Solwise Ltd, www.solwise.co.uk, sales@solwise.co.uk

Wireless Networking Prima

Increased use of laptop computers and the desire to network computers within peoples homes and buildings has, in the last few years, dramatically boosted the development and sales of wireless networking. In turn this has the effect of causing a crash in the prices for wireless products which, of course, has fuelled the increase in popularity even more! ☺ Increased worker mobility have also fuelled the demand for wireless networks for people to use in places like airports, fast food outlets etc

The following is intended as a basic prima covering general aspects of wireless networks. It's a not definitive document and more detained technical notes can be found on our site covering certain specifics in the technology.

So just what is a wireless network?

The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. Usually this refers to wireless LANs however there are now also systems that allow you to network via the mains cabling in your building doing away with the normal LAN cables but they're another story. The introduction, a few years ago, of a set of IEEE 802.11 wireless standards there has now produced a number of affordable wireless solutions that are growing in popularity with business, schools, and home users as well as applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

Types of wireless networks

There are two kinds of wireless networks:

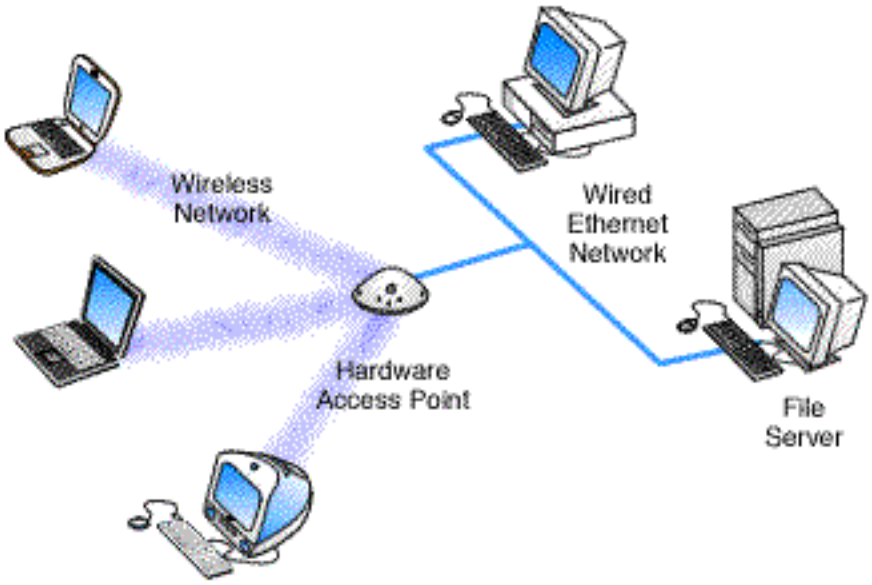
Ad-Hoc Networks

An ad-hoc, or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless you use peering Access Point client to act as a bridge between the wireless network and a LAN port.

An Ad-Hoc or Peer-to Peer Networking.
Each computer with a wireless interface can communicate directly with all of the others.

An Infrastructure wireless Network

A wireless network can also use an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity. In this type on network all wireless communications take place through the Access Point – there is no direct client to client communications.



Access Point.
Wireless connected computers using a Hardware Access Point.

The advantage of a network line this is it allows your wireless LAN clients to communicated with computers on a wired LAN as well.

IEEE 802.11 Standards, frequencies and speeds

The most widely used standard for wireless technology is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE). This is a standard defining all aspects of Radio Frequency Wireless networking. Because most wireless networking hardware supports the 802.11 standard they can inter operate as long as they conform to the same 802.11 standard.

IEEE 802.11 denotes a set of Wireless LAN standards developed by working group 11 of IEEE 802. The term is also used to refer to the original 802.11, which is now sometimes called "802.11legacy".

The 802.11 family currently includes six over-the-air modulation techniques that all use the same protocol, the most popular (and prolific) techniques are those defined by the a, b, and g amendments to the original standard; security was originally included, and was later enhanced via the 802.11i amendment. Other standards in the family (c–f, h–j, n) are service enhancement and extensions, or corrections to previous specifications. 802.11b was the first widely accepted wireless networking standard, followed (somewhat counter intuitively) by 802.11a and 802.11g.

802.11b and 802.11g standards use the unlicensed 2.4 GHz band. The 802.11a standard uses the 5 GHz band. Operating in an unregulated frequency band, 802.11b and 802.11g equipment can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz band.

802.11b

The 802.11b amendment to the original standard was ratified in 1999. 802.11b has a maximum raw data rate of 11 Mbit/s and uses the same CSMA/CA media access method defined in the original standard. Due to the CSMA/CA protocol overhead, in practice the maximum 802.11b throughput that an application can achieve is about 5.9 Mbit/s over TCP and 7.1 Mbit/s over UDP.

802.11b operates in the 2.4 GHz RF spectrum. Hence, metal, water, and thick walls absorb 802.11b signals and decrease the range drastically.

802.11b products appeared on the market very quickly, since 802.11b is a direct extension of the DSSS modulation technique defined in the original standard. Hence, chipsets and products were easily upgraded to support the 802.11b enhancements. The dramatic increase in throughput of 802.11b (compared to the original standard) along with substantial price reductions lead to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to twelve kilometres This is usually done to replace costly leased lines, or in place of very cumbersome microwave communications equipment. Current cards can operate at 11 Mbit/s, but will scale back to 5.5, then 2, then 1, if signal quality becomes an issue.

Extensions have been made to the 802.11b protocol (e.g., channel bonding and burst transmission techniques) in order to increase speed to 22, 33, and 44 Mbit/s, but the extensions are proprietary and have not been endorsed by the IEEE. Many companies call enhanced versions "802.11b+".

Channels and international compatibility

802.11b and 802.11g divide the spectrum into 14 overlapping, staggered channels of 22 megahertz (MHz) each. Channels 1, 6 and 11 (and in some geographic areas channel 14) do not overlap and those channels (or other sets with similar gaps) can be used such that multiple networks can operate in close proximity without interfering with each other.

Channels 10 and 11 are the only channels which work in all parts of the world, because Spain hasn't licensed channels 1 to 9 for 802.11b operation. The full frequency list from IEEE STD 802.11b-1999/Cor 1-2001 is:

Channel	MHz	Europe ETSI X30	Spain X31	France X32	US X10
1	2412	x		x	x
2	2417	x		x	x
3	2422	x		x	x
4	2427	x		x	x
5	2432	x		x	x
6	2437	x		x	x
7	2442	x		x	x
8	2447	x		x	x
9	2452	x		x	x
10	2457	x	x	x	x
11	2462	x	x	x	x
12	2467	x		x	
13	2472	x		x	

802.11a

The 802.11a amendment to the original standard was ratified in 1999. The 802.11a standard uses the same core protocol as the original standard, operates in 5 GHz band, and uses a new modulation technique with a maximum raw data rate of 54 Mbit/s, which yields realistic net achievable throughput in the mid-20 Mbit/s. The data rate is reduced to 48, 36, 34, 18, 12, 9 then 6 Mbit/s if required. 802.11a has 19 channels, 8 dedicated to indoor and 11 to outdoor use.

802.11a products starting shipping in 2001, lagging 802.11b products due to the slow availability of the 5 GHz components needed to implement products. 802.11a has not seen wide adoption because of the high adoption rate of 802.11b, and because of concerns about range: at 5 GHz, 802.11a cannot reach as far as 802.11b at the same power level though this is largely compensated for by permitted higher power levels e.g. the permitted power limit for 2.4GHz operation is 20db BUT, for 5GHz outdoor use the limit is 30db. Other factors such as reduced adsorbtion by water and better scatter are now encouraging people to pay more attention to the 5GHz equipment.

See our article 5GHz Frequency Bands for a more in-depth discussion of 5GHz products and their restrictions.

802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This system also works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 24.7 Mbit/s net throughput like 802.11a. It is fully backwards compatible with b and uses the same frequencies. However, the presence of an 802.11b participant significantly reduces the speed of an 802.11g network.

While 802.11g has the promise of higher throughput, actual results are compromised by a number of factors: conflict with 802.11b-only devices, exposure to the same interference sources as 802.11b, limited numbers of free channels, and the fact that the higher data rates of 802.11g are often more susceptible to interference than 802.11b and simultaneously very reduce signal sensitivities at higher speeds, causing the 802.11g device to reduce the data rate to effectively the same rates used by 802.11b.

A new proprietary feature called Turbo or Super G is now integrated in certain access points. These can boost network speeds up to 108 Mbit/s by using channel bonding. This feature may interfere with other networks and may not support all b and g client cards. In addition, packet bursting techniques are also available in some chipsets and products which will also considerably increase speeds. Again, they may not be compatible with some equipment.

Overview

Standard	Modulation Method	Frequencies	Data Rates Supported (Mbit/s)
802.11b	DSSS, HR-DSSS	2.4 GHz	1, 2, 5.5, 11
"802.11b+" non-standard	DSSS, HR-DSSS (PBCC)	2.4 GHz	1, 2, 5.5, 11, 22, 33, 44
802.11a	OFDM	5.1-5.7 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11g	DSSS, HR-DSSS, OFDM	2.4 GHz	1, 2, 5.5, 11; 6, 9, 12, 18, 24, 36, 48, 54

The IEEE 802.11 standard defines various physical-layer rates for different types of WLANs, such as 1, 2, 5.5 and 11 Mbps for 802.11b and 802.11g. Rates for 802.11g and 11a include 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. The user throughput is less than these link rates for several reasons:

- Each packet includes additional data, such as preambles, headers (MAC, IP, TCP, etc.) and checksums.
- When every directed (unicast) packet is received, the receiver transmits a short acknowledge packet back to the sender. You might also come across some devices quoting speeds of 108Mbps called 11g Turbo or similar. The Turbo system is not *really* 108Mbps. What actually happens is two wireless channels are simultaneously used: One for transmit and one for receive. In this way the devices can simultaneously send and receive data at the same time. Although this won't actually materialize as 108Mbps transfer speed, because the devices don't have to wait for a reply on the same channel there is a significant speed improvement.
- Transmitters wait for short random times between packets to allow other users to contend for and share the channel.

Given these reasons, the theoretical maximum user-level performance for the various 802.11 systems is:

Standard	Wireless Speed	Actual TCP Speed	Actual UDP Speed
802.11b	11 Mbps	5.9 Mbps	7.1 Mbps
802.11g (with 11b compatibility enabled)	54 Mbps	14.4 Mbps	19.5 Mbps
802.11g (11g-only mode)	54 Mbps	24.4 Mbps	30.5 Mbps
802.11gTURBO	108 Mbps	42.9 Mbps	54.8 Mbps
802.11a	54 Mbps	24.4 Mbps	30.5 Mbps

Range

Each access point has a finite range within which a wireless connection can be maintained between the client computer and the access point. The actual distance varies depending upon the environment; manufacturers typically state both indoor and outdoor ranges to give a reasonable indication of reliable performance. Also it should be noted that when operating at the limits of range the performance may drop, as the quality of connection deteriorates and the system compensates.

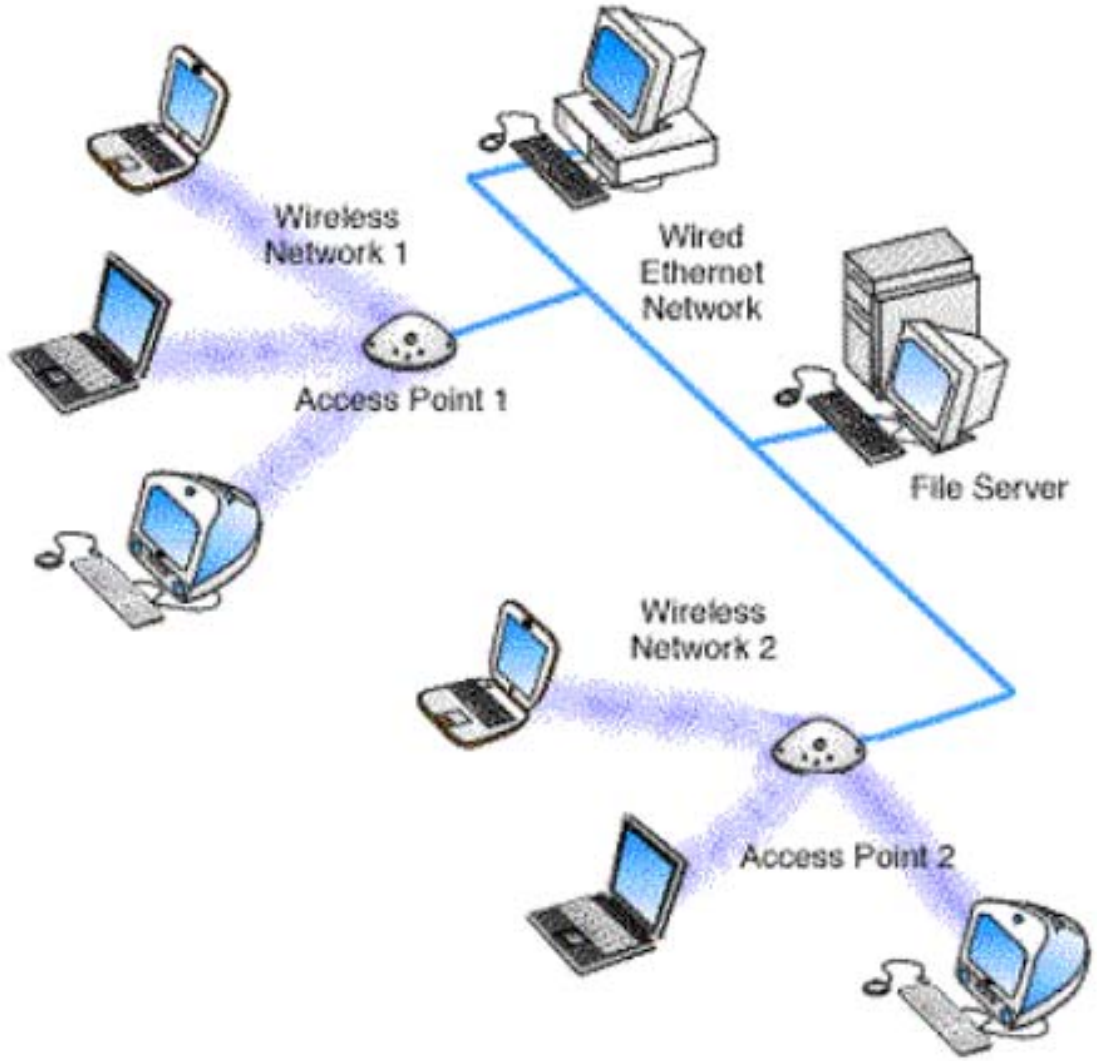
Typical indoor ranges are 150-300 feet, but can be shorter if the building construction interferes with radio transmissions. Longer ranges are possible, but performance will degrade with distance.

Outdoor ranges are quoted up to 1000 feet, but again this depends upon the environment. There are ways to extend the basic operating range of Wireless communications, for example by changing to higher gain

antenna or by using more than a single access point or using a wireless relay /extension point.

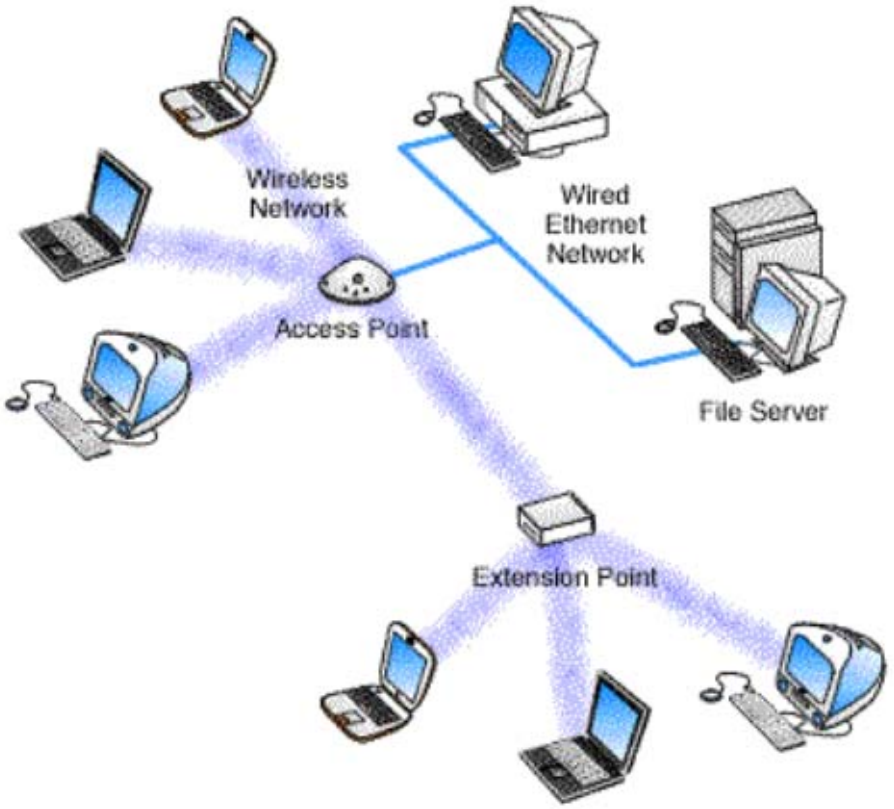
Using multiple access points

In most cases, separate access points can be interconnected via a wired LAN to provide extended wireless connectivity in specific areas such as offices or classrooms and also to allow access to network resources, such as file servers.



Multiple Access Points.
Wireless connected computers using Multiple Access Points.

If a single area is too large to be covered by a single access point, then multiple access points can be used as distinct, separate wireless networks connected by a wired backbone (as shown above). Alternatively you can use a system of wireless repeaters or extensions (see below). When using multiple access points, each access point wireless area should overlap its neighbors. This provides a seamless area for users to move around in using a feature called "roaming".

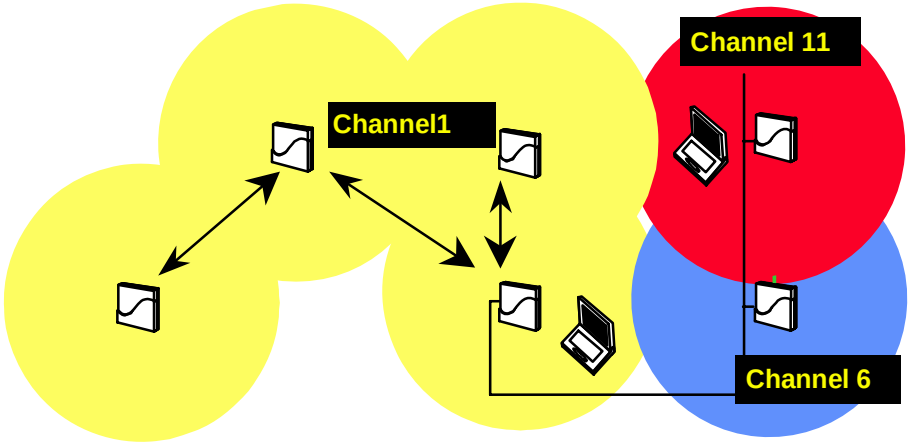


Repeater/Extension Point.
Wireless connected computers using an Access Point with an Extension Point.

Repeaters and WDS

Using a series of Access Points operating as repeaters or extensions offers a potentially painless way of extending a wireless network. Traditional repeating technology was very proprietary with problems with interoperability between different makes or even models of wireless products. The new 802.11 WDS standard now promises a problem free way for repeating technology.

In the diagram below the three access points on the right hand side of the picture are connected by Ethernet cable and hence use a wired distribution system, while the four access points in the left portion are wirelessly connected, and are said to use WDS.



One important aspect of WDS is the fact that a WDS Access Point can assume multiple roles at the same time. It can “drive” a cell (as in wired connected APs), and as such connects wireless clients to the infrastructure, and it can also, simultaneously maintain up to six different wireless connections to other Access Points. For that to be possible the operational (frequency) channel needs to be the same for the cell that is controlled by the AP and for the wireless links to the other APs. In the diagram above this is illustrated by the four cells on the left hand portion of the picture all operating on channel 1.

When to use WDS and when not

WDS offers great flexibility at low cost and as such can be applied in many useful situations. However there are also a few considerations that may lead a user to decide not to use WDS.

Pro's

Cost effective. No additional expense in terms of adding a wireless link to an already installed AP Adding a WDS link merely requires adding an additional AP configured to WDS mode.

Flexible. Expanding an existing wired infrastructure network by adding coverage for office space that is not adjacent to the existing office can be easily achieved, providing great flexibility.

WDS is also an excellent solution to create a roaming network in an area where wired connections between the APs cannot be established.

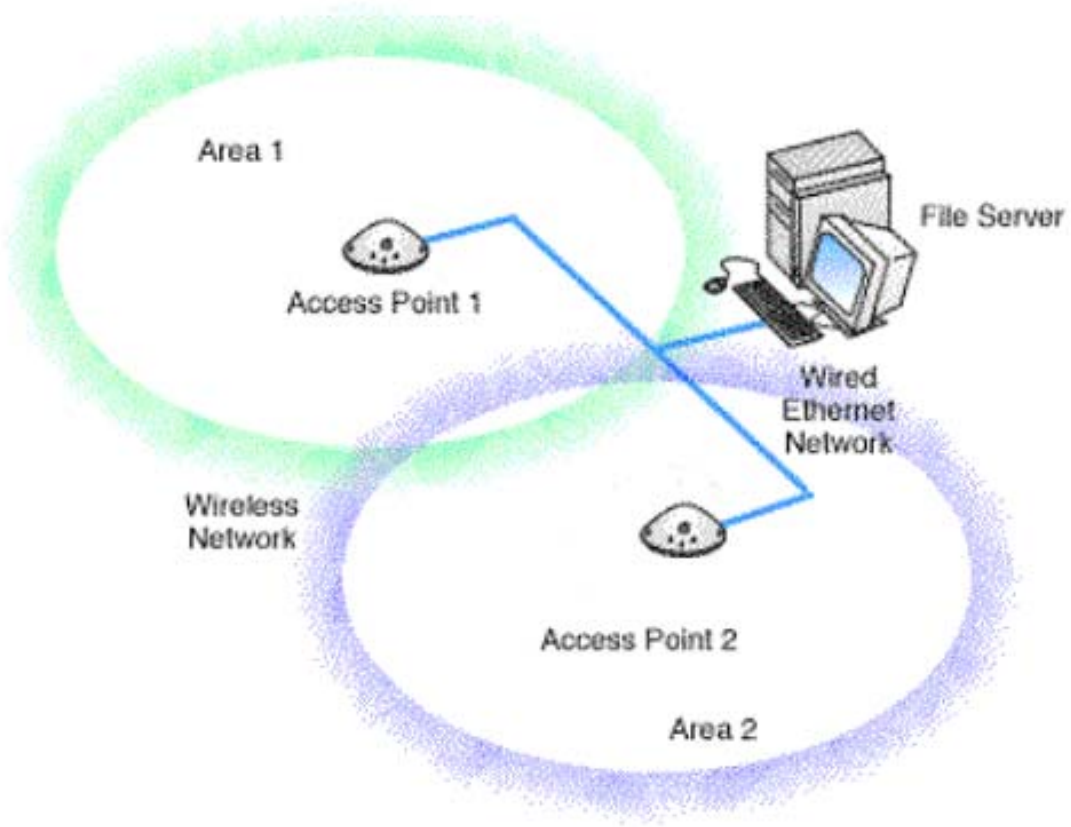
Drawbacks

Performance. As the traffic flow example shows the frame goes through the air three times, and because of the CSMA/CA technology used and the fact that a single radio device (and a single channel) is used at each station, the end-to- end throughput will be about one third of the maximum attainable value. It also has to be remembered that each WDS point needs to get a good quality signal to repeat from. If the source signal is weak or poor quality then the repeating process will be significantly slowed due to frequent packet resends. In some respects, the requirement for a good signal to repeat from can mean increase the number of WDS points required.

Roaming

A wireless computer can "roam" from one access point to another, with the software and hardware maintaining a steady network connection by monitoring the signal strength from in- range access points and locking on to the one with the best quality. Usually this is completely transparent to the user; they are not aware that a different access point is being used from area to area. Some access point configurations require security authentication when swapping access points, usually in the form of a password dialog box.

Access points are required to have overlapping wireless areas to achieve this as can be seen in the following diagram:

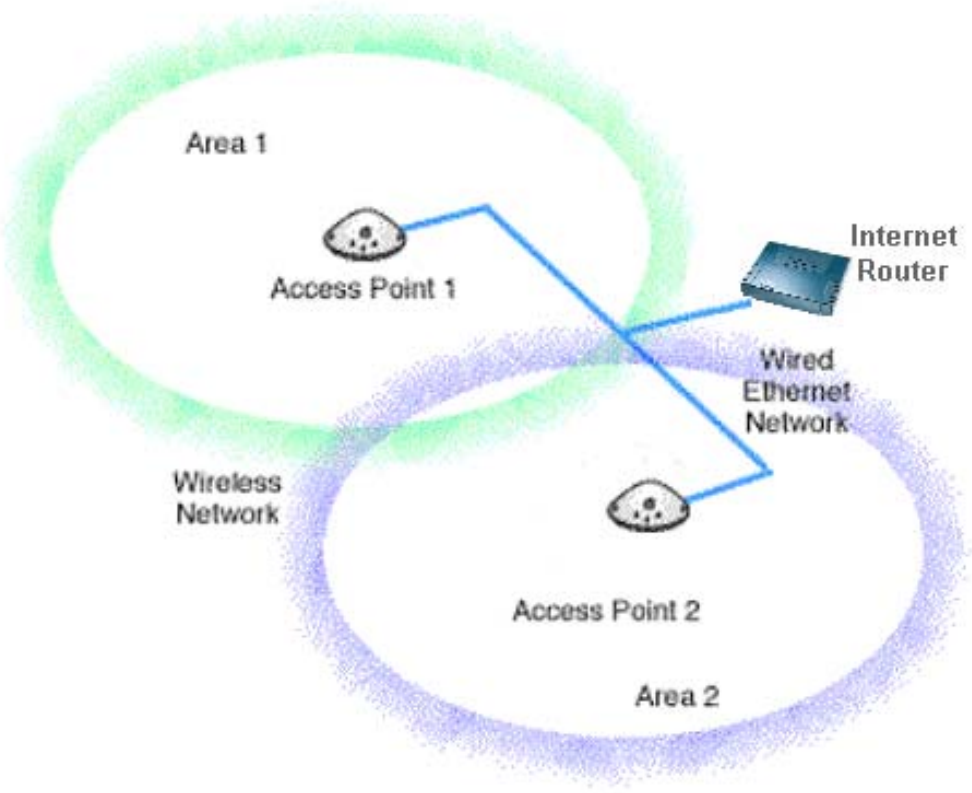


Roaming.

A user can move from Area 1 to Area 2 transparently. The Wireless networking hardware automatically swaps to the Access Point with the best signal.

However there are problems with roaming ☹

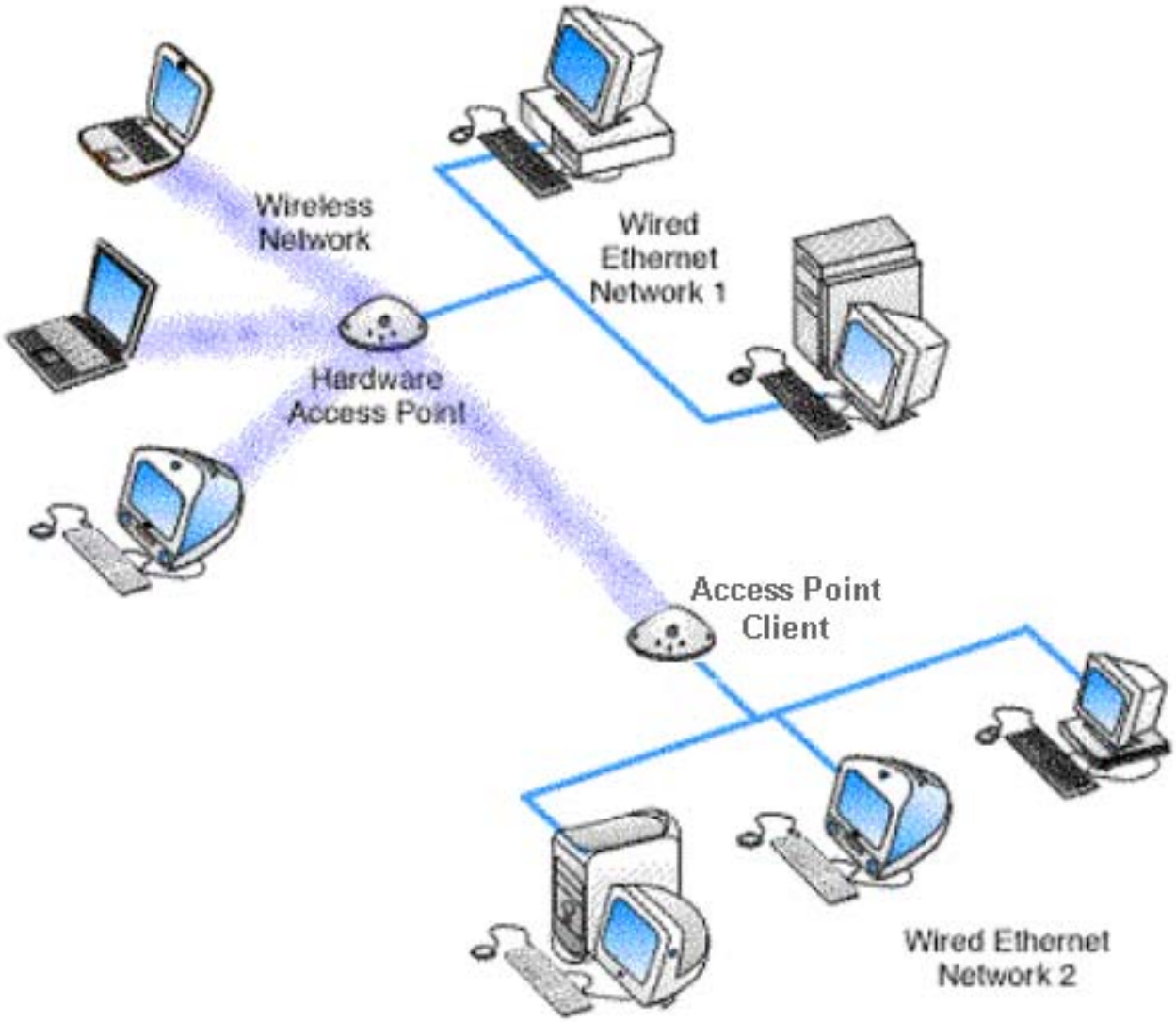
1. Not all access points are capable of being configured to support roaming so check this feature.
2. The second problem is a rather unexpected one and concerns the use of devices like routers or servers on the wired part of a roaming network.



Consider the network above. Now it would be nice to think that you could casually walk, with your wireless laptop, from area 1 to area 2 whilst still maintaining constant internet access through the router. Not so ☹ The reason is all to do with the ARP table in the router. All network products use a thing called an ARP table. The ARP table is a software map which tells each network device where to send it packets of data to in order to reach a specific end user or client. So, in the case above, let's imagine that the router is sending data to Access Point 1 in order to reach your laptop which you are using in Area 1. That's fine. Now you move to Area 2 and now connect to Access Point 2. Problem is the Internet Router doesn't know this! So it carries on sending data for you to Access Point 1. Of course, because you are not there you don't get the data. Also, therefore, the router doesn't get any data acknowledgements back from you via Access Point 1. It's confused ☺ After a while (typically 30-50 seconds) the router realizes something is wrong so it does a broadcast to ALL points asking where you've gone. Of course it then gets a reply from you via Access Point 2 so it then starts talking to you through that point and everything's working again. Problem is though there is this long delay in switching between Access Points. In practice this tends to make roaming a bit of a no go ☹

Using a wireless network to interconnect two LANs

Wireless networking offers a cost-effective solution to users with difficult physical installations such as campuses, hospitals or businesses with more than one location in immediate proximity but separated by public thoroughfare. This type of installation requires two access points. Each access point acts as a bridge between its own LAN to the wireless connection. The wireless connection allows the two access points to communicate with each other, and therefore interconnect the two LAN's.



LAN to LAN Wireless Communications
A Hardware Access Point providing wireless connectivity to local computers and a remote access point client allows LAN-to-LAN connectivity for Wired Ethernet network 2 computers and Wired Network 1 computers.

Note that not all hardware access points have the ability to directly interconnect to another hardware access point. You need to ensure that the AP supports Client mode or specifically states it can bridge to AP's.

Wireless security

Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications.

To protect against any potential security issues, 802.11 wireless communications have a number of security features. These include WEP, WPA, 802.1x, etc… However it seems to be a constant catch-up game between those developing new security measures and toe-rags on the internet publishing systems to break the security ☹ However, don't get too paranoid about wireless security. Okay, if you are a bank sending ultra sensitive data then security is something to worry about. For the rest of us it really isn't that big a deal. It's probably best to implement some form of wireless security on your network but don't loose sleep over it.

The best form on wireless security is to creat ea VPN link.

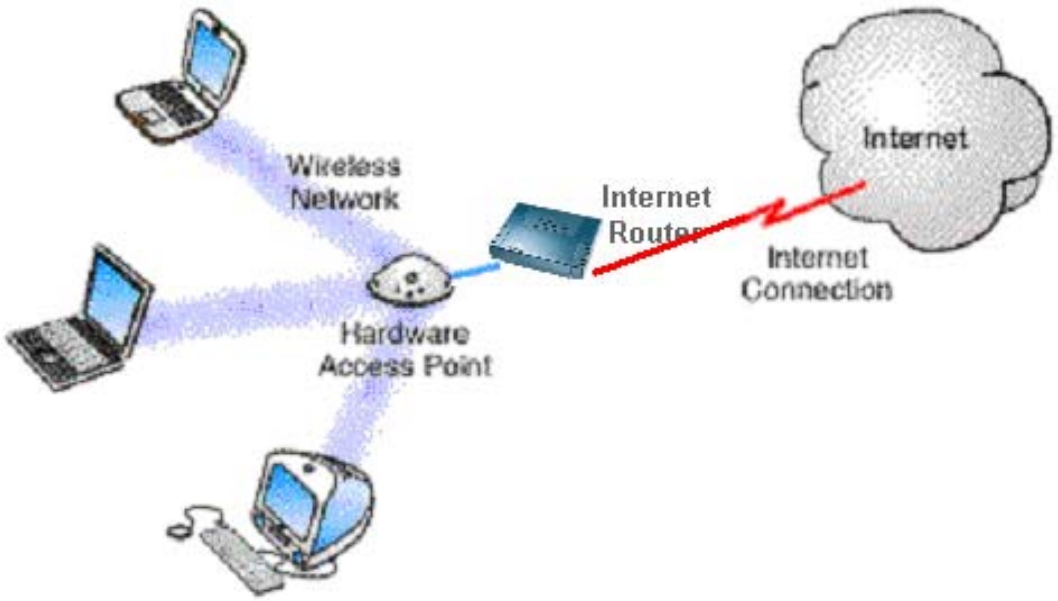
Using a wireless network to share an Internet connection

To share an Internet connection across any LAN (be that wirered or wireless) you need two things:

An Internet sharing hardware device; typically an internet router

A way of network linking your clients (computers) to the router.

If your LAN is wireless then you need an Infrastructure network which either uses a separate Access Point connected to your router or an Internet Router with a built in Access Point:



Hardware Access Point and router.
Wireless connected computers using a Hardware Access Point for shared Internet access.

Additional Reading

See our article Wireless Around the Home for more information on wireless technology within buildings.

For long range and building-to-building operations you have more expensive bridging AP's and high gain, directional antenna giving ranges up to 30Km! (see our article Wireless Technical Discussion for more information on linking building using wireless).

For information on Powerline networking then see

http://www.solwise.co.uk/net-powerline.htm

I've also written a separate article just on 5GHz technology which is worth reading…

5GHz Frequency Bands