

Deploying a Wireless LAN


 11

Wireless connectivity offers users a high degree of mobility and provides another networking option when traditional wired networks are impractical. The Microsoft® Windows® Server 2003 operating system provides the networking services needed to deploy a secure and manageable wireless local area network (WLAN) infrastructure within an enterprise environment. The deployment of WLANs — the primary wireless networking support for an enterprise environment provided by Windows Server 2003 and the Microsoft® Windows® XP operating system — is detailed in this chapter.

In This Chapter

Overview of Deploying a Wireless LAN	558
Adapting the Network Infrastructure for a WLAN	561
Designing a Wireless Network Access Solution	568
Implementing a WLAN Test Environment	584
Additional Resources	598

Related Information

- For more information about the Internet Authentication Service (IAS), see “Deploying IAS” in this book and the *Networking Guide* of the *Microsoft® Windows® Server 2003 Resource Kit* (or see the *Networking Guide* on the Web at <http://www.microsoft.com/reskit>).
- For information about designing a certificate infrastructure, see “Designing a Public Key Infrastructure” in *Designing and Deploying Directory and Security Services* of this kit.
- For more information about implementing the Active Directory® directory service, see “Designing and Deploying Directory Services” in *Designing and Deploying Directory and Security Services*.

Overview of Deploying a Wireless LAN

To provide authorization and authentication, automatic IP address assignment, and name resolution for wireless users, your networking infrastructure should include the following services:

- Active Directory directory service
- Remote Authentication Dial-In User Service (RADIUS) servers and proxies
- A certificate infrastructure, also known as a *public key infrastructure (PKI)*
- Dynamic Host Configuration Protocol (DHCP) services
- Domain Name System (DNS) services

These services together provide the security, availability, and scalability needed for an enterprise WLAN solution. Before you begin designing and deploying an enterprise WLAN, all of the supporting components and services in your networking infrastructure should be in place.

All of the components required for an enterprise WLAN solution are included with Windows Server 2003 and Windows XP. Windows Server 2003 includes DHCP, DNS, and Certificate Services, and support for RADIUS (through the Internet Authentication Service [IAS]), the IEEE 802.1X standard, and certificate authentication. Windows XP with wireless network adapters provides support for wireless devices such as laptops and personal digital assistants (PDAs), the IEEE 802.1X standard, and certificate authentication.



Note

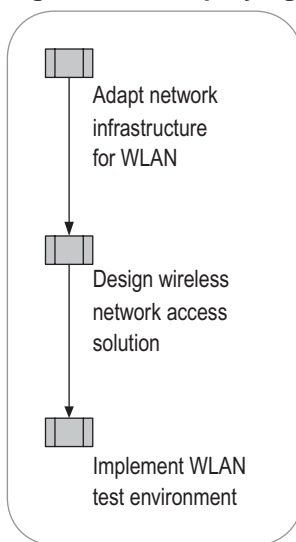
Though the WLAN components are included in the Microsoft® Windows® Server 2003, Standard Edition; Windows® Server 2003, Enterprise Edition; and Windows® Server 2003, Datacenter Edition operating systems, there are differences in the levels of features supported and the capabilities. For information about differences in these services among the Windows Server 2003 operating systems, see Help and Support Center for Windows Server 2003.

After designing your enterprise WLAN and deploying the networking components and services needed for the WLAN, you will be able to maintain a secure and manageable wireless network by using supported features such as the Wireless Zero Configuration (WZC) service included in Windows XP and Windows Server 2003, RADIUS-based 802.1X authentication, and interoperability with other networking services.

Process for Deploying a Wireless LAN

In deploying a wireless LAN, adapt your existing network infrastructure for a WLAN before designing the wireless network access solution — that is, deciding where to locate wireless access points (APs) and how to deploy them; designing wireless security and unauthenticated access; optionally designing a public space WLAN; and designing for better manageability. Before embarking on a full-scale WLAN deployment, implement a WLAN test environment and test your wireless networking solution. Figure 11.1 shows the major steps in the process for deploying a WLAN.

Figure 11.1 Deploying a Wireless LAN



WLAN Technology Background

The WLAN solution provided by Windows XP and Windows Server 2003 is based on IEEE standards 802.11 and 802.1X.

IEEE 802.11 IEEE 802.11, the standard for WLANs, specifies a technology that operates in the 2.4 through 2.5 GHz Industrial, Scientific, and Medical (ISM) band and has a maximum bit rate of 2 megabits per second (Mbps). IEEE 802.11b supports two additional speeds, 5.5 Mbps and 11 Mbps, in the ISM band.



Note

The latest IEEE standard, IEEE 802.11a, specifies a technology that operates in a 5.725 through 5.875 GHz band with a maximum bit rate of 54 Mbps.

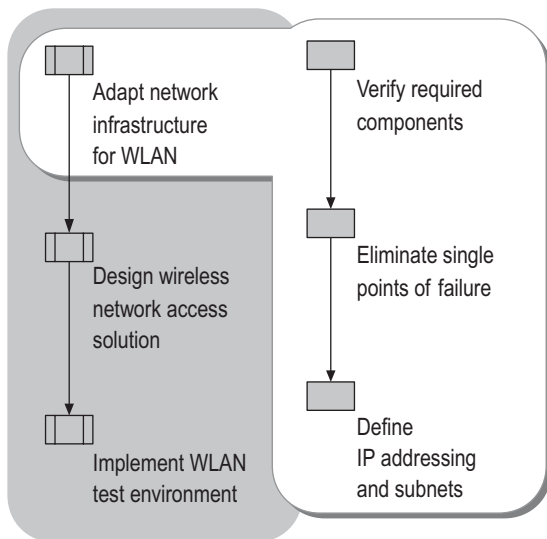
The 802.11 standard defines an *access point* (AP) as a device that functions as a transparent bridge between the wireless clients and the existing wired network. The AP contains at least one interface to connect to the existing wired network, and transmitting equipment to connect with the wireless clients. The AP also contains IEEE 802.1D bridging software, thereby acting as a transparent bridge between wireless and wired data-link layers.

IEEE 802.1X The 802.1X standard defines port-based network access control to provide authenticated network access for Ethernet networks. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. Although this standard is designed for wired Ethernet networks, it applies to 802.11 WLANs as well.

Adapting the Network Infrastructure for a WLAN

In adapting your network infrastructure for a WLAN, verify you have the required components; eliminate any potential single points of failure; and define IP addressing and subnets needed to support your wireless clients. Figure 11.2 shows the process for adapting your existing network infrastructure for a WLAN.

Figure 11.2 Adapting the Network Infrastructure for a WLAN



Verifying Required Components

To support a secure wireless solution, your existing network infrastructure must include the following components:

- Active Directory, to store account properties and validate password-based credentials.
- DHCP services, to provide automatic IP configuration to wireless clients.

- DNS services, to provide name resolution.
- RADIUS support, to provide centralized connection authentication, authorization, and accounting.
- A certificate infrastructure, also known as a PKI, to issue and validate the certificates required for Extensible Authentication Protocol–Transport Level Security (EAP-TLS) and Protected EAP (PEAP)–TLS authentication. TLS can use either smart cards or registry-based user certificates for authenticating the wireless client.
- For PEAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) authentication, computer certificates for the RADIUS servers and root CA certificates of the issuing CAs on the wireless clients (if needed).

Windows Server 2003 provides all of these components, with some variations in the levels of features supported and capabilities in different editions of the operating system (Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition). For information about differences in these services among the different editions of Windows Server 2003, see Help and Support Center for Windows Server 2003.

After verifying that your existing network infrastructure includes the appropriate components, update the design to support your WLAN.

Active Directory: Planning Groups and Group Policy for Wireless Access

Active Directory contains the user and computer accounts that are used for authentication and authorization of wireless users. It also contains the Group Policy settings that govern wireless connections — for example, information regarding autoenrollment for the user and computer certificates that are installed on wireless clients, and the Wireless Network (IEEE 802.11) Policies settings that specify preferred networks, Wired Equivalent Privacy (WEP) settings, and IEEE 802.1X settings for wireless connections.

To plan for the configuration of Active Directory for your wireless clients, identify the user and computer accounts for wireless users, and add them to a group that will be used in conjunction with a remote access policy to manage wireless access. You must also determine how to set the remote access permission on the user and computer accounts.



Note

For a native-mode domain, you can use universal groups and nested global groups. For example, you might create a universal group named WirelessUsers that contains global groups of wireless user and computer accounts for intranet access.

For information about designing group policies for a WLAN, see “Designing a Group Policy Infrastructure” in *Designing a Managed Environment* of this kit.

For information about configuring Active Directory for a WLAN, see “Implementing a WLAN Test Environment” later in this chapter. For information about the design and deployment of Active Directory, see “Designing and Deploying Directory Services” in *Designing and Deploying Directory and Security Services*.

**Note**

You can configure a computer running Windows Server 2003 or the Microsoft® Windows® 2000 Server operating system as an Active Directory domain controller. To configure a Windows 2000 Server–based computer as an Active Directory domain controller for wireless access, you must install Service Pack 3 (SP3) or later.

DNS: Identifying Zones Where Wireless Clients Will Register

In DNS, identify the DNS zones where the wireless computers will register DNS address records, and ensure that the zones are configured for dynamic updates. Optionally specify that the DNS zones are Active Directory–integrated zones, which provide secured updates, and that the DNS zones are updated by DHCP. For information about configuring DNS zones, see “Deploying DNS” in this book.

DHCP: Creating Scopes and Leases for Wireless Clients

On the DHCP server, you must configure the scope and lease duration differently for wireless clients than for clients connected to the wired LAN.

A DHCP *scope* is the full, consecutive range of possible IP addresses for a network, which typically defines a single physical subnet where DHCP services are offered. A DHCP *lease duration* is the specified time during which the IP addresses within the DHCP scope can be leased.

Define separate scopes for your wired subnets and your wireless subnets, so that you can configure the lease duration differently for the clients requiring DHCP services on your WLAN than for the clients on your wired LAN.

The default lease duration for a DHCP scope is eight days. This might be optimal for clients on your wired network. Because wireless clients do not release their addresses when the wireless user roams to a new subnet, you should decrease the lease duration substantially for wireless clients. By setting a shorter lease duration for wireless clients, you free IP addresses for reuse throughout the day instead of leaving the addresses unavailable for as long as eight days. When determining the optimal lease duration for the wireless clients in your environment, keep in mind the additional processing load that the shorter lease duration places on your DHCP server.

For more information about configuring scopes and lease durations on a DHCP server, see “Deploying DHCP” in this book.

RADIUS: Verifying Support for 802.1X and EAP-TLS

Verify that the RADIUS servers, such as IAS, support EAP-TLS and PEAP-MS-CHAP v2 authentication. Optionally, verify that the RADIUS servers support the use of the NAS-Port-Type attribute in their Access-Request messages. IAS uses the NAS-Port-Type attribute to identify the wireless connection types.

Computers running Windows Server 2003 or Windows 2000 Server IAS can be used for RADIUS support. A Windows 2000 IAS server must have Service Pack 3 (SP3) or later installed.



Note

You can configure IAS in Windows Server 2003, Standard Edition, with a maximum of 50 RADIUS clients and a maximum of 2 remote RADIUS server groups. You can define a RADIUS client by using a fully qualified domain name or an IP address, but you cannot define groups of RADIUS clients by specifying an IP address range. If the fully qualified domain name of a RADIUS client resolves to multiple IP addresses, the IAS server uses the first IP address returned in the DNS query.

With IAS in Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition, you can configure an unlimited number of RADIUS clients and remote RADIUS server groups. In addition, you can configure RADIUS clients by specifying an IP address range.

By using IAS as your RADIUS server and Active Directory as your directory service, you can provide a single sign-on solution. IAS uses Active Directory as its user accounts database. The same set of credentials is used to control network access (authenticating and authorizing access to a network), to log the user on to an Active Directory domain, and to control access to resources in the domain.

The RADIUS server must support the EAP-TLS authentication protocol, which is used in certificate-based security environments. In addition, EAP-TLS is required if you are using smart cards for network access authentication. The RADIUS server also must support the PEAP-MS-CHAP v2 authentication protocol, which is used in password-based security environments.

Certificate Infrastructure: Verifying Support for EAP-TLS and PEAP-MS-CHAP v2

To support EAP-TLS authentication, verify that the certificate infrastructure supports issuing user and computer certificates to wireless client computers and issuing computer certificates to your RADIUS servers.

To support PEAP-MS-CHAP v2 authentication, verify that your RADIUS servers have the appropriate computer certificates installed, and that each wireless client computer has the root certification authority (CA) certificates of the issuers of the computer certificates of the RADIUS servers installed.

You can use a third-party CA to issue certificates for wireless access, as long as the certificates that you install fulfill the requirements for TLS authentication.

For more information about certificate requirements, see the discussion of deploying a certificate infrastructure in “Implementing a WLAN Test Environment” later in this chapter. For information about designing and deploying a certificate infrastructure, see “Designing a Public Key Infrastructure” in *Designing and Deploying Directory and Security Services*.

Eliminating Single Points of Failure

To ensure that wireless clients can continue to be authenticated on the network and can access resources and applications, eliminate single points of failure in your network infrastructure by including:

- Redundant services (such as Active Directory domain controllers) on separate subnets.
- Clustered DHCP services, in the event that one of the cluster nodes fails.
- DNS on all domain controllers, in the event that a DNS server fails.
- Redundant RADIUS servers and proxies, to provide fault tolerance for RADIUS-based authentication.
- Redundant switches and routers, in the event that a switch or router fails.
- Redundant network paths between switches and routers.

Defining IP Addressing and Subnets

Determine how many additional IP addresses your wireless clients will require, and whether or not to define additional subnets.

► **To determine the number of additional IP addresses that you will need for wireless access:**

1. Calculate the number of additional IP addresses that wireless users will require:
 - a. Determine the average number of wireless clients currently using your corporate network at any given time.
 - b. Add to this the estimated number of additional concurrent wireless clients your network will need to support in the future.
2. Estimate the number of APs (and associated IP addresses) that you will need for wireless network access. For information about how to determine how many wireless APs to deploy, see “Designing Wireless AP Location” later in this chapter.

Based on the number of IP addresses that you will add to accommodate your WLAN, decide whether or not to add additional subnets.

Creating separate subnets for your wireless networking components offers many benefits, including:

- Wired network components do not have to draw from the same pool of existing IP addresses as your wireless clients.
- IP addresses for wireless clients are easier to identify, which assists in easier management and troubleshooting.
- Separate subnets give you increased control over DHCP lease times.
- You can associate each of your physical subnets (both wireless and wired) with sites within Active Directory, which enables you to assign network access policies to the specific subnets.
- If all APs are on the same subnet, you can provide seamless network-layer roaming for the wireless clients. *Network-layer roaming* allows a wireless client to associate with a new AP within the same subnet, in the same wireless network. When crossing subnets, applications that cannot handle a change of address, such as some e-mail applications, might fail.



Note

Network-layer roaming is to be distinguished from *general roaming*, which allows a wireless client to associate with a new AP within the same wireless network. In network-layer roaming, the wireless client associates with a new AP on the same subnet, within the same wireless network.

Example: An Enterprise Corporation Designs Subnets and IP Addressing for a WLAN

IEEE 802.11 APs are designed with Ethernet ports and use TCP/IP as a networking protocol. Thus, an enterprise corporation designed their network so that the wireless APs in the building are all attached to the same separate subnet, which is connected to a router.

To avoid using IP addresses from existing subnets, they assigned all of the wireless components to a separate subnet. Because they used a separate subnet for wireless components, the wireless components did not adversely affect the available number of host addresses allocated on previously configured wired subnets.

To keep track of the allocation of IP addresses, they created the IP address numbering scheme shown in Table 11.1. The corporation adopted this numbering convention for all of their buildings that have wireless network connectivity.

Table 11.1 Example IP Address Allocation for IP Subnet 172.16.50.0/24

IP Address	Device
172.16.50.1	Router
172.16.50.2–172.16.50.10	Servers (terminal, proxy, IAS, and so forth)
172.16.50.11–172.16.50.x	Wireless APs
172.16.50.x+1–172.16.50.254	Wireless clients

Under this addressing scheme, addresses were assigned in the following manner:

- Within the IP subnet 172.16.50.0/24, they assigned the router connecting to the rest of the network the first IP address of 172.16.50.1.
- They assigned other devices — such as terminal servers, proxy servers, and IAS servers — addresses from 172.16.50.2 through 172.16.50.10.
- They assigned the wireless APs sequential IP addresses starting with 11. To make it easier to keep track of the wireless APs, they assigned IP addresses that were 10 digits higher than the wireless AP number. For example, Wireless AP 1 was assigned 172.16.50.11, Wireless AP 2 was assigned 172.16.50.12, and so forth.

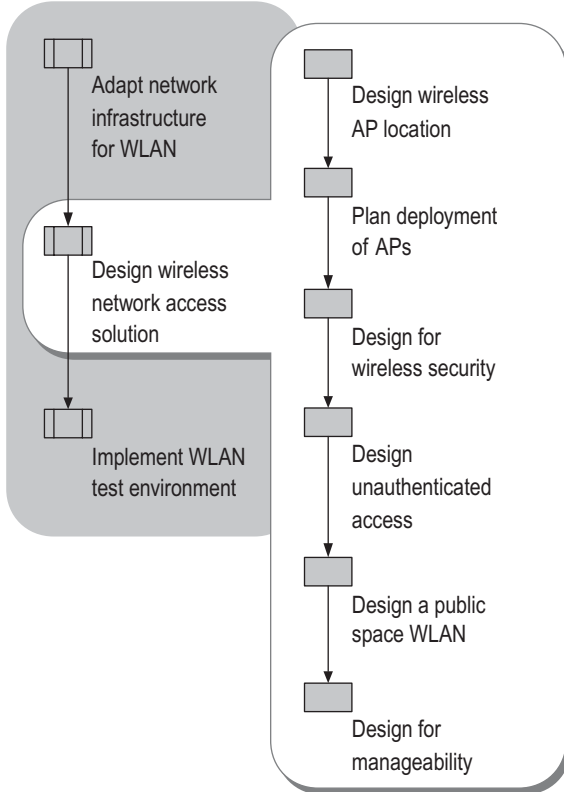
As is usual practice, they assigned static IP addresses to the APs and any servers on the subnet. To prevent the DHCP server from allocating a static IP address to a wireless client, they created a DHCP scope for the wireless subnet that did not include the assigned servers and APs (the scope range was 172.16.50.x+1 through 172.16.50.254).

They located all APs in a building on the same subnet, which allowed network-layer roaming throughout the building. This also made IP addressing by DHCP servers more manageable. The DHCP server assigned wireless clients dynamic IP addresses.

Designing a Wireless Network Access Solution

In designing your wireless network access solution, determine where to locate wireless APs and plan how to deploy the APs; design security for wireless access; if needed, design for unauthenticated access and for a public space WLAN; and, finally, optimize your design for manageability. Figure 11.3 shows the process for designing your wireless network access solution.

Figure 11.3 Designing Your Wireless Network Access Solution



Designing Wireless AP Location

After designing and verifying that the services needed for your network infrastructure to support an enterprise WLAN are in place, begin the design process for the location of the wireless APs.

To determine where to locate your wireless APs:

- Identify the areas of coverage for wireless users.
- Determine how many wireless APs to deploy.
- Determine where to place wireless APs.
- Select the channel frequencies for wireless APs.

Identifying the Areas of Coverage for Wireless Users

To identify the areas of coverage for wireless users:

1. Obtain or create scaled architectural drawings of each floor for each building, in each geographic location in your organization that has wireless users.
2. On the drawing, identify the offices, conferences rooms, lobbies, or other areas where you want to provide wireless coverage.

It might be useful to enable wireless coverage for a building in its entirety rather than for specific locations within the building. For example, this can prevent connectivity problems that might result from undocking a laptop from an office for use in a different part of your building.

3. Indicate any devices that interfere with the wireless signals.

Any device that operates on the same frequencies as your wireless devices (in the 2.4 through 2.5 GHz ISM range) might interfere with the wireless signals. Devices that operate on the same frequency include:

- Existing Bluetooth-enabled devices
- Microwave ovens
- Some models of cordless telephones
- Wireless video cameras
- Medical equipment

4. Indicate any building construction materials that interfere with wireless signals.

Metal objects used in the construction of a building can affect the wireless signal. For example, the following common objects interfere with signal propagation:

- Support girders
- Elevator shafts
- Rebar reinforcement in concrete
- Heating and air-conditioning ventilation ducts
- Wire mesh that reinforces plaster or stucco in walls



Note

Radio frequency attenuation (the reduction of signal strength), shielding, and reflection can affect how you deploy your APs. Refer to the manufacturer of your APs for information regarding the different scenarios that might increase the radio frequency attenuation. Testing software is available with most APs to check for signal strength, error rate, and data throughput. This can be very beneficial during the deployment of your APs.

Determining How Many Wireless APs to Deploy

To determine how many wireless APs to deploy, following these guidelines:

- Include enough wireless APs to ensure that wireless users have sufficient signal strength from anywhere in the area of coverage.

Wireless APs typically have an indoor range within a 150-foot radius. Include enough wireless APs to ensure signal overlap between the wireless APs.

- Determine the maximum number of simultaneous wireless users per coverage area.
- Estimate the data throughput that the average wireless user requires.

Add additional wireless APs to:

- Improve wireless client network bandwidth capacity.
- Increase the number of wireless users supported within a coverage area

Based on the total data throughput of all users, determine the number of users that you can connect through a wireless AP. Obtain a clear picture of throughput before deploying the network or making changes. Some wireless vendors provide an 802.11 simulation tool, which you can use to model traffic in a network and view throughput levels under various conditions.

- Ensure redundancy, in the event that a wireless AP fails.

Determining Where to Place Wireless APs

It is important to locate the APs close enough together to provide ample wireless coverage but far enough apart to not interfere with each other and increase the error rate. The actual distance needed between any two APs depends upon the combination of the type of AP, the type of AP antenna, and the construction of the building, as well as on sources of signal degradation, shielding, and reflection. For specifications and guidelines for placing wireless APs, see the manufacturer's documentation for the APs and the antennas used with them.

Maintain the best average ratio of wireless clients to APs. The greater the number of wireless clients that are associated with the AP, the lower the effective data transmission rate. Too many wireless clients attempting to use the same AP degrade the effective throughput or available bandwidth for each wireless client. By adding APs, you can increase throughput. To increase the number of APs per wireless client, you must increase the number of APs in a given coverage area. You can move APs closer together up to a point before they start to interfere with each other.

To determine where to place the wireless APs:

1. On the architectural drawings, place wireless APs so that each wireless AP is no further than 300 feet from an adjacent wireless AP.
2. To test the wireless AP placement, perform a site survey:
 - Temporarily place wireless APs in the locations specified on the architectural drawings.
 - Using a laptop equipped with an 802.11 wireless adapter and site survey software (site survey software ships with most wireless adapters), determine the signal strength within each coverage area.
3. In coverage areas where signal strength is low, make any of the following adjustments:
 - Reposition existing APs to increase the signal strength for that coverage area.
 - Reposition or eliminate devices that interfere with signal strength (such as Bluetooth devices or microwave ovens).
 - If possible, reposition or eliminate metal obstructions that interfere with signal propagation (such as filing cabinets and appliances).
 - Add additional wireless APs to compensate for the weak signal strength.

It is important to remember that radio frequency is three-dimensional. It can be conceptualized as a sphere of signal.

 - Purchase antennas to meet the requirements of your building infrastructure.
For example, to eliminate interference between APs located on adjoining floors in your building, you can purchase directional antennas that flatten the signal (forming a donut-shaped signal distribution) to increase the horizontal range and decrease the vertical range.
4. Update the architectural drawings to reflect the final number and placement of the wireless APs.

Example: An Enterprise Corporation Determines AP Location

An enterprise corporation used information from the manufacturer of its APs and from internal testing to determine the best locations for their APs when using IEEE 802.11b. They determined that a 30-foot radius for each AP (with 60 feet between adjacent APs) would provide the best coverage without interference between the APs.

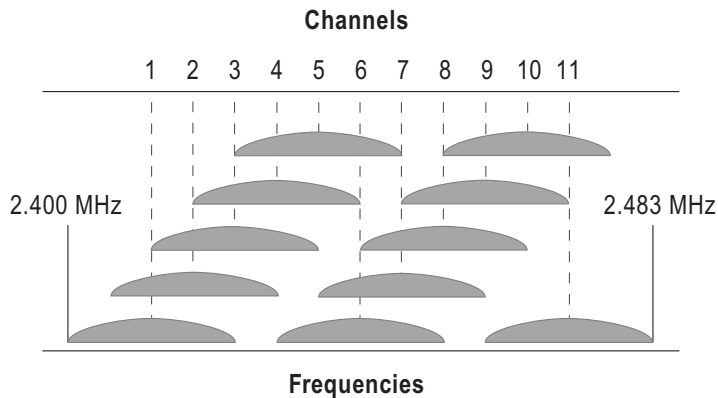
To assist them in designing AP locations, the IT staff created a plan view of the building, with one drawing per floor. The floor plans displayed the location, name, IP address, and channel information for each AP. Based on the information in the floor plans, the IT staff determined that they could locate their APs in the plenum area between the lowered ceiling and the next floor up, which simplified troubleshooting for the AP equipment.

Selecting Channel Frequencies for Wireless APs

Direct communication between an 802.11 wireless network adapter and an AP occurs over a common channel corresponding to a frequency range in the S-Band ISM frequency range. You set the channel in the AP, and the wireless network adapter automatically tunes to the channel of the AP with the strongest signal. The wireless network adapter continues communication with the AP until the signal gets weak, at which time it attempts to locate another AP with a stronger signal.

To reduce interference between wireless APs, ensure that wireless APs with overlapping signals use unique channel frequencies. The 802.11b standard reserves 14 frequency channels for use with wireless APs. Within the United States, the Federal Communications Commission (FCC) allows channels 1 through 11. In most of Europe, you can use channels 1 through 13. In Japan, you have only one choice: channel 14.

Figure 11.4 shows the 11 802.11b frequency channels available in the United States. Notice that the 802.11b signals overlap with adjacent channel frequencies. As a result, you can only use three channels (in the United States, channels 1, 6, and 11) without causing interference between adjacent APs.

Figure 11.4 Channel Overlap for 802.11b APs in the United States

To select the channel frequencies for the wireless APs:

1. Identify any wireless networks owned by other organizations in the same building. Find out the placement of their wireless APs and the channel frequencies assigned to the APs.

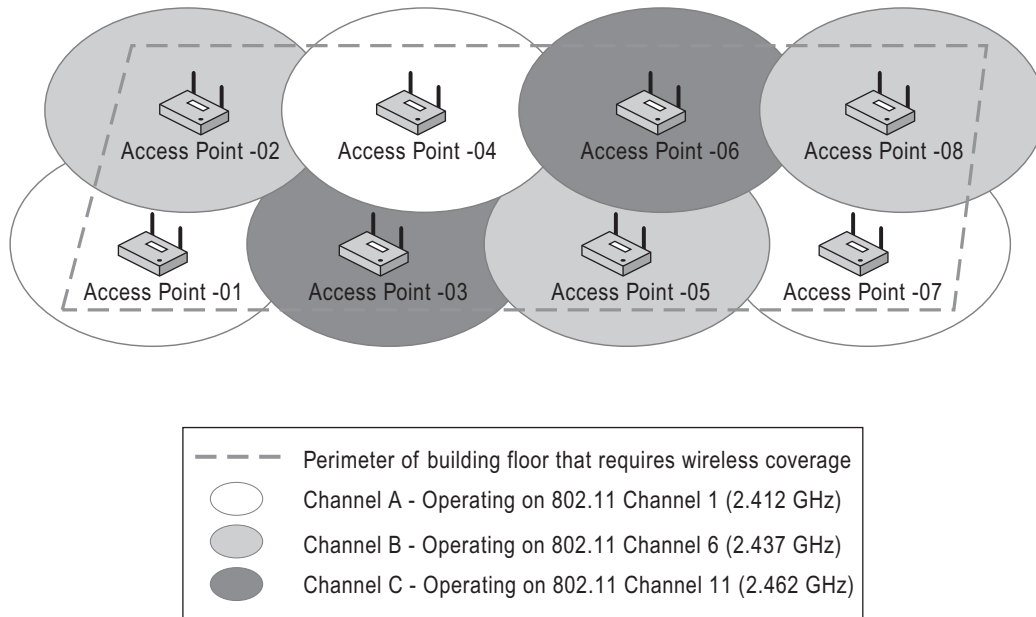
Radio waves travel through floors and ceilings, so APs located near each other on different floors need to be set to non-overlapping channels. If another organization located on a floor adjacent to your organization's offices has a wireless network, the wireless APs for that organization might interfere with the wireless APs in your network. Contact the other organization to determine the placement and frequencies of their wireless APs so that you can ensure that any of your own wireless APs that provide overlapping coverage use a different channel frequency.
2. Identify overlapping wireless signals on adjacent floors within your own organization.
3. After identifying overlapping coverage areas outside and within your organization, assign channel frequencies for your wireless APs.
 - a. Assign channel 1 to the first wireless AP.
 - b. Assign channels 6 and 11 to any wireless APs that overlap coverage areas with the first wireless AP, to ensure that those APs do not interfere with one another.
 - c. Continue assigning channel frequencies to the wireless APs, ensuring that any two wireless APs with overlapping coverage are assigned different channel frequencies.

Example: An Enterprise Corporation Determines IEEE 802.11b Channels

An enterprise corporation occupies multiple floors in a building. Because of this, they had to pay attention to both the horizontal and vertical dimensions when determining which IEEE 802.11b channel to assign to each AP. For example, if a certain spot on the first floor used channel 1, they assigned channel 6 to the same location on the second floor, and assigned channel 11 to the same location on the third floor. They did not use channel 1 again until the fourth floor.

Figure 11.5 illustrates the selection of channels for the wireless APs on a building floor. The wireless AP channels were selected to ensure that no two overlapping areas of coverage have the same channel (frequency).

Figure 11.5 Example of 802.11b Channel Allocation



Planning the Deployment of APs

After determining where to locate APs, you need to make additional decisions about how you will deploy the APs. These decisions affect the types of equipment required, where the equipment should be located, and how the equipment will be installed

Will you install the APs on the walls of your building or in the plenum area?

If you place your APs in the plenum area, you must determine the best method for powering the APs. Consult with the AP manufacturer to determine how to meet the power requirements for the APs. Some wireless APs can receive electrical power through the Ethernet cable.

The plenum area is regulated by fire codes. Therefore, for plenum placement, you must purchase APs that are fire-rated.

Will you preconfigure APs before installing them or configure them remotely?

Preconfiguring the APs before installing them on location can speed up the deployment process and can save labor costs, because less skilled workers can perform the physical installation. You can preconfigure APs by using the console port (serial port), Telnet, or a Web server that is integrated with the AP. If you will use a terminal server for console configuration of APs, decide where to locate the terminal server. Regardless of whether you decide to preconfigure the APs, make sure that you can access them remotely, particularly if you deploy many APs. This enables you to configure or upgrade the APs remotely by using scripts.

The terminal server can be located on the same subnet as the APs, or elsewhere.

It is helpful to physically locate the terminal server in the same wiring closet as the hub or patch panel connecting the AP. With this arrangement, you can pull together the Ethernet and console (serial) wires at the same time. This is only possible if the wires are run to and from the same place. You can then complete the configuration of many APs from a central location.

What model of antenna will you use for the APs?

For example, in a building with multiple floors, an omnidirectional antenna — which propagates the signal equally in all directions except the vertical — might work best. For information about which type of antenna will work best for your WLAN deployment, see the documentation for your APs.

What model of AP will you purchase?

The AP must be able to be configured as a RADIUS client and must support Wired Equivalent Privacy (WEP) and 802.1X authentication.

Example: An Enterprise Corporation Mounts APs in the Plenum Area

An enterprise corporation learned that mounting its APs in the plenum area would resolve some of the issues raised during their pilot test of their wireless network deployment.

For instance, users often disconnected data and power cables from the APs in order to plug their portable computers into the network. The unavailable APs prompted many service calls to the Help desk.

In addition, the IT staff found that by mounting APs in the plenum area, they could install APs in doorways and halls, avoiding users' offices. Though the initial installation cost was higher, they believe the placement will pay off in the long term in decreased user interference during working hours.

The enterprise corporation worked closely with the manufacturer of the APs to ensure that all procedures were followed and that the wireless APs were fire-rated for plenum placement.

Designing for Wireless Security

In designing security for your wireless LAN, choose the appropriate level of basic security available under IEEE 802.11 and 802.1X. Then, to close inherent security risks associated with wireless networking, require authorization and authentication of wireless clients before they exchange data with the network attached to the wireless APs, and encrypt the data sent between wireless clients and APs.

Choosing the Right Basic Security for Your WLAN

IEEE 802.11 open system or shared key authentication does not scale appropriately for a large, infrastructure mode wireless network (corporate offices and public places, such as airports and malls). In a large enterprise environment, you should not deploy 802.11 without also deploying 802.1X and RADIUS support.

To ensure the highest level of security for a WLAN in a corporate enterprise environment, use 802.1X with EAP-TLS authentication, a PKI, and RADIUS. The wireless clients must support 802.1X in a WLAN deployment using EAP-TLS.

Microsoft 802.1X Authentication Client provides 802.1X support for computers running any of the following Windows operating systems: Microsoft® Windows® 2000, Windows® 98, and Windows NT® version 4.0 Workstation. For more information, see Microsoft 802.1X Authentication Client link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.



Note

The Microsoft 802.1X Authentication Client is only available for Windows® 98 and Windows NT® version 4.0 Workstation to customers who have Microsoft Premier Support.

Windows XP provides 802.1X support and additional wireless support, including automatic wireless configuration.

Closing Inherent Security Risks for WLANs

While providing convenience, wireless networking technologies and wireless APs present security risks. In wireless networks, the signals can be intercepted because the data is broadcast using an antenna. Furthermore, if the signals are not encrypted, an eavesdropper outside the premises can view the packets sent on a wireless network.

Wireless networking technologies and wireless APs present two security risks:

- Any person with a compatible wireless network adapter can associate with your wireless APs and attach to your network.
- Because wireless networking signals use radio waves to send and receive information, anyone within a certain distance of a wireless AP can detect and receive all data sent to and from the wireless AP.

Enforcing authorization and authentication

To counter the first security risk, wireless APs must require authentication and authorization of the wireless client before data can be sent to, and received from, the network attached to the wireless AP.

The solution is to use the combination of an 802.1X-enabled wireless client, such as Windows XP; an IEEE 802.1X-enabled and RADIUS-capable wireless AP; and EAP-capable RADIUS servers such as Windows Server 2003 IAS.

With this combination, wireless APs can send connection requests and accounting messages to central RADIUS servers. The RADIUS servers have access to a user accounts database, such as Active Directory, and a set of rules for granting authorization, such as IAS remote access policies. The RADIUS server processes the wireless AP connection request, and either accepts or rejects it.

Encrypting data

To counter the second security risk, encrypt the data sent between the wireless clients and the wireless APs. The method of encryption defined by the IEEE 802.11b standard is Wired Equivalent Privacy (WEP). To provide per-session strong cryptographic keys for WEP encryption, use EAP-TLS, PEAP-TLS, or PEAP-MS-CHAP v2 as the authentication method. IAS has been enhanced to support both PEAP-MS-CHAP v2 and EAP-TLS.

EAP-TLS, as defined in RFC 2716, is the TLS authentication scheme as an EAP type. TLS is used in certificate-based security environments. EAP-TLS is a secure channel (SChannel) authentication protocol that provides for mutual authentication, integrity-protected cipher-suite negotiation, and key exchange between the two endpoints by means of public key cryptography.

PEAP-MS-CHAP v2 provides a secure wireless authentication solution for small businesses without requiring a certificate infrastructure (PKI) and the installation of a user or computer certificate on each wireless client. With PEAP, you can use a password-based authentication method to securely authenticate wireless connections. PEAP creates an encrypted channel before the password-based authentication occurs. Therefore, password-based authentication exchanges such as occur in MS-CHAP v2 are not subject to offline dictionary attacks.



Note

PEAP with MS-CHAP v2 is provided with Windows XP Service Pack 1 (SP1) and later, Windows Server 2003, and Microsoft 802.1X Authentication Client.

Designing Unauthenticated Access

Unauthenticated EAP-TLS access can be useful in both corporate and public space environments.

In a corporate environment, this feature can be used to grant guest access to visitors such as consultants. The unauthenticated users are redirected to a specific virtual LAN (VLAN), which provides only limited network access, such as access to the Internet.

In a public space environment, a wireless Internet service provider (ISP) can use this feature to give potential subscribers access to a restricted VLAN with local information. When the person subscribes for Internet access, the ISP provides connectivity to the Internet.

EAP-TLS unauthenticated access provides a means to grant guest access for a wireless client that does not have a certificate installed. EAP-TLS supports one-way authorization or unauthenticated access when a client does not send credentials. If a network access client does not provide credentials, IAS determines whether unauthenticated access is enabled in the remote access policy that matched the connection attempt.

Windows Server 2003 and IAS support unauthenticated wireless connections. For more information about unauthenticated wireless access, see “Wireless access” in Help and Support Center for Windows Server 2003.

Designing a Public Space WLAN

If you plan to deploy a public space WLAN in a venue such as an airport or shopping mall, you need to design your WLAN to meet some additional requirements.

- Plan for a single wireless network infrastructure that multiple service providers can share and access.

A single wireless network infrastructure eliminates radio frequency interference. Because of the finite number of non-overlapping channels available in 802.11b, multiple wireless network infrastructures in the same location cause interference among wireless APs with overlapping channel frequencies.

- Make sure that the APs support VLANs, the capability for beaconing multiple Service Set Identifiers (SSIDs, also known as *network names*), and the capability for binding each SSID to a separate VLAN.

Enhanced APs are necessary in a public space WLAN deployment. VLAN support enables the AP to route the wireless client to the correct network path. The capability for beaconing multiple SSIDs enables multiple service providers to share the same wireless network infrastructure. After the wireless client associates with the correct SSID, the AP must bind that SSID to the correct VLAN in order to route the network traffic to the correct destination. The AP maintains a table that maps each SSID to its respective VLAN number. The public space WLAN also must allow non-802.1X wireless clients access. To support this, you must assign a VLAN number for all non-802.1X wireless clients. The VLAN number routes the non-802.1X clients to a VLAN that is configured to provide non-802.1X clients with 802.1X credentials.

- To provide security, you need an IEEE 802.1X and RADIUS-capable wireless AP, and an EAP-capable RADIUS server such as Windows Server 2003 IAS.
- You might need to provide billing and accounting for services provided to customers connecting through the public space WLAN.

A public space WLAN must provide a means for charging for services provided, typically by an ISP, to customers connecting through the public space WLAN. An ISP can charge the customer for this service in several ways. It can bill for the total time connected, the quantity of data transferred, or a combination of the two methods.

You can configure the same IAS server that is used for the authorization of wireless users to capture this connection data and save it to an accounting log file. The log file contains the connection time, the amount of data transferred during a session, and other data that can be used to produce billing records for ISP customers. Database exporting can convert the log files into a format that can be read and interpreted to provide the billing records. IAS for Windows Server 2003 can also be configured to send accounting information to a SQL server database.

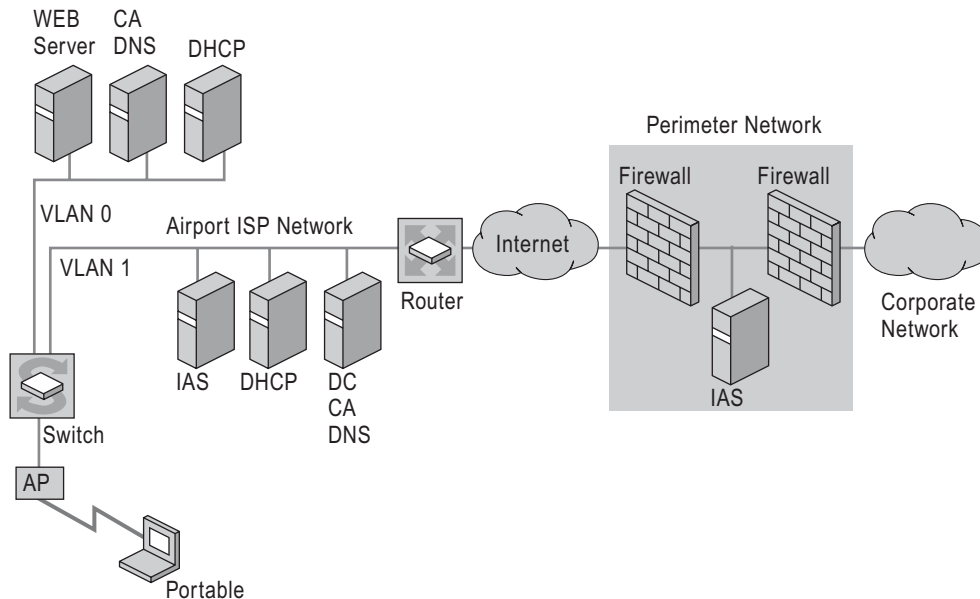
In addition, third-party software is available to create billing solutions.

- Provide sufficient bandwidth to support the volume of users likely to use a public space WLAN.

In designing a public space WLAN, consider how many users need to connect simultaneously through each AP. For example, if you design for an average bandwidth of 56 kilobits per second (Kbps), approximating a 56K modem, more users will be able to associate with the network than if you design the average bandwidth to be more than 56 Kbps.

Figure 11.6 shows the infrastructure for a public space WLAN with 802.1X designed for an airport. This public space WLAN enables ISPs to provide Internet access for general and corporate users with wireless devices that are 802.11b-capable.

Figure 11.6 Example of a Public Space WLAN Infrastructure in an Airport



Example: Public Space WLAN Access

A user with a computer running Windows XP (with the Wireless Zero Configuration [WZC] service and IEEE 802.1X) starts his computer. The wireless adapter attempts to authenticate with an AP, but can only associate with VLAN 0 since it has no authorization for VLAN 1, the ISP network for the airport. When associated with VLAN 0, the wireless device is directed to the airport's ISP Web server.

The Web server queries the user about access to the Internet or another company's network. As a free service, the ISP's Web site provides local travel information, including arrival and departure times and restaurants. If the user chooses to set up an account, the ISP creates the account for billing purposes and provides the wireless user with a certificate to join VLAN 1.

The wireless user now has a certificate and can access VLAN 1. The user is authenticated using IAS, which simultaneously creates or appends a log file. The log file and new user account are both used for billing purposes. The wireless user is granted permission to access the Internet.

If the user decides to access his own corporate network across the Internet, a virtual private network (VPN) connection can be created from the wireless client to a VPN server in the perimeter network.



Note

As an alternative to a VLAN, a public space wireless network can support IP filtering. This requires the use of APs that are capable of IP filtering and can be configured to restrict access to only the IP addresses for the ISP's certificate, DHCP, and Web servers. These servers provide the minimum connectivity and services that are required in order to obtain authenticated access.

If an AP is associated with repeatedly when you use IP filtering for authentication, the AP can consume the allotted quantity of IP addresses that the DHCP server has set aside, preventing additional wireless clients from obtaining an IP address. Although the infrastructure for IP filtering is less costly, because IP filtering saves a switch and a server, IP filtering is less secure. For these reasons, it is better to use a VLAN than IP filtering for a public space wireless network.

Designing for Manageability

For a large wireless deployment to be practical, it must be easy to manage. The combination of Windows XP and Windows Server 2003 allows for efficient management of your wireless network.

For optimal manageability of your wireless network, ensure that your wireless clients use Windows XP, which provides support for automatic switching between APs during roaming and support for zero configuration through the WZC. Although you can use other Windows operating systems with Microsoft 802.1X Authentication Client, they do not support zero configuration.

Automatic Switching Between APs During Roaming

Windows XP supports automatic switching between APs when roaming, autodetection of wireless networks, 802.1X, and automatic wireless configuration.

Windows XP has improved and built upon the wireless support for clients that Windows 2000 provides. In Windows 2000, *media sense capability* (the capability for detecting an attached network) is used to control the configuration of the network stack and inform the user and applications when the network is unavailable. With Windows XP, media sense capability is used to enhance the wireless roaming experience. This is done by detecting a move to a new AP and then forcing re-authentication and DHCP renewal to ensure appropriate network access during roaming. Windows XP in addition supports autodetection of a wireless network, and automatic wireless configuration with the Wireless Zero Configuration (WZC) service.

Distributing Certificates Through Autoenrollment

An IAS server, which acts as a RADIUS server and proxy, also supports EAP-TLS. Because both Windows XP and IAS in Windows Server 2003 support EAP-TLS, the combination gives you support for a strong authentication method and a per-session key management system. To ease deployment, you can distribute the computer and user certificates used for authentication through certificate autoenrollment. *Autoenrollment* is the automatic requesting and issuing of certificates based on Group Policy settings.

Table 11.2 lists the types of certificates (user, computer, or both) for which autoenrollment is supported with each combination of client and server operating system. When using any other clients, such as Windows NT or Windows 98, you must manually enroll each client or use a scripted solution.

Table 11.2 Support for Autoenrollment of Certificates Provided in Windows

Client	Server	Computer	User
Windows XP or Windows Server 2003	Windows Server 2003	•	
Windows XP or Windows Server 2003	Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition	•	•
Windows XP or Windows Server 2003	Windows 2000 Server	•	
Windows 2000	Windows Server 2003	•	
Windows 2000	Windows 2000 Server	•	

For more information about the design and deployment of IAS, see “Deploying IAS” in this book.

Taking Advantage of Autoconfiguration

The addition of the Wireless Zero Configuration (WZC) service in Windows XP improves the manageability of your wireless network. The WZC service dynamically selects the wireless network to which to attempt connection based either on your preferences or on default settings. When a more preferred wireless network becomes available, the WZC service automatically selects and connects to that network. If none of the preferred wireless networks is found nearby, the WZC service configures the wireless adapter so that there is no accidental connection until the wireless client roams within the range of a preferred network.

To improve the roaming experience by automating the process of configuring the network adapter to associate with an available network, Microsoft partnered with 802.11 wireless adapter vendors. The wireless network adapter scans for available networks and passes them to Windows XP, which then configures the wireless network adapter with an available network. If you are not using a WZC-capable network adapter, you must configure the network adapter manually by using the configuration software that the manufacturer provides.

For improved manageability of your wireless network, ensure that your wireless clients are using Windows XP so the WZC service is available. Windows Server 2003 also provides this service, which is known in Windows Server 2003 as the Wireless Configuration service. The Microsoft 802.1X Authentication Client does not provide WZC and roaming support.

Managing APs Remotely

For better manageability, design your network so that you can manage your APs from a remote location. You can remotely manage APs by using the AP console port (serial port) and an asynchronous terminal server, a Telnet session, or a Web server that is integrated with the AP.

To configure an AP for network access by an asynchronous terminal server, use the two unused pairs of Ethernet cable to return the serial communication lines to the data closet where they can be connected to an asynchronous terminal server. This enables you to configure an AP remotely if necessary. If you arrange to switch power off remotely, you can also restart APs remotely when they are not responding to a signal from an Ethernet or console port.

Using these methods, you will be able to completely manage APs remotely except when an AP fails and must be repaired or replaced.

Using Active Directory-based Wireless Network Policies

To centrally manage the configuration of secure wireless connections for wireless client computers, you can create Active Directory-based wireless network policies that specify the types of networks that users can access, preferred networks, WEP settings, IEEE 802.X settings, and other settings for wireless connections. The settings are configured in Group Policy, in Wireless Network (IEEE 802.1) Policies. The wireless network policy is replicated to computers that are associated with the computer configuration Group Policy object. Users do not need to enter the configurations or select settings.

For example, you can configure the following items in the Wireless Network (IEEE 802.11) Policies settings:

- Types of networks that users can access
For example, you might restrict users' access to an AP (infrastructure) network only, or to a computer-to-computer (ad hoc) network only.
- Network name (SSID)
- WEP settings
- Enabling of network access control using IEEE 802.1X
- Authentication methods and settings

The Wireless Network (IEEE 802.11) Policies settings are only supported by wireless clients running Windows XP (SP1 and later) and Windows Server 2003.

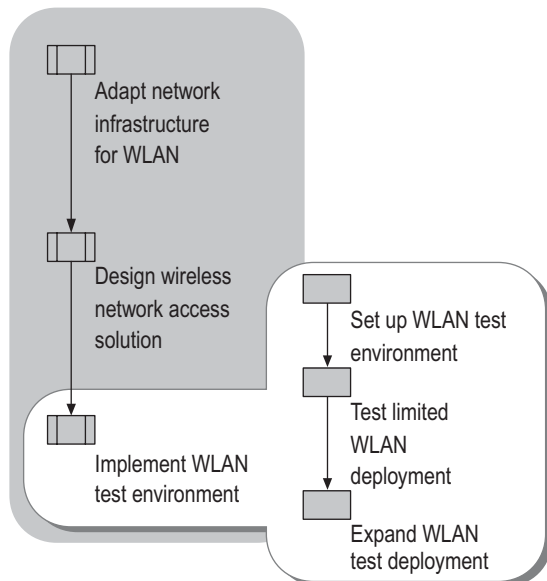
For information about:

- Opening the Group Policy Object Editor, see “Ways to open the Group Policy Object Editor” in Help and Support Center for Windows Server 2003. (Click the **Index** button, and in the keyword box type **Group Policy Object Editor**; then select **opening**.)
- Adding and defining wireless network policies, see “Define Active Directory-based wireless network policies” in Help and Support Center for Windows Server 2003.
- Designing wireless network policies, see “Deploying Security Policy” in *Designing a Managed Environment*.

Implementing a WLAN Test Environment

Before embarking on a full-scale WLAN deployment on your enterprise network, perform a trial deployment on a WLAN test network in your lab to familiarize yourself with how the technology works and resolve any issues that arise before deploying the enterprise WLAN. After setting up your WLAN test environment, perform a limited test to ensure that all components are working together under a simplified certificate infrastructure. Then expand the test environment, testing your Group Policy design and a three-tier CA infrastructure. Figure 11.7 shows the process for implementing a WLAN test environment.

Figure 11.7 Implementing Your WLAN Test Environment



Setting Up Your WLAN Test Environment

Keep your initial WLAN test deployment simple so that you can focus on successfully installing and configuring the essential components. To simplify your initial test:

- Test a basic, single-tier PKI.

When you deploy your enterprise WLAN, it is recommended that you provide the extra security of a three-tiered certificate infrastructure in which the root CA is offline. For guidelines for designing a certificate infrastructure, see “Designing a Public Key Infrastructure” in *Designing and Deploying Directory and Security Services*.

- Omit using Group Policy in your initial test.

In your production deployment, you will want to use Group Policy to preconfigure and control the following Wireless Network (IEEE 802.11) Policies settings for Windows XP (SP1 and later) and Windows Server 2003 wireless clients:

- Types of networks that users can access
For example, you might restrict users’ access to an AP (infrastructure) network only, or to a computer-to-computer (ad hoc) network only.
- Network name (SSID)
- Wireless network key (WEP) settings
- Enabling of network access control using IEEE 802.1X
- Authentication methods and settings

In your initial test deployment, install and configure the following components and services:

- Wireless APs
- Active Directory
- DNS and DHCP
- A single-tier PKI
- At least one RADIUS server (IAS)
- Wireless clients

After successfully deploying your initial WLAN test environment, add the use of Group Policy and deploy a WLAN with a three-tier PKI in your lab, and confirm that your WLAN still functions properly, to prepare for a successful production deployment.

Configuring Wireless APs

Configure your wireless APs according to the manufacturer's specifications.

To provide secure wireless connectivity, the APs must support WEP and 802.1X authentication.

Because your WLAN uses 802.1X and RADIUS, you do not need to manually enter the WEP keys: They are generated automatically during the EAP-TLS and PEAP-MS-CHAP v2 authentication process. (Most APs include the option for manually entering the WEP keys on the AP, which you can do if needed for the test deployment.)

In configuring the AP, you enter a value for the RADIUS shared secret, which you will later enter on the IAS server when you add the AP as a RADIUS client on the IAS server.

Configuring Active Directory for the WLAN

Your test deployment must include at least one Active Directory–based domain controller.

Perform the following configuration tasks in Active Directory:

- Configure the remote access permission on wireless user and computer accounts.
- Create a group for wireless user and computer accounts. You will create a remote access policy for the group.
- Register the IAS server in Active Directory.

Configuring the Remote Access Permission

To grant wireless user accounts and wireless computer accounts permission to access the network remotely, set the remote access permission in the computer and user accounts.

► To configure the remote access permission on wireless user and computer accounts

1. On a domain controller (or on a member server on which the Active Directory snap-ins are installed), open Active Directory Users and Computers.
2. To configure each wireless user account with the permission to access the network remotely, right-click the user object in the **Users** folder, click **Properties**, click the **Dial-in** tab, and then under **Remote Access Permission (Dial-in or VPN)**, select either **Control access through Remote Access Policy** (for native-mode domains) or **Allow access** (for mixed-mode domains).
3. To configure each computer account with the permission to create wireless connections, right-click the computer object in the **Computers** folder, click **Properties**, click the **Dial-in** tab, and then under **Remote Access Permission (Dial-in or VPN)**, select either **Control access through Remote Access Policy** (for native-mode domains) or **Allow access** (for mixed-mode domains).

Create a Group for Wireless Users and Computers

Create an Active Directory group to contain wireless users and computers. Later in the test deployment, you will create a group-based remote access policy for wireless connections and specify the group.

► To create a group for wireless users and computers

1. Open Active Directory Users and Computers.
2. Create a group for wireless users. For the test deployment, accept the default group scope — that is, create a global group.

For information about how to add a group, see “Creating user and group accounts” in Help and Support Center for Windows Server 2003.

3. Add each user account for wireless users and each computer account to be used for wireless access as a group member.

For information about how to add a member to a group, see “Changing group memberships” in Help and Support Center for Windows Server 2003.



Tip

If you are unable to add computer objects when adding members to a group, use the **Object Types** button in the **Select Users, Contacts, Computers, or Groups** dialog box to add computers to the types of objects that you can add to a group.

Register the IAS Server in Active Directory

The next step in setting up your WLAN test environment is to use the IAS snap-in to register the IAS server in Active Directory. The following procedure registers the IAS server by using the Internet Authentication snap-in.

► To register the IAS server in Active Directory

1. Open the Internet Authentication Service snap-in on the IAS computer.
2. Right-click **Internet Authentication Service (Local)** for the IAS server, and then click **Register Server in Active Directory**.
3. When asked if you want to authorize this computer to read users' dial-in properties for this domain, click **OK**.



Note

This procedure registers the IAS server only in its member domain, which is all that you need for your test deployment. For your production deployment, you will need to register the IAS server in its member domain, trusted domains, and so on. For information, see “Enable the IAS server to read user accounts in Active Directory” in Help and Support Center for Windows Server 2003.

Configuring DNS and DHCP

To support wireless computers in your test lab, your test deployment must include one or more servers running the DNS and DHCP services.

Configure the DNS and DHCP services as follows:

1. On the DNS server:
 - a. Ensure that the DNS zone in which the wireless computers will register DNS address records is configured for dynamic updates.
 - b. Optionally, specify that the DNS zone is an Active Directory-integrated zone, which provides secured updates, and that the DNS zone is to be updated by DHCP.
2. On the DHCP server, configure a separate scope and lease duration for your wireless client computers.

The DHCP scope should not include the static IP addresses of your APs or any of your servers.

For more information about configuring DHCP for your wireless deployment, see “Adapting the Network Infrastructure for a WLAN” earlier in this chapter. For information about configuring scopes and lease durations on a DHCP server, see “Deploying DHCP” in this book.

Deploying a Certificate Infrastructure

For your initial test lab deployment, use a simple certificate infrastructure. To be able to integrate the certificate services with Active Directory in your test environment (and, later, to use Group Policy to provide easier management of wireless clients), you must install the CA as an enterprise CA. After installing your enterprise root CA, you can install a computer certificate on the IAS server and install user and computer certificates on your wireless computers.

To set up the certificate infrastructure for your initial test environment, perform the following tasks:

- Install a single-tier CA.
- Install a computer certificate on the IAS server.
- Install user and computer certificates on wireless computers.

Installing a Single-Tier CA

To keep your initial test deployment simple, install a single-tier CA.

► To install a single-tier CA in your test environment

- Install the enterprise root CA either on the domain controller or on a separate member server in your test environment.

You must be logged on as a member of both the Enterprise Admins group and the Domain Admins group for the root domain.

For installation instructions, see “Install an enterprise root certification authority” in Help and Support Center for Windows Server 2003. For your test lab deployment, you do not need to add certificate templates to the CA or configure the CA to allow subjects to request a certificate based on a template.

Installing a Computer Certificate on the IAS Server

On the IAS server, install a computer certificate from the issuing CA, which, in the single-tier CA infrastructure that you will deploy in your WLAN test environment, is the enterprise root CA. For your test lab deployment, use the Certificates Request Wizard located in the Certificates snap-in to obtain a computer certificate.

Start by creating a Certificates console on the IAS server that contains the Certificates - Local Computer snap-in, which you will use to request the computer certificate.

► To install a computer certificate on the IAS Server

1. Create a Certificates console on your IAS server that contains the Certificates - Local Computer snap-in. For the test lab deployment, name the console Certificates.

For information about how to add a snap-in to manage certificates, see “Manage certificates for a computer” in Help and Support Center for Windows Server 2003. To perform this task, you must be a member of the Domain Admins group (or a member of the Administrators group on the local computer).

2. Use the Certificates console to request a computer certificate for the IAS server.

To install a computer certificate, click **Certificates - Local Computer** in the console tree, and select **Computer** as the certificate type (unless your IAS server is also a domain controller, in which case your only option is to select **Domain Controller**). For more information about how to use the Certificates console to request a certificate, see “Request a certificate” in Help and Support Center for Windows Server 2003.

For more information about using the Certificates Request Wizard for installing computer certificates, in addition to two alternative methods, see “Computer certificates for certificate-based authentication” in Help and Support Center for Windows Server 2003.

Verifying that the computer certificates meet IAS requirements

Each computer certificate installed on an IAS server must meet the following requirements:

- The certificate must be installed in the Local Computer certificate store.
- The cryptographic service provider for the certificate must support the secure channel (Schannel) security package. If not, the IAS server cannot use the certificate, and the certificate is not available for selection in the properties of the **Smart Card or other certificate** EAP type in the remote access policy.

The computer certificate for the IAS server must meet additional requirements. The following procedure tells how to verify each requirement.

► **To verify that the computer certificate for the IAS server meets all requirements**

1. From the **Certificates** console, double-click the certificate to open it.
2. On the **General** tab, confirm that **You have a private key that corresponds to this certificate** appears.
3. On the **Details** tab, under **Field**, click **Enhanced Key Usage**, and then confirm that there is an object identifier for Server Authentication (1.3.6.1.5.5.7.3.1).
4. On the **Details** tab, under **Field**, click **Subject Alternative Name**, and then confirm that the fully qualified domain name (FQDN) of the computer account for the IAS server (for example, **DNS Name=IASServerName.TestDomainName.com**) appears.
5. On the **Certification Path** tab, confirm that a valid certification path appears and that the statement **This certificate is OK** appears.

Verifying the root CA certificate

The root CA certificate of the CA that will issue the wireless client computer and user certificates must be installed in the Trusted Root Certification Authorities certificate store. The following procedure tells how to verify this.

► **To verify that the root CA is in the Trusted Root Certification Authorities store**

1. From the Certificates console, expand **Certificates - Local Computer**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
2. In the **Details** pane, confirm that the name of your test lab enterprise root CA appears in the **Issued To** list.

If the root CA is not in the list, you might need to refresh the display. To do this, **click Action**, and then click **Refresh**.

Installing User and Computer Certificates on Wireless Clients

When EAP-TLS is in use, as in your test lab deployment, wireless clients should have both a computer certificate and a user certificate in order to be authenticated to the network. When PEAP-MS-CHAP-v2 is in use, the root CA certificates of the issuing CAs for the computer certificates on the RADIUS servers must be installed on the wireless clients. You can do this manually by importing the root CA certificate on each wireless client, or you can publish the root CA certificate using Group Policy.

For your test lab deployment, use the Certificate Request Wizard located in the Certificates snap-in on the wireless client computer to obtain both a computer certificate and a user certificate for each wireless computer in your test lab.

▶ Before you begin

- Connect the wireless client directly to the wired network that contains the CA infrastructure. The connection is required in the test environment in order for the wireless client to receive computer and user certificates. In your enterprise environment, this step might not be necessary, depending upon how you decide to deploy certificates.

If you connect the wireless client to the wired network, you can install the user certificate on the wireless client by using the Certificates - Current User snap-in (as described in the procedure), by using autoenrollment, by submitting a certificate request over the Web, or by implementing a CAPICOM program or script. If you prefer not to make a temporary connection between the wireless client and the wired network, you can install the certificate from a floppy disk.



Note

CAPICOM is a COM client, supporting Automation, that performs cryptographic functions (the CryptoAPI) using Microsoft® ActiveX® controls and COM objects. For information about CAPICOM, see the CAPICOM link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources>.

▶ To install user and computer certificates on a wireless client

1. Create a single console that contains two snap-ins, for managing computer certificates and user certificates. For the test deployment, name the console Certificates.

- a. Install the snap-in for computer accounts under the name **Certificates - Local Computer**.

For information about how to install a snap-in for managing computer certificates, see “Manage certificates for a computer” in Help and Support Center for Windows Server 2003.

- b. Install the snap-in for user accounts under the name **Certificate - Current User**.

For information about how to install a snap-in for managing user certificates, see “Manage certificates for your user account” in Help and Support Center for Windows Server 2003.

To install both snap-ins, log on under a user account with administrative credentials for the local computer. (You can install the user certificates snap-in but not the computer certificates snap-in if you log on under a user account in the test domain.)



Note

For the initial test deployment, to receive computer and user certificates, the wireless client must be connected directly to the wired network that has the CA infrastructure.

2. Use the **Certificates - Local Computer** snap-in to request a computer certificate for the wireless client.

For instructions telling how to use the Certificates console to request a computer certificate, see “Request a certificate” in Help and Support Center for Windows Server 2003.

The Help topic provides instructions for requesting a *user* certificate. To request a *computer* certificate, instead of clicking **Certificates - Current User** in the console tree, click **Certificates - Local Computer**. Then, when prompted for a certificate type, select **Computer**.

3. Use the **Certificates - Current User** snap-in to request a user certificate.

For instructions telling how to use the Certificates console to request a user certificate, see “Request a certificate” in Help and Support Center for Windows Server 2003. When prompted for a certificate type, select **User**.

Verifying that the certificates meet all requirements

After installing the computer and user certificates, perform the following procedures to verify that the certificates meet all requirements for the client to perform properly over a wireless connection.

► To verify that the computer certificate for the wireless client meets requirements

1. Verify that the computer certificate is installed in the Local Computer certificate store (required for EAP-TLS authentication).

After verifying the correct certificate store, verify the certificate configuration.

2. From the **Certificates** console, double-click the certificate to open it.
3. On the **General** tab, confirm that the statement **You have a private key that corresponds to this certificate** appears.
4. On the **Details** tab, under Field :
 - a. Click **Enhanced Key Usage**, and confirm that the object identifier for Client Authentication is 1.3.6.1.5.5.7.3.2.
 - b. Click **Subject Alternative Name**, and confirm that the FQDN of the wireless computer account (for example, **DNS Name=LaptopName.TestDomainName.com**) appears.
5. On the **Certification Path** tab:
 - a. Confirm that a valid certification path appears.
 - b. Confirm that the statement **This certificate is OK** appears.

► **To verify that the user certificate for the wireless client meets requirements**

1. Verify that the user certificate is installed in the Current User certificate store (required for EAP-TLS authentication).
2. From the **Certificates** console, double-click the certificate to open it
3. On the **General** tab, confirm that **You have a private key that corresponds to this certificate** appears.
4. On the **Details** tab, under **Field**, confirm the following items:
 - a. Click **Enhanced Key Usage**, and confirm that the object identifier for Client Authentication is 1.3.6.1.5.5.7.3.2.
 - b. Click **Subject Alternative Name**, and confirm that the universal principal name (UPN) of the user account (**PrincipalName=WirelessUserName@TestDomainName.com**, for example) appears.
5. On the **Certification Path** tab:
 - a. Confirm that a valid certification path appears.
 - b. Confirm that the statement **This certificate is OK** appears.

Configuring the RADIUS (IAS) Server

Before you configure your RADIUS server, open Active Directory Users and Computers and verify that your IAS server is a member of the RAS and IAS Servers group.

Configure your RADIUS (IAS) server by performing the following tasks:

1. Add each wireless AP to the IAS server as a RADIUS client.
2. Create a remote access policy for wireless clients.

Adding APs as RADIUS Clients

On the IAS server, add each wireless AP as a RADIUS client. You will need to type the RADIUS shared secret that you configured earlier on the wireless AP.

► **To add a wireless AP as a RADIUS client on the IAS server**

1. Open the Internet Authentication Service snap-in.
2. In the console tree, right-click the **RADIUS Clients** folder, and then click **New RADIUS Client**.
3. In the **Friendly name** field, type a name for the AP.
4. In the **Client address (IP or DNS)** field, type the IP address of the wireless AP. Then click **Next**.
5. If the remote access policy for wireless users is designed for a specific model of wireless AP (for example, a remote access policy that contains vendor-specific attributes), in the **Client Vendor** list, select the manufacturer's name.
If you do not know the manufacturer, accept the default value, **RADIUS Standard**.
6. In the **Shared secret** and **Confirm shared secret** fields, type the shared secret value that you assigned when you configured the AP.

Creating a Remote Access Policy for Wireless Clients

To give wireless users access to the network, create a remote access policy for wireless clients, and then configure that policy for the highest level of encryption. To use IAS, you must be logged on using an account that has administrative credentials.

► **To add a remote access policy for wireless clients**

1. Open the Internet Authentication Service snap-in.
2. In the console tree, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
3. Complete the New Remote Access Policy Wizard using the information provided in Table 11.3. Accept default settings when no information is specified.

Table 11.3 Adding a Remote Access Policy for Wireless Users

Wizard Page	Action
Policy Configuration Method	For Policy Name, type an appropriate name, such as WLAN Test Policy.
Access Method	Select Wireless.
User or Group Access	Click Group, and then click Add. In the Select Groups dialog box, type the name of the group that you created for wireless users, and then click Check Names to confirm that the name you typed is correct.
Authentication Methods	Select Smart Card or other certificate.

- ▶ **To configure encryption for the new remote access policy**
 1. In the console tree of the Internet Authentication Service snap-in, right-click the newly created wireless access policy, and then click **Properties**.
 2. Verify that **Grant remote access permission** is selected, and then click **Edit Profile**.

Configuring the Wireless Adapter on Wireless Clients

On each wireless client, you can manually configure the wireless adapter to recognize the wireless network that the client must access in order to gain wireless connectivity. However, this is generally not necessary, because Windows XP will sense the wireless network and prompt the user via the notification bar. Once the user selects the network name, the network is automatically added to the preferred networks list.

▶ **To manually configure the client computer's wireless adapter to recognize the AP**

1. On the wireless computer, log on under a user account with administrative credentials on the local computer, and open **Network Connections**.
2. Right-click the wireless adapter icon, and click **Properties** to display properties for the wireless network adapter.
3. To configure TCP/IP for the wireless adapter, on the **General** tab, type the static IP address for your DNS server.
4. On the **Wireless Networks** tab, confirm that the name of the wireless network that you added appears in the **Available Networks** list.
5. Disable the network adapter that connects the client computer to the wired network, and then disconnect the client computer from the wire that connects it to the network.

Testing Your Limited WLAN Deployment

To test the deployment of your wireless network, roam the entire coverage area for your wireless network, associating with one AP after another. Use your floor plan (with the APs marked on it) to mark the areas that provide adequate coverage and those that require more troubleshooting. You should be able to roam around the building, associating with one AP after another, and test applications.

As you roam through coverage areas, perform the following tests to ensure that your wireless network will provide strong, uninterrupted coverage for wireless clients:

- Use the client software that the adapter manufacturer provided for the wireless device to determine that the wireless client associates with the nearest AP.

If the wireless client does not readily associate with the closest AP when you move from one AP's coverage area to the next, turn the network adapter's radio off and back on using software provided by the adapter manufacturer. This forces the wireless adapter to find the strongest signal, which usually is the closest AP.

The wireless client's ability to associate with an AP is determined by the error rate of the data packets and the signal strength. If the coverage from the first AP is still strong, the wireless transceiver receives few bad packets and maintains its association. If the closest AP is failing to associate with the wireless client, restarting the radio of the wireless network adapter forces the wireless adapter to find the strongest signal, which usually is the closest AP.

- Check the statistics for error rates and signal strength to be sure that they are within limits. Check the AP for throughput to determine whether the data transfer rate is adequate.

The following troubleshooting tools also can be useful when testing and deploying your WLAN:

- Use the Wireless Monitor MMC snap-in, included with Windows Server 2003, to gather and view statistical and configuration information for wireless APs and the Windows Server 2003 wireless client.
- Use a spectrum analyzer to determine the location and strength of interfering signals as you move from one signal area to another. A *spectrum analyzer* measures radio frequency radiation from low to high frequencies across a frequency spectrum. These signals are plotted on a graph that shows their strength and frequency. If necessary, you can shield or move any devices that are causing interference.
- Use a *protocol analyzer* to document usage intervals and traffic load. You can use Network Monitor or third-party tools to capture 802.11 packets sent between a wireless client and a wireless AP. With a protocol analyzer, you can capture 802.11 packets, but cannot view the contents of the encrypted payloads.

Expanding Your WLAN Test Deployment

After successfully deploying and testing a simple wireless network, you can add more complex features — such as Group Policy settings to more easily deploy and manage wireless clients, and a three-tier CA infrastructure to provide greater security for your enterprise WLAN.

Each time that you add a new component or feature, test your new deployment before expanding your test deployment further.

Configuring Group Policy Settings

For your initial test deployment, you configured your wireless clients without creating the Active Directory-based wireless network policies that enable you to preconfigure and replicate the wireless client configuration to all wireless clients. Wireless network policies are created by configuring Wireless Network (IEEE 802.11) Policies settings in Group Policy.

In addition, you did not use Group Policy to configure autoenrollment, which enables you to install certificates for the wireless clients automatically.

Instead, you manually configured some of the wireless client settings and used the Certificates console on the client computer to request the computer certificate. (Alternatively, you could have used Web enrollment to request the user or computer certificate.)

However, in your production WLAN deployment, you will want to use Group Policy to provide easier deployment and management of wireless clients and to enable autoenrollment for the installation of the certificates. Before embarking on an enterprise deployment of your WLAN, configure and test Group Policy settings to enable these features.



Note

To support automatic computer certificate allocation, the issuing CA must be an enterprise CA server running either Windows 2000 or Windows Server 2003. To support automatic user and computer certificate allocation, the issuing CA must be an enterprise CA server running either Windows Server 2003, Enterprise Edition or Windows Server 2003, Data Center Edition.

When you configure Group Policy settings to support your WLAN, decide whether you want to manage wireless connections through the domain or create a separate organizational unit (OU) for this purpose. Using an OU might be more efficient than entering Group Policy settings for the domain, which includes both wired and wireless clients.



Note

If you need to force a Group Policy update on the wireless client during your testing, you can use Gpupdate command-line tool. For Gpupdate parameters, see “Gpupdate: Command-line reference” in Help and Support Center for Windows Server 2003.

For more information about:

- Designing OUs, see “Designing the Active Directory Logical Structure” in *Designing and Deploying Directory and Security Services*.
- Designing group policies, see “Designing a Group Policy Infrastructure” in *Designing a Managed Environment*.

- Deploying autoenrollment, see “Planning for autoenrollment deployment” in Help and Support Center for Windows Server 2003.
- The appropriate way to open Group Policy Object Editor for a specific type of object, see “Ways to open the Group Policy Object Editor” in Help and Support Center for Windows Server 2003. (Click the **Index** button, and in the keyword box type **Group Policy Object Editor**; then select **opening**.)
- Adding and defining wireless network policies, see “Define Active Directory-based wireless network policies” in Help and Support Center for Windows Server 2003.

Installing a Three-Tier CA

When you deploy your enterprise WLAN, it is recommended that you provide the extra security of a three-tier certificate infrastructure in which the root CA is offline. Therefore, after you finish deploying and testing your WLAN test environment with a single-tier CA, and then introducing Group Policies and retesting, it is a good practice to install a test version of the CA infrastructure that you plan to implement in your enterprise environment in your lab before doing so in your production environment.

For information about designing and deploying a certificate infrastructure, see “Designing a Public Key Infrastructure” in *Designing and Deploying Directory and Security Services*.

Additional Resources

Related Information

- “Deploying DHCP” in this book for more information about deploying a DHCP solution on your network.
- “Deploying DNS” in this book for more information about deploying DNS within your client/server infrastructure.
- “Deploying ISA Server” in this book for more information about perimeter networks.
- “Deploying IAS” in this book and the *Networking Guide of the Windows Server 2003 Resource Kit* (or see the *Networking Guide* on the Web at <http://www.microsoft.com/reskit>) for more information about deploying an IAS infrastructure in your network.
- The Wi-Fi (IEEE 802.11b) link on the Web Resources page at <http://www.microsoft.com/windows/reskits/webresources> for more information about Microsoft support for IEEE 802.11b.

Related Help Topics

For best results in identifying Help topics by title, in Help and Support Center, under the **Search** box, click **Set search options**. Under **Help Topics**, select the **Search in title only** checkbox.

- “Enable the IAS server to read user accounts in Active Directory” in Help and Support Center for Windows Server 2003.
- “Install an enterprise root certification authority” in Help and Support Center for Windows Server 2003.
- “Request a certificate” in Help and Support Center for Windows Server 2003 for information about using the Certificates console to request a certificate.
- “Computer certificates for certificate-based authentication” in Help and Support Center for Windows Server 2003 for information about using the Certificates Request Wizard and other methods for installing computer certificates.
- “Manage certificates for a computer” in Help and Support Center for Windows Server 2003.
- “Manage certificates for your user account” in Help and Support Center for Windows Server 2003 for instructions telling how to install the **Certificates - My User Account** snap-in.
- “Planning for autoenrollment deployment” in Help and Support Center for Windows Server 2003.
- “Define Active Directory-based wireless network policies” in Help and Support Center for Windows Server 2003.
- “Gpupdate: Command-line reference” in Help and Support Center for Windows Server 2003 for information about forcing a Group Policy update on a wireless client.
- “Ways to open the Group Policy Object Editor” in Help and Support Center for Windows Server 2003. (Click the **Index** button and in the keyword box type **Group Policy Object Editor**; then select **opening**.)
- “Creating user and group accounts” in Help and Support Center for Windows Server 2003.
- “Changing group memberships” in Help and Support Center for Windows Server 2003.

