



b2bsolutionsgroup

*innovative
spirit™*



WIRELESS NETWORKS

Where Have All the Cables Gone

18th June 2005

What is wireless networking?

The term wireless networking refers to technology that enables computers to communicate using standard network protocols broadcasted on a radio frequency instead of cables. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs or WLAN's. This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11 (in the form of 802.11g, 802.11b and 802.11a), has produced a number of affordable wireless solutions that are growing in popularity with homes, business and schools as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

Are all wireless networks compatible?

Not all 802.11 networks are compatible. Knowing these simple rules will help you build a compatible network. 802.11b and 802.11g use the 2.4GHz radio frequency spectrum as 802.11a use the 5GHz spectrum. 802.11a and 802.11g networks are both 54 Mbps however they do not use the same spectrum; therefore they are not compatible. 802.11b networks are compatible with 802.11g networks. 802.11b are 11 Mbps and also come in turbo mode of 22 Mbps.

What is a wireless network made up of?

There are two kinds of wireless networks:

Ad-Hoc or Peer-to-Peer Networking.

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 one of the computers acts as a bridge to the wired LAN using special software and/or additional hardware to connect to the wired LAN.

Infrastructure Networking.

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 the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.

There are two types of access points:

Dedicated Hardware Access Points (HAP), that offer comprehensive support of wireless features, and are usually used as an extension of a wired network, providing additional access in remote areas or providing for a mobile workforce.

Integrated Access Points are multi functional devices which include features not commonly found in access points, such as integrated PPPoE support and extensive configuration flexibility. Generally they provide both wired and wireless access in one unit. With appropriate networking support, users on the wireless LAN can share files and printers located on the wired LAN and vice versa. All current configurations provide total support of the TCP/IP protocol.

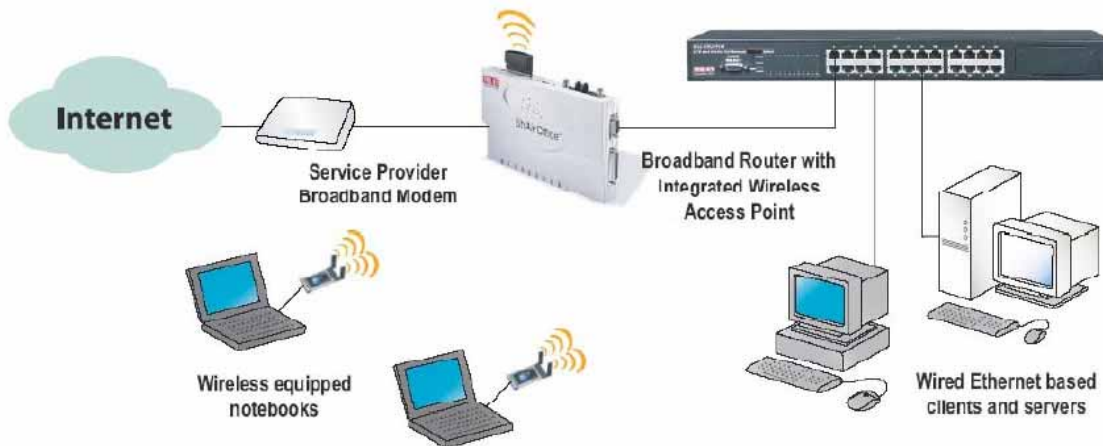
Hardware Access Point

Wireless connected computers using a Hardware Access Point.



Integrated Access Point

Wireless connected computers using an Integrated Access Point.





What is IEEE 802.11?

The Institute of Electrical and Electronic Engineers (IEEE) forms workgroups from technical experts in the field. The 802.11 group was created to bring standard based means of communications to wireless devices using the free unlicensed frequencies of 2.4GHz and 5.4GHz.

Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as data transmission. The more commonly known standards include 802.11a, b and g. 802.11b wireless access points have a majority of the marketing place but that will soon change due to the release of inexpensive 802.11g access points.

Can I mix wireless equipment from different manufacturers?

Most wireless networking hardware vendors support the 802.11 standards today, and can interoperate with each other. Within a short time we have seen all new wireless cards, like Ethernet cards, become inexpensive, ubiquitous of standardizing on 802.11b/g and totally interoperable.

What is the range of a wireless network?

Distance is affected by the speed desired, obstructions and radio interference. 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 350-700 metres, 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 2.5km, but again this depends upon the environment.

There are ways to extend the basic operating range of wireless communications, by using more than a single access point or using a wireless relay or extension point.

How many wireless networked computers can use a single access point?

This depends upon the manufacturer. Some hardware access points limit to 10, however newer models will support up to 255 wireless connections. This is a shared media, using more computers than recommended will cause performance and reliability to suffer.

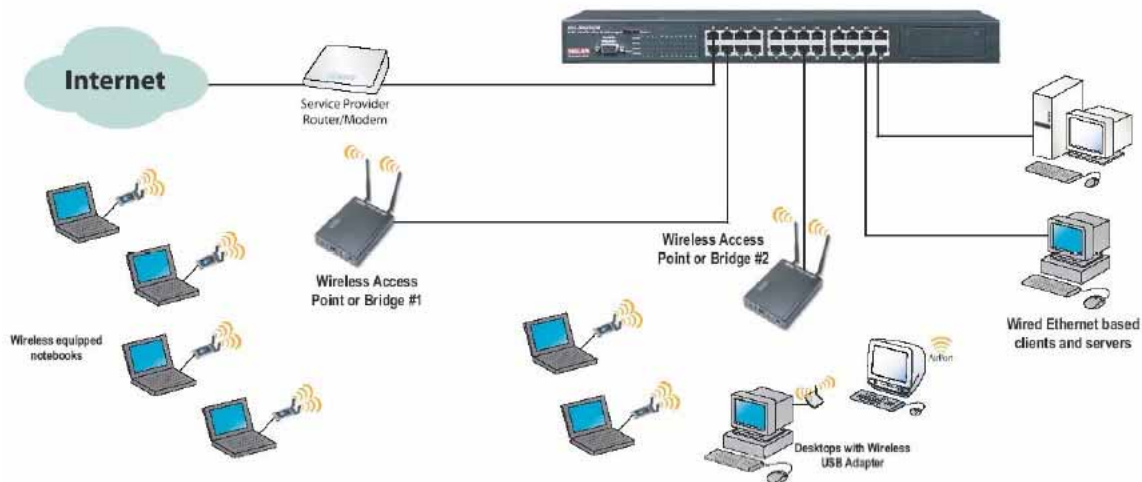
Can I have more than one access point?

Yes, multiple access points can be connected to a wired LAN, or sometimes even to a second wireless LAN if the access point supports this.

In most cases, separate access points are interconnected via a wired LAN, providing wireless connectivity in specific areas such as offices or classrooms, but connected to a main wired LAN for 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. When using multiple access points, each access point wireless area should overlap its neighbours. This provides a seamless area for users to move around in using a feature called "roaming."

What is Roaming?

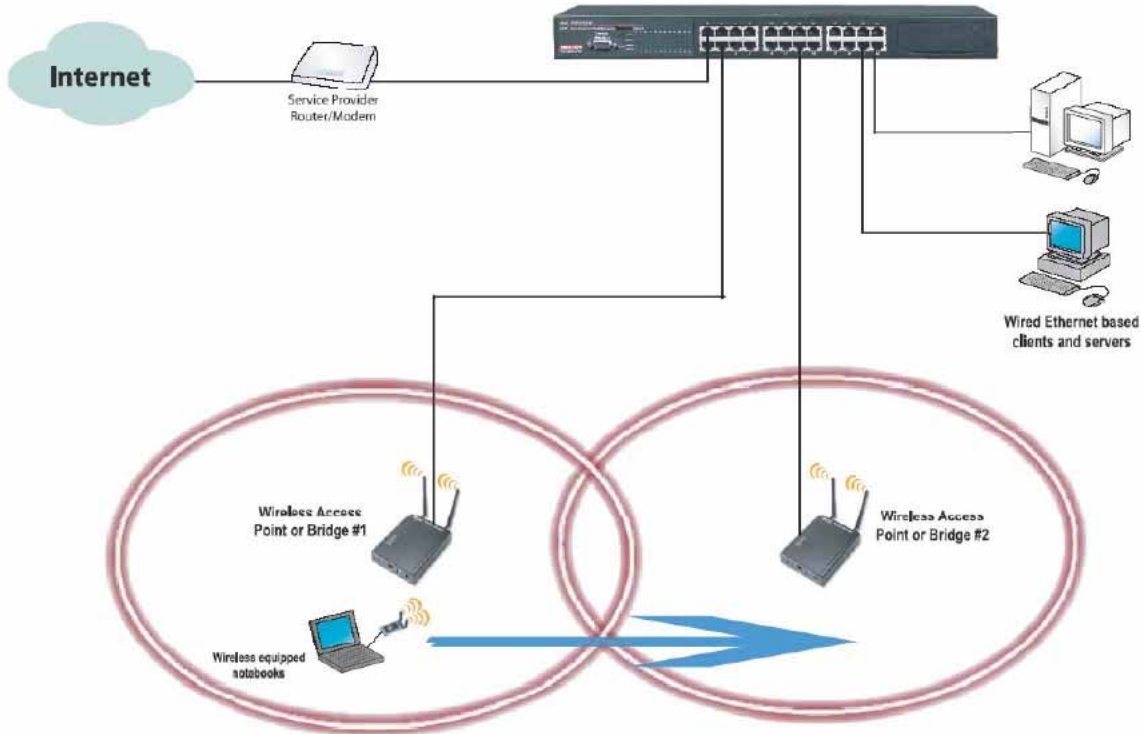
A wireless computer can "roam" from one access point to another, with the software and hardware maintaining a steady network connection by monitoring the signal strength from in-range access points and locking on to the one with the best quality. Usually this is completely transparent to the user; they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

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.



Not all access points are capable of being configured to support roaming. Also note that access points from a single vendor should be used when implementing roaming, as there is no official standard for this feature.

Can I use a wireless network to interconnect two LANs?

Yes. 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. There are two types of bridging, point to point and point to multipoint. This type of installation requires two or more access points. Each access point acts as a bridge or router connecting its own LAN to the wireless connection. The wireless connection allows the two or more access points to communicate with each other, and therefore interconnecting the two LAN's.

WLAN bridging connections can be significantly less costly and a much faster installation compared to time consuming permit process and trenching needed for installing fiber. Antennas are often used to increase the range of your WLAN systems, but proper antenna selection can also enhance the security of your WLAN. Using a directional antenna will decrease the chances of signal interception. Some bridges support repeater mode; repeater mode is used to extend the length of your WLAN bridge.



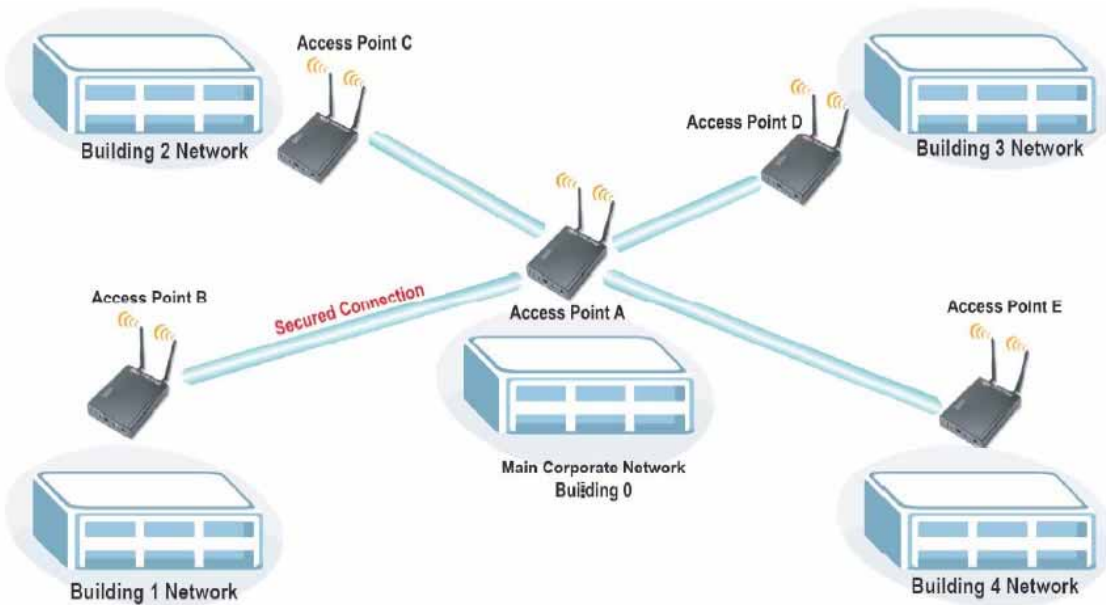
Point to Point

Wireless connecting two buildings in point to point mode.



Point to Multipoint

Wireless connecting two or more buildings in point to multipoint mode.



Repeater mode

Wireless connecting two buildings with a repeater.



Is it true that wireless networking is only good for laptop computers?

Although wireless networking offers obvious benefits to users of laptops who move from location to location throughout the day, there are benefits for users of fixed position computers as well.

Many locations have unsuitable building layouts or walls that cannot be wired for various reasons making it difficult or impossible to build a wired network. Wireless networking in these environments is a very cost effective alternative also providing future flexibility.

In cases where a small number of computers are separated from a main network, a wireless link may be more cost effective than network cabling although the latter is perfectly feasible.

Temporary wireless LANs can easily be created for exhibitions, school or business projects, all without any cabling.

What about 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. However, 802.11 wireless communications cannot be received --much less decoded-- by simple scanners, short wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all. However, eavesdropping is possible using specialized equipment.

To protect against any potential security issues, 802.11 wireless communications have a function called WEP (Wired Equivalent Privacy), a form of encryption which provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels. This security protocol is available in 40 bit to 512 bit encryption. Most access points and interface providers offer these protocols.

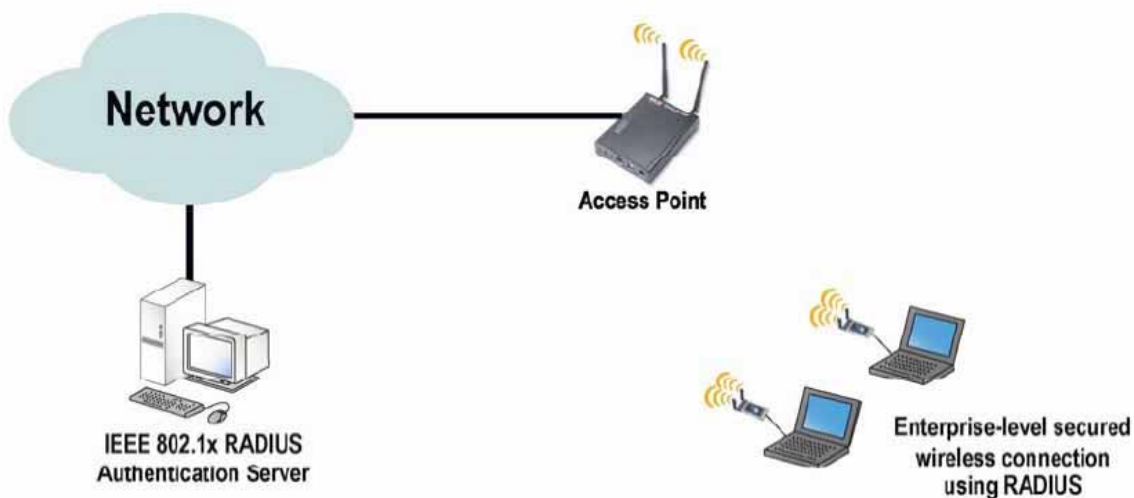
The Wi-Fi Alliance is developing its own standard known as Wi-Fi Protected Access (WPA). Wi-Fi Protected Access was developed to eliminate the vulnerabilities of WEP. WPA is based on the 802.11i draft standard and will work on existing access points and client cards. 802.11i standard was designed to improve the security of WLAN's. The standard is based around 802.1x port based authentication for both users and devices. The standard includes Wi-Fi Protected Access (WPA) and Robust Security Network (RSN).

WPA uses Temporal Key Integrity Protocol (TKIP) as the protocol and algorithm to improve security of keys used with WEP. It changes the way keys are derived and rotates keys more often for security. It also adds a message-integrity-check function to prevent packet forgeries. RSN uses dynamic negotiation of authentication and encryption algorithms between access points and mobile devices. The authentication schemes proposed in the draft standard are based on 802.1X and Extensible Authentication Protocol (EAP). The encryption algorithm is Advanced Encryption Standard (AES).

Wireless network using WEP or WPA



Wireless network using 802.1x security



Conclusion

Wireless networking has become a widely used technology. Wireless not only adds mobility but provides an alternate solution for LAN's and WAN's instead of expensive cabling. Whether you're installing a simple access point or linking two or more buildings several miles apart wireless networking may be a more reasonable solution. Most vendors are Wi-Fi compatible; following the 802.11 standards ensuring interoperability and lowering the total cost of ownership for your network.

For further information on wireless networks and professional advice please contact us directly and our friendly IT team will answer all your questions.

B2B Solutions Group Limited
5 Collingwood Street
PO Box 10013
Hamilton, NZ
Phone: 07 958 4422
Facsimile: 07 958 2041
E-mail: business@b2bsolutions.co.nz
Web: www.b2bsolutions.co.nz

