Ethernet employs twisted-pair wiring, coaxial cable, and optical fiber for interconnecting network devices, such as access points and other distribution equipment. The use of coaxial cables in older wired LANs was common 10 years ago, but today most companies use twisted-pair wiring and optical fiber. The Electronic Industries Association (EIA) and Telecommunications Industry Association (TIA) specifies Category 5 (referred to as Cat 5) twisted-pair wiring, the most popular of all twisted-pair cables in use today with Ethernet.

Cat 5 consists of four unshielded twisted pairs of 24-gauge wires that support Ethernet signals over 100 meters (m)— about 300 feet— of cabling. Ethernet repeaters increase this range if necessary, which is one method of reaching a wireless network base station that's beyond 100 m from a communications closet.

There are also other variations of twisted-pair wiring. Enhanced Cat 5 (referred to as Cat5e) makes use of all four pairs of wires to support short-range Gigabit Ethernet (1000 Mbps) connectivity. It is also backward compatible with regular Cat 5. Cat 6 and Cat 7 cable are now available, bringing more bandwidth and range to copper-based Gigabit Ethernet networks. Cat 7 cable features individually shielded twisted pairs (STP) of wires, making it ideal for installation in locations where there is a high potential for electromagnetic interference.

The following are specific types of twisted-pair options for Ethernet common to wireless LAN distribution systems:

- 10BASE-T— 10BASE-T is one of the 802.3 physical layers and specifies data rates of 10 Mbps. A typical 10BASE-T cable uses two of the four pairs within a Cat 5 cable for sending and receiving data. Each end of the cable includes RJ-45 connectors that are a little larger than the common RJ-11 telephone connector used within North America.
  The advantage of having extra pairs of wires open is support for other uses, such as Power-over-Ethernet (PoE). This is a mechanism

Exhibit 1010
Page 073 of 292

in which a module injects DC current into the Cat 5 cable, enabling you to supply power to the access point from the communications closet. PoE often eliminates the need for having an electrician install new electrical outlets at every access point. For larger networks, definitely consider the use of PoE.

- 100BASE-T— Another 802.3 physical layer, 100BASE-T supports data rates of 100 Mbps. Similar to 10BASE-T Ethernet, 100-Base-T uses twisted-pair wiring, with the following options:

  - 100BASE-TX uses two pairs of Cat 5 twisted-pair wires.
  - 100BASE-T4 uses four pairs of older, lower-quality (Cat 3) twisted-pair wires.

  Most implementations today use 100BASE-TX cabling. As with 10BASE-T, PoE can make use of unused pairs of wires. 100-Base-T4 was popular when needing to support 100-Mbps data rates over the older Cat 3 cabling, which was prominent during the early 1990s.
- Optical Fiber— Optical fiber is more expensive than twisted pair, but fiber can be cost effective because it supports gigabit speeds and has a range of up to two kilometers. Instead of using the traditional electrical-signal-over-copper-wire approach, optical fiber cable uses pulses of light over tiny strips of glass or plastic. This makes optical fiber cable resistant to electromagnetic interference, making it valuable in situations where electronic emissions are a concern. In addition, it's nearly impossible to passively monitor the transmission of data through optical fiber cable, making it more secure than twisted-pair wiring.
  With wireless LANs, optical fiber is a possible solution for reaching an access point located beyond a 100 m from a communications closet. This requires the use of an expensive pair of transceivers, however, which transforms electrical signals into light (and vice versa). One issue when dealing with optical fiber cable is the difficulties in splicing cables. You must work with glass or plastic materials that require precise alignment. You need special tools and training to make effective optical fiber cables. You should purchase

Exhibit 1010
Page 074 of 292

precut fiber cables to avoid problems that are difficult to troubleshoot.

Management Systems

As with other types of networks, enterprise wireless networks require effective management that ensures user needs are met over the life of the network. A network management system, which involves both people and software tools, satisfies this need. The following are functions that management systems should provide.

Security

The security element involves mechanisms that avoid the compromise or damage of network resources, such as databases and e-mail messages. This includes enforcing security policies for the configuration of the wireless network in a way that counters issues related to the propagation of wireless signals. For example, policies could specify the use of a particular type of encryption to ensure a mischievous person can't receive and decode e-mail messages being sent between a user and an access point.

For more details on wireless network security methods, refer to **Chapter 8**, “Wireless Network Security: Protecting Information Resources.”

Help Desk

The help desk provides the first level of support for users. A user having difficulties with a wireless connection should know how to reach the help desk. Users often have problems with association or experience erratic performance.

Help desk personnel are capable of solving simple connection problems, such as assisting the user configure a radio card and operating system to comply with specific wireless network policies. The help

Exhibit 1010
Page 075 of 292

desk should have a communications interface with more advanced support functions, such as maintenance and engineering, to solve more complex problems that arise from contact with users.

Configuration Management

Configuration management consists of controlling changes made to the wireless network architecture and installed system. Changes might consist of installing or moving access points, changing access point parameters, and updating firmware. Because of the dynamic nature of wireless networks, changes are more common than with wired networks.

An enterprise should review all wireless network modification proposals that impact the performance or security of the network. This review enables a company to take into account relevant implications that involve additional costs and use of resources. The company should implement an independent design review process that evaluates each proposed wireless network solution and verifies conformance to a common architecture and support elements. The verification should, for example, include reviewing access point placement, radio frequency channel assignments, and security settings.

Network Monitoring

Network monitoring includes continuously measuring various attributes of the wireless network, including access point utilization and user traffic routes through the distribution system. This plays a key role in proactively managing the wireless network to support a growth of users and solve issues before they hamper the performance and security of the network.

An enterprise should continually measure the usage of base stations to properly scale the wireless network as user traffic changes. Base stations act as a gauge to indicate when additional base stations, access controllers, and Internet bandwidth are necessary. A problem with

Exhibit 1010
Page 076 of 292

wireless networks is that network managers might not notice that a base station is inoperative for quite some time.

In most cases, coverage from base stations overlaps, and users will likely associate with another base station at lower performance if the primary access point is not available. Network monitoring tools, however, will notice the outage immediately and alert the appropriate support person. If possible, a company should integrate the wireless network monitoring function with tools already in use in the existing corporate network. This simplifies operational support.

Reporting

The reporting element offers information regarding various aspects of the wireless network, including usage statistics, security alarm notifications, and performance. These reports are necessary for managers to effectively gauge the operation of the network and make decisions on changes. This reporting should, at a minimum, indicate potential breaches of security, inoperable access points, and utilization. This type of information should be available to all operational support functions, such as the help desk, maintenance, and engineering.

Engineering

The engineering element provides advanced technical support for reengineering the wireless network to include newer technologies and solve problems to ensure effective performance and security. Ordinarily, the company or group that designs the initial wireless network will perform the engineering functions. The engineering function should review and verify compliance of designs with the common architectural design. In addition, the engineering group should continually monitor the evolution of wireless network technologies and products to ensure effective migration in a manner that meets growing network utilization.

Maintenance

Exhibit 1010
Page 077 of 292

The maintenance element repairs and configures the wireless network, including replacing broken antennae, setting channels on access points, and re-evaluating radio wave propagation. Some maintenance tasks might result from the engineering support function. For example, engineers might find the need to install an additional access point in an area where new coverage is necessary. In this case, maintenance personnel would install the access point at a location that the engineer identifies.

An important task for maintaining the wireless network is to periodically upgrade the firmware in access points. This ensures that the access point operates with the latest features and freedom from defects, which maximizes performance and security. As a result, a company should institute regular upgrades to firmware as new versions become available.

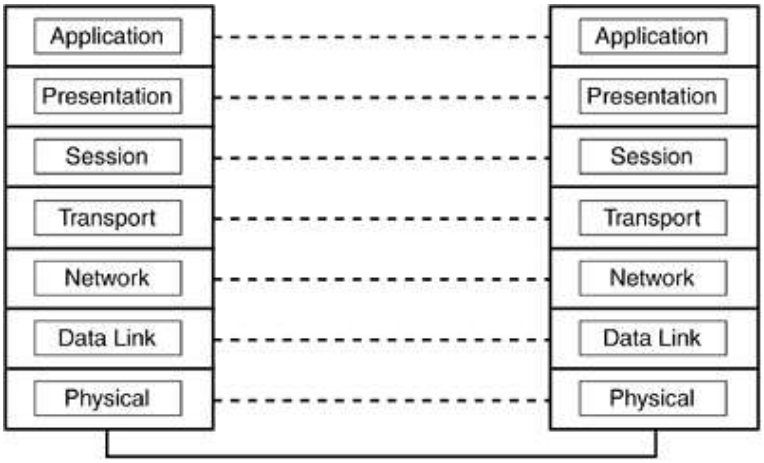
The maintenance group should also periodically perform coverage tests to ensure that the access points are properly covering the facilities at applicable levels of performance. This is necessary as the company modifies the structure of the facilities, which changes the radio wave propagation characteristics. If discrepancies are found, the maintenance group should report findings to the engineering group for resolution.

Exhibit 1010
Page 078 of 292

Network Architecture

The architecture of a network defines the protocols and components necessary to satisfy application requirements. One popular standard for illustrating the architecture is the seven-layer Open System Interconnect (OSI) Reference Model, developed by the International Standards Organization (ISO). OSI specifies a complete set of network functions, grouped into layers (see **Figure 2-6**), which reside within each network component. The OSI Reference Model is also a handy model for representing the various standards and interoperability of a wireless network.

Figure 2-6. Layers of the OSI Reference Model Represent All Functions of a Network



The OSI layers provide the following network functionality:

- Layer 7—Application layer: Establishes communications among users and provides basic communications services such as file

Exhibit 1010
Page 079 of 292

transfer and e-mail. Examples of software that runs at this layer include Simple Mail Transfer Protocol (SMTP), HyperText Transfer Protocol (HTTP) and File Transfer Protocol (FTP).

- Layer 6—Presentation layer: Negotiates data transfer syntax for the application layer and performs translations between different data formats, if necessary. For example, this layer can translate the coding that represents the data when communicating with a remote system made by a different vendor.
- Layer 5—Session layer: Establishes, manages, and terminates sessions between applications. Wireless middleware and access controllers provide this form of connectivity over wireless networks. If the wireless network encounters interference, the session layer functions will suspend communications until the interference goes away.
- Layer 4—Transport layer: Provides mechanisms for the establishment, maintenance, and orderly termination of virtual circuits, while shielding the higher layers from the network implementation details. In general, these circuits are connections made between network applications from one end of the communications circuit to another (such as between the web browser on a laptop to a web page on a server). Protocols such as Transmission Control Protocol (TCP) operate at this layer.
- Layer 3—Network layer: Provides the routing of packets though a network from source to destination. This routing ensures that data packets are sent in a direction that leads to a particular destination. Protocols such as Internet Protocol (IP) operate at this layer.
- Layer 2—Data link layer: Ensures medium access, as well as synchronization and error control between two entities. With wireless networks, this often involves coordination of access to the common air medium and recovery from errors that might occur in the data as it propagates from source to destination. Most wireless network types have a common method of performing data link layer functions independent of the actual means of transmission.
- Layer 1—Physical layer: Provides the actual transmission of information through the medium. Physical layers include radio waves

Exhibit 1010
Page 080 of 292

and infrared light.

The combined layers of a network architecture define the functionality of a wireless network, but wireless networks directly implement only the lower layers of the model. A wireless NIC, for example, implements the data link layer and physical layer functions. Other elements of the network (such as wireless middleware), however, offer functions that the session layer implements. In some cases, the addition of a wireless network might impact only the lower layers, but attention to higher layers is necessary to ensure that applications operate effectively in the presence of wireless network impairments.

Each layer of the OSI model supports the layers above it. In fact, the lower layers often appear transparent to the layers above. For example, TCP operating at the transport layer establishes connections with applications at a distant host computer, without awareness that lower layers are taking care of synchronization and signaling.

As shown in **Figure 2-6**, protocols at each layer communicate across the network to the respective peer layer. The actual transmission of data, however, occurs at the physical layer. As a result, the architecture allows for a layering process where a particular layer embeds its protocol information into frames that are placed within frames at lower layers. The frame that is sent by the physical layer actually contains frames from all higher layers. At the destination, each layer passes applicable frames to higher layers to facilitate the protocol between peer layers.

Exhibit 1010
Page 081 of 292

Information Signals

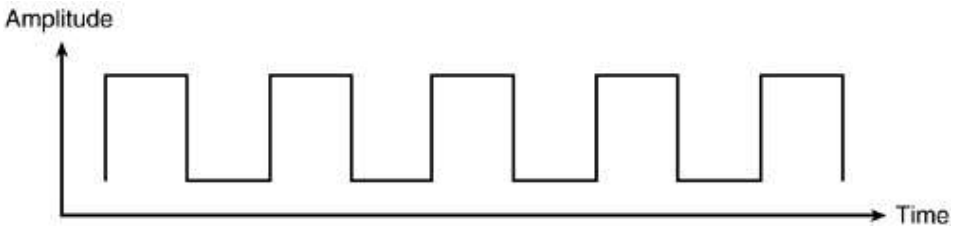
Data is a type of information that the network stores in a computer or retrieves from it. As a result, wireless networks transfer data from one computer to another. This data can include e-mail messages, files, web pages, video, music, and voice conversations.

Communications systems—such as a wireless network— symbolize data using codes that electrical, radio, and light signals efficiently represent. The signals carry the information through the system from one point to another. The signals are either digital or analog, depending on their location within the system.

Digital Signals

Digital signals, which are found inside computers, vary in amplitude steps as time advances. (See **Figure 2-7**.) Digital signals are usually binary (two-state); therefore, it is common to refer to the signal as a string of binary digits (bits) or binary data. Digital circuitry inside the computer easily stores and processes these digital signals in binary form.

Figure 2-7. Digital Signals Are Ideal for Use in Computers



Binary is a system that only uses 0s and 1s to represent the numbers. Conversions are easy from the more familiar decimal numbering system to binary, and computers can readily store binary numbers. With some protocols, the binary values within a data frame represent specific protocol information.

One of the advantages of digital signals is easy signal regeneration. As a signal propagates through the air medium, it might encounter noise or interference that changes the appearance of the signal's waveform. To clean up and regenerate the signal, digital circuitry can detect if a digital pulse is present at a certain period of time and create a new pulse that is exactly equal to the one originally sent. As a result, a digital signal can be sent over vast distances through periodic repeaters while preserving the integrity of the information. This is not possible with analog signals.

For security purposes, it is often necessary to encrypt and later decode a signal at the destination. This process is simple with digital signals because all that is necessary is to rearrange the bits using some type of secret keying process. When the destination receives the data, a device can use the same key and decrypt the data.

The following defines important characteristics of digital signals:

- Data rate— The data rate corresponds to the speed that a digital signal transfers data across a wireless network. As a result, the data rate of a digital signal gives some insight on how long it will take to send data from one point to another, as well as identify the amount of bandwidth that the medium must supply to effectively support the signal.
  The data rate of a signal is equal to the total number of bits transmitted in relation to the time it takes to send them. The common unit of measure for bit rate is bits per second (bps). As an example,

Exhibit 1010
Page 083 of 292

consider a signal that moves 1,000,000 bits in 1 second. The data rate is 1,000,000/1 = 1,000,000 bps (or 1 Mbps).

- Throughput— Throughput is similar to data rate; however, throughput calculations generally exclude the bits that correspond to the overhead that communications protocols include. There are no standards for representing throughput, but it usually includes only the actual information being sent across the network. As a result, throughput gives a more accurate way of representing the true performance and efficiency of a network. This makes throughput important when comparing wireless networks because it's directly related to performance. The higher the throughput, the higher the performance.

  The data rate of a wireless LAN, for example, might be 11 Mbps, but the throughput might be only 5 Mbps. After removing the overhead—frame headers, error checking fields, acknowledgement frames, and retransmissions because of errors—the resulting information transfer is considerably lower. As the number of users increases, contention for the shared medium increases, which drives throughput even lower because computer devices (wireless NICs, to be more precise) must wait longer before sending data. This delay, which is a form of overhead, can significantly lower the throughput.

With wireless networks, it is common to say that the system sends data bits. In reality, a wireless network converts the binary digital signals into analog before transmitting the signal through the air medium.

Analog Signals

An **analog signal**, shown in **Figure 2-8**, is one where the amplitude of the signal varies continuously as time progresses. Much of the natural environment produces signals that are analog in form. Examples of this are light and the human voice. Man-made signals, such as radio waves, are also analog in form.

Exhibit 1010
Page 084 of 292