

What is wireless networking? How does it work?

A wireless network uses radio signals or microwaves to broadcast data and information. Rather than being transmitted through traditional coaxial, CAT5 Ethernet or other standard wired methods, the data is beamed out over the airwaves.

Wireless networks offer advantages for some. Users with personal digital assistant (PDA) handhelds such as Palm Pilots, Wi-Fi enabled cell phones, or users with laptops can use wireless technology to allow them the convenience to move about while maintaining their network connectivity. Another pro is the ability for users to network desktop computers at various locations without having to deal with the hassle or expense of running a wired connection to that spot.

There are some cons as well. First, most wired networks operate at 100mbps, and many organizations have upgraded to the newer standard of 1gbps. In contrast, a large percentage of wireless networks operate at 11mbps, roughly equivalent to the old wired speed of 10mbps. Most wireless network equipment available today is compatible with both 802.11b and the faster 802.11g which operates at speeds up to 54mbps. There is also a new, emerging wireless network standard, 802.11n, which theoretically increases both the speed and the range of the wireless network.

Wireless network speeds are affected by obstructions such as walls and floors. Most wireless network equipment, for consumers in particular, also operates in the 2.4Ghz frequency range. This is the same range as other household devices such as cordless phones, baby monitors, etc. The interference from these devices, as well as microwave ovens and other electrical interference can greatly impact the range, speed and quality of your wireless network.

Question: How fast is wireless computer networking?

Answer: The speed of a wireless network depends on several factors.

First, wireless local area networks (WLANs) feature differing levels of performance depending on which Wi-Fi standard they support. 802.11b WLANs offer maximum theoretical bandwidth of **11 Mbps**. 802.11a and 802.11g WLANs offer theoretical bandwidth up to **54 Mbps**. (In contrast, typical wired Ethernets run at 100 Mbps.)

The performance of Wi-Fi networks in practice never approaches the theoretical maximum. 802.11b networks, for example, generally operate no faster than about 50% of theoretical peak, or **5.5 Mbps**. Likewise, 802.11a and 802.11g networks generally run no faster than **20 Mbps**. The disparity between theoretical and practical performance comes from protocol overhead, signal interference, and decreasing signal distance with distance. In addition, the more devices communicating on a WLAN simultaneously, the slower the network will appear.

On home networks, keep in mind that the performance of an Internet connection is often the limiting factor in network speed. Even though files can be shared on a wireless LAN at speeds of 5 or 20 Mbps, wireless clients will still connect to the Internet at the speed typically offered by Internet Service Providers, usually **less than 1 Mbps**.

Finally, wireless network technology is capable of more speed than what Wi-Fi supports today. Industry vendors continue to develop improved technologies like 802.16 WiMAX that offer wireless communications with faster speeds and longer range.

Question: What hardware is required to build a wireless network?

Answer: Wireless network adapters (also known as wireless NICs or wireless network cards) are required for each device on a wireless network. Some newer laptop computers incorporate wireless adapters as a built-in feature of the system. Separate add-on adapters must be purchased for most computers, however.

Popular wireless network adapters for PCs exist in the form of a PCMCIA "credit card." Macintosh computers use the distinctive AirPort card. USB wireless adapters that do not resemble cards also exist.

Strictly speaking, no wireless hardware other than adapters is required to build a small wireless LAN (WLAN). However, to increase the performance of a WLAN, accommodate more computers, and increase the network's range, wireless access points and/or wireless routers can be deployed.

Wireless routers function comparably to traditional routers for wired networks. One generally deploys wireless routers when building an all-wireless network from the ground up.

An alternative to routers, access points allow wireless networks to join an existing wired network. One typically deploys access points when growing a network that already has a wired switch or router installed. In home networking, a single access point (or router) possesses sufficient range to span most homes. Businesses in office buildings often must deploy multiple access points and/or routers.

Access points and routers often utilize a wireless antenna that significantly increase the communication range of the wireless radio signal. These antennas are optional and removable on most equipment. It's also possible to mount antennas on wireless clients to increase the range of wireless adapters. This is common practice for wardrivers, but add-on antennas are generally not required in typical home or business networks.

Question: Are Wireless Networks Secure?

No computer network is truly secure, but how does wireless network security stack up to that of traditional wired networks?

Answer: Unfortunately, no computer network is truly secure. It's always theoretically possible for eavesdroppers to view or "snoop" the traffic on any network, and it's often possible to add or "inject" unwelcome traffic as well. However, some networks are built and managed much more securely than others. For both wired and wireless networks alike, the real question to answer becomes - is it secure enough?

Wireless networks add an extra level of security complexity compared to wired networks. Whereas wired networks send electrical signals or pulses of light through cable, wireless radio signals propagate through the air and are naturally easier to intercept. Signals from most wireless LANs (WLANs) pass through exterior walls and into nearby streets or parking lots.

Network engineers and other technology experts have closely scrutinized wireless network security because of the open-air nature of wireless communications. The practice of wardriving, for example, exposed the vulnerabilities of home WLANs and accelerated the pace of security technology advances in home wireless equipment.

Overall, conventional wisdom holds that wireless networks are now "secure enough" to use in the vast majority of homes, and many businesses. Security features like 128-bit WEP and WPA can scramble or "encrypt" network traffic so that its contents can not easily be deciphered by snoopers. Likewise, wireless routers and access points (APs) incorporate access control features such as MAC address filtering that deny network requests from unwanted clients.

Obviously every home or business must determine for themselves the level of risk they are comfortable in taking when implementing a wireless network. The better a wireless network is administered, the more secure it becomes. However, the only truly secure network is the one never built!