CF form factors until recently. A CF card is small, weighing half an ounce, and is less than half the thickness of a PC Card. It also holds only one quarter the volume of PC Card radio card. The CF cards draw little power, which enables the batteries to last longer than devices using PC Cards. Some PDAs come with direct CF interfaces, which results in a lightweight and compact wireless PDA. If the computer device doesn't have a CF slot, you can purchase an adapter so that the CF card will fit into a standard PC Card slot. A CF radio card is definitely the way to go, especially for compact computing devices.

In addition to the internal NICs, a variety of external network interfaces connect to the computer device through parallel, serial, and USB ports. These might be suitable for stationary computers, but they certainly hinder mobility in most wireless applications.

As **Chapter 3**, "Radio Frequency and Light Signal Fundamentals: The Invisible Medium," discusses in detail, a wireless NIC includes an antenna that converts electrical signals to radio or light waves for propagation through the air medium. Antennae employ many structures, and they can be external, internal, permanent, or detachable. The antenna for a PC Card, for example, generally attaches to the end of the card and protrudes out the side of the laptop.

Mini-PCI cards, however, might have an antenna that resides inside the outer edge of a laptop monitor. Some NICs have antennaes that are permanent, which have one particular propagation pattern. Other NICs allow the replacement of the antenna, which increases flexibility in choosing an antenna that best satisfies requirements.

Air Medium

Air serves many purposes, such as providing a basis for speech, enabling air travel, and sustaining life. Air also provides a medium for the propagation of wireless communications signals, which is the

Exhibit 1010
Page 062 of 292

heart of wireless networking. Air is the conduit by which information flows between computer devices and the wireless infrastructure. Think of communication through a wireless network as similar to talking to someone. As you move farther apart, it's more difficult to hear each other, especially when a loud noise is present.

Wireless information signals also travel through the air, but they have special properties that enable propagation over relatively long distances. Wireless information signals cannot be heard by humans, so it's possible to amplify the signals to a higher level without disturbing human ears. The quality of transmission, however, depends on obstructions in the air that either lessen or scatter the strength and range of the signals.

Rain, snow, smog, and smoke are examples of elements that impair propagation of wireless communications signals. In fact, a heavy downpour of rain can limit signal range by 50 percent while the rain is occurring. Other obstacles, such as trees and buildings, can impact the propagation and performance of the wireless network. These issues become most important when planning the installation of a wireless MAN or WAN.

With wireless networks, the air medium supports the propagation of radio and light waves that travel from one point to another. These types of signals have been in use for more than 100 years, but they are still somewhat mysterious and not well understood by most computer professionals. **Chapter 3** provides details on signal characteristics and impairments that relate to the air medium.

Wireless Network Infrastructures

The infrastructure of a wireless network interconnects wireless users and end systems. The infrastructure might consist of **base stations**, access controllers, application connectivity software, and a distribution

Exhibit 1010
Page 063 of 292

system. These components enhance wireless communications and fulfill important functions necessary for specific applications.

Base Stations

The base station is a common infrastructure component that interfaces the wireless communications signals traveling through the air medium to a wired network—often referred to as a distribution system. Therefore, a base station enables users to access a wide range of network services, such as web browsing, e-mail access, and database applications. A base station often contains a wireless NIC that implements the same technology in operation by the user's wireless NIC.

Base stations go by different names, depending on their purpose. An **access point**, for instance, represents a generic base station for a wireless LAN. A collection of access points within a wireless LAN, for example, supports roaming throughout a facility. The NIC within a user's computer device connects with the nearest access point, which provides an interface with systems within the infrastructure and users associated with other access points. As the user moves to a part of the facility that's closer to another access point, the NIC automatically reconnects with the closest access point to maintain reliable communications.

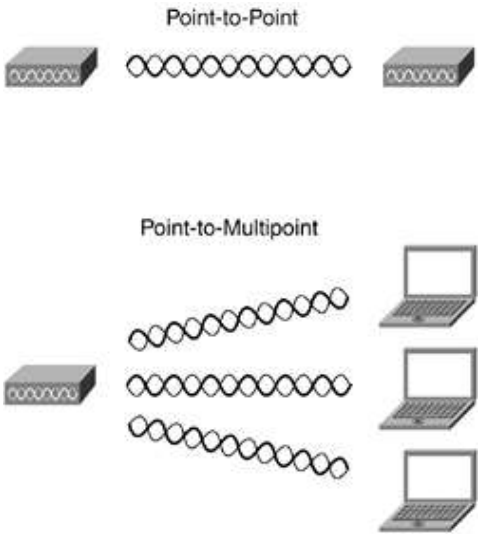
Residential gateways and routers are more advanced forms of base stations that enable additional network functions. The gateway might have functions, such as access control and application connectivity, that better serve distributed, public networks. On the other hand, a **router** would enable operation of multiple computers on a single broadband connection.

As show in **Figure 2-4**, a base station might support point-to-point or point-to-multipoint communications. Point-to-point systems enable communications signals to flow from one particular base station or computer device directly to another one. This is a common infrastruc-

Exhibit 1010
Page 064 of 292

ture for supporting long-range wireless communications links. For example, a wireless Internet service provider (WISP) can use this system to transport communications signals from a base station at a remote site— such as a home or office— to a base station near a communications facility.

Figure 2-4. Base Stations Support Different Configurations



As the name implies, point-to-multipoint functionality enables a base station to communicate with more than one wireless computer device or base station. An access point within a wireless LAN implements this form of communications. The access point represents a single point whereby many computer devices connect to and communicate with each other and systems within the wireless infrastructure.

Access Controllers

In the absence of adequate security, quality of service (QoS), and roaming mechanisms in wireless network standards, companies offer access-control solutions to strengthen wireless systems. The key component to these solutions is an access controller, which is typically hardware that resides on the wired portion of the network between

Exhibit 1010
Page 065 of 292

the access points and the protected side of the network. Access controllers provide centralized intelligence behind the access points to regulate traffic between the open wireless network and important resources. In some cases, the access point contains the access control function.

Access controllers apply to a wide range of applications. In a public wireless LAN, for example, an access controller regulates access to the Internet by authenticating and authorizing users based on a subscription plan. Similarly, a corporation can implement an access controller to help a hacker sitting in the company's parking lot from getting entry to sensitive data and applications.

The use of an access controller reduces the need for smart access points, which are relatively expensive and include many non-802.11 features. Generally, vendors refer to these smarter access points as being enterprise-grade components. Proponents of access controllers, however, argue that 802.11 access points should focus on RF excellence and low cost. Proponents also argue that access points should centralize access control functions in an access controller that serves all access points. These thin access points primarily implement the basic wireless network standard (such as IEEE 802.11), and not much more.

The users of access controllers realize the following benefits when deployed with thin access points:

- Lower Costs— Access points with limited functionality cost less, which generally results in lower overall system costs. This is especially true for networks requiring a larger number of access points, such as an enterprise system. The use of thin access points results in cost savings of approximately $400 per access point. In larger networks, this savings far outweighs the additional cost of an access controller, which costs $5000 on the average.

Exhibit 1010
Page 066 of 292

- Open Connectivity— Smart access points offer enhancements related to security and performance to the basic wireless connectivity that wireless network standards offer. The problem in many cases is that these enhancements are only possible if the user devices implement a wireless NIC made by the same vendor as the access point. This significantly reduces the openness of the system and limits the selection of vendors. On the other hand, thin access points can easily communicate using the basic wireless network protocol with wireless NICs made by multiple vendors, while the access controller transparently provides enhancements.
- Centralized Support— An advantage of placing the smarts of the network in an access controller is that the system is easier to support, primarily because fewer touch points are in the network. If all of the intelligence of the network is within the access points, support personnel must interface with many points when configuring, monitoring, and troubleshooting the network. An access controller enables the access points to have fewer functions, reducing the need to interface with the access points when performing support tasks.

Access controllers often provide port-based access control, allowing administrators to configure access to specific applications on a per-user basis. The port, which is actually a number (such as 80 for http), corresponds to a specific type of application. For example, an access controller can block access to port 80, which forces a user to log in before being able to browse web pages. After users enter their username and password, the access controller will validate their identity through an authentication server. The network application could, as an alternative, use **digital certificates** for authentication purposes. This function regulates the user access to the protected network.

Access controllers generally employ the following features:

- Authentication— Most access controllers have a built-in database for authenticating users; however, some offer external interfaces to

Exhibit 1010
Page 067 of 292

authentication servers such as Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP). For smaller, private networks, an internal database might suffice. For enterprise solutions, however, external and centralized authentication servers provide better results.

- Encryption— Some access controllers provide encryption of data from the client to the server and back, using such common methods such as **IPSec**. This provides added protection beyond what the native wireless network standard provides. Some of these features, however, are also part of web browsers.
- Subnet Roaming— In order to support roaming from one network to another, access controllers provide roaming across subnets without needing to re-authenticate with the system. As a result, users can continue utilizing their network applications without interruption as they roam about a facility. This feature is especially useful for larger installations where access to the network for specific users will span multiple subnets.
- Bandwidth Management— Because users share bandwidth in a wireless network, it's important to have a mechanism to ensure specific users don't hog the bandwidth. Access controllers provide this form of bandwidth management through the assignment of user profiles based on required QoS levels. A profile specifies the types of services, such as web browsing, e-mail, and video streaming, as well as performance limits. For example, an unsubscribed visitor attempting to utilize a public wireless LAN could classify as fitting a “visitor” profile, which might only allow access to information related to the local hotspot. A subscriber, however, could have a different role that allows him to have a broadband Internet connection.

Application Connectivity Software

Web surfing and e-mail generally perform well over wireless networks. All it takes is a browser and e-mail software on the **client device**. Users might lose a wireless connection from time to time, but the

Exhibit 1010
Page 068 of 292

protocols in use for these relatively simple applications are resilient under most conditions.

Beyond these simple applications, however, special application connectivity software is necessary as an interface between a user's computer device and the end system hosting the application's software or database. Applications could be warehouse management software running on an IBM AS/400, a modeling application located on a UNIX box, or a time-management system residing on an old mainframe system. The databases are part of a client/server system where part, or all of the application software, resides on the client device and interfaces with a database such as Oracle or Sybase. In these cases, application connectivity software is important in addition to access points and controllers to enable communications between the user's computer device and the application software or databases located on a centralized server.

The following are various types of application connectivity software:

- Terminal Emulation— Terminal emulation software runs on a computer device, making the device operate as a terminal that provides a relatively simple user interface to application software running on another computer. The terminal merely presents screens to the user and accepts input rendered by the applications software. For example, VT220 **terminal emulation** communicates with applications running on a UNIX host, 5250 terminal emulation works with IBM AS/400-based systems, and 3270 terminal emulation interfaces with IBM mainframes.
  The advantage of using terminal emulation is its low initial cost and changes made to the application automatically take affect when the user logs in. Wireless systems using terminal emulation, however, might not be able to maintain continuous connections with legacy applications, which have timeouts set for more reliable wired networks. Timeouts will automatically disconnect a session if they don't sense activity within a given time period. As a result, IT

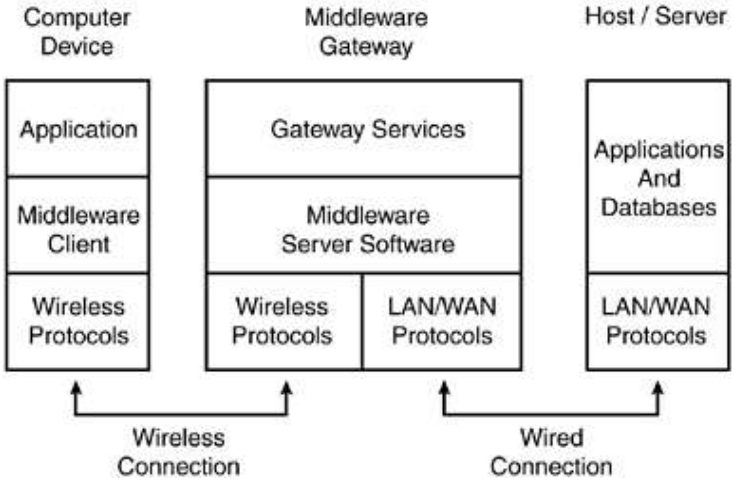
Exhibit 1010
Page 069 of 292

groups might spend a lot of time responding to end-user complaints of dropped connections and incomplete data transactions. Therefore, implementing terminal emulation can have a disastrous effect on long-term support costs.

- Direct Database Connectivity— Direct database connectivity, sometimes referred to as client/server, encompasses application software running on the user's computer device. With this configuration, the software on the end-user device provides all application functionality and generally interfaces to a database located on a central server. This enables flexibility when developing applications because the programmer has complete control over what functions are implemented—and is not constrained by a legacy application located on a central computer. Direct database connections are often the best approach when needing flexibility in writing the application software. A problem, however, is that the direct database approach depends on the use of Transmission Control Protocol/Internet Protocol (TCP/IP), which is not well-suited for communications across a wireless network.
- Wireless Middleware— Wireless middleware software provides intermediate communications between user computer devices and the application software or database located on a server. (See **Figure 2-5**.) The middleware—which runs on a dedicated computer (middleware gateway) attached to the wired network—processes the packets that pass between the user computer devices and the servers. The middleware software primarily offers efficient and reliable communications over the wireless network while maintaining appropriate connections to application software and databases on the server through the more reliable wired network. Sometimes this is referred to as session persistence.

Figure 2-5. Wireless Middleware Efficiently Interconnects Computer Device Applications to Hosts and Servers

Exhibit 1010
Page 070 of 292



Look for the following features in middleware products:

- Optimization techniques— Many middleware products include data compression to help reduce the number of packets sent over the wireless link. Some implementations of middleware use proprietary communications protocols, which have little overhead as compared to traditional protocols, such as TCP/IP.

- Intelligent restarts— With wireless networks, a transmission can be unexpectedly cut at midstream. Intelligent restart is a recovery mechanism that detects the premature end of a transmission. When the connection is reestablished, the middleware resumes transmission from the break point instead of at the beginning. This avoids errors from occurring in applications that utilize databases.

- Data bundling— Some middleware is capable of combining smaller data packets into a single large packet for transmission over the wireless network, which can help lower transmission service costs of WANs. Since some wireless data services charge users by the packet, data bundling results in a lower aggregate cost.

- Screen scraping and reshaping— The development environment of some middleware products allows developers to use visual tools to shape and reshape portions of existing application screens to more effectively fit data on the smaller display of some non-PC wireless devices, such as PDAs and bar code scanners.

Exhibit 1010
Page 071 of 292

- End system support— Wireless middleware interfaces with a variety of end system applications and databases. If clients need access to tomultiple types of applications and databases, wireless middleware acts as a concentrator. For example, a user can use the middleware connection to interface with applications on an AS/400 and UNIX box simultaneously without needing to be concerned about running the correct terminal emulation software.

Distribution System

A wireless network is seldom entirely free of wires. The distribution system, which often includes wiring, is generally necessary to tie together the access points, access controllers, and servers. In most cases, the common Ethernet comprises the distribution system.

The IEEE **802.3** standard is the basis for Ethernet and specifies the use of the carrier sense multiple access (CSMA) protocol to provide access to a shared medium, such as twisted-pair wiring, coaxial cable, and optical fiber. CSMA is the predominant medium access standard in use today by both wired and wireless networks.

CSMA enables sharing of a common medium by allowing only one NIC to transmit information at any particular time. This is similar to a meeting environment where people (like NICs) speak only when no one else is talking. This gives each person responsibility in a way that distributes speaking decisions to each person. If more than one person talks at the same time, a collision occurs, and each person needs to take turns repeating what he said.

All computer devices on the network must take turns using the medium with Ethernet hubs. An Ethernet switch, however, enables multiple collision domains that can allow simultaneous transmission among users to improve performance. For larger networks beyond the size of a home or small office application, be sure to use switches for optimum performance.

Exhibit 1010
Page 072 of 292