Chapter 1 Similarities and differences between wireless and wired local area networks (LANs)

There are many similarities and differences between wired LANs and the IEEE 802.11™ wireless LAN (WLAN). This chapter will describe them.

SIMILARITIES BETWEEN WLANS AND WIRED LANS

From the beginning, the IEEE 802.11 WLAN was designed to look and feel like any IEEE 802® wired LAN. In other words, it must appear to be the same as the wired networks to which a user may be accustomed. It must support all of the protocols and all of the LAN management tools that operate on a wired network.

To maintain similarity to wired LANs, IEEE 802.11 is designed to the same interface as IEEE 802.3™. IEEE 802.11 operates under the IEEE 802.2™ logical link control (LLC) sublayer, providing all of the services required to support that sublayer. In this fashion, IEEE 802.11 is indistinguishable from IEEE 802.3 by the protocols that may be running above IEEE 802.2.

Using the IEEE 802.2 interface guarantees that protocol layers above LLC need not be aware of the network that is actually transporting their data.

DIFFERENCES BETWEEN WLANS AND WIRED LANS

There are also a number of differences between wired LANs and WLANs. The two most important differences are that there are no wires (the air link) and the mobility thus conferred by the lack of a wired tether. These differences lead to both the tremendous benefits of a WLAN, as well as the perceived drawbacks to them.

The air link is the radio or infrared link between WLAN transmitters and receivers. Because WLAN transmissions are not confined to a wire, there may

be concerns that the data carried by a WLAN are not private, i.e., not protected. This concern is certainly valid; the data on a WLAN are broadcast for all to hear. Many proprietary WLANs do not provide any protection for the data carried. The designers of IEEE 802.11 realized that this concern could be a significant problem for users wishing to use a WLAN and designed strong cryptographic mechanisms into the protocol to provide protection for the data that is at least as strong as sending the data over a wire. Details of this protection are described in Chapter 4.

The air link also exposes the transmissions of a WLAN to the vagaries of electromagnetic propagation. For both radio- and infrared-based WLANs, everything in the environment is either a reflector or an attenuator of the signal carrying the LAN data. This variability can cause significant changes in the strength of a signal received by a WLAN station (STA) and sometimes sever the STA from the LAN entirely. At the wavelengths used in the IEEE 802.11 WLAN, small changes in position can cause large changes in the received signal strength. This fluxuation is due to the signal's traveling many paths of differing lengths to arrive at the receiver. Each individual arriving signal is of a slightly different phase from all of the others. Adding these different phases together results in the composite signal that is received. Because these individual signals sometimes add up in phase and sometimes out of phase, the overall received signal strength is sometimes large and sometimes small. Objects moving in the environment, such as people, aluminized Mylar balloons, doors, and other objects, can also affect the strength of a signal at a receiver by changing the attenuation or reflection of the many individual signals.

Figure 1–1 is taken from the IEEE 802.11 standard and shows the result of a ray tracing simulation in a closed office environment. The various shades of gray depict the different signal strengths at each location in the room. Dealing with the variability of the air link is also designed into the IEEE 802.11 WLAN. For more on this, see Chapter 9.

The second significant difference a WLAN has from a wired LAN is mobility. The user of a WLAN is not tethered to the network outlet in the wall. This mobility is both the source of the benefits of a WLAN and the cause of much of the internal complexity.

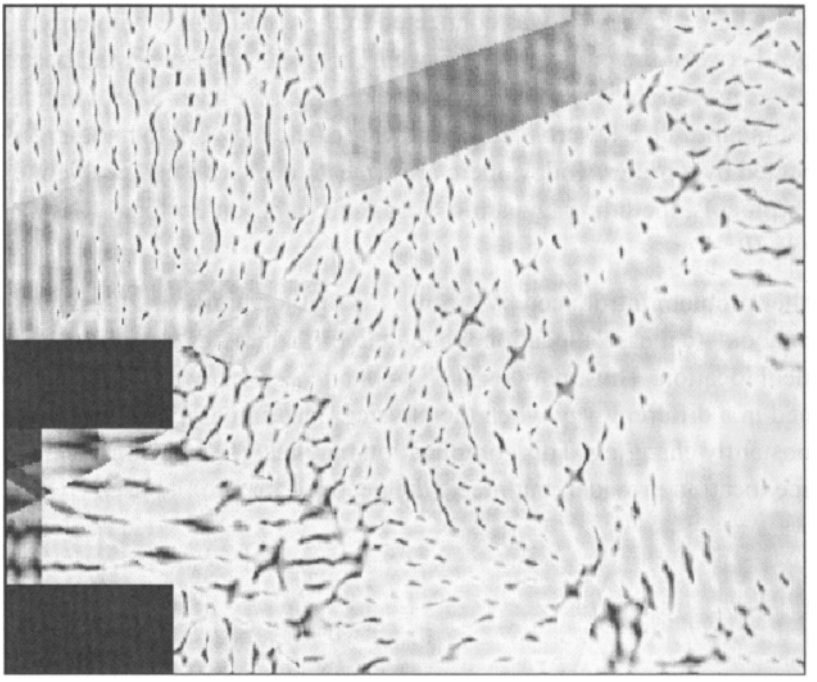

Figure 1–1: Ray tracing simulation results

The benefit of mobility is that the LAN goes wherever you are, instantly and without the need to search out outlets or to arrange in advance with the network administrators. In a laptop equipped with an IEEE 802.11 WLAN connection, the connection to the network is available in a coworker's office, down the hall in the conference room, downstairs in the lobby, across the parking lot in another building, even across the country on another campus. In other words, all of the information available over the network, while sitting in your office, is still available in all these locations: email, file servers, the company-internal web sites, and the Internet.

Of course, there is a flip side to the benefits of mobility. Most of the network protocols and equipment in use today were not designed to cope with mobility. They were designed with an assumption that the addresses assigned to a network node would remain in a fixed location on the network. For

example, early WLANs required that a mobile STA could roam only within an area where the WLAN was connected to the wired LAN, with only layer-2 bridges between the parts of the WLAN. This requirement existed because there was no simple way to deal with the change of a layer-3 network address should the mobile STA cross from one part of the network to another that is connected by a router. Today, there are ways to deal with this problem using new protocols, including Dynamic Host Configuration Protocol (DHCP) and Mobile-IP.

Another problem introduced by mobility is that location-based services lose their "hook" to a user's location when network addresses are not locked to a physical location. Thus, notions such as *the nearest network printer* must be defined in a different way when the physical location of a network user may be constantly changing. This complication may increase the complexity of the service location provider, but meets the needs of the mobile user.