Wireless Networks

Conventional Ethernet networks require cables connected computers via hubs and switches. This has the effect of restricting the computer's mobility and requires that even portable computers be physically connected to a hub or switch to access the network. An alternative to cabled networking is wireless networking. The first wireless network was developed at the University of Hawaii in 1971 to link computers on four islands without using telephone wires. Wireless networking entered the realm of personal computing in the 1980s, with the advent to networking computers. However, it was only in the early 1990s that wireless networks started to gain momentum when CPU processing power became sufficient to manage data transmitted and received over wireless connections. Wireless networks use network cards, called Wireless Network Adapters, that rely radio signals or infrared (IR) signals to transmit and receive data via a Wireless Access Point (WAP). The WAP uses has an RJ-45 port that can be attached to attach to a 10BASE-T or 10/100BASE-T Ethernet hub or switch and contains a radio transceiver, encryption, and communications software. It translates conventional Ethernet signals into wireless Ethernet signals it broadcasts to wireless network adapters on the network and performs the same role in reverse to transfer signals from wireless network adapters to the conventional Ethernet network. WAP devices come in many variations, with some providing the Cable Modem Router and Switch functions in addition to the wireless connectivity. Note: Access points are not necessary for direct peer-to-peer networking, which is called ad hoc mode, but they are required for a shared Internet connection or a connection with another network. When access points are used, the network is operating in the infrastructure mode. Wireless Network Standards In the absence of an industry standard, the early forms of wireless networking were single-vendor proprietary solutions that could not communicate with wireless network products from other vendors. In 1997, the computer industry developed the IEE 802.11 wireless Ethernet standard. Wireless network products based on this standard are capable of multivendor interoperability. The IEEE 802.11 wireless Ethernet standard consists of the IEEE 802.11b standard, the IEEE 802.11a standard, and the newer IEEE 802.11g standard. Note: The Bluetooth standard for short-range wireless networking is designed to complement, rather than rival, IEEE 802.11-based wireless networks. . IEEE 802.11 was the original standard for wireless networks that was ratified in 1997. It operated at a maximum speed of 2 Mbps and ensured interoperability been wireless products from various vendors. However, the standard had a few ambiguities allowed for potential problems with compatibility between devices. To ensure compatibility, a group of companies formed the Wireless Ethernet Compatibility Alliance (WECA), which has come to be known as the Wi-Fi Alliance, to ensure that their products would work together. The term Wi-Fi is now used to refer to any IEEE 802.11 wireless network products that have passed the Wi-Fi Alliance certification tests. . IEEE 802.11b, which is also called 11 Mbps Wi-Fi, operates at a maximum speed of 11 Mbps and is thus slightly faster than 10BASE-T Ethernet. Most IEEE 802.11b hardware is designed to operate at four speeds, using three different data-encoding methods depending on the speed range. It operates at 11 Mbps using quatenery phase-shift keying/complimentary code keying (QPSK/CCK); at 5.5 Mbps also using QPSK/CCK; at 2 Mbps using differential quaternary phase-shift keying (DQPSK); and at 1 Mbps using differential binary phase-shift keying (DBPSK). As distances change and signal strength increases or decreases, IEEE 802.11b hardware switches to the most suitable data-encoding method. Wireless networks running IEEE 802.11b hardware use the 2.4 GHz radio frequency band that many portable phones, wireless speakers, security devices, microwave ovens, and the Bluetooth short-range networking products use. Although the increasing use of these products is a potential source of interference, the short range of wireless networks (indoor ranges up to 300 feet and outdoor ranges up to 1,500 feet, varying by product) minimizes the practical risks. Many devices use a spread-spectrum method of connecting with other products to minimize potential interference. IEEE 802.11b networks can connect to wired Ethernet networks or be used as independent networks. . IEEE 802.11a uses the 5 GHz frequency band, which allows for much higher speeds, reaching a maximum speed of 54 Mbps. The 5 GHz frequency band also helps avoid interference from devices that cause interference with lower-frequency IEEE 802.11b networks. IEEE 802.11a hardware maintains relatively high speeds at both short and relatively long distances. Because IEEE 802.11a uses the 5 GHz frequency band rather than the 2.4 GHz frequency band used by IEEE 802.11b, standard IEEE 802.11a hardware cannot communicate with 802.11b hardware. A solution to this compatibility problem is the use of dual-band hardware. Dual-band hardware can work with either IEEE 802.11a or IEEE 802.11b networks, enabling you to move from an IEEE 802.11b wireless network at home or at Starbucks to a faster IEEE 802.11a office network. . IEEE 802.11g is also known as Wireless-G and combines compatibility with IEEE 802.11b with the speed of IEEE 802.11a at longer distances. This standard was ratified in mid-2003, however, many network vendors were already selling products based on the draft IEEE 802.11g standard before the final standard was approved. These early IEEE 802.11g hardware was slower and less compatible than the specification promises. In some cases, problems with early-release IEEE 802.11g hardware can be solved through firmware upgrades. Wireless Network Modes Wireless networks work in one of two modes that are also referred to as topologies. These two modes are ad-hoc mode and infrastructure mode. The mode you implement depends on whether you

want your computers to communicate directly with each other, or via a WAP. . In ad-hoc mode, data is transferred to and from wireless network adapters connected to the computers. This cuts out the need to purchase a WAP. Throughput rates between two wireless network adapters are twice as fast as when you use a WAP. However, a network in ad-hoc mode cannot connect to a wired network as a WAP is required to provide connectivity to a wired network. An ad-hoc network is also called a peer-to-peer network. . In infrastructure mode, data is transferred between computers via a WAP. Because a WAP is used in infrastructure mode, it provides connectivity with a wired network, allowing you to expand a wired network with wireless capability. Your wired and wirelessly networked computers can communicate with each other. In addition, a WAP can extend your wireless network's range as placing a WAP between two wireless network adapters doubles their range. Also, some WAPs have a built-in router and firewall. The router allows you to share Internet access between all your computers, and the firewall hides your network. Some of these multifunction access points include a hub with RJ-45 ports. Security Features Because wireless networks can be accessed by anyone with a compatible wireless network adapter, most models of wireless network adapters and WAPs provide for encryption options. Some devices with this feature enable you to set a security code known as an SSID on the wireless devices on your network. This seven-digit code prevents unauthorized users from accessing your network and acts as an additional layer of security along with your normal network authentication methods, such as user passwords. Other wireless network adapters and WAPs use a list of authorized MAC numbers to limit access to authorized devices only. All Wi-Fi products support at least 40-bit encryption through the wired equivalent privacy (WEP) specification, but the minimum standard on newer products is 64-bit WEP encryption. Many vendors also offer 128-bit or 256-bit encryption on some of their products. However, the WEP specification is insecure. It is vulnerable to brute-force attacks at shorter key lengths, and it is also vulnerable to differential cryptanalysis attacks, which is the process of comparing an encrypted text with a known portion of the plain text and deriving the key by computing the difference between them. Because WEP encrypts TCP headers, hackers know what the headers should contain in many cases, and they can attempt to find patterns in a large body of collected WEP communications in order to decrypt the key. The attack is complex and difficult to automate, so it is unlikely to occur for most networks, especially at key lengths greater than 128 bits. Furthermore, WEP does not prevent an intruder from attaching a hidden WAP on the network and using it to exploit the network. New network products introduced in 2003 and beyond now incorporate a new security standard known as Wi-Fi Protected Access (WPA). WPA is derived from the developing IEEE 802.11i security standard, which will not be completed until mid-decade. WPA-enabled hardware works with existing WEP-compliant devices, and software upgrades might be available for existing devices.