don't change the name to something that gives them information about you or your company (such as the company name or your physical address).

**7. Use MAC filtering**  
Most WAPs (although not some of the cheapest ones) will allow you to use media access control (MAC) address filtering. This means you can set up a "white list" of computers that are allowed to connect to your wireless network, based on the MAC or physical addresses assigned to their network cards. Communications from MAC addresses that aren't on the list will be refused.

The method isn't foolproof, since it's possible for hackers to capture packets transmitted over the wireless network and determine a valid MAC address of one of your users and then spoof the address. But it does make things more difficult for a would-be intruder, and that's what security is really all about.

**8. Isolate the wireless network from the rest of the LAN**  
To protect your wired internal network from threats coming over the wireless network, create a wireless DMZ or perimeter network that's isolated from the LAN. That means placing a firewall between the wireless network and the LAN. Then you can require that in order for any wireless client to access resources on the internal network, he or she will have to authenticate with a remote access server and/or use a VPN. This provides an extra layer of protection.

**9. Control the wireless signal**  
The typical 802.11b WAP transmits up to about 300 feet. However, this range can be extended by a more sensitive antenna. By attaching a high gain external antenna to your WAP, you can get a longer reach but this may expose you to war drivers and others outside your building. A directional antenna will transmit the signal in a particular direction, instead of in a circle like the omni directional antenna that usually comes built into the WAP. Thus, through antenna selection you can control both the signal range and its direction to help protect from outsiders. In addition, some WAPs allow you to adjust signal strength and direction via their settings.

10. Transmit on a different frequency  
One way to "hide" from hackers who use the more common 802.11b/g wireless technology is to go with 802.11a instead. Since it operates on a different frequency (the 5 GHz range, as opposed to the 2.4 GHz range in which b/g operate), NICs made for the more common wireless technologies won't pick up its signals. Sure, this is a type of "security through obscurity" — but it's perfectly valid when used in conjunction with other security measures. After all, security through obscurity is exactly what we advocate when we tell people not to let others know their social security numbers and other identification information. A drawback of 802.11a, and one of the reasons it's less popular than b/g, is that the range is shorter: about half the distance of b/g. It also has difficulty penetrating walls and obstacles. From a security standpoint, this "disadvantage" is actually an advantage, as it makes it more difficult for an outsider to intercept the signal even with equipment designed for the technology.c

**Appendix B IEEE 802.1x**

IEEE802.1x is part of the IEEE802.1 standard family that defines management functionality for IEEE802-based networks.

Designed for securing wired and also wireless networks like the IEEE802.11 WLAN standard 802.1x defines a generic framework that is able to use different authentication mechanisms without implementing these mechanisms outside the backend authentication infrastructure and the client devices.

## Supplicant Module

The acticom IEEE802.1X supplicant software module offers the basic functionality for providing secure authentication for client devices (supplicants in IEEE 802.1X terminology). The supplicant module provides generic interfaces for integration in wired and wireless endsystem target platforms. The supplicant modules provides a system independent EAP-API for accessing external, dynamic loadable EAP authentication modules. The stack is prepared for currently developed 802.1X extensions like compound binding.

## Authenticator Module

an IEEE 802.1X compliant authenticator module provides an implementation ready-to-use for integration in terminal access systems like network switches or wireless access points. Beneath the authenticator functionality the stack also provides RADIUS support for accessing a backend authentication infrastructure. IETF related IEEE802.1X/RADIUS interworking extensions have been included. 802.1X modules are delivered with a command line interface for easy debugging and system integration. It is also used as a management interface for accessing all parameters from the 802.1X-Management Information Base.