Wireless Local-Area Networking

What Is Wireless Local-Area Networking?

In the simplest of terms, a wireless local-area network (WLAN) does exactly what the name implies: it provides all the features and benefits of traditional LAN technologies such as Ethernet and Token Ring without the limitations of wires or cables. But to view a WLAN just in terms of the cables it does not have is to miss the point: WLANs redefine the way we view LANs. Connectivity no longer implies attachment. Local areas are measured not in feet or meters, but miles or kilometers. An infrastructure need not be buried in the ground or hidden behind the walls—an "infrastructure" can move and change at the speed of the organization. This technology has several immediate applications, including:

- IT professionals or business executives who want mobility within the enterprise, perhaps in addition to a traditional wired network
- Business owners or IT directors who need flexibility for frequent LAN wiring changes, either throughout the site or in selected areas
- Any company whose site is not conducive to LAN wiring because of building or budget limitations, such as older buildings, leased space, or temporary sites
- Any company that needs the flexibility and cost savings offered by a line-of-sight, building-to-building bridge to avoid expensive trenches, leased lines, or right-of-way issues

Current vertical markets include:
- Education
- Finance
- Health care
- Hospitality and retail
- Manufacturing and industrial

WLANs use a transmission medium, just like wired LANs. Instead of using twisted-pair or fiber-optic cable, WLANs use either infrared light (IR) or radio frequencies (RF). Of the two, RF is far more popular for its longer-range, higher-bandwidth, and wider coverage. Most wireless LANs today use the 2.4-gigahertz (GHz) frequency band, the only portion of the RF spectrum reserved around the world for unlicensed devices. The freedom and flexibility of wireless networking can be applied both within buildings and between buildings.

In-Building WLANs

WLAN technology can take the place of a traditional wired network or extend its reach and capabilities. Much like their wired counterparts, in-building WLAN equipment consists of PC Card, Personal Computer Interface (PCI), and Industry-Standard Architecture (ISA) client adapters, as well as access points[1], which perform functions similar to wired networking hubs. Similar to wired LANs for small or temporary installations, a WLAN can be arranged in a peer-to-peer or ad hoc topology[2] using only client adapters.

---

1. A wireless LAN transceiver that acts as a hub, and bridges between wireless and wired networks.
2. A wireless network composed only of stations without access points.

CISCO SYSTEMS

For added functionality and range, access points can be incorporated to act as the center of a star topology and function as a bridge to an Ethernet network as well.

Within a building, wireless enables computing that is both mobile and connected. With a PC Card client adapter installed in a notebook or hand-held PC, users can move freely within a facility while maintaining access to the network.

Applying wireless LAN technology to desktop systems provides an organization with flexibility impossible with a traditional LAN. Desktop client systems can be located in places where running cable is impractical or impossible. Desktop PCs can be redeployed anywhere within a facility as frequently as needed, making wireless ideal for temporary workgroups and fast-growing organizations.

Building-to-Building WLANs
In much the same way that a commercial radio signal can be picked up in all sorts of weather miles from its transmitter, WLAN technology applies the power of radio waves to truly redefine the "local" in LAN. With a wireless bridge, networks located in buildings miles from each other can be integrated into a single local-area network. When bridging between buildings with traditional copper or fiber-optic cable, freeways, lakes, and even local governments can be impassible obstacles. A wireless bridge makes them irrelevant, transmitting data through the air and requiring no license or right of way.

Without a wireless alternative, organizations frequently resort to wide area networking (WAN) technologies to link together separate LANs. Contracting with a local telephone provider for a leased line presents a variety of drawbacks. Installation is typically expensive and rarely immediate. Monthly fees are often quite high for bandwidth that by LAN standards is very low. A wireless bridge can be purchased and then installed in an afternoon for a cost that is often comparable to a T1 installation charge alone. Once the investment is made, there are no recurring charges. And today's wireless bridges provide the bandwidth one would expect from a technology rooted in data, rather than voice, communications.

The Wireless LAN Standard
In the wired world, Ethernet has grown to become the predominant LAN technology. Its evolution parallels, and indeed foreshadows, the development of the wireless LAN standard. Defined by the Institute of Electrical and Electronics Engineers (IEEE) with the 802.3 standard, Ethernet provides an evolving, high-speed, widely available and interoperable networking standard. It has continued to evolve to keep pace with the data rate and throughput requirements of contemporary LANs. Originally providing for 10 megabit per second (Mbps) transfer rates, the Ethernet standard evolved to include the 100 Mbps transfer rates required for network backbones and bandwidth-intensive applications. The IEEE 802.3 standard is open, decreasing barriers to market entry and resulting in a wide range of suppliers, products, and price points from which Ethernet users can choose. Perhaps most importantly, conformance to the Ethernet standard allows for interoperability, enabling users to select individual products from multiple vendors while secure in the knowledge that they will all work together.

The first wireless LAN technologies were low-speed (1-2 Mbps) proprietary offerings. Despite these shortcomings, the freedom and flexibility of wireless allowed these early products to find a place in vertical markets such as retail and warehousing where mobile workers use hand-held devices for inventory management and data collection. Later, hospitals applied wireless technology to deliver patient information right to the bedside. And as computers made their way into the classrooms, schools and universities began installing wireless networks to avoid cabling costs and share Internet access. The pioneering wireless vendors soon realized that for the technology to gain broad market acceptance, an Ethernet-like standard was needed. The vendors joined together in 1991, first proposing, and then building, a standard based on contributed technologies. In June 1997, the IEEE released the 802.11 standard for wireless local-area networking.

Just as the 802.3 Ethernet standard allows for data transmission over twisted-pair and coaxial cable, the 802.11 WLAN standard allows for transmission over different media. Compliant media include infrared light and two types of radio transmission within the unlicensed 2.4-GHz frequency band: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). Spread spectrum is a modulation technique developed in the 1940s that spreads a transmission signal over a broad band of radio frequencies. This technique is ideal for data

communications because it is less susceptible to radio noise and creates little interference. FHSS is limited to a 2-Mbps data transfer rate and is recommended for only very specific applications such as certain types of watercraft. For all other wireless LAN applications, DSSS is the better choice. The recently released evolution of the IEEE standard, 802.11b, provides for a full Ethernet-like data rate of 11 Mbps over DSSS. FHSS does not support data rates greater than 2 Mbps.

The Future of Wireless Local-Area Networking

The history of technology improvement in the wired LANs can be summed up with the mantra "Faster, Better, and Cheaper." Wireless LAN technology has already started down that road: data rates have increased from 1 to 11 Mbps, interoperability became reality with the introduction of the IEEE 802.11 standard, and prices have dramatically decreased. The improvements seen so far are just a beginning.

Performance

IEEE 802.11b standard 11 Mbps WLANs operate in the 2.4-GHz frequency band where there is room for increased bandwidth. Using an optional modulation technique within the 802.11b specification, it is possible to double the current data rate. Cisco already has 22 Mbps on the road map for the future. Wireless LAN manufacturers migrated from the 900-MHz band to the 2.4-GHz band to improve data rate. This pattern promises to continue, with a broader frequency band capable of supporting higher bandwidth available at 5-GHz. The IEEE has already issued a specification (802.11a) for equipment operating at 5-GHz that supports up to a 54-Mbps data rate. This generation of technology will likely carry a significant price premium when it is introduced sometime in 2001. As is typical, this premium will decrease over time while data rates increase: the 5.7-GHz band promises to allow for the next breakthrough data rate—100 Mbps. While performance will unquestionably continue to improve, customers will continue to require a reliable partner to integrate these dynamic technologies seamlessly into the existing network. Cisco provides the stability and network expertise to make such integration a reality.

Security

The wired equivalent privacy (WEP) option to the 802.11 standard is only the first step in addressing customer security concerns. Cisco provides the greatest level of security available today for wireless networking, offering up to 128-bit encryption and supporting both the encryption and authentication options of the 802.11 standard. As specified in the standard, Cisco uses the RC4 algorithm with a 40- or 128-bit key. When WEP is enabled, each station (clients and access points) has up to four keys. The keys are used to encrypt the data before it is transmitted through the airwaves. If a station receives a packet that is not encrypted with the appropriate key, the packet will be discarded and never delivered to the host.

Although the 802.11 standard provides strong encryption services to secure the WLAN, the means by which the secure keys are granted, revoked, and refreshed is undefined. Fortunately, several key administration architectures are available for use in the enterprise. The best approach for large networks is centralized key management, which uses centralized encryption key servers. The ongoing Cisco strategy includes the addition of encryption key servers, to ensure that valuable data is protected. Encryption key servers provide for centralized creation of keys, distribution of keys, and ongoing key rotation. Key servers enable the network administrator to command the creation of RSA public/private key pairs at the client level that are required for client authentication. The Cisco key server will also provide for the generation and distribution to clients and access points of the RC4 keys needed for packet encryption. This implementation eases administration and helps avoid compromising confidential keys. Cisco will continue to enhance security measures to ensure best-of-class security throughout the enterprise network.

Mobility Services

A primary advantage of WLANs is mobility, but no industry standard currently addresses the tracking or management of mobile devices in its Management Information Base (MIB). This omission would prohibit users from roaming between wireless access points that cover a common area, such as a complete floor of a building. Cisco has addressed this issue, providing its own versions of mobility algorithms that facilitate roaming within an IP domain (such as a floor) with an eye towards optimizing roaming across IP domains (such as an enterprise campus).

Management

Wireless access points share the functions of both hubs and switches. Wireless clients associating with access points share the wireless LAN, similar to the way a hub functions, but the access point can additionally track movement of clients across its domain and permit or deny specific traffic or clients from communicating through it. For network managers to use these services to advantage, it is necessary to instrument the access point like a hub and a switch.

The Cisco WLAN devices are manageable through common Telnet or SNMP (I or II) services and a Web browser interface to facilitate its monitoring and control. In addition to bridge statistics and counters, the access point also offers additional features that make it powerful and manageable, including mapping of wireless access points and their associated clients as well as monitoring and reporting of client statistics. Access points can also control access and the flow of traffic through the wireless LAN via Media Access Control (MAC) and protocol-level access lists. Configuration parameters, as well as code images for access points, can be centrally configured and managed to facilitate consistency of WLAN network policy.

Price

Declining wireless LAN equipment prices have opened up whole new markets. As volumes continue to increase, manufacturing efficiencies and cost-reduction engineering will allow for even further price reductions. Although it is unlikely that the price of a wireless client adapter will ever match that of a wired one when cabling cost and labor are accounted for, the difference will become increasingly insignificant.

Conclusion

Today, the WLAN has redefined what it means to be connected. It has stretched the boundaries of the local-area network. It makes an infrastructure as dynamic as it needs to be. And it's only just starting: the standard is less than three years old, with the high-speed 802.11b yet to reach its first birthday. With standard and interoperable wireless products, LANs can reach scales unimaginable with a wired infrastructure. They can make high-speed interconnections for a fraction of the cost of traditional wide-area technologies. In a wireless world, users can roam not just within a campus but within a city, while maintaining a high-speed link to extranets, intranets, and the Internet itself. The future of wireless local-area networking is now—and it's at Cisco.

CISCO SYSTEMS