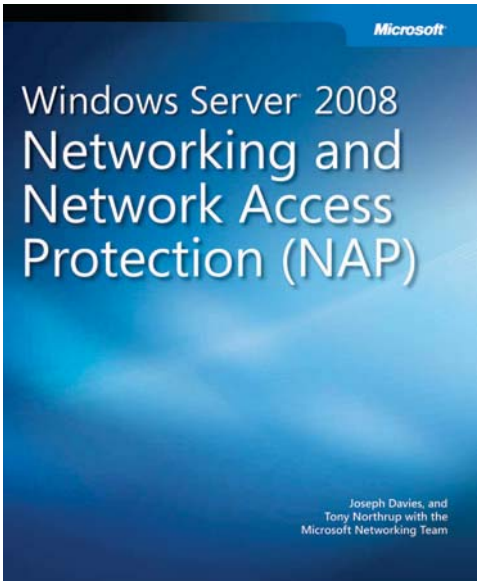

Windows Server® 2008 Networking and Network Access Protection (NAP)

Joseph Davies and Tony Northrup with the Microsoft Networking Team

To learn more about this book, visit Microsoft Learning at
http://www.microsoft.com/MSPress/books/11160.aspx

Microsoft® Press

978-0-7356-2422-1

Table of Contents

3 Dynamic Host Configuration Protocol

- Concepts
  - DHCP Clients, Servers, and Relay Agents
  - DHCP Messages and Options
- Planning and Design Considerations
  - DHCP Relay Agents
  - DHCP Servers
  - DHCP and Network Access Protection
  - High Availability for DHCP
  - DHCP with DNS and WINS
  - DHCP and Active Directory
  - Designing Scopes
- Deployment Steps
  - DHCP Relay Agents
  - DHCP Servers
  - DHCP Client Configuration
- Ongoing Maintenance
  - Adding and Removing DHCP Servers
  - Migrating DHCP Servers
- Troubleshooting
  - Tools
  - Common Problems

4 Windows Firewall with Advanced Security

- Concepts
  - Filtering Traffic with Windows Firewall
  - Protecting Traffic with IPsec
- Planning and Design Considerations
  - Exceptions for Windows Firewall
  - Protected Traffic with IPsec
- Deployment Steps
  - Firewall Settings with Group Policy
  - Server Isolation
  - Domain Isolation
  - Secure Server
- Ongoing Maintenance
  - Adding and Removing Windows Firewall Exceptions
  - Adding and Removing IPsec Exemptions
- Troubleshooting
  - Tools
  - Common Problems

5 Policy-Based Quality of Service

- Concepts
- The Causes of Network Performance Problems
- How QoS Can Help
- QoS for Outbound Traffic
- QoS for Inbound Traffic
- QoS Implementation
- Planning and Design Considerations
- Setting QoS Goals
- Planning DSCP Values
- Planning Traffic Throttling
- Hardware and Software Requirements
- Planning GPOs and QoS Policies
- QoS Policies for Mobile Users of Computers Running Windows Vista
- Deployment Steps
- How to Configure QoS by Using Group Policy
- How to Configure System-Wide QoS Settings
- Ongoing Maintenance
- Removing QoS Policies
- Editing QoS Policies
- Monitoring QoS
- Troubleshooting
- Analyzing QoS Policies
- Verifying DSCP Resilience
- Isolating Network Performance Problems

6 Scalable Networking

- Concepts
  - TCP Chimney
  - Receive-Side Scaling
  - NetDMA
  - IPsec offload
- Planning and Design Considerations
  - Designating Servers for Scalable Networking
- Deployment Steps
  - Configuring TCP Chimney
  - Configuring Receive-Side Scaling
  - Configuring NetDMA
  - Configuring IPsec Offload
- Ongoing Maintenance
  - Adding or Removing Scalable Networking Servers
  - Migrating Scalable Networking Servers
- Troubleshooting

Part III Network Access Infrastructure

9 Authentication Infrastructure

Concepts
Active Directory Domain Services
Public Key Infrastructure
Group Policy
RADIUS
Planning and Design Considerations
Active Directory
PKI
Group Policy
RADIUS
Deployment Steps
Deploying Active Directory
Deploying PKI
Group Policy
RADIUS Servers
Using RADIUS Proxies for Cross-Forest Authentication
Using RADIUS Proxies to Scale Authentications
Ongoing Maintenance
Active Directory
PKI
Group Policy
RADIUS
Troubleshooting Tools
Active Directory
PKI
Group Policy
RADIUS

10 IEEE 802.11 Wireless Networks

Concepts
Support for IEEE 802.11 Standards
Wireless Security
Components of 802.11 Wireless Networks
Planning and Design Considerations
Wireless Security Technologies
Wireless Authentication Modes
Intranet Infrastructure
Wireless AP Placement
Authentication Infrastructure
Wireless Clients
PKI

12 Remote Access VPN Connections

Concepts
Components of Windows Remote Access VPNs
Planning and Design Considerations
VPN Protocols
Authentication Methods
VPN Servers
Internet Infrastructure
Intranet Infrastructure
Concurrent Intranet and Internet Access for VPN Clients
Authentication Infrastructure
VPN Clients
PKI
VPN Enforcement with NAP
Additional Security Considerations
Strong Link Encryption
VPN Traffic Packet Filtering on the VPN Server
Firewall Packet Filtering for VPN Traffic
Multi-Use VPN Servers
Blocking Traffic Routed from VPN Clients
Concurrent Access
Unused VPN Protocols
Deploying VPN-Based Remote Access
Deploying Certificates
Configuring Internet Infrastructure
Configuring Active Directory for User Accounts and Groups
Configuring RADIUS Servers
Deploying VPN Servers
Configuring Intranet Network Infrastructure
Deploying VPN Clients
Ongoing Maintenance
Managing User Accounts
Managing VPN Servers
Updating CM Profiles
Troubleshooting
Troubleshooting Tools
Troubleshooting Remote Access VPNs

13 Remote Access VPN Connections

Concepts
Components of Windows Remote Access VPNs
Planning and Design Considerations
VPN Protocols

Chapter 10
IEEE 802.11 Wireless Networks

This chapter provides information about how to design, deploy, maintain, and troubleshoot Institute of Electrical and Electronic Engineers (IEEE) 802.11 wireless networks. Once deployed, the protected wireless network solution can be modified for the 802.1X Enforcement method of Network Access Protection (NAP) as described in Chapter 17, "802.1X Enforcement."

> **Note** This chapter assumes that you understand the role of the Active Directory, public key infrastructure (PKI), Group Policy, and Remote Authentication Dial-In User Service (RADIUS) elements of a Windows-based authentication infrastructure for network access. For more information, see Chapter 9, "Authentication Infrastructure."

Concepts

IEEE 802.11 wireless local area network (LAN) networking provides the following benefits:

- Wireless connections can extend or replace a wired infrastructure in situations where it is costly, inconvenient, or impossible to lay cables. This benefit includes the following:
    1. To connect the networks in two buildings separated by a physical, legal, or financial obstacle, you can either use a link provided by a telecommunications vendor (for a fixed installation cost and ongoing recurring costs), or you can create a point-to-point wireless link using wireless LAN technology (for a fixed installation cost but no recurring costs). Eliminating recurring telecommunications charges can provide significant cost savings to organizations.
    2. Wireless LAN technologies can be used to create a temporary network, which is in place for only a specific amount of time. For example, you can set up a wireless network for a convention or trade show rather than deploying the physical cabling required for a traditional Ethernet network.
    3. Some types of buildings, such as historical buildings, might be governed by building codes that prohibit the use of wiring, making wireless networking an important alternative.
- The wiring-free aspect of wireless LAN networking is also very attractive to homeowners who want to connect the various computers in their home together without having to drill holes and pull network cables through walls and ceilings.
- Increased productivity for the mobile employee. This benefit includes the following:
    1. The mobile user whose primary computer is a laptop or notebook computer can change location and always remain connected to the network. This enables the mobile user to travel to various places—meeting rooms, hallways, lobbies, cafeterias, classrooms, and so forth—and still have access to networked data. Without wireless access, the user has to carry cabling and is restricted to working near a network jack.

2. Wireless LAN networking is well suited for environments where movement is required. For example, retail environments can benefit when employees use a wireless laptop or palmtop computer to enter inventory information directly into the store database from the sales floor.
3. Even if no wireless infrastructure is present, wireless laptop computers can still form their own ad-hoc networks to communicate and share data with each other.

- Easy access to the Internet in public places. Beyond the corporate campus, access to the Internet and even corporate sites can be made available through public wireless "hot spot" networks. Airports, restaurants, rail stations, and common areas throughout cities can be provisioned to provide this service. When the traveling worker reaches his or her destination, perhaps meeting a client at their corporate office, limited access can be provided to the traveling worker through the local wireless network. The network can recognize that a user is from another corporation and create a connection that is isolated from the local corporate network but provides Internet access to the visiting user. Wireless infrastructure providers are enabling wireless connectivity in public areas around the world. Many airports, conference centers, and hotels provide wireless access to the Internet for their visitors.

Support for IEEE 802.11 Standards

Windows Vista, Windows Server 2008, Windows XP, and Microsoft Windows Server 2003 provide built-in support for 802.11 wireless LAN networking. An installed 802.11 wireless LAN network adapter appears as a wireless network connection in the Network Connections folder. Although there is built-in support for 802.11 wireless LAN networking, the wireless components of Windows are dependent upon the following:

The capabilities of the wireless network adapter

- The installed wireless network adapter must support the wireless LAN or wireless security standards that you require. For example, Windows Vista supports configuration options for the Wi-Fi Protected Access (WPA) security standard. However, if the wireless network adapter does not support WPA, you cannot enable or configure WPA security options.

The capabilities of the wireless network adapter driver

- To allow you to configure wireless network options, the driver for the wireless network adapter must support the reporting of all of its capabilities to Windows. Verify that the driver for your wireless network adapter was written for the capabilities of Windows Vista or Windows XP and is the most current version by checking Microsoft Update or the Web site of the wireless network adapter vendor.

Table 10-1 lists the IEEE wireless standards supported by Windows and by wireless network adapters, their maximum bit rate, range of frequencies, and their typical usage.

Table 10-1 802.11 Standards

Standard	Maximum Bit Rate	Range of Frequencies	Usage
802.11	2 megabits per second (Mbps)	S-Band Industrial, Scientific, and Medical (ISM) frequency range (2.4 to 2.5 GHz)	Obsolete. Not widely used.
802.11b	11 Mbps	S-Band ISM	Widely used.
802.11a	54 Mbps	C-Band ISM (5.725 to 5.875 GHz)	Not widely used due to expense and limited range.
802.11g	54 Mbps	S-Band ISM	Widely used. 802.11g devices are backward-compatible with 802.11b devices.
802.11n (standards development in progress)	250 Mbps	C-Band and S-Band ISM	Pre-standard ratification devices are available starting in August 2007. 802.11n devices can be backward-compatible with 802.11a, b, and g devices.

Note The S-Band ISM uses the same frequency range as microwave ovens, cordless phones, baby monitors, wireless video cameras, and Bluetooth devices. The C-Band ISM uses the same frequency range as newer cordless phones and other devices. Due to this overlapping use, there may be contention when multiple devices are active at the same time.

802.11 Operating Modes

Wireless LAN networks for all the IEEE 802.11 standards use the following operating modes:

Infrastructure mode

- The wireless network contains at least one wireless access point (AP), a device that bridges wireless-based computers to each other and to a wired network such as the Internet or an intranet.

Ad-hoc mode

- The wireless network contains no wireless APs. Wireless-based computers connect and communicate directly with each other. This chapter does not describe ad-hoc mode wireless networks.

Regardless of the operating mode, a *Service Set Identifier* (SSID), also known as the wireless network name, identifies a specific wireless network. You configure the SSID on the wireless AP for infrastructure mode or the initial wireless client for ad-hoc mode. The wireless AP or the initial wireless client periodically advertise the SSID so that other wireless nodes can discover and join the wireless network.

Wireless Security

Although IEEE 802.11 wireless LAN technologies provide the benefits previously described, they introduce security issues that do not exist for wired networks. Unlike the closed cabling system of an Ethernet network, which can be physically secured, wireless frames are sent as radio transmissions that propagate beyond the physical confines of your office. Any computer within range of the wireless network can receive wireless frames and send its own. Without protecting your wireless network, malicious users can use your wireless network to access your private information or launch attacks against your computers or other computers across the Internet.

To protect your wireless network, you must use authentication and encryption, as described as follows:

- Authentication requires that computers provide either valid account credentials (such as a user name and password) or proof that they have been configured with a specific authentication key before being allowed to send data frames on the wireless network. Authentication prevents malicious users from being able to join your wireless network.
- Encryption requires that the content of all wireless data frames be encrypted so that only the receiver can interpret its contents. Encryption prevents malicious users from capturing wireless frames sent on your wireless network and determining sensitive data. Encryption also helps prevent malicious users from sending valid frames and accessing your private resources or the Internet.

IEEE 802.11 wireless LANs support the following security standards:

- IEEE 802.11
- IEEE 802.1X
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)

IEEE 802.11

The original IEEE 802.11 standard defined the open system and shared key authentication methods for authentication and Wired Equivalent Privacy (WEP) for encryption. WEP can use either 40-bit or 104-bit encryption keys. However, the original IEEE 802.11 security standard has proven to be relatively weak and because there was no specified method for WEP encryption key management, cumbersome for widespread public and private deployment. Because of its susceptibility to attack and the widespread support of newer security standards such as WPA and WPA2, its use is highly discouraged.

IEEE 802.1X

IEEE 802.1X was a standard that existed for Ethernet switches and was adapted to 802.11 wireless LANs to provide much stronger authentication than the original 802.11 standard. IEEE 802.1X authentication is designed for medium and large wireless LANs that contain an authentication infrastructure consisting of Remote Authentication Dial-In User Service (RADIUS) servers and account databases such as the Active Directory domain service.

IEEE 802.1X prevents a wireless node from joining a wireless network until the node is successfully authenticated and authorized. Authentication verifies that wireless clients have valid account credentials and prevents users without valid credentials from being able to join your wireless network. Authorization verifies that the wireless client is allowed to make a connection to the wireless AP. IEEE 802.1X uses the Extensible Authentication Protocol (EAP) to exchange authentication credentials. IEEE 802.1X authentication can be based on different EAP authentication methods such as those using user name and password credentials or a digital certificate.

To address the key management issues of the original 802.11 standard, 802.1X authentication can produce dynamic WEP keys, which are mutually determined by the wireless client and RADIUS server. The RADIUS server sends the WEP key to the wireless AP after authentication completes. The combination of WEP encryption and dynamic keys determined for each 802.1X authentication is known as dynamic WEP.

WPA

Although 802.1X addresses the weak authentication and key management issues of the original 802.11 standard, it provides no solution to the weaknesses of the WEP encryption algorithm. While the IEEE 802.11i wireless LAN security standard, which will be discussed in the "WPA2" section later in this chapter, was being finalized, the Wi-Fi Alliance, an organization of wireless equipment vendors, created an interim standard known as Wi-Fi Protected Access (WPA). WPA replaces WEP with a much stronger encryption method known as the Temporal Key Integrity Protocol (TKIP). WPA also allows the optional use of the Advanced Encryption Standard (AES) for encryption.

WPA is available in two different modes:

WPA-Enterprise

- Uses 802.1X authentication and is designed for medium and large infrastructure mode networks

WPA-Personal

- Uses a preshared key (PSK) for authentication and is designed for small office/home office (SOHO) infrastructure mode networks

WPA2

The IEEE 802.11i standard formally replaces WEP and the other security features of the original IEEE 802.11 standard. Wi-Fi Protected Access 2 (WPA2) is a product certification available through the Wi-Fi Alliance that certifies wireless equipment as being compatible with the IEEE 802.11i standard. The goal of WPA2 certification is to support the additional mandatory security features of the IEEE 802.11i standard that are not already included for products that support WPA. For example, WPA2 requires support for both TKIP and AES encryption. WPA2 includes fast roaming techniques such as Pairwise Master Key (PMK) caching and pre-authentication.

How It Works: Fast Roaming for WPA2

When a wireless client authenticates using 802.1X, there are a series of messages sent between the wireless client and the wireless AP to exchange credentials (802.1X authentication) and to determine the pairwise transient keys (the 4-way handshake). The pairwise transient keys are used for encryption and data integrity of WPA2-protected wireless data frames. This message exchange introduces a delay in the connection process. When a wireless client roams from one wireless AP to another, the delay to perform 802.1X authentication can cause noticeable interruptions in network connectivity, especially for time-dependent traffic such as voice or video-based data streams. To minimize the delay associated with roaming to another wireless AP, WPA2 wireless equipment can optionally support PMK caching and preauthentication.

PMK Caching

As a wireless client roams from one wireless AP to another, it must perform a full 802.1X authentication with each wireless AP. WPA2 allows the wireless client and the wireless AP to cache the results of a full 802.1X authentication so that if a client roams back to a wireless AP with which it has previously authenticated, the wireless client needs to perform only the 4-way handshake and determine new pairwise transient keys. In the Association Request frame, the wireless client includes a PMK identifier that was determined during the initial authentication and stored with both the wireless client and wireless AP's PMK cache entries. PMK cache entries are stored for a finite amount of time as configured on the wireless client and the wireless AP.

To make the transition faster for wireless networking infrastructures that use a switch that acts as the 802.1X authenticator, Windows Vista and Windows Server 2008 calculate the PMK identifier value so that the PMK as determined by the 802.1X authentication with the switch can be reused when roaming between wireless APs that are attached to the same switch. This practice is known as *opportunistic PMK caching*.

Preauthentication

With preauthentication, a WPA2 wireless client can optionally perform 802.1X authentications with other wireless APs within its range while connected to its current wireless AP. The wireless client sends preauthentication traffic to the additional wireless AP over its existing wireless connection. After preauthenticating with a wireless AP and storing the PMK and its associated information in the PMK cache, a wireless client that connects to a wireless AP with which it has preauthenticated needs to perform only the 4-way handshake.

WPA2 clients that support preauthentication can preauthenticate only with wireless APs that advertise their preauthentication capability in Beacon and Probe Response frames.

WPA2 is available in two different modes:

WPA2-Enterprise

- Uses 802.1X authentication and is designed for medium and large infrastructure mode networks

WPA2-Personal

- Uses a PSK for authentication and is designed for SOHO infrastructure mode networks

Table 10-2 summarizes the 802.11 wireless LAN security standards.

Table 10-2 802.11 Wireless LAN Security Standards

Security Standard	Authentication Methods	Encryption Methods	Encryption Key Size (bits)	Comments
IEEE 802.11	Open system and shared key	WEP	40 and 104	Weak authentication and encryption. Use is highly discouraged.
IEEE 802.1X	EAP authentication methods	N/A	N/A	Strong EAP methods provide strong authentication.
WPA-Enterprise	802.1X	TKIP and AES (optional)	128	Strong authentication (with strong EAP method) and strong (TKIP) or very strong (AES) encryption.
WPA-Personal	PSK	TKIP and AES (optional)	128	Strong authentication (with strong PSK) and strong (TKIP) or very strong (AES) encryption.
WPA2-Enterprise	802.1X	TKIP and AES	128	Strong authentication (with strong EAP method) and strong (TKIP) or very strong (AES) encryption.
WPA2-Personal	PSK	TKIP and AES	128	Strong authentication (with strong PSK) and strong (TKIP) or very strong (AES) encryption.

Windows Vista and Windows Server 2008 support the following security standards for 802.11 wireless LAN networking (the wireless network adapter and driver must also support the standard):

- 802.11 with WEP
- 802.1X
- WPA-Enterprise
- WPA-Personal
- WPA2-Enterprise
- WPA2-Personal

Components of 802.11 Wireless Networks

Figure 10-1 shows the components of Windows-based 802.11 protected wireless networks.

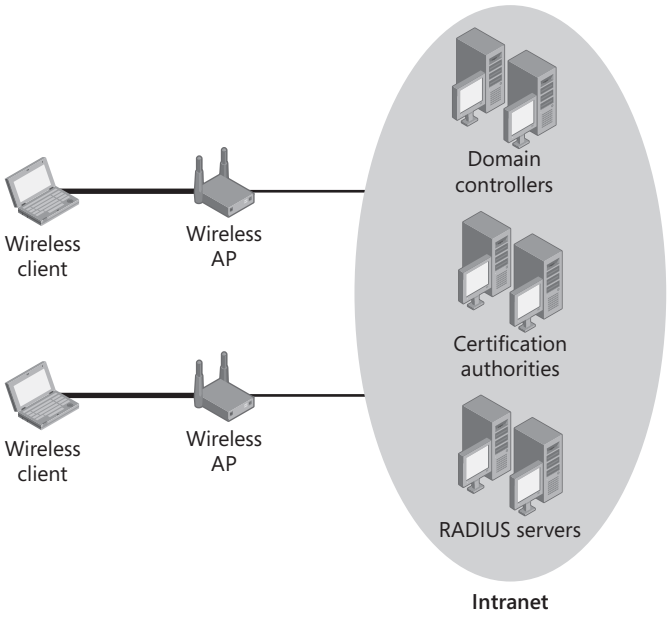

Figure 10-1 Components of Windows-based 802.11 protected wireless networks

The components are:

Wireless clients

- Initiate wireless connections to wireless APs and communicate with intranet resources or other wireless clients once connected

Wireless APs

- Listen for wireless connection attempts, enforce authentication and connection requirements, and forward frames between wireless clients and intranet resources

RADIUS servers

- Provide centralized authentication and authorization processing and accounting for network access attempts from wireless APs and other types of access servers

Active Directory domain controllers

- Validate user credentials for authentication and provide account information to the RADIUS servers to evaluate authorization

Certification authorities

- Part of the PKI that issues computer or user certificates to wireless clients and computer certificates to RADIUS servers

Planning and Design Considerations

When deploying a protected 802.11 wireless network solution, you need to consider the following for planning and design issues:

- Wireless security technologies
- Wireless authentication modes
- Intranet infrastructure
- Wireless AP placement

- Authentication infrastructure
- Wireless clients
- PKI
- 802.1X Enforcement with NAP

Wireless Security Technologies

Wireless security technologies are a combination of a wireless security standard (WPA2 or WPA) and an EAP authentication method. To authenticate the computer or the user that is attempting to make a protected wireless connection, Windows Vista and Windows Server 2008 support the following EAP authentication methods:

- EAP-TLS
- Protected EAP (PEAP)-TLS
- PEAP-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2)

EAP-TLS and PEAP-TLS are used in conjunction with a PKI and computer certificates, user certificates, or smart cards. With EAP-TLS, the wireless client sends its computer certificate, user certificate, or smart card certificate for authentication, and the RADIUS server sends its computer certificate for authentication. By default, the wireless client validates the RADIUS server's certificate. With PEAP-TLS, the wireless client and RADIUS server create an encrypted TLS session, and then the wireless client and RADIUS server exchange certificates. PEAP-TLS is the strongest authentication method because the certificate exchange between the wireless client and the RADIUS server is encrypted.

In the absence of computer certificates, user certificates, or smart cards, use PEAP-MS-CHAP v2. PEAP-MS-CHAP v2 is a password-based authentication method in which the exchange of authentication messages is protected with an encrypted TLS session, making it much more difficult for a malicious user to determine the password of a captured authentication exchange with an offline dictionary attack.

Despite the encrypted TLS session, however, both EAP-TLS and PEAP-TLS are much stronger than PEAP-MS-CHAP v2 because they do not rely on passwords.

Design Choices for Wireless Security Technologies

Microsoft recommends that you use one of the following combinations of wireless security technologies (in order of most to least secure):

- WPA2 with AES encryption, PEAP-TLS or EAP-TLS authentication, and both user and computer certificates
- WPA2 with AES encryption, PEAP-MS-CHAP v2 authentication, and a requirement for users to set strong user passwords
- WPA with EAP-TLS or PEAP-TLS authentication and both user and computer certificates
- WPA with PEAP-MS-CHAP v2 authentication and a requirement for users to set strong user passwords

Requirements for Wireless Security Technologies

The requirements for wireless security technologies are the following:

- For a protected wireless network, you must use either WPA or WPA2. If you use WEP, even dynamic WEP, your wireless network will not be secure. Dynamic WEP should not be used except temporarily when transitioning to a WPA2 or WPA-based security configuration.
- EAP-TLS or PEAP-TLS requires the installation of a computer certificate on the RADIUS server and a computer certificate, user certificate, or smart card on all wireless client computers. To validate the RADIUS servers' computer certificates, the root CA certificate of the issuing CA of the RADIUS server computer certificates must be installed on all wireless client computers. To validate the wireless clients' computer or user certificates, the root CA certificate of the issuing CA of the wireless client certificates must be installed on each of the RADIUS servers.
- PEAP-MS-CHAP v2 requires the installation of computer certificates on each of the RADIUS servers. It also requires that the root CA certificates of the RADIUS server computer certificates be installed on each of the wireless client computers.
- For WPA2, some wireless equipment might have to be replaced. Older wireless equipment that supports only 802.11 can typically be upgraded to support WPA but not WPA2.
- If you are planning to eventually deploy the 802.1X Enforcement method of NAP, you should use a PEAP-based authentication method such as PEAP-MS-CHAP v2 or PEAP-TLS.

Best Practices for Wireless Security Technologies

The best practices for wireless security technologies are the following:

- Do not use SSID suppression. The SSID (also known as the wireless network name) is by default included in the Beacon frames sent by wireless APs. Configuring your wireless APs to suppress the advertising of the SSID information element in Beacon frames does prevent the casual wireless client from discovering your wireless network. However, SSID suppression does not prevent a more sophisticated hacker from capturing other types of wireless management frames sent by your wireless AP and determining your SSID. Wireless networks with SSID suppression enabled are known as *non-broadcast* or *hidden* networks.

  Besides being a weak form of wireless network name privacy, non-broadcast wireless networks also create problems for authorized wireless clients that want to automatically connect to the non-broadcast wireless network. For example, because the wireless network name is not being advertised, the wireless client must send Probe-Request messages containing the wireless network name in an attempt to locate a wireless AP for the wireless network. These messages advertise the name of the wireless network, reducing the privacy of the wireless configuration of the wireless client.
- Do not use media access control (MAC) address filtering. MAC address filtering allows you to configure your wireless APs with the set of MAC addresses for allowed wireless clients. MAC address filtering adds administrative overhead in order to keep the list of

allowed MAC addresses current and does not prevent a hacker from spoofing an allowed MAC address.

- If you must use PEAP-MS-CHAP v2, require the use of strong passwords on your network. Strong passwords are long (longer than 8 characters) and contain a mixture of upper and lower case letters, numbers, and punctuation. In an Active Directory domain, use Group Policy settings in Computer Configuration/Windows Settings/Security Settings/Account Policies/Password Policy to enforce strong user passwords requirements.

Wireless Authentication Modes

Windows-based wireless clients can perform authentication using the following modes:

Computer-only

- Windows performs 802.1X authentication with computer credentials before displaying the Windows logon screen. This allows the wireless client to have access to networking resources such as Active Directory domain controllers before the user logs on. Windows does not attempt authentication with user credentials after the user logs on.

User-only

- By default, Windows performs 802.1X authentication with user credentials after the user logon process has completed. Windows does not attempt authentication with computer credentials before the user logon.

Computer-or-user

- Windows performs an 802.1X authentication with computer credentials before displaying the Windows logon screen. Windows performs another 802.1X authentication with user credentials either after the user has logged on or when the wireless client roams to a new wireless AP.

Problems with the default behavior of user-only authentication mode are as follows:

- A user cannot perform an initial domain logon to a computer because locally cached credentials for the user's user account are not available and there is no connectivity to the domain controller to authenticate new logon credentials.
- Domain logon operations will not be successful because there is no connectivity to the domain controllers of the Active Directory domain during the user logon process. Logon scripts, Group Policy updates, and user profile updates will fail, resulting in Windows event log errors.

Some network infrastructures use different virtual LANs (VLANs) to separate wireless clients that have authenticated with computer credentials from wireless clients that have authenticated with user credentials. If the user-level authentication to the wireless network and the switch to the user-authenticated VLAN occurs after the user logon process, a Windows wireless client will not have access to resources on the user-authenticated VLAN—such as Active Directory domain controllers—during the user logon process. This can lead to unsuccessful initial logons and domain logon operations such as logon scripts, Group Policy updates, and user profile updates.

To address the availability of network connectivity when performing user logon in user-only authentication mode and user-or-computer authentication mode when using

separate VLANs, Windows Vista and Windows Server 2008 wireless clients support Single Sign On. With Single Sign On., you can specify that wireless network authentication with user credentials occur before the user logon process. To enable and configure Single Sign On., you can use the Wireless Network (IEEE 802.11) Policies Group Policy extension to configure a Windows Vista policy, or you can run **netsh wlan** with the appropriate parameters. For more information, see the section "Configuring Wireless Clients" in this chapter.

Requirements for Wireless Authentication Modes

Only wireless clients running Windows Vista or Windows Server 2008 support Single Sign On.

Best Practices for Wireless Authentication Modes

Best practices for wireless authentication modes are the following:

- Use user-or-computer authentication mode; user authentication occurs after user logon. This is the default authentication mode.
- If you are using user-only authentication mode, configure your wireless profiles to enable Single Sign On. and perform wireless authentication with user credentials before user logon to prevent initial and domain logon problems.
- If you are using different VLANs for computer- and user-authenticated wireless clients and computer-or-user authentication mode, configure your wireless profiles to enable Single Sign On. and perform wireless authentication with user credentials before user logon to prevent initial and domain logon problems.

Intranet Infrastructure

Wireless clients need the same TCP/IP configuration settings and connectivity as wired clients, but there are differences in how you should configure wireless clients because of their inherent mobility. For this reason, place your wireless clients on different subnets than your wired clients rather than have a mixture of wired and wireless clients on the same subnet.

Subnet Design for Wireless Clients

Creating separate subnets for your wireless clients provides the following benefits:

- Wired network components do not have to draw from the same pool of existing IPv4 addresses as your wireless clients.
- Wireless clients are easier to identify from their IPv4 and IPv6 address prefixes, which makes it easier to manage and troubleshoot wireless clients.
- Separate IPv4 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 allows you to assign Group Policy settings to specific subnets.
- If all of your wireless APs are on the same subnet, your wireless clients can seamlessly perform network-layer roaming.

Network-layer roaming occurs when a wireless client connects to a different wireless AP for the same wireless network within the same subnet. For network-layer roaming, the wireless client renews its current DHCP configuration. When a wireless client connects to a different wireless AP for the same wireless network that is on a different subnet, the wireless client gets a new DHCP configuration that is relevant to that new subnet. When you cross a subnet boundary, applications that cannot handle a change of IPv4 or IPv6 address, such as some e-mail applications, might fail.

When creating an IPv4 subnet prefix for your wireless clients, consider that you need at least one IPv4 address for the following:

- Each wireless AP's LAN interface that is connected to the wireless subnet
- Each router interface that is connected to the wireless subnet
- Any other TCP/IP-capable host or device that is attached to the wireless subnet
- Each wireless client that can connect to the wireless network. If you underestimate this number, Windows wireless clients that connect after all of the available IPv4 addresses have been assigned through DHCP to connected wireless clients will automatically configure an IP address with no default gateway using Automatic Private IP Addressing (APIPA). This configuration does not allow connectivity to the intranet. Wireless clients with APIPA configurations will periodically attempt to obtain a DHCP configuration.

Because each IPv6 subnet can support a very large number of hosts, you do not need to determine the number of IPv6 addresses needed for the IPv6 subnet prefix.

DHCP Design for Wireless Clients

With different subnets for wired and wireless clients, you must configure separate DHCP scopes. Because wireless clients can easily roam from one wireless subnet to another, you should configure the lease for the DHCP scopes to have a shorter duration for wireless subnets than for wired subnets.

The typical lease duration for a DHCP scope for wired networks is a specified number of days. Because wireless clients do not release their addresses when roaming to a new subnet, you should shorten the lease duration to several hours for DHCP scopes corresponding to wireless subnets. By setting a shorter lease duration for wireless subnets, the DHCP server will automatically make IPv4 addresses that are no longer being used by wireless clients available for reuse throughout the day instead of leaving the addresses unavailable for 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 DHCP scopes, see Chapter 3, "Dynamic Host Configuration Protocol."

Wireless AP Placement

An important and time-consuming task in deploying a wireless LAN is determining where to place the wireless APs in your organization. Wireless APs must be placed to provide seamless coverage across the floor, building, or campus. With seamless coverage, wireless

users can roam from one location to another without experiencing an interruption in network connectivity, except for a change in IPv4 and IPv6 addresses when crossing a subnet boundary. Determining where to place your wireless APs is not as simple as installing them and turning them on. Wireless LAN technologies are based on propagation of a radio signal, which can be obstructed, reflected, shielded, and interfered with.

When planning the deployment of wireless APs in an organization, you should take the following design elements into consideration (as described in the following sections):

- Wireless AP requirements
- Channel separation
- Signal propagation modifiers
- Sources of interference
- Number of wireless APs

Note For additional specifications and guidelines for placing wireless APs, see the manufacturer's documentation for the wireless APs and the antennas used with them.

Wireless AP Requirements

You must identify the requirements for your wireless APs, which might include the following features:

- WPA
- WPA2
- 802.1X and RADIUS
- 802.11a, b, g, and n

Depending on your budget and bandwidth requirements, you might need wireless APs that support 802.11b, 802.11a, 802.11g, or a combination of technologies.

Building or fire code compliance

- The plenum area (the space between the suspended ceiling and the ceiling) is regulated by building and fire codes. Therefore, for plenum placement of APs and associated wiring, you must purchase wireless APs that are fire-rated and in compliance with building and fire codes. If you place your wireless APs in the plenum area, you must determine the best method for powering the wireless APs. Consult with the wireless AP manufacturer to determine how to meet the power requirements for the wireless APs. Some wireless APs can receive electrical power through the Ethernet cable that connects them to the wired network.

Preconfiguration and remote configuration

- Preconfiguring the wireless 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 wireless APs by using the console port (serial port), Telnet, or a Web server that is integrated with the wireless AP. Regardless of whether you decide to preconfigure the wireless APs, make sure that you can access

them remotely, configure the wireless APs remotely through a vendor-supplied configuration tool, or upgrade the wireless APs by using scripts.

Antenna types

- Verify that the wireless AP supports different types of antennas. For example, in a building with multiple floors, a loop antenna—which propagates the signal equally in all directions except vertically—might work best.

> **Note** For information about which type of antenna will work best for your wireless WLAN deployment, see the documentation for your wireless APs.

IPsec support

- Although not a requirement, if possible, choose wireless APs that use Internet Protocol security (IPsec) and Encapsulating Security Payload (ESP) with encryption to provide data confidentiality for RADIUS traffic sent between wireless APs and RADIUS servers. Use Triple Data Encryption Standard (3DES) encryption and, if possible, certificates for Internet Key Exchange (IKE) main mode authentication.

Channel Separation

Direct communication between an 802.11b or 802.11g wireless network adapter and a wireless AP occurs over a common channel, which corresponds to a frequency range in the S-Band ISM. You configure the wireless AP for a specific channel, and the wireless network adapter automatically configures itself to the channel of the wireless AP with the strongest signal.

To reduce interference between 802.11b wireless APs, ensure that wireless APs with overlapping coverage volumes use unique frequency channels. The 802.11b or 802.11g standards reserve 14 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 10-2 shows the channel overlap for 802.11b and 802.11g wireless APs in the United States.

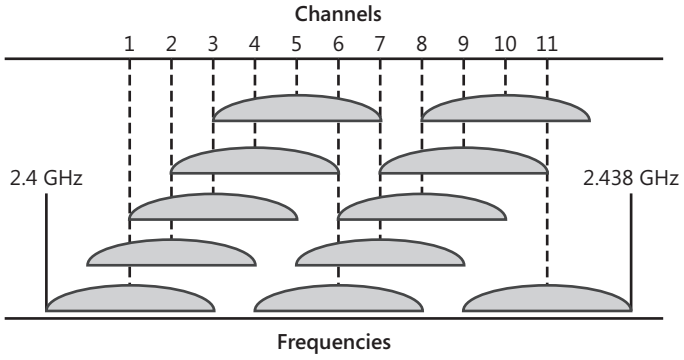

Figure 10-2 Channel overlap for 802.11b and 802.11g wireless APs in the United States

To prevent signals from adjacent wireless APs from interfering with one another, you must set their channel numbers so that they are at least five channels apart. To get the most usable channels in the United States, you can set your wireless APs to use one of three channels: 1, 6, or 11. If you need fewer than three usable channels, ensure that the channels you choose maintain the five-channel separation.

Figure 10-3 shows an example of a set of wireless APs deployed in multiple floors of a building so that overlapping signals from adjacent wireless APs use different usable channel numbers.

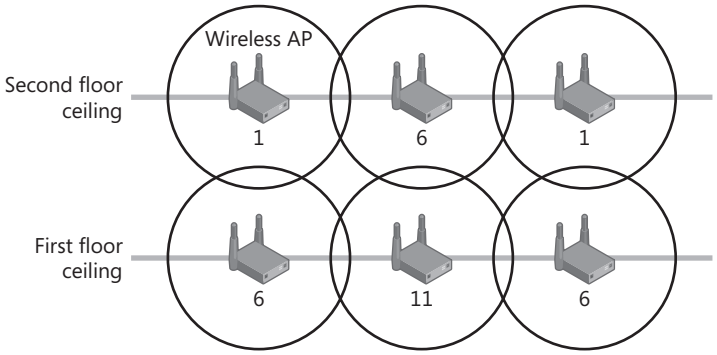

Figure 10-3 Example of assigning 802.11b channel numbers

Signal Propagation Modifiers

The wireless AP is a radio transmitter and receiver that has a limited range. The volume around the wireless AP for which you can send and receive wireless data for any of the supported bit rates is known as the *coverage volume*. (Many wireless references use the term *coverage area*; however, wireless signals propagate in three dimensions.) The shape of the coverage volume depends on the type of antenna used by the wireless AP and the presence of signal propagation modifiers and other interference sources.

With an idealized omnidirectional antenna, the coverage volume is a series of concentric spherical shells of signal strengths corresponding to the different supported bit rates. For example, Figure 10-4 shows an example of the idealized coverage volume for 802.11b and an omnidirectional antenna.

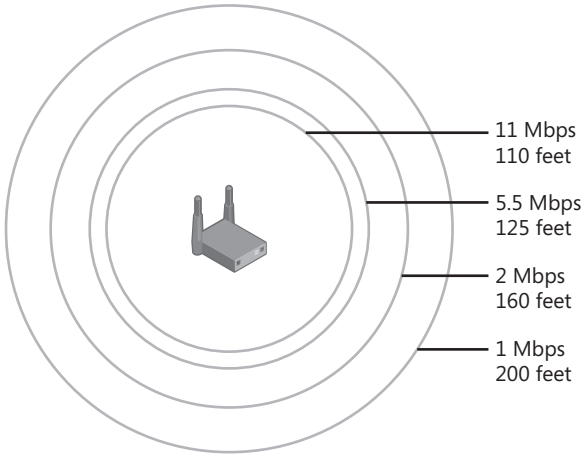

Figure 10-4 Idealized coverage volume example

Signal propagation modifiers change the shape of the ideal coverage volume through radio frequency (RF) attenuation (the reduction of signal strength), shielding, and reflection, which can affect how you deploy your wireless APs. Metal objects within a

building or used in the construction of a building can affect the wireless signal. Examples of such objects include:

- Support beams
- Elevator shafts
- Steel reinforcement in concrete
- Heating and air-conditioning ventilation ducts
- Wire mesh that reinforces plaster or stucco in walls
- Walls that contain metal, cinder blocks, and concrete
- Cabinets, metal desks, or other types of large metal equipment

Sources of Interference

Any device that operates on the same frequencies as your wireless devices (in the S-Band ISM, which operates in the frequency range of 2.4 GHz to 2.5 GHz, or the C-Band ISM, which operates in the frequency range of 5.725 GHz to 5.875 GHz) might interfere with the wireless signals. Sources of interference also change the shape of a wireless AP's ideal coverage volume.

Devices that operate in the S-Band ISM include the following:

- Bluetooth-enabled devices
- Microwave ovens
- 2.4 GHz cordless phones
- Wireless video cameras
- Medical equipment
- Elevator motors

Devices that operate in the C-Band ISM include the following:

- 5 GHz cordless phones
- Wireless video cameras
- Medical equipment

Number of Wireless APs

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

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

  Typical wireless APs use antennas that produce a vertically flattened sphere of signal that propagates across the floor of a building. Wireless APs typically have indoor coverage within a 200-foot radius. Include enough wireless APs to ensure signal overlap between the wireless APs.

- Determine the maximum number of simultaneous wireless users per coverage volume.

- Estimate the data throughput that the average wireless user requires. If needed, add more wireless APs, which will:
    1. Improve wireless client network bandwidth capacity.
    2. 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 can connect to 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.
    3. Ensure redundancy in case a wireless AP fails.
- When designing wireless AP placement for performance, use the following best practices:
    1. Do not overload your wireless APs with too many connected wireless clients. Although most wireless APs can support hundreds of wireless connections, the practical limit is 20–25 connected clients. An average of 2–4 users per wireless AP is a good average to maximize the performance while still effectively utilizing the wireless LAN.
    2. For higher density situations, lower the signal strength of the wireless APs to reduce the coverage area, thereby allowing more wireless APs to fit in a specific space and more wireless bandwidth to be distributed to more wireless clients.

Authentication Infrastructure

The authentication infrastructure exists to:

- Authenticate the credentials of wireless clients
- Authorize the wireless connection
- Inform wireless APs of wireless connection restrictions
- Record the wireless connection creation and termination for accounting purposes

The authentication infrastructure for protected wireless connections consists of:

- Wireless APs
- RADIUS servers
- Active Directory domain controllers
- Issuing CAs of a PKI (optional)

If you are using a Windows domain as the user account database for verification of user or computer credentials and for obtaining dial-in properties, use Network Policy Server (NPS) in Windows Server 2008. NPS is a full-featured RADIUS server and proxy that is tightly integrated with Active Directory. See Chapter 9, "Authentication Infrastructure," for additional design and planning considerations for NPS-based RADIUS servers.

NPS performs the authentication of the wireless connection by communicating with a domain controller over a protected remote procedure call (RPC) channel. NPS performs

authorization of the connection attempt through the dial-in properties of the user or computer account and network policies configured on the NPS server.

By default, NPS logs all RADIUS accounting information in a local log file (*%SystemRoot%*\System32\Logfiles*Logfile*.log by default) based on settings configured in the properties dialog box of the Local File Logging object in the Accounting node in the Network Policy Server snap-in.

Best Practices for Authentication Infrastructure

Best practices to follow for the authentication infrastructure are the following:

- To better manage authorization for wireless connections, create a universal group in Active Directory for wireless access that contains global groups for the user and computer accounts that are allowed to make wireless connections. For example, create a universal group named WirelessAccounts that contains the global groups based on your organization's regions or departments. Each global group contains allowed user and computer accounts for wireless access. When you configure your network policy for wireless connections, specify the WirelessAccounts group name.
- Use the NPS New Network Policy wizard to create a wireless-specific network policy to authorize wireless connections and specify connection constraints and requirements. For example, create a wireless network policy to grant access based on group membership and to require a specific authentication method.

Wireless Clients

A Windows-based wireless client is one that is running Windows Vista, Windows Server 2008, Windows XP with Service Pack 2, or Windows Server 2003. You can configure wireless connections on Windows-based wireless clients in the following ways:

Group Policy

- The Wireless Network (IEEE 802.11) Policies Group Policy extension is part of a Computer Configuration Group Policy Object that can specify wireless network settings in an Active Directory environment.

Command line

- You can configure wireless settings by using Netsh.exe (running the command **netsh wlan** with the desired parameters). These commands apply only to wireless clients running Windows Vista or Windows Server 2008.

Wireless XML profiles

- Wireless XML profiles are XML files that contain wireless network settings. You can use the Netsh tool to export these settings from the Wireless Network (IEEE 802.11) Policies Group Policy extension or from a wireless client running Windows Vista or Windows Server 2008, and then import the settings to a wireless client running Windows Vista or Windows Server 2008.

Manually

- For a Windows Vista– or Windows Server 2008–based wireless client, connect to the wireless network when prompted or use the Connect to a Network wizard from the Network and Sharing Center. For a Windows XP with SP2– or Windows Server 2003–based wireless client, connect to the wireless network when prompted or use the Wireless Network Setup Wizard from the Network Connections folder.

Wireless Network (IEEE 802.11) Policies Group Policy Extension

To automate the configuration of wireless network settings for Windows wireless client computers, Windows Server 2008 and Windows Server 2003 Active Directory domains support a Wireless Network (IEEE 802.11) Policies Group Policy extension. This extension allows you to configure wireless network settings as part of Computer Configuration Group Policy for a domain-based Group Policy Object. By using the Wireless Network (IEEE 802.11) Policies Group Policy extension, you can specify a list of preferred networks and their settings to automatically configure wireless LAN settings for wireless clients running Windows Vista, Windows Server 2008, Windows XP with SP2, Windows XP with SP1, or Windows Server 2003.

For each preferred network, you can specify the following:

- Connection settings, such as the wireless network name and whether the wireless network is a non-broadcast network
- Security settings, such as the authentication and encryption method, the EAP type, and the authentication mode
- Advanced 802.1X security settings such as Single Sign-On (for Windows Vista and Windows Server 2008 wireless clients)

These settings are automatically applied to wireless clients running Windows Vista, Windows Server 2008, Windows XP with SP2, and Windows Server 2003 that are members of a Windows Server 2008 or Windows Server 2003 Active Directory domain. You can configure wireless policies by using the Computer Configuration/Windows Settings/Security Settings/Wireless Network (IEEE 802.11) Policies node in the Group Policy Management Editor snap-in.

By default, there are no Wireless Network (IEEE 802.11) policies. To create a new policy for a Windows Server 2008–based Active Directory domain, right-click Wireless Network (IEEE 802.11) Policies in the console tree Group Policy Management Editor snap-in, and then click Create A New Windows XP Policy or Create A New Windows Vista Policy. For each type of policy, you can create only a single policy. A Windows XP Policy can contain profiles with settings for multiple wireless networks, and each network must have a unique SSID. A Windows Vista Policy can also contain profiles with settings for multiple wireless networks with unique SSIDs. Additionally, different profiles can contain multiple instances of the same SSID, each with unique settings. This allows you to configure profiles for mixed-mode deployments in which some clients are using different security technologies, such as WPA and WPA2.

The Windows Vista–based wireless policy contains policy settings specific to Windows Vista and Windows Server 2008 wireless clients. If both types of wireless policies are configured, Windows XP with SP2– and Windows Server 2003–based wireless clients will use only the Windows XP policy settings, and the Windows Vista and Windows Server 2008 wireless clients will use only the Windows Vista policy settings. If there are no Windows Vista policy settings, Windows Vista and Windows Server 2008 wireless clients will use the Windows XP policy settings.

Windows Vista Wireless Policy

The properties dialog box of a Windows Vista wireless policy consists of a General tab and a Network Permissions tab. Figure 10-5 shows the General tab.

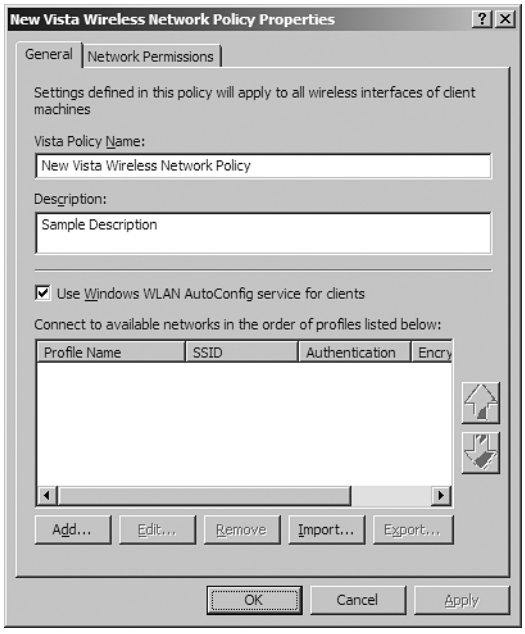

Figure 10-5 The General tab of a Windows Vista wireless policy

On the General tab, you can configure a name and description for the policy, specify whether to enable the WLAN AutoConfig service (Wireless Auto Configuration), and configure the list of wireless networks and their settings (known as *profiles*) in preferred order. On the General tab, you can import and export profiles as files in XML format. To export a profile to an XML file, select the profile and click Export. To import an XML file as a wireless profile, click Import, and then specify the file's location.

Figure 10-6 shows the Network Permissions tab for a Windows Vista wireless network policy.

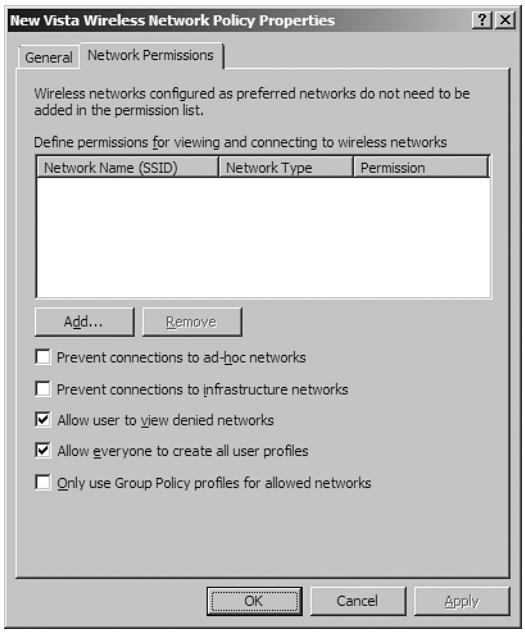

Figure 10-6 The Network Permissions tab of a Windows Vista wireless policy

The Network Permissions tab is new for Windows Vista and Windows Server 2008 and allows you to specify wireless networks by name that are either allowed or denied access. For example, you can create allow or deny lists.

With an allow list, you can specify the set of wireless networks by name to which a Windows Vista or Windows Server 2008 wireless client is allowed to connect. This is useful for network administrators who want an organization's laptop computers to connect to a specific set of wireless networks, which might include the organization's wireless network in addition to wireless Internet service providers.

With a deny list, you can specify the set of wireless networks by name to which the wireless clients are not allowed to connect. This is useful to prevent managed laptop computers from connecting to other wireless networks that are within range of the organization's wireless network—for example, when an organization occupies a floor of a building and there are other wireless networks of other organization on adjoining floors—or to prevent managed laptop computers from connecting to known unsecured wireless networks.

On the Network Permissions tab, there are also settings to prevent connections to either ad-hoc or infrastructure mode wireless networks, to allow the user to view the wireless networks in the list of available networks that have been configured as denied, and to allow any user to create an all-user profile. An *all-user profile* can be used to connect to a specific wireless network by any user with an account on the computer. If this setting is disabled, only users in the Domain Admins or Network Configuration Operators groups can create all-user wireless profiles on the computer. Last, there is a setting to require that the wireless client use Group Policy-based profiles for allowed profiles, rather than local profiles of the same name.

To manage a wireless network profile from the General tab of the New Windows Vista Wireless Policy Properties dialog box, either select an existing profile and click Edit, or click Add and then specify whether the new wireless profile is for an infrastructure or ad-hoc mode wireless network. The profile properties dialog box of a Windows Vista wireless network profile consists of a Connection tab and a Security tab. Figure 10-7 shows the default Connection tab for a Windows Vista wireless network profile.

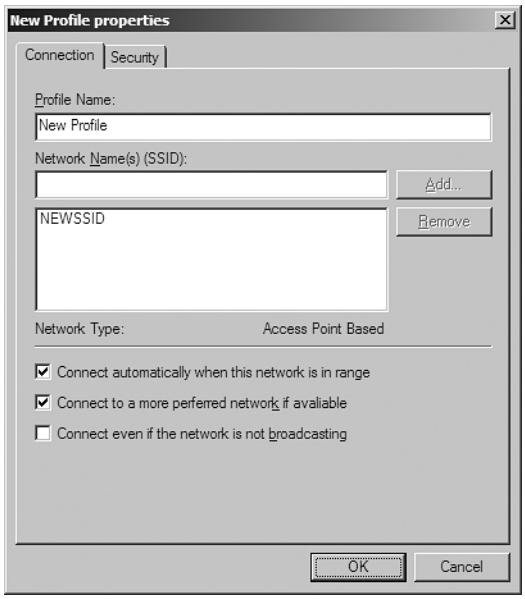

Figure 10-7 The Connection tab for a Windows Vista wireless network profile

On the Connection tab, you can configure a name for the profile and a list of wireless network names to which this profile applies. You can add new names by typing the name in the Network Name(s) (SSID) box and clicking Add. You can also specify whether the wireless client using this profile will automatically attempt to connect to the wireless networks named in the profile when in range (subject to the preference order of the list of wireless profiles on the General tab for the Windows Vista policy), whether to automatically disconnect from this wireless network if a more preferred wireless network comes within range, and to indicate that the wireless networks in this profile are non-broadcast networks (also known as hidden networks).

Figure 10-8 shows the Security tab for a Windows Vista wireless network profile.

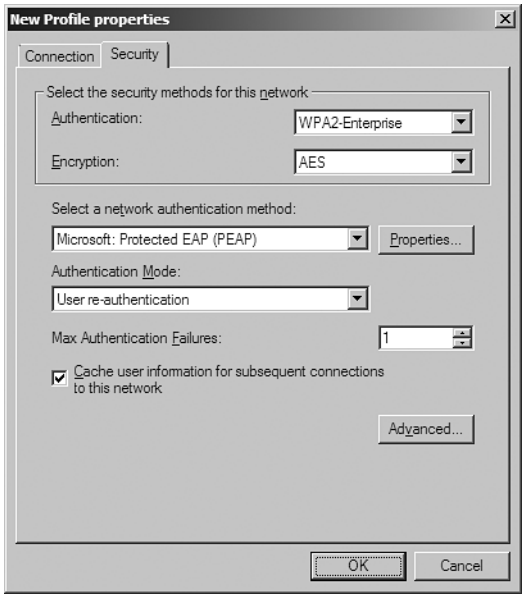

Figure 10-8 The Security tab for a Windows Vista wireless network profile

On the Security tab, you can configure the authentication and encryption methods for the wireless networks in the profile. For authentication methods, you can select Open, Shared, Wi-Fi Protected Access (WPA)-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, and Open with 802.1X. For encryption methods, you can select Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES). The choice of encryption methods depends on your choice of authentication method.

If you select Open with 802.1X, WPA-Enterprise, or WPA2-Enterprise as the authentication method, you can also configure the network authentication method (the EAP type), the authentication mode (user re-authentication, computer authentication, user authentication, or guest authentication), the number of times authentication attempts can fail before authentication is abandoned, and whether to cache user information for subsequent connections. If you configure this last setting not to cache the user information, when the user logs off, the user credential data is removed from the registry. The result is that when the next user logs on, that user will be prompted for credentials (such as user name and password).

Direct from the Source

For wireless clients running Windows Vista or Windows Server 2008, the cached credentials are stored at:

HKEY_CURRENT_USER\Software\Microsoft\Wlansvc\UserData\Profiles*ProfileGUID*\MSMUserdata

For wireless clients running Windows XP or Windows Server 2003, the cached credentials are stored at:

HKEY_CURRENT_USER\Software\Microsoft\Eapol\UserEapInfo

Clay Seymour

Technical Lead

To configure advanced security settings for the WPA-Enterprise, WPA2-Enterprise, or Open with 802.1X authentication methods, in the New Profile Properties Dialog Box, on the Security tab, click Advanced. Figure 10-9 shows the default Advanced Security Settings dialog box.

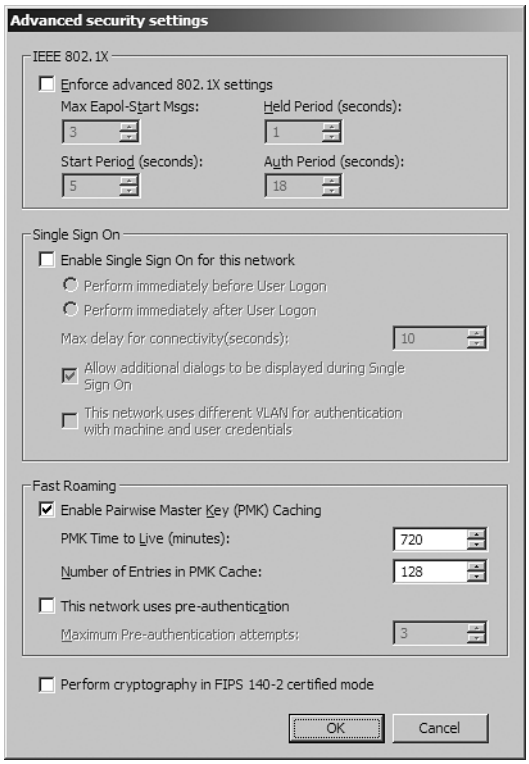

Figure 10-9 The Advanced Security Settings dialog box

In the IEEE 802.1X section, there are settings to specify the number of successive EAP over LAN (EAPOL)-Start messages that are sent out when no response to the initial EAPOL-Start messages is received, the time interval between the retransmission of EAPOL-Start messages when no response to the previously sent EAPOL-Start message is received, the period for which the authenticating client will not perform any 802.1X authentication activity after it has received an authentication failure indication from the authenticator, and the interval for which the authenticating client will wait before retransmitting any 802.1X requests after end-to-end 802.1X authentication has been initiated.

In the Single Sign On section, there are settings to perform wireless authentication immediately before or after the user logon process, specify the number of seconds of delay for connectivity before the user logon process begins, choose whether to prompt the user for additional dialog boxes, and choose whether the wireless networks for this profile use a different virtual LAN (VLAN) for computer or user authentication and to perform a DHCP renewal when switching from the computer-authenticated VLAN to the

user-authenticated VLAN. For information about when to use Single Sign On, see the section "Wireless Authentication Modes" in this chapter.

In the Fast Roaming section, you can configure Pairwise Master Key (PMK) caching and preauthentication options. The Fast Roaming section appears only when you select WPA2-Enterprise as the authentication method on the Security tab. With PMK caching, wireless clients and wireless APs cache the results of 802.1X authentications. Therefore, access is much faster when a wireless client roams back to a wireless AP to which the client already authenticated. You can configure a maximum time to keep an entry in the PMK cache and the maximum number of entries. With preauthentication, a wireless client can perform an 802.1X authentication with other wireless APs in its range while it is still connected to its current wireless AP. If the wireless client roams to a wireless AP with which it has preauthenticated, access time is substantially decreased. You can configure the maximum number of times to attempt preauthentication with a wireless AP.

Note Fast roaming for WPA2 is different than fast reconnect. Fast reconnect minimizes the connection delay in wireless environments when a wireless client roams from one wireless AP to another when using PEAP. With fast reconnect, the Network Policy Server service caches information about the PEAP TLS session so that when reauthenticating, the wireless client does not have to perform PEAP authentication, only TLS or MS-CHAP v2 authentication. Fast reconnect is enabled by default for Windows wireless clients and for NPS network policies.

A final check box allows you to specify whether to perform AES encryption in a Federal Information Processing Standard (FIPS) 140-2 certified mode. FIPS 140-2 is a U.S. government computer security standard that specifies design and implementation requirements for cryptographic modules. Windows Vista and Windows Server 2008 are FIPS 140-2 certified. When you enable FIPS 140-2 certified mode, Windows Vista or Windows Server 2008 will perform the AES encryption in software, rather than relying on the wireless network adapter.

Windows XP Wireless Policy

To create a new Windows XP wireless policy, in the Group Policy Management Editor snap-in, in the console tree, right-click Wireless Network (IEEE 802.11) Policies, and then click Create A New Windows XP Policy. The properties dialog box of a Windows XP wireless policy consists of a General tab and a Preferred Networks tab.

Figure 10-10 shows the General tab for a Windows XP wireless network policy.

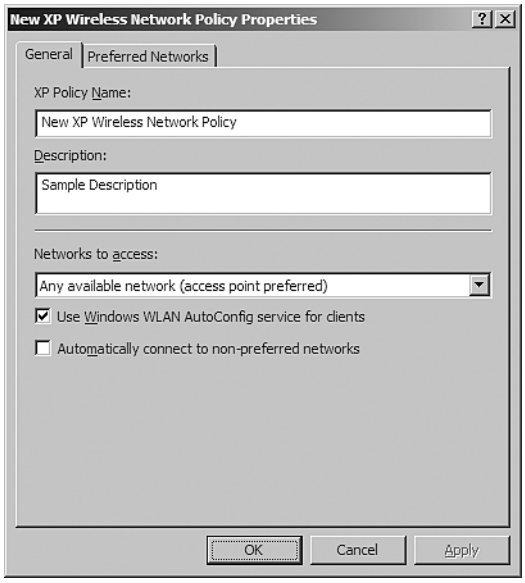

Figure 10-10 The General tab for a Windows XP wireless network policy

On the General tab, you can configure a name and description for the policy, specify whether the Wireless Zero Configuration service is enabled, select the types of wireless networks to access (any available, infrastructure, or ad-hoc networks), and specify whether to automatically connect to non-preferred networks.

Figure 10-11 shows the Preferred Networks tab for a Windows XP wireless policy.

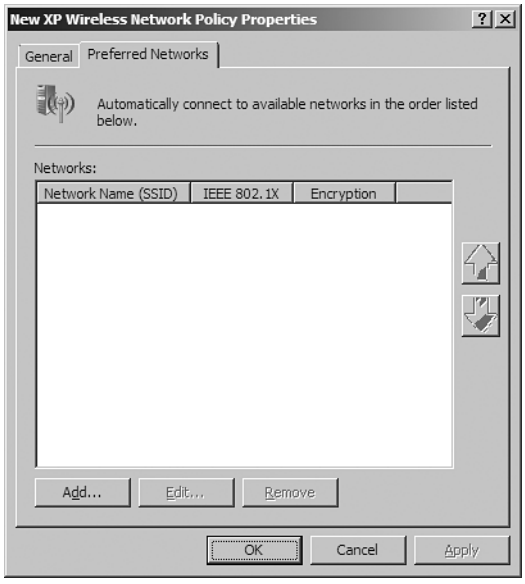

Figure 10-11 The Preferred Networks tab for a Windows XP wireless policy

On the Preferred Networks tab, you can manage the list of preferred wireless networks and their order of preference. To manage a wireless network profile from the Preferred Networks tab of the Windows XP wireless policy properties dialog box, either select an existing profile and click Edit, or click Add and then specify whether the new wireless profile is for an infrastructure or ad-hoc mode wireless network. The properties dialog box of a preferred wireless network consists of a Network Properties tab and an IEEE 802.1X tab.

Figure 10-12 shows the Network Properties tab for a preferred wireless infrastructure network.

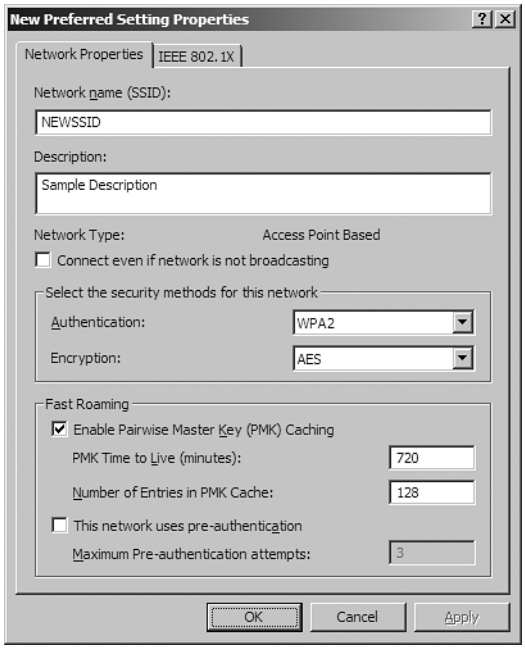

Figure 10-12 The Network Properties tab for a preferred wireless infrastructure network

On the Network Properties tab, you can add a description for the preferred network, specify whether the wireless network is a non-broadcast network (infrastructure), select the authentication and encryption methods, and, for WPA2, set advanced fast roaming settings.

Figure 10-13 shows the default IEEE 802.1X tab for a preferred wireless network.

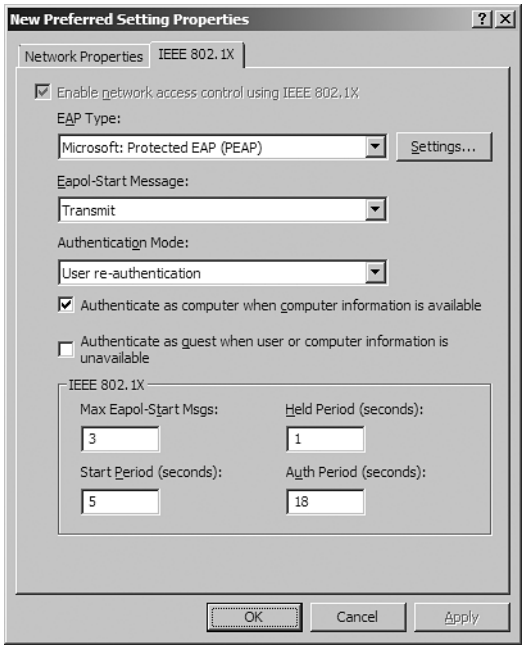

Figure 10-13 The IEEE 802.1X tab for a preferred wireless network

On the IEEE 802.1X tab, you can specify the EAP type and configure its settings, specify when to send the EAPOL-Start message, choose the authentication mode, specify whether to authenticate with computer credentials or as a guest, and set advanced 802.1X settings.

Command-Line Configuration

Windows Vista and Windows Server 2008 support a command-line interface that allows you to configure the wireless settings that are available from the wireless dialog boxes in the Network Connections folder or through the Wireless Network (IEEE 802.11) Policies Group Policy extension. Command-line configuration of wireless settings can help deployment of wireless networks in the following situations:

Automated script support for wireless settings without using Group Policy

- The Wireless Network (IEEE 802.11) Policies Group Policy extension applies only in an Active Directory domain. For an environment without a Group Policy infrastructure, a script that automates the configuration of wireless connections can be run either manually or automatically, such as part of the logon script.

Bootstrap of a wireless client onto the organization's protected wireless network

- A wireless client computer that is not a member of the domain cannot connect to the organization's protected wireless network. Additionally, a computer cannot join the domain until it has successfully connected to the organization's protected wireless network. A command-line script provides a method to connect to the organization's secure wireless network to join the domain.

To perform command-line configuration of Windows Vista– and Windows Server 2008–based wireless clients, run the **netsh wlan** command with the appropriate parameters. For more information about **netsh wlan** command syntax, see Netsh Commands for Wireless Local Area Network (WLAN) at *http://technet.microsoft.com/en-us/windowsvista/aa905085.aspx*

XML-Based Wireless Profiles

To simplify command-line configuration of wireless clients, you can export the configuration of a wireless profile to an XML file that can be imported on other wireless clients. You can export a wireless profile from a wireless client by running the **netsh wlan export profile** command or by using the General tab of the Windows Vista wireless policy properties dialog box. To import a wireless profile, run **netsh wlan add profile**.

Design Choices for Wireless Clients

The design choices for wireless clients are the following:

- To prevent your Windows Vista or Windows Server 2008 wireless clients from connecting to certain wireless networks, configure a list of denied wireless networks on the Network Permissions tab of the Windows Vista wireless policy properties dialog box, or run the **netsh wlan add filter** command.
- To configure your Windows Vista or Windows Server 2008 wireless clients to connect to only specific wireless networks, configure a list of allowed wireless networks on the Network Permissions tab of the Windows Vista wireless policy dialog box, or run the **netsh wlan add filter** command.

Requirements for Wireless Clients

The requirements for wireless clients are the following:

- To use WPA2, wireless clients must be running Windows XP with SP2 and the Wireless Client Update for Windows XP with Service Pack 2, Windows Vista, or Windows Server 2008.
- Command-line configuration using the **netsh wlan** command, export and import of wireless XML profiles, and Single Sign On are supported by wireless clients running only Windows Vista or Windows Server 2008.

Best Practices for Wireless Clients

Best practices for wireless clients are the following:

- For a small number of wireless clients, configure each wireless client manually.
- For enterprise deployment of wireless configuration in an Active Directory environment, use the Wireless Network (IEEE 802.11) Wireless Policies Group Policy extension.
- For enterprise deployment of wireless configuration through the use of scripts, create wireless XML profiles and configure wireless clients with a script containing the **netsh wlan add profile** command.

PKI

To perform authentication for wireless connections using PEAP-TLS or EAP-TLS, a PKI must be in place to issue computer or user certificates to wireless clients and computer certificates to RADIUS servers. For PEAP-MS-CHAP v2–based authentication, a PKI is not required. It is possible to purchase certificates from a third-party CA to install on your NPS

servers. You might also need to distribute the root CA certificate of third-party computer certificates to your wireless client computers.

PKI for Smart Cards

The use of smart cards for user authentication is the strongest form of user authentication in Windows. For wireless connections, you can use smart cards with the EAP-TLS or PEAP-TLS authentication method. The individual smart cards are distributed to users who have a computer with a smart card reader. To log on to the computer, you must insert the smart card into the smart card reader and type the smart card personal identification number (PIN). When the user attempts to make a wireless connection, the smart card certificate is sent during the connection negotiation process.

PKI for User Certificates

User certificates that are stored in the Windows registry for user authentication can be used in place of smart cards. However, it is not as strong a form of authentication. With smart cards, the user certificate issued during the authentication process is made available only when the user possesses the smart card and has knowledge of the PIN to log on to their computer. With user certificates, the user certificate issued during the authentication process is made available when the user logs on to the computer using a domain-based user name and password. Just as with smart cards, authentication using user certificates for wireless connections use the EAP-TLS or PEAP-TLS authentication methods.

To deploy user certificates in your organization, first deploy a PKI. You'll then need to install a user certificate for each user. The easiest way to accomplish this is if Windows Certificate Services is installed as an enterprise CA. Then configure group policy settings for user certificate autoenrollment. For more information, see "Deploying Certificates" in this chapter.

When the wireless client attempts user-level authentication for a wireless connection, the wireless client computer sends the user certificate during the authentication process.

PKI for Computer Certificates

Computer certificates are stored in the Windows registry for computer-level authentication for wireless access with the EAP-TLS or PEAP-TLS authentication methods. To deploy computer certificates in your organization, first deploy a PKI. You'll then need to install a computer certificate for each computer. The easiest way to accomplish this is if Windows Certificate Services is installed as an enterprise CA. then, configure group policy settings for computer certificate autoenrollment. For more information, see "Deploying Certificates" in this chapter.

When the wireless client attempts computer-level authentication for a wireless connection, the wireless client computer sends the computer certificate during the authentication process.

Requirements for PKI

Requirements for PKI for a protected wireless network are the following:

- For computer-level authentication with EAP-TLS or PEAP-TLS, you must install computer certificates, also known as *machine* certificates, on each wireless client.

The computer certificates of the wireless clients must be valid and verifiable by the NPS servers; the NPS servers must have a root CA certificate for the CA that issued the computer certificates of the wireless client.

- For user-level authentication with EAP-TLS or PEAP-TLS, you must use a smart card or you must install a user certificate on each wireless client.

  The smart card or user certificates of the wireless clients must be valid and verifiable by the NPS servers; the NPS servers must have the root CA certificates of the issuing CAs of the smart card or user certificates of the wireless clients.

- You must install the root CA certificates of the issuing CA of the NPS server computer certificates on each wireless client.

  The computer certificates of the NPS servers must be valid and verifiable by each wireless client; the wireless clients must have a root CA certificates for the CAs that issued the computer certificates of the NPS servers.

  The computer certificates of the NPS servers must be verifiable by the wireless clients; the wireless clients must have the root CA certificate of the issuing CA of the computer certificates of the NPS servers.

- For EAP-TLS authentication, the requirements for the user certificate, smart card certificate, or computer certificate of the wireless client are as follows:

  1. The certificate must contain a private key.
  2. The certificate must be issued by an enterprise CA or mapped to a user or computer account in Active Directory.
  3. The certificate must be chained to a trusted root CA on the NPS server and must not fail any of the checks that are performed by CryptoAPI and specified in the network policy for wireless connections.
  4. The certificate must be configured with the Client Authentication purpose in the Enhanced Key Usage field (the object identifier for Client Authentication is 1.3.6.1.5.5.7.3.2).
  5. The Subject Alternative Name field must contain the user principal name (UPN) of the user or computer account.

- For EAP-TLS authentication, the requirements for the computer certificate of the NPS server are as follows:

  1. The certificate must contain a private key.
  2. The Subject field must contain a value.
  3. The certificate must be chained to a trusted root CA on the wireless clients and must not fail any of the checks that are performed by CryptoAPI and specified in the network policy for wireless connections.
  4. The certificate must be configured with the Server Authentication purpose in the Enhanced Key Usage field (the object identifier for Server Authentication is 1.3.6.1.5.5.7.3.1).

5. The certificate must be configured with a required cryptographic service provider (CSP) value of Microsoft RSA SChannel Cryptographic provider.
6. The Subject Alternative Name field of the certificate, if used, must contain the DNS name of the NPS server.

Best Practices for PKI

Best practices for the PKI for protected wireless access are the following:

- For computer certificates with EAP-TLS or PEAP-TLS, if you are using a Windows Server 2008 enterprise CA as an issuing CA, configure your Active Directory domain for autoenrollment of computer certificates using a Computer Configuration group policy. Each computer that is a member of the domain automatically requests a computer certificate when the Computer Configuration group policy is updated.
- For registry-based user certificates for EAP-TLS or PEAP-TLS, if you are using a Windows Server 2008 enterprise CA as an issuing CA, use a User Configuration group policy to configure your Active Directory domain for autoenrollment of user certificates. Each user who successfully logs on to the domain automatically requests a user certificate when the User Configuration group policy is updated.
- If you have purchased third-party computer certificates for your NPS servers for PEAP-MS-CHAP v2 authentication and the wireless clients do not have the root CA certificate of the issuing CA of the NPS server computer certificates installed, use a group policy to install the root CA certificate of the issuing CA of the NPS server computer certificates on your wireless clients. Each computer that is a member of the domain automatically receives and installs the root CA certificate when the Computer Configuration group policy is updated.
- For EAP-TLS, PEAP-TLS, and PEAP-MS-CHAP v2 authentication, it is possible to configure the wireless clients so that they do not validate the certificate of the NPS server. If so, it is not required to have computer certificates on the NPS servers and their root CA certificates on wireless clients. However, having the wireless clients validate the certificate of the NPS server is recommended for mutual authentication of the wireless client and NPS server. With mutual authentication, you can protect your wireless clients from connecting to rogue wireless APs with spoofed authentication servers.

802.1X Enforcement with NAP

Network Access Protection (NAP) for Windows Server 2008, Windows Vista, and Windows XP provides components and an application programming interface (API) set that help you enforce compliance with health policies for network access or communication. Developers and network administrators can create solutions for validating computers that connect to their networks, can provide needed updates or access to needed resources, and can limit the access of noncompliant computers.

802.1X Enforcement is one of the NAP enforcement methods included with Windows Server 2008, Windows Vista, and Windows XP. With 802.1X Enforcement, an 802.1X-authenticated wireless client must prove that it is compliant with system health requirements before being allowed full access to the intranet. If the wireless client is not

compliant with system health requirements, the wireless AP places the wireless client on a restricted network containing servers that have resources to bring the wireless client back into compliance. The wireless AP enforces the restricted access through IPv4 and IPv6 packet filters that are placed on the wireless connection. After correcting its health state, the wireless client validates its health state again, and if compliant, the packet filters on the wireless connection that confine the access to the restricted network are removed.

In order for 802.1X Enforcement to work, you must already have a working protected wireless deployment. For the details on deploying 802.1X Enforcement after successfully deploying a protected wireless network solution, see Chapter 17, "802.1X Enforcement."

Deploying Protected Wireless Access

To deploy a protected wireless network using Windows Vista and Windows Server 2008, follow these steps:

1. Deploy certificates.
2. Configure Active Directory for user accounts and groups.
3. Configure NPS servers.
4. Deploy wireless APs.
5. Configure wireless clients.

Deploying Certificates

Each wireless client in the following authentication configurations needs a computer certificate:

Computer authentication with EAP-TLS or PEAP-TLS and computer certificates

- Each wireless client computer needs a computer certificate.

User authentication with EAP-TLS or PEAP-TLS and either smart cards or registry-based user certificates

- Each wireless user needs a smart card or each wireless client computer needs a user certificate.

User or computer authentication with PEAP-MS-CHAP v2

- Each wireless client needs the root CA of the issuing CA of the NPS server's computer certificate.

Deploying Computer Certificates

To install computer certificates for EAP-TLS or PEAP-TLS authentication, a PKI must be present to issue certificates. Once the PKI is in place, you can install a computer certificate on wireless clients and NPS servers in the following ways:

- By configuring autoenrollment of computer certificates to computers in an Active Directory domain (recommended)
- By using the Certificates snap-in to request a computer certificate

- By using the Certificates snap-in to import a computer certificate
- By executing a CAPICOM script that requests a computer certificate

For more information, see "Deploying PKI" in Chapter 9, "Authentication Infrastructure."

Deploying User Certificates

You can install a user certificate on wireless clients in the following ways:

- By configuring autoenrollment of user certificates to users in an Active Directory domain (recommended)
- By using the Certificates snap-in to request a user certificate
- By using the Certificates snap-in to import a user certificate
- By requesting a certificate over the Web
- By executing a CAPICOM script that requests a user certificate

For more information, see "Deploying PKI" in Chapter 9, "Authentication Infrastructure."

Deploying Root CA Certificates

If you use PEAP-MS-CHAP v2 authentication, you might need to install the root CA certificates of the computer certificates that are installed on your NPS servers on your wireless clients. If the root CA certificate of the issuer of the computer certificates that are installed on the NPS servers is already installed as a root CA certificate on your wireless clients, no other configuration is necessary. For example, if your root CA is a Windows Server 2008–based online root enterprise CA, the root CA certificate is automatically installed on each domain member computer through a group policy.

To verify whether the correct root CA certificate is installed on your wireless clients, you need to determine:

- The root CA of the computer certificates installed on the NPS servers.
- Whether a certificate for the root CA is installed on your wireless clients.

To determine the root CA of the computer certificates installed on the NPS servers

1. In the console tree of the Certificates snap-in for the NPS server computer account, open Certificates (Local Computer or Computer Name), open Personal, and then click Certificates.
2. In the details pane, double-click the computer certificate that is being used by the NPS server for PEAP-MS-CHAP v2 authentication.
3. In the Certificate properties dialog box, on the Certification Path tab, note the name at the top of the certification path. This is the name of the root CA.

To determine whether a certificate for the root CA is installed on your wireless client

1. In the console tree of the Certificates snap-in for the wireless client computer account, open Certificates (Local Computer or Computer Name), open Trusted Root Certification Authorities, and then click Certificates.
2. Examine the list of certificates in the details pane for a name matching the root CA for the computer certificates issued to the RADIUS servers.

You must install the root CA certificates of the issuers of the computer certificates of the NPS servers on each wireless client that does not contain them. The easiest way to install a root CA certificate on all your wireless clients is through Group Policy. For more information, see "Deploying PKI" in Chapter 9, "Authentication Infrastructure."

Configuring Active Directory for Accounts and Groups

To configure Active Directory for wireless access, do the following for the user and computer accounts that will be used to authenticate wireless connections:

- On the Dial-in tab, set the network access permission to Allow Access or Control Access Through NPS Network Policy. With this setting, the permission for access to the network is set by the Access Permission in the NPS network policy. By default, in native-mode domains, new user accounts and computer accounts have the network access permission set to Control Access Through NPS Network Policy.
- Organize the computer and user accounts into the appropriate universal and global groups to take advantage of group-based network policies.

Configuring NPS Servers

Configure and deploy your NPS servers as described in Chapter 9, "Authentication Infrastructure," taking the following steps:

1. Install a computer certificate on each NPS server.
2. Install the root CA certificates of the computer or user certificates of the wireless clients on each NPS server (if needed).
3. Configure logging on the primary NPS server.
4. Add RADIUS clients to the primary NPS server corresponding to each wireless AP.
5. Create a new network policy on the primary NPS server that is customized for wireless connections using the universal group name for your wireless accounts.

For the details of Steps 1–4, see Chapter 9, "Authentication Infrastructure."

To create a new network policy for wireless connections

1. In the console tree of the Network Policy Server snap-in, click NPS.
2. In the details pane, under Standard Configuration, select RADIUS Server For 802.1X Wireless Or Wired Connections from the drop-down list, and then click Configure 802.1X.

3. In the Configure 802.1X wizard, on the Select 802.1X Connections Type page, click Secure Wireless Connections, and then type the name of the new NPS network policy. Click Next.
4. On the Specify 802.1X Switches page, add RADIUS clients as needed that correspond to your wireless APs. Click Next.
5. On the Configure An Authentication Method page, configure the EAP type to use for wireless connections.

   To configure EAP-TLS, in the Type drop-down list, select Microsoft: Smart Card Or Other Certificate, and then click Configure. In the Smart Card Or Other Certificate Properties dialog box, select the computer certificate to use for wired connections, and then click OK. If you cannot select the certificate, the cryptographic service provider for the certificate does not support Secure Channel (SChannel). SChannel support is required for NPS to use the certificate for EAP-TLS authentication.

   To configure PEAP-MS-CHAP v2, in the Type drop-down list, select Protected EAP (PEAP), and then click Configure. In the Edit Protected EAP Properties dialog box, select the computer certificate to use for wired connections, and then click OK. If you cannot select the certificate, the cryptographic service provider for the certificate does not support SChannel. SChannel support is required for NPS to use the certificate for PEAP authentication.

   To configure PEAP-TLS, in the Type drop-down list, select Protected EAP (PEAP), and then click Configure. In the Edit Protected EAP Properties dialog box, select the computer certificate to use for wired connections. If you cannot select the certificate, the cryptographic service provider for the certificate does not support SChannel. Under EAP Types, click Secured Password (EAP-MSCHAP v2) and then click Remove. Click Add. In the Add EAP dialog box, click Smart Card Or Other Certificate, and then click OK. In the Edit Protected EAP Properties dialog box, under EAP Types, click Smart Card Or Other Certificate, and then click Edit. In the Smart Card Or Other Certificate Properties dialog box, select the computer certificate to use for wired connections, and then click OK. If you cannot select the certificate, the cryptographic service provider for the certificate does not support Secure Channel (SChannel). Click OK twice.
6. Click Next. On the Specify User Groups page, add the groups containing the wireless computer and user accounts (for example, WirelessAccounts).
7. On the Configure A Virtual LAN (VLAN) page, click Configure if needed to specify the RADIUS attributes and their values that configure your wireless APs for the appropriate VLAN for this NPS network policy. Click Next.
8. On the Completing New IEEE 802.1X Secure Wired And Wireless Connections And RADIUS Clients page, click Finish.

After you have configured the primary NPS server with the appropriate logging, RADIUS client, and network policy settings, copy the configuration to the secondary or other NPS servers. For more information, see Chapter 9, "Authentication Infrastructure."

Deploying Wireless APs

To deploy your wireless APs, do the following:

1. Perform an analysis of wireless AP locations based on plans of floors and buildings.
2. Temporarily install your wireless APs.
3. Perform a site survey analyzing signal strength in all areas.
4. Relocate wireless APs or sources of RF attenuation or interference.
5. Verify the coverage volume.
6. Update the architectural drawings to reflect the final number and placement of the wireless APs.
7. Configure TCP/IP, security, and RADIUS settings.

These steps are discussed in more detail in the following sections.

Note An alternate method of performing a site survey is to move a single wireless AP around to various locations within your site to discover interference issues and identify the eventual locations of your wireless APs. This method allows you to determine the feasibility of a wireless network within your site before you install numerous wireless APs.

Perform an Analysis of Wireless AP Locations

Obtain or create scaled architectural drawings of each floor for each building for which wireless access is being planned. On the drawing for each floor, 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. This type of coverage can prevent connectivity problems that might result from undocking a laptop from an office for use in a different part of your building.

On the plans, indicate the devices that interfere with the wireless signals, and mark the building construction materials or objects that might attenuate, reflect, or shield wireless signals. Then indicate the locations of wireless APs so that each wireless AP is no farther than 200 feet from an adjacent wireless AP.

After you have determined the initial locations of the wireless APs, you must determine their channels and then assign those channel numbers to each wireless AP.

To select the channels for the wireless APs

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

   Wireless network signal waves travel through floors and ceilings, so wireless 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 channel numbers of their wireless APs to ensure that your own wireless APs that provide overlapping coverage use a different channel number.

2. Identify overlapping wireless signals on adjacent floors within your own organization.
3. After identifying overlapping coverage volumes outside and within your organization, assign channel numbers to your wireless APs.

To assign the channel numbers to the wireless APs

1. Assign channel 1 to the first wireless AP.
2. Assign channels 6 and 11 to the wireless APs that overlap coverage volumes with the first wireless AP ensuring that those wireless APs do not also interfere with other coverage volumes with the same channel.
3. Continue assigning channel numbers to the wireless APs ensuring that any two wireless APs with overlapping coverage are assigned different channel numbers, and separated by at least five channels.

Temporarily Install Your Wireless APs

Based on the locations and channel configurations indicated in your plan-based analysis of wireless AP locations, temporarily install your wireless APs.

Perform a Site Survey

Perform a site survey by walking around the building and its floors with a laptop computer equipped with an 802.11 wireless adapter and site survey software (site survey software ships with most wireless adapters and wireless APs). Determine the signal strength and bit rate for the coverage volume for each installed wireless AP.

Relocate Wireless APs or Sources of RF Attenuation or Interference

In locations where signal strength is low, you can make any of the following adjustments to improve the signal:

- Reposition the temporarily installed wireless APs to increase the signal strength for that coverage volume.
- Reposition or eliminate devices that interfere with signal strength (such as Bluetooth devices or microwave ovens).
- Reposition or eliminate metal obstructions that interfere with signal propagation (such as filing cabinets and appliances).
- Add more wireless APs to compensate for the weak signal strength.

> **Note** If you add a wireless AP, you might have to change the channel numbers of adjacent wireless APs.

- Purchase antennas to meet the requirements of your building infrastructure.

For example, to eliminate interference between wireless APs located on adjoining floors in your building, you can purchase directional antennas that flatten the signal (forming a donut-shaped coverage volume) to increase the horizontal range and further decrease the vertical range.

Verify Coverage Volume

Perform another site survey to verify that the changes made to the configuration or placement of the wireless APs eliminated the locations with low signal strength.

Update Your Plans

Update the architectural drawings to reflect the final number and placement of the wireless APs. Indicate the boundaries of the coverage volume and where the data rate changes for each wireless AP.

Configure TCP/IP, Security, and RADIUS Settings

Configure your wireless APs with the following:

- A new wireless network name and strong administrator password
- A static IPv4 address, subnet mask, and default gateway for the wireless subnet on which it is placed
- WPA2 or WPA with 802.1X authentication (WPA2-Enterprise or WPA-Enterprise).

Configure the following RADIUS settings:

- The IP address or name of a primary RADIUS server, the RADIUS shared secret, UDP ports for authentication and accounting, and failure detection settings
- The IP address or name of a secondary RADIUS server, the RADIUS shared secret, UDP ports for authentication and accounting, and failure detection settings

  To balance the load of RADIUS traffic between the two NPS servers, configure half of the wireless APs with the primary NPS server as the primary RADIUS server and the secondary NPS server as the secondary RADIUS server. Then, configure the other half of the wireless APs with the secondary NPS server as the primary RADIUS server and the primary NPS server as the secondary RADIUS server.

  If the wireless APs require vendor-specific attributes (VSAs) or additional RADIUS attributes, you must add the VSAs or attributes to the wireless network policy of the NPS servers. If you add VSAs or RADIUS attributes to the wireless network policy on the primary NPS server, copy the primary NPS server configuration to the secondary NPS server.

Configuring Wireless Clients

You can configure wireless clients in the following three ways:

- Through Group Policy
- By configuring and deploying wireless XML profiles
- Manually

Configuring Wireless Clients Through Group Policy

To configure Wireless Network (IEEE 802.11) Policies group policy settings, perform the following steps:

1. From a computer running Windows Server 2008 that is a member of your Active Directory domain, click Start, type mmc, and then press Enter.
2. In the MMC console window, click File, and then click Add/Remove Snap-in.
3. In the list of available snap-ins, double-click the Group Policy Management Editor.
4. In the Select Group Policy Object dialog box, click Browse. In the Browse For A Group Policy Object dialog box, click the appropriate Active Directory Group Policy Object (such as Default Domain Policy), and then click OK.
5. Click Finish, and then click OK.
6. In the console tree, open the Group Policy Object, then Computer Configuration, then Windows Settings, then Security Settings, and then Wireless Network (IEEE 802.11) Policies.
7. Right-click Wireless Network (IEEE 802.11) Policies, and then click either Create a New Windows Vista Policy or Create a New Windows XP Policy.

For a new Windows Vista wireless policy, perform the following steps:

1. In the details pane, double-click your newly created Windows Vista wireless network policy. The policy's Properties dialog box appears.
2. On the General tab, type a name for the policy and a description.
3. On the Network Permissions tab, add allowed and denied wireless networks by name as needed.
4. On the General tab, click Add to add a wireless network profile, and then click Infrastructure to specify an infrastructure mode wireless network.
5. On the Connection tab, type the wireless network name (SSID) and a description (optional), and then specify connection settings as needed.
6. On the Security tab, specify the authentication and encryption security methods.
7. For WPA2, in the Authentication section, select WPA2, and then in the Encryption area, select AES.
8. For WPA, select WPA in Authentication and either TKIP or AES in Encryption. Select AES only if both your wireless clients and wireless APs support WPA with AES encryption.
9. In the Select A Network Authentication Method drop-down list, specify the EAP type.

   For EAP-TLS:

   a. Select Smart Card Or Other Certificate, and then click Properties.
   b. In the Smart Card Or Other Certificate Properties dialog box, configure EAP-TLS settings as needed, and then click OK. By default, EAP-TLS uses a registry-based certificate and validates the server certificate.

c. For PEAP-MS-CHAP v2, no additional configuration is required. PEAP-MS-CHAP v2 is the default authentication method.

10. Specify the authentication mode and other settings as needed.

11 To configure advanced settings for 802.1X, including Single Sign On and Fast Roaming, click Advanced and specify settings as needed. Click OK when complete.

12 Click OK to save the changes.

For a new Windows XP wireless policy, perform the following steps:

1. In the details pane, double-click your newly created Windows XP wireless network policy. The Properties dialog box appears.
2. On the General tab, change settings as needed.
3. On the Preferred Networks tab, click Add to add a preferred network, and then click Infrastructure to specify an infrastructure mode wireless network.
4. On the Network Properties tab, type the wireless network name (SSID), a description (optional), specify whether this wireless network is non-broadcast, and then specify the security methods.
   - For WPA2, in the Authentication drop-down list, select WPA2, and then in the Encryption drop-down list, select AES.
   - For WPA, in the Authentication drop-down list, select WPA, and then in the Encryption drop-down list, select TKIP.
5. On the IEEE 802.1X tab, specify the EAP type.

   For EAP-TLS:

   a. In the EAP Type drop-down list, select Smart Card Or Other Certificate, and then click Settings.

   b. In the Smart Card Or Other Certificate Properties dialog box, configure EAP-TLS settings as needed, and then click OK. By default, EAP-TLS uses a registry-based certificate and validates the server certificate.

   c. For PEAP-MS-CHAP v2, no additional configuration is required. PEAP-MS-CHAP v2 is the default authentication method.
6. Also on the IEEE 802.1X tab, specify the authentication mode and other settings as needed.
7. Click OK twice to save changes.

The next time your Windows Vista, Windows Server 2008, Windows XP with SP2, Windows XP with SP1, or Windows Server 2003 wireless clients update the Computer Configuration group policy, the wireless network settings in the Group Policy Object will be automatically applied.

Configuring and Deploying Wireless Profiles

You can also manually configure wireless clients running Windows Vista on a wireless network by importing a wireless profile in XML format by running the **netsh wlan add profile** command. To create an XML-based wireless profile, configure a Windows Vista wireless client with a wireless network that has all the appropriate settings including the

authentication method, encryption methods, and EAP type. Then, run the **netsh wlan export profile** command to write the wireless network profile to an XML file. You can also create, configure, and export an XML profile from a Windows Vista wireless policy.

Manually Configuring Wireless Clients

If you have a small number of wireless clients, you can manually configure wireless connections for each wireless client. For Windows Vista and Windows Server 2008 wireless clients, run the Set Up a Connection Wizard or the Network Wizard. For Windows XP with SP2 wireless clients, run the New Connection Wizard. The following sections describe how to manually configure the EAP-TLS, PEAP-TLS, and PEAP-MS-CHAP v2 authentication methods for Windows wireless clients.

EAP-TLS

To manually configure EAP-TLS authentication on a wireless client running Windows Vista or Windows Server 2008, do the following:

1. In the Network and Sharing Center, click the Manage Wireless Networks task. In the Manage Wireless Networks window, double-click your wireless network name.
2. On the Security tab, in the Security Type box, select WPA-Enterprise or WPA2-Enterprise. In the Choose A Network Authentication Method drop-down list, select Smart Card Or Other Certificate, and then click Settings.
3. In the Smart Card Or Other Certificate Properties dialog box, to use a registry-based user certificate, select Use A Certificate On This Computer. For a smart card–based user certificate, select Use My Smart Card.

   If you want to validate the computer certificate of the NPS server, select Validate Server Certificate (recommended and enabled by default). If you want to specify the names of the NPS servers that must perform the TLS authentication, select Connect To These Servers and type the names. Click OK twice.

To manually configure EAP-TLS authentication on a wireless client running Windows XP with SP2, Windows XP with SP1, or Windows Server 2003, do the following:

1. Obtain properties of the wireless connection in the Network Connections folder. On the Wireless Networks tab, in the list of preferred networks, click the name of the wireless network, and then click Properties.
2. On the Authentication tab, select Enable Network Access Control Using IEEE 802.1X and the Smart Card Or Other Certificate EAP type. This is enabled by default.
3. Click Properties. In the properties dialog box of the Smart Card or other Certificate EAP type, to use a registry-based user certificate, select Use A Certificate On This Computer. For a smart card–based user certificate, select Use My Smart Card.

   If you want to validate the computer certificate of the NPS server, select Validate Server Certificate (recommended and enabled by default). If you want to specify the names of the authentication servers that must perform the TLS authentication, select Connect To These Servers and type the names.
4. Click OK to save changes to the Smart Card or other Certificate EAP type.

PEAP-TLS

To manually configure PEAP-TLS authentication on a wireless client running Windows Vista, do the following:

1. In the Network and Sharing Center, click the Manage Wireless Networks task. In the Manage Wireless Networks window, double-click your wireless network name.
2. On the Security tab, in the Security Type drop-down list, select WPA-Enterprise or WPA2-Enterprise. In Choose A Network Authentication Method, select Protected EAP (PEAP), and then click Settings.
3. In the Protected EAP Properties dialog box, if you want to validate the computer certificate of the NPS server for the PEAP authentication, select Validate Server Certificate (recommended and enabled by default). If you want to specify the names of the NPS servers that must perform the PEAP authentication, select Connect To These Servers and type the names.
4. In the Select Authentication Method drop-down list, click Smart Card Or Other Certificate. Click Configure. To use a registry-based user certificate, in the Smart Card Or Other Certificate Properties dialog box, select Use A Certificate On This Computer .For a smart card–based user certificate, select Use My Smart Card.

   If you want to validate the computer certificate of the NPS server for the user-level authentication, select the Validate Server Certificate check box (recommended and enabled by default). If you want to specify the names of the NPS servers that must perform the TLS authentication, select Connect To These Servers and type the names.
5. Click OK to save changes to the Smart Card or other Certificate PEAP type. Click OK to save the changes to the Protected EAP type. Click OK to save the changes to the wireless network configuration.

To manually configure PEAP-TLS authentication on a wireless client running Windows XP with SP2, Windows XP with SP1, or Windows Server 2003, do the following:

1. Obtain properties of the wireless connection in the Network Connections folder. On the Wireless Networks tab, in the list of preferred networks, click the name of the wireless network, and then click Properties. The Wireless Network's properties dialog box appears.
2. On the Authentication tab, select Enable Network Access Control Using IEEE 802.1X and the Protected EAP (PEAP) type.
3. Click Properties. In the Protected EAP Properties dialog box, select the Validate Server Certificate check box to validate the computer certificate of the NPS server for the PEAP authentication (recommended and enabled by default). If you want to specify the names of the authentication servers that must perform PEAP authentication, select Connect To These Servers and type the names. In the Select Authentication Method drop-down list, click Smart Card Or Other Certificate.
4. Click Configure. In the Smart Card Or Other Certificate Properties dialog box, to use a registry-based user certificate, select Use A Certificate On This Computer. For a smart card–based user certificate, select Use My Smart Card.

If you want to validate the computer certificate of the NPS server for the user-level authentication, select Validate Server Certificate (recommended and enabled by default). If you want to specify the names of the NPS servers that must perform the TLS authentication, select Connect To These Servers and type the names.

5. Click OK to save changes to the Smart Card or other Certificate PEAP type. Click OK to save the changes to the Protected EAP type. Click OK to save the changes to the wireless network configuration.

PEAP-MS-CHAP v2

To manually configure PEAP-MS-CHAP v2 authentication on a wireless client running Windows Vista, do the following:

1. In the Network and Sharing Center, click the Manage Wireless Networks task. In the Manage Wireless Networks window, double-click your wireless network name.
2. On the Security tab, in the Security Type drop-down list, select WPA-Enterprise or WPA2-Enterprise. In the Choose a network authentication method drop-down list, select Protected EAP (PEAP), and then click Settings.
3. In the Protected EAP Properties dialog box, if you want to validate the computer certificate of the NPS server for the PEAP authentication, select the Validate Server Certificate check box (recommended and enabled by default). If you want to specify the names of the NPS servers that must perform the PEAP authentication, select Connect To These Servers and type the names.
4. In Select Authentication Method, select Secured Password (EAP-MS-CHAP v2), and then click OK twice.

To manually configure PEAP-MS-CHAP v2 authentication on a wireless client running Windows XP with SP2, Windows XP with SP1, or Windows Server 2003, do the following:

1. Obtain properties of the wireless connection in the Network Connections folder. Click the Wireless Networks tab, click the name of the wireless network in the list of preferred networks, and then click Properties. The wireless network's properties dialog box appears.
2. On the Authentication tab, select Enable Network Access Control Using IEEE 802.1X and the Protected EAP (PEAP) EAP type.
3. Click Properties. In the Protected EAP Properties dialog box, select Validate Server Certificate to validate the computer certificate of the NPS server (enabled by default). If you want to specify the names of the authentication servers that must perform validation, select Connect To These Servers and type the names. In Select Authentication Method, click Secured Password (EAP-MSCHAP v2), and then click OK twice.

Ongoing Maintenance

The areas of maintenance for a protected wireless solution are as follows:

- Manage user and computer accounts

- Manage wireless APs
- Update wireless profiles

Managing User and Computer Accounts

When a new user or computer account is created in Active Directory and that user or computer is allowed wireless access, do the following:

- If you are managing network access permission by account, no additional action is necessary. By default, new accounts created in native-mode Active Directory domains have their network access permission set to Control Access Through NPS Network Policy.
- If you are managing network access permission by group, add the new account to the appropriate group for wireless connections. For example, add the new account to the WirelessAccounts security group, which is specified in the network policy for wireless connections.

When user or computer accounts are deleted in Active Directory, no additional action is necessary to prevent wireless connections.

As needed, you can create additional universal groups and network policies to set wireless network access for different sets of users. For example, you can create a global WirelessAccessContractors group and a network policy that allows wireless connections to members of the WirelessAccessContractors group only during normal business hours or for access to specific intranet resources.

Managing Wireless APs

Once deployed, wireless APs do not need a lot of ongoing maintenance. Most of the ongoing changes to wireless AP configuration are due to managing wireless network capacity and changes in network infrastructure.

Adding a Wireless AP

To add a wireless AP, do the following:

1. Follow the design points and deployment steps in the "Deploying Wireless APs" section of this chapter to add a new wireless AP to your wireless network.
2. Add the wireless AP as a RADIUS client to your NPS servers.

Removing a Wireless AP

When removing a wireless AP, update the configuration of your NPS servers to remove the wireless AP as a RADIUS client.

Configuration for Changes in NPS Servers

If the NPS servers change (for example, because of additions or removals of NPS servers on the intranet), you will need to do the following:

1. Ensure that new NPS servers are configured with RADIUS clients corresponding to the wireless APs and with the appropriate network policies for wireless access.

2. Update the configuration of the wireless APs for the new NPS server configuration as needed.

Updating Wireless XML Profiles

To update a wireless XML profile and apply it to your Windows Vista or Windows Server 2008 wireless clients, do the following:

1. If you are using a Windows Vista or Windows Server 2008 wireless client or if you have a Windows Vista wireless policy, create an updated XML profile by running the netsh wlan export profile command.
2. Execute the netsh wlan add profile command to import the XML profile on your wireless clients through a script or other method.

Troubleshooting

Because of the different components and processes involved, troubleshooting wireless connections can be a difficult task. This section describes the following:

- The tools that are provided with Windows Server 2008 and Windows Vista to troubleshoot wireless connections
- How to troubleshoot wireless connection problems from the wireless client
- How to troubleshoot wireless connection problems from the wireless AP
- How to troubleshoot wireless connection problems from the NPS server

Direct from the Source

One of the most difficult aspects of troubleshooting wireless connectivity is knowing where to start. Generally, the client is the device that shows the symptom, but it is only one piece in a chain of devices and technologies that could fail.

As a general rule to follow, if the wireless client fails to see the wireless network or establish an association, the issue lies between the wireless client and the wireless AP. Most of these issues are resolved by driver or firmware updates for the wireless network adapter and the wireless AP. Having the latest drivers and firmware installed is a required first step in the troubleshooting process.

If authentication is failing, you most likely can rule out hardware as an issue. First review your client-side System event logs. Windows XP and Windows Server 2003 do not have any diagnostic logs, but Windows Vista and Windows Server 2008 log quite a bit of useful information that may point you to a configuration issue such as a missing certificate.

After reviewing these logs, review the System event log on the NPS server. If you have a failed authentication, there will be log entries with a reason code and description. If, however, you do not see any log entries related to the wireless authentication attempt, this is a strong indicator that NPS did not receive the authentication attempt or the process timed out. Take a look at the wireless AP to confirm that its RADIUS settings are appropriate for the NPS server.

Clay Seymour

Technical Lead

Wireless Troubleshooting Tools in Windows

Windows Server 2008 provides the following tools to troubleshoot wireless connections:

- TCP/IP troubleshooting tools
- The Network Connections folder
- Netsh wlan commands
- Network Diagnostics Framework support for wireless connections
- Wireless diagnostics tracing
- NPS authentication and accounting logging
- NPS event logging
- SChannel logging
- SNMP agent
- Reliability and Performance snap-in
- Network Monitor 3.1

TCP/IP Troubleshooting Tools

The Ping, Tracert, and Pathping tools use Internet Control Message Protocol (ICMP) Echo and Echo Reply and ICMPv6 Echo Request and Echo Reply messages to verify connectivity, display the path to a destination, and test path integrity. The Route tool can be used to display the IPv4 and IPv6 routing tables. The Nslookup tool can be used to troubleshoot domain name system (DNS) name resolution issues.

The Network Connections Folder

When you obtain status on the wireless connection in the Network Connection folder, you can view information such as the signal speed, which is shown on the General tab. Click Details to view the TCP/IP configuration.

If the wireless adapter is assigned an Automatic Private IP Addressing (APIPA) address in the range 169.254.0.0/16 or the configured alternate IP address, the wireless client is still associated with the wireless AP, but either authentication has failed or the DHCP server is not available. If the authentication fails and the association is still in place, the wireless adapter is enabled and TCP/IP performs its normal configuration process. If a DHCP server is not found (either authenticated or not), Windows Vista automatically configures an APIPA address unless there is an alternate address configured.

Direct from the Source

You may notice that a Windows Vista wireless client will automatically configure an APIPA address sooner or more frequently than in previous versions of Windows. A

computer running Windows Vista will wait only six seconds to contact a DHCP server before using an APIPA address, and will then continue to attempt to contact a DHCP server. By contrast, a computer running Windows XP will wait a full minute before using an APIPA address. This change in behavior is by design and is meant to facilitate ad-hoc connectivity when there are no DHCP servers available.

Tim Quinn

Knowledge Engineer

Netsh Wlan Commands

You can run the **netsh wlan** command with the following parameters to gather information for troubleshooting wireless issues:

netsh wlan show autoconfig
- Displays whether the WLAN Autoconfig service is enabled

netsh wlan show blockednetworks
- Displays whether blocked networks are visible in the list of available networks

netsh wlan show createalluserprofile
- Displays whether everyone is allowed to create all-user profiles

netsh wlan show drivers
- Displays the properties of the drivers for the installed wireless network adapters

netsh wlan show interfaces
- Displays properties for the installed wireless network adapters

netsh wlan show networks
- Displays the list and properties of the available wireless networks

netsh wlan show profiles
- Displays the list of group policy and local wireless profiles

netsh wlan show settings
- Displays the global wireless settings, which includes the state of Wireless Auto Configuration and whether everyone is allowed to create all-user profiles.

netsh wlan show tracing
- Displays the state of tracing and the location of the wireless tracing logs (by default in *%SystemRoot%*\Tracing\Wireless)

netsh wlan show all
- Displays complete wireless network adapter information and information on available wireless networks

Network Diagnostics Framework Support for Wireless Connections

To provide a better user experience when encountering network connectivity issues, Windows Vista and Windows Server 2008 include the Network Diagnostics Framework (NDF), a set of technologies and guidelines that allows a set of troubleshooters (also known as *helper classes*) to assist in the diagnosis and possible automatic correction of

networking problems. When a user experiences a networking problem in Windows Vista, NDF will provide the user the ability to diagnose and repair the problem within the context of that problem. This means that the diagnostics assessment and resolution steps are presented to the user within the application or dialog box that they were using when the problem occurred or based on the failed network operation.

Windows Vista and Windows Server 2008 include a troubleshooter to diagnose failed wireless connections. If a wireless connection fails, Windows displays a dialog box with information about the error. The dialog box includes a Diagnose button that launches the wireless NDF troubleshooter. In the diagnosis session, users can repair their wireless connection problem without needing to involve IT support staff. The wireless NDF troubleshooter will help users resolve many common issues that arise with wireless network connectivity, such as:

- The network adapter radio being turned off
- The wireless AP not being powered
- A missing or mismatched configuration of security options, encryption types, or network keys between the wireless AP and wireless client
- Disconnected media
- Missing certificates

Windows logs all wireless connection attempts in the System event log. When Windows Network Diagnostics runs, it creates additional events in the System event log that contain the following information:

- The name of the wireless network adapter and whether its driver is designed for Windows Vista and/or Windows Server 2008.
- A list of visible wireless networks with the signal strength, channel, protocol (such as 802.11b or 802.11g), and operating mode (infrastructure or ad hoc) for each.
- The list of preferred wireless networks and each network's configuration settings.
- The diagnostic conclusions, such as, "The wireless connection on this computer appears to be working correctly," "The Internet connection on the wireless router or access point might not be working correctly," and "The computer has a low signal strength from ContosoWLAN."
- The repair options offered to the user, such as, "Try moving the computer to a different location, eliminating any sources of possible interference, and then try connecting to ContosoWLAN again."
- The repair options chosen by the user and whether the repair solved the problem.

You can view these events in the Event Viewer snap-in to understand the network environment at the time the problem occurred without needing to re-create the scenario, and you need no longer rely on users to explain the symptoms of the problem.

To obtain additional information about the diagnostics process, Windows creates a detailed diagnostic log that is separate from the System event log.

To access this diagnostics log, do the following

1. In the Event Viewer snap-in, in the tree view, open Applications and Services Logs/Microsoft/Windows/Diagnostics-Networking.
2. Click Operational.
3. In the contents pane, view the events for the wireless diagnostics session.

Wireless Diagnostics Tracing

Occasionally, you might need to escalate a wireless networking problem to Microsoft or another support specialist in your organization. To perform a detailed analysis, Microsoft or your support specialists need in-depth information about the computer's state and wireless components in Windows and their interaction when the problem occurred. You can obtain this information from wireless diagnostics tracing in Windows Vista and Windows Server 2008. To use wireless diagnostics tracing, you must start tracing, reproduce the problem, stop tracing, and then collect the tracing report.

To start wireless diagnostics tracing, do one of the following:

- Type the **netsh wlan set tracing mode=yes** command at a command prompt.
- In the console tree of the Reliability and Performance Monitor snap-in, open Data Collector Sets/System. Right-click Wireless Diagnostics, and then click Start.

After you have reproduced the problem and want to stop wireless diagnostics tracing, do one of the following:

- Type the netsh wlan set tracing mode=no command.
- In the console tree of the Reliability and Performance Monitor snap-in, open Data Collector Sets/System. Right-click Wireless Diagnostics, and then click Stop.

> **Note** It is important to stop the wireless diagnostics tracing prior to viewing or gathering the trace logs to initiate a process that converts the trace files into a readable format.

To view the report generated by wireless diagnostics tracing, in the console tree of the Reliability and Performance Monitor snap-in, open Reports/System/Wireless Diagnostics.

The report includes the following information:

- Wireless configuration, including allowed and blocked wireless networks
- Current TCP/IP configuration (including data provided by the **ipconfig /all** command)
- A list of all connection attempts and detailed information about each step of the connection process
- A detailed list of all Windows Network Diagnostics events
- Wireless client certificate configuration
- Wireless profiles and their locations
- Wireless network adapter driver information
- Wireless networking system files and versions

- Raw network tracing information
- Computer make and model
- Operating system version
- A list of all services, their current states, and their process identifiers

This report and its associated files are stored by default in the *%SystemRoot%*\Tracing\Wireless folder.

In addition to wireless diagnostic tracing, Windows Vista and Windows Server 2008 support tracing for components of the Remote Access Connection Manager and Routing and Remote Access services, which are also used for wireless connections. Like the wireless diagnostic tracing, tracing for these components creates information that you can use to troubleshoot complex problems for specific components. The information in these additional tracing files is typically useful only to Microsoft support engineers, who might request that you create trace files for a connection attempt during their investigation of a support issue. You can enable this additional tracing by using the Netsh tool.

To enable and disable tracing for a specific component of the Remote Access Connection Manager and Routing and Remote Access services, the command is:

netsh ras set tracing *component* enabled|disabled

in which ***component*** is a component in the list of components found in the registry under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing.

To enable tracing for all components, the command is:

netsh ras set tracing * enabled

To disable tracing for all components, the command is:

netsh ras set tracing * disabled

The tracing log files are stored in the *%SystemRoot%*\Tracing folder. The most interesting log files for wireless authentication are the following:

Eapol.log
- EAP over LAN (EAPOL) activity.

Rastls.log
- TLS authentication activity.

Raschap.log
- MS-CHAP v2 authentication activity.

NPS Authentication and Accounting Logging

By default, NPS supports the logging of authentication and accounting information for wireless connections in local log files. This logging is separate from the events recorded in the System event log. You can use the information in the logs to track wireless usage and authentication attempts. Authentication and accounting logging is especially useful for troubleshooting network policy issues. For each authentication attempt, the name of the network policy that either accepted or rejected the connection attempt is recorded. You

can configure authentication and accounting logging options from the Settings tab in the properties dialog box of the Local File Logging object in the Accounting folder in the Network Policy Server snap-in.

The authentication and accounting information is stored in a configurable log file or files stored in the *%SystemRoot%*\System32\LogFiles folder. The log files are saved in Internet Authentication Service (IAS) or database-compatible format, meaning that any database program can read the log file directly for analysis. NPS can also send authentication and accounting information to a SQL Server database.

NPS Event Logging

Check the System event log on the NPS server for events with the source NPS for rejected or accepted connection attempts. NPS event log entries contain a lot of information on the connection attempt including the name of the network policy that accepted or rejected the connection attempt. NPS event logging for rejected or accepted connection attempts is enabled by default and is configured from the General tab in the properties dialog box of an NPS server in the Network Policy Server snap-in.

NPS events are stored in the System event log, which can be viewed from the Event Viewer snap-in. To see NPS events, filter the System event log to display only events with the source of NPS. To view the failed authentication events, set the filter for the Source of NPS and the Event ID of 2.

Viewing the NPS events in the System event log is one of the most useful troubleshooting tools for obtaining information about failed authentications. The NPS events are also helpful when troubleshooting network policies. The Proxy-Policy-Name or Policy-Name field in the description of the event records the name of the network policy that either accepted or rejected the connection attempt.

SChannel Logging

Secure channel (SChannel) logging is the logging of detailed information for SChannel events in the System event log. By default, only SChannel error messages are recorded. To log errors, warnings, and informational and successful events, set the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogging registry value to 4 (as a DWORD type). With SChannel logging recording all events, it is possible to obtain more information about the certificate exchange and validation process on the NPS server.

SNMP Agent

You can use the Simple Network Management Protocol (SNMP) agent software included with Windows Server 2008 to monitor status information for your NPS server from an SNMP console. NPS supports the RADIUS Authentication Server MIB (RFC 2619) and the RADIUS Accounting Server MIB (RFC 2621). Use Features in the Server Manager console to install the optional SNMP service.

The SNMP service can be used in conjunction with your existing SNMP-based network management infrastructure to monitor your NPS RADIUS servers or proxies.

Reliability and Performance Snap-In

You can use the Reliability and Performance snap-in to monitor counters, create logs, and set alerts for specific NPS components and program processes. You can also use charts and reports to determine how efficiently your server uses NPS and to both identify and troubleshoot potential problems.

You can use the Reliability and Performance snap-in to monitor counters within the following NPS-related performance objects:

- NPS Accounting Clients
- NPS Accounting Proxy
- NPS Accounting Server
- NPS Authentication Clients
- NPS Authentication Proxy
- NPS Authentication Server
- NPS Remote Accounting Servers
- NPS Remote Authentication Servers

For more information about how to use the Reliability and Performance snap-in, see the Help and Support Center in Windows Server 2008.

Network Monitor 3.1

You can use Microsoft Network Monitor 3.1 (or later) or a commercial packet analyzer (also known as a network sniffer), to capture and view the authentication and data traffic sent and received by the wireless network adapter. Network Monitor 3.1 (or later) is available as a free download from the Microsoft Download Center at *http://www.microsoft.com/downloads*. Network Monitor 3.1 includes RADIUS, 802.1X, EAPOL, and EAP parsers. A *parser* is a component included with Network Monitor that can separate the fields of a protocol header and display their structure and values. Without a parser, Network Monitor 3.1 displays the hexadecimal bytes of a header, which you must parse manually.

For Windows wireless client authentications, you can use Network Monitor 3.1 to capture the set of frames exchanged between the wireless client computer and the wireless AP during the wireless authentication process. You can then use Network Monitor 3.1 to view the individual frames and determine why the authentication failed. Network Monitor 3.1 is also useful for capturing the RADIUS messages that are exchanged between a wireless AP and its RADIUS and for determining the RADIUS attributes of each message.

The proper interpretation of wireless traffic with Network Monitor 3.1 requires an in-depth understanding of EAPOL, RADIUS, and other protocols. Network Monitor 3.1 captures can be saved as files and sent to Microsoft support for analysis.

Troubleshooting the Windows Wireless Client

When troubleshooting wireless connectivity, it is important to first determine whether some or all of your wireless clients are experiencing problems. If all of your wireless clients

are experiencing problems, issues may exist in your authentication infrastructure. If some of your wireless clients are experiencing problems, issues may exist for your wireless APs or individual wireless clients.

The following are some common problems with wireless connectivity and authentication that are encountered by a Windows wireless client:

Wireless network is not found.

- Verify that you are within range of the wireless AP for the wireless network by using tools provided by the wireless adapter vendor. You can move the wireless AP or the wireless client, adjust the transmission power level on the wireless AP, or reposition or remove sources of radio frequency attenuation or interference.

Unable to authenticate.

- Some wireless network adapters have a link light that indicates sent or received data frames. However, because IEEE 802.1X authentication occurs before the wireless network adapter begins sending or receiving data frames, the link light does not reflect 802.1X authentication activity. If the link light does not indicate any wireless traffic, the cause could be a failed 802.1X authentication.

  Verify that the user or computer account for the wireless client exists, is enabled, and is not locked out (via account properties or remote access account lockout); and that the connection is being attempted during allowed logon times.

  Verify that the connection attempt for the user or computer account matches a network policy. For example, if you are using a group-based network policy, verify that the user or computer account is a member of the group specified in the Windows Groups condition of the appropriate network policy.

  Verify that the root CA certificates for the issuing CAs of the NPS server certificates are installed in the Trusted Root Certification Authorities Local Computer store on the wireless client computer.

  For an EAP-TLS– or PEAP-TLS–based wireless client, verify that the computer or user certificate meets the conditions described in the "Validating the Wireless Client's Certificate" section of this chapter.

  For a PEAP-MS-CHAP v2–based wireless client, investigate whether the wireless client's account password has expired and verify that the Allow Client to Change Password After It Has Expired check box in the EAP MS-CHAP v2 Properties dialog box is enabled on the NPS servers.

Unable to authenticate with a certificate.

- The most typical cause for this message is that you do not have either a user or computer certificate installed. Depending on the configured authentication mode, you might need to have both installed. Verify that you have a computer certificate, a user certificate, or both installed by using the Certificates snap-in.

  Another possible cause for this message is that you have certificates installed, but they either cannot be used for wireless authentication, or they cannot be validated by all of your NPS servers. For more information, see the section "Troubleshooting Certificate-Based Validation" in this chapter.

Troubleshooting the Wireless AP

If you have multiple wireless access points (APs) and are unable to connect or authenticate with one of them, you might have a problem with that specific wireless AP. This section describes the common troubleshooting tools of wireless APs and the common problems of connecting and authenticating with a wireless AP.

Wireless AP Troubleshooting Tools

Although the set of troubleshooting tools for wireless APs varies with each manufacturer and with each model, some of the more common troubleshooting tools are the following:

- Panel indicators
- Site survey software
- SNMP support
- Diagnostics

These tools are described in the following sections. Consult your wireless AP documentation for information about the set of troubleshooting tools provided with your wireless AP.

Panel Indicators

Most wireless APs have one or more indicators, which are status lights that are visible on the housing of the wireless AP, from which you can obtain a quick assessment of the wireless AP's hardware status. For example, you might see the following:

- An indicator to show that the wireless AP has electrical power.
- An indicator to show general operation status. For example, the indicator might show whether the wireless AP is associated with any wireless clients.
- An indicator to show wireless network traffic. This indicator might blink for each frame received on the wireless network.
- An indicator to show data collisions. If the blinking of this indicator seems excessive, evaluate the performance of the link by using the methods suggested by the wireless AP vendor.
- An indicator to show wired network traffic. This indicator might blink for each frame received on the wired network.

Alternatively, the wireless AP might have a liquid crystal display (LCD) panel that shows icons that indicate its current status. Consult your wireless AP documentation for information about panel indicators and their interpretation.

Site Survey Software

Site survey software, which you use during the deployment of wireless APs to determine their optimal placement, is typically installed on a wireless-capable laptop computer from a CD-ROM provided by the wireless AP or wireless network adapter vendor.

As described in the section "Deploying Wireless APs," the site survey software is used to determine the coverage volume and where the data rate changes for each wireless AP.

If wireless clients cannot connect to a specific wireless AP, use the site survey software to perform a site survey for that wireless AP. There might have been a change in the devices that create interference and objects that interfere with signal propagation since the original site survey and AP placement was done.

SNMP Support

Many wireless APs include a Simple Network Management Protocol (SNMP) agent with support for the following SNMP Management Information Bases (MIBs):

- IEEE 802.11 MIB
- IEEE 802.1 PAE (Port Access Entity) MIB
- SNMP Management MIB (described in RFC 1157)
- SNMP MIB II (described in RFC 1213)
- Bridge MIB (described in RFC 1286)
- Ethernet Interface MIB (described in RFC 1398)
- IETF Bridge MIB (described in RFC 1493)
- Remote Monitoring (RMON) MIB (described in RFC 1757)
- RADIUS Client Authentication MIB (described in RFC 2618)

The SNMP agent on the wireless AP can be used in conjunction with your existing SNMP-based network management infrastructure to configure your wireless APs, set trap conditions, and monitor loads on your wireless APs.

Diagnostics

Diagnostics for wireless APs can be in the following forms:

- Diagnostic facilities that are available through the main wireless AP configuration program, such as a Windows program provided on the wireless AP vendor product CD-ROM or a series of Web pages.
- Diagnostic facilities that are available through a command-line tool or facility, such as terminal access to the wireless AP.

The exact diagnostic facilities of a wireless AP vary from one wireless AP to another; however, the purpose of the diagnostics is to ensure that the wireless AP is operating properly (from a hardware standpoint) and to validate its current configuration.

Common Wireless AP Problems

The following are common problems with wireless APs:

- Unable to see the wireless AP
- Unable to authenticate with the wireless AP
- Unable to communicate beyond the wireless AP

These common problems are discussed in detail in the following sections.

Unable to See the Wireless AP

If wireless clients are unable to see the wireless AP in a scan of wireless networks, one or more of the following may be happening:

The wireless AP is not beaconing.

- All wireless APs should be sending periodic beacon messages that contain the Service Set Identifier (SSID)—unless the wireless AP has been configured to suppress the SSID in the beacon message—and the wireless AP's capabilities (such as supported bit rates and security options). To verify that the wireless AP is beaconing, you can use the site survey software or a packet sniffer that can capture wireless beacon frames. A simple packet sniffer that can capture beacon frames and other types of wireless management frames might be included on the CD-ROM provided by your wireless AP vendor.

The wireless AP is not configured for the correct channel.

- If the wireless AP is using the same channel as an adjacent wireless AP, signal interference might be impairing the wireless clients' ability to connect. Change the wireless AP channel if needed.

The wireless AP is not advertising the correct set of capabilities.

- Confirm that the wireless AP is configured to operate for the correct technology (802.11b, 802.11a, or 802.11g) and with the correct bit rates and security options (WPA or WPA2). By capturing the beacon frame with a network sniffer, you can compare the configured wireless options to those being advertised in the beacon frame.

The wireless AP has inadequate signal strength in the anticipated coverage volume.

- Use your site survey software to confirm that the coverage volume of the wireless AP is as described in your plans after initially deploying the wireless APs. If there are new sources of signal attenuation, reflection, or interference, make the appropriate changes to the locations of either interfering equipment or the wireless AP.

Unable to Authenticate with the Wireless AP

If you have multiple wireless APs, and your wireless clients cannot authenticate with any of them, you might have a problem with your authentication infrastructure. See the section "Troubleshooting the Authentication Infrastructure" in this chapter for instructions on how to troubleshoot this situation. If you have multiple wireless APs, and the wireless clients cannot authenticate with an individual wireless AP, you need to troubleshoot the authentication-related configuration of the wireless AP. The three areas of authentication configuration you need to investigate are as follows:

- 802.1X configuration
- RADIUS configuration
- WPA configuration

802.1X Configuration

Ensure that the wireless AP has 802.1X authentication enabled. Some wireless APs might refer to 802.1X authentication as Extensible Authentication Protocol (EAP) authentication.

RADIUS Configuration

The RADIUS configuration consists of the following elements:

Wireless AP RADIUS configuration

- Ensure that the wireless AP has been properly configured for RADIUS. The wireless AP should contain the following configuration information:
  1. The IPv4 or IPv6 address of a primary NPS server
  2. The destination User Datagram Protocol (UDP) ports for RADIUS traffic sent to the primary RADIUS server (UDP port 1812 for RADIUS authentication traffic and UDP port 1813 for RADIUS accounting traffic)
  3. The RADIUS shared secret for the primary NPS server
  4. The IPv4 or IPv6 address of a secondary NPS server
  5. The destination UDP ports for RADIUS traffic sent to the secondary NPS server
  6. The RADIUS shared secret for the secondary NPS server

NPS server reachability

- Ensure that the primary and secondary NPS servers are reachable from the wireless AP by doing the following:
  1. If the wireless AP has a ping facility—the capability to send an Internet Control Message Protocol (ICMP) Echo message to an arbitrary unicast IPv4 destination—try pinging the IPv4 address of the primary and secondary NPS servers.
  2. If the wireless AP does not have a ping facility, try pinging the IPv4 address of the primary and secondary NPS servers from a network node that is attached to the same subnet as the wireless AP.

     If the ping from the network node succeeds and the ping from the wireless AP does not, examine the IPv4 configuration of the wireless AP to ensure that it has been configured with the correct IPv4 address, subnet mask, and default gateway for the attached wired subnet. If neither ping works, troubleshoot the lack of IPv4 connectivity between the attached subnet and the RADIUS servers.

> **Note** The ping test is not necessarily a definitive test of IPv4 reachability. There might be routers in the path between the wireless AP and the RADIUS server that are filtering ICMP traffic, or the NPS server might be configured with packet filters to discard ICMP traffic.

     To ensure that RADIUS traffic is reaching the primary and secondary NPS servers, use a network sniffer such as Network Monitor 3.1 on the NPS servers to capture the RADIUS traffic sent from and to the wireless AP during an authentication attempt.

NPS server configuration

- If RADIUS traffic is reaching the primary and secondary NPS servers, verify that the primary and secondary NPS servers are configured with a RADIUS client that corresponds to the wireless AP, including the following:
  1. The IPv4 address of the wireless AP's interface on the wireless subnet

2. The destination UDP ports for RADIUS traffic sent by the wireless AP (UDP port 1812 for RADIUS authentication traffic and UDP port 1813 for RADIUS accounting traffic)
3. The RADIUS shared secret configured at the wireless AP

Check the System event log for authentication failure events corresponding to connection attempts to the wireless AP. To view the failed authentication events, use the Event Viewer to view the events in the System event log with the Source of NPS and the Event ID of 2.

IPsec for RADIUS traffic

- If you are using IPsec to encrypt the RADIUS traffic sent between the wireless AP and the NPS server, check the IPsec settings on both the wireless AP and NPS server to ensure that they can successfully negotiate security associations and authenticate each other.

Note For more information about how to configure IPsec policies in Windows Server 2008 to provide protection for RADIUS traffic, see Chapter 4, "Windows Firewall with Advanced Security." For more information about how to configure IPsec settings for a wireless AP, see your wireless AP's product documentation.

WPA or WPA2 Configuration

If your wireless AP is WPA- or WPA2-capable and you want to use WPA or WPA2 for wireless security, ensure that WPA or WPA2 is enabled.

Unable to Communicate Beyond the Wireless AP

The wireless AP is a transparent bridge and Layer 2 switching device, forwarding packets between the wired network to which it is attached and the connected wireless clients. If wireless clients can connect and authenticate but cannot reach locations beyond the wireless AP, one or more of the following may be happening.

The wireless AP is not forwarding frames as a bridge.

- All transparent bridges support the spanning tree protocol, which is used to prevent loops in a bridged section of the network. The spanning tree protocol uses a series of multicast messages to communicate bridge configuration information and automatically configure bridge interfaces to forward frames or block forwarding to prevent loops. While the spanning tree algorithm is determining forwarding and blocking interfaces, the bridge is not forwarding frames. Check the wireless AP's forwarding status and bridge configuration.

The wireless AP is not configured with the correct VLAN IDs.

- Many wireless APs support VLANs, which are switch ports grouped so that they appear on the same link or subnet. Each group is assigned a separate VLAN ID. Verify that the VLAN IDs for your wireless client and your wired interfaces are correctly configured. For example, you might use one VLAN ID for authenticated wireless clients (that connects them to the organization intranet) and a separate VLAN ID for guest wireless clients (that connects them to an alternate subnet or the Internet).

Troubleshooting the Authentication Infrastructure

If you have multiple wireless APs and are unable to authenticate with any of them, you might have a problem with your authentication infrastructure, which consists of your NPS servers, PKI, and Active Directory accounts. In this section we examine common issues with NPS authentication and authorization, and validation of certificate- and password-based authentications.

Troubleshooting NPS Authentication and Authorization

To troubleshoot the most common issues with NPS authentication and authorization, verify the following:

That the wireless AP can reach the NPS servers

- To test this, try to ping the IP address of the wireless AP's interface on the wired network from each of the NPS servers. Additionally, ensure that IPsec policies, IP packet filters, and other mechanisms that restrict network traffic are not preventing the exchange of RADIUS messages between the wireless AP and its configured NPS servers. RADIUS traffic to the NPS servers uses a source IPv4 or IPv6 address of the wireless AP, a destination IPv4 or IPv6 address of the NPS server, and a UDP destination port of 1812 for authentication messages and UDP destination port 1813 for accounting messages. RADIUS traffic from the NPS servers uses a source IPv4 or IPv6 address of the NPS server, a destination IPv4 or IPv6 address of the wireless AP, and a UDP source port of 1812 for authentication messages and UDP source port 1813 for accounting messages. These examples assume that you are using the RADIUS UDP ports defined in RFC 2865 and 2866 for RADIUS authentication and accounting traffic.

That each NPS server/wireless AP pair is configured with a common RADIUS shared secret

- Each NPS server/wireless AP pair is not necessarily required to use a unique RADIUS shared secret, but it must use the same value for the RADIUS shared secret for the members of the pair. For example, when you copy the NPS configuration from one NPS server to another, verify all of the shared secret pairs between the NPS servers and the wireless APs.

That the NPS servers can reach a global catalog server and an Active Directory domain controller

- The NPS server uses a global catalog server to resolve the user principal name (UPN) of the computer or user certificate or the MS-CHAP v2 account name to the distinguished name of the corresponding account in Active Directory. The NPS server uses an Active Directory domain controller to validate the credentials of the computer and user account and obtain account properties to evaluate authorization.

That the computer accounts of the NPS servers are members of the RAS and IAS Servers security group for the appropriate domains

- Adding the NPS server computer accounts to the RAS and IAS Servers security group for the appropriate domains is normally done during the initial configuration of the NPS server. To add the NPS server computer account to the appropriate domains, you can run the **netsh nps add registeredserver** command.

That there are no configured restrictions blocking access

- Ensure that the user or computer account is not locked out, expired, or disabled or that the time the connection is being made corresponds to the permitted logon hours.

That the user account has not been locked out by remote access account lockout

- Remote access account lockout is an authentication counting and lockout mechanism designed to prevent an online dictionary attack against a user's password. If remote access account lockout is enabled, you can reset account lockout for the account by deleting the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout*DomainName:AccountName* registry value on the NPS server.

That the connection is authorized

- For authorization, the parameters of the connection attempt must:
  - Match all the conditions of at least one network policy. If there is no matching policy, all wireless authentication requests are rejected.
  - Be granted network access permission through the user account (set to Allow Access), or if the user account has the Control Access Through NPS Network Policy option selected, the network access permission of the first matching network policy must be set to Grant Access.
  - Match all the settings of the profile. Verify that the authentication settings of the profile have EAP-TLS or PEAP-MS-CHAP v2 enabled and properly configured.
  - Match all the settings of the dial-in properties of the user or computer account.

    To obtain the name of the network policy that rejected the connection attempt, ensure that NPS event logging is enabled for rejected authentication attempts, and use the Event Viewer to view the events that have the Source of NPS and Event ID set to 2. In the text of the event message, look for the network policy name in the Proxy-Policy-Name or Policy-Name field.

That you have not changed the mode of your domain from mixed mode to native mode

- If you have just changed your Active Directory domain from mixed mode to native mode, NPS servers can no longer authenticate valid connection requests. You must restart every domain controller in the domain for the change to replicate.

Troubleshooting Certificate-Based Validation

Troubleshooting certificate validation for EAP-TLS or PEAP-TLS authentication consists of verifying the wireless client's computer and user certificates and the computer certificates of the NPS servers.

Validating the Wireless Client's Certificate

For an NPS server to validate the certificate of a wireless client, the following must be true for each certificate in the certificate chain sent by the wireless client:

The current date is within the validity dates of the certificate.

- When certificates are issued, they are issued with a valid date range, before which they cannot be used and after which they are considered expired.

The certificate has not been revoked.

- Issued certificates can be revoked at any time. Each issuing certification authority (CA) maintains a list of certificates that should no longer be considered valid by publishing an up-to-date certificate revocation list (CRL). The server will first attempt to validate the certificate using the Online Certificate Status Protocol (OSCP). If the OSCP validation is successful the validation verification is satisfied, otherwise it will then attempt to perform a CRL validation of the user or computer certificate. By default, the NPS server checks all the certificates in the wireless client's certificate chain (the series of certificates from the wireless client certificate to the root CA) for revocation. If any of the certificates in the chain have been revoked, certificate validation fails. This behavior can be modified by changing registry settings as described later in this chapter.

  To view the CRL distribution points for a certificate in the Certificates snap-in, in the contents pane, double-click the certificate, click the Details tab, and then click the CRL Distribution Points field. To perform a revocation check, the NPS server must be able to reach the CRL distribution points.

  The certificate revocation check works only as well as the CRL publishing and distribution system. If the CRL is not updated often, a certificate that has been revoked can still be used and considered valid because the published CRL that the NPS server is checking is out of date. Verify that the CRLs available to the NPS servers have not expired. If the CRLs available to the NPS servers have expired, EAP-TLS and PEAP-TLS authentication fails.

The certificate has a valid digital signature.

- CAs digitally sign certificates they issue. The NPS server verifies the digital signature of each certificate in the chain (with the exception of the root CA certificate) by obtaining the public key from the certificate's issuing CA and mathematically validating the digital signature.

  The wireless client certificate must also have the Client Authentication certificate purpose (also known as Enhanced Key Usage [EKU]) and must contain either a UPN of a valid user account or a fully qualified domain name (FQDN) of a valid computer account in the Subject Alternative Name field of the certificate.

  To view the EKU for a certificate in the Certificates snap-in, double-click the certificate in the contents pane, and then on the Details tab, click the Enhanced Key Usage field.

  To view the Subject Alternative Name field for a certificate in the Certificates snap-in, in the contents pane, double-click the certificate, click the Details tab, and then click the Subject Alternative Name field.

The NPS server must have the appropriate certificate installed correctly.

- To trust the certificate chain offered by the wireless client, the NPS server must have the root CA certificate of the issuing CA of the wireless client certificate installed in its Trusted Root Certification Authorities Local Computer store.

> **Note** In addition to performing normal certificate validation, the NPS server verifies that the identity sent in the initial EAP-Response/Identity message is the same as the name in the Subject Alternative Name property of the received certificate. This prevents a malicious user from masquerading as a different user or computer from that specified in the EAP-Response/Identity message.

For additional requirements for the wireless client's certificate, see the section "Requirements for PKI" in this chapter.

By default, NPS performs certificate revocation checking on the certificate received from the wireless clients. You can use the following registry values in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\E AP\13 on the NPS server to modify certificate revocation checking behavior:

IgnoreNoRevocationCheck

- When set to 1, NPS accepts EAP-TLS authentications, even when it does not perform or cannot complete a revocation check of the client's certificate chain (excluding the root certificate). Typically, revocation checks fail because the certificate does not include CRL information.

  IgnoreNoRevocationCheck is set to 0 (disabled) by default. NPS rejects an EAP-TLS or PEAP-TLS authentication unless it can complete a revocation check of the client's certificate chain (including the root certificate) and verify that none of the certificates has been revoked.

  Set IgnoreNoRevocationCheck to 1 to accept EAP-TLS or PEAP-TLS authentications when the certificate does not include CRL distribution points, such as those from third-party CAs.

IgnoreRevocationOffline

- When set to 1, NPS accepts EAP-TLS or PEAP-TLS authentications even when a server that stores a CRL is not available on the network. IgnoreRevocationOffline is set to 0 by default. NPS rejects an EAP-TLS or PEAP-TLS authentication unless it can access CRLs and complete a revocation check of their certificate chain and verify that none of the certificates has been revoked. When it cannot connect to a location that stores a CRL, EAP-TLS or PEAP-TLS considers the certificate to have failed the revocation check.

  Set IgnoreRevocationOffline to 1 to prevent certificate validation failure because of poor network conditions that inhibit revocation checks from completing successfully.

NoRevocationCheck

- When set to 1, NPS does not perform a revocation check on the wireless client's certificate. The revocation check verifies that the wireless client's certificate and the certificates in its certificate chain have not been revoked. NoRevocationCheck is set to 0 by default.

NoRootRevocationCheck

- When set to 1, NPS does not perform a revocation check of the wireless client's root CA certificate. This entry eliminates only the revocation check of the client's root CA certificate. A revocation check is still performed on the remainder of the wireless client's certificate chain. NoRootRevocationCheck is set to 0 by default.

You can use NoRootRevocationCheck to authenticate clients when the root CA certificate does not include CRL distribution points, such as those from third-party CAs. Also, this entry can prevent certification-related delays that occur when a certificate revocation list is offline or is expired.

All these registry values must be added as a DWORD type (a registry data type composed of hexadecimal data with a maximum allotted space of 4 bytes) and set to 0 or 1. The Windows wireless client does not use these values.

Validating the NPS Server's Certificate

For the wireless client to validate the certificate of the NPS server, the following must be true for each certificate in the certificate chain sent by the NPS server:

The current date must be within the validity dates of the certificate.

- When certificates are issued, they are issued with a range of valid dates before which they cannot be used and after which they are considered expired.

The certificate has a valid digital signature.

- CAs digitally sign certificates they issue. The wireless client verifies the digital signature of each certificate in the chain with the exception of the root CA certificate by obtaining the public key from the certificate's issuing CA and mathematically validating the digital signature.

Additionally, the NPS server computer certificate must have the Server Authentication EKU (object identifier [OID] 1.3.6.1.5.5.7.3.1). To view the EKU for a certificate in the Certificates snap-in, in the contents pane, double-click the certificate, click the Details tab, and then click the Enhanced Key Usage field.

Finally, to trust the certificate chain offered by the NPS server, the wireless client must have the root CA certificate of the issuing CA of the NPS server certificate installed in its Trusted Root Certification Authorities Local Computer store.

For additional requirements for the computer certificate of the NPS server, see the section "Requirements for PKI" in this chapter.

Notice that the wireless client does not perform certificate revocation checking for the certificates in the certificate chain of the NPS server's computer certificate. The assumption is that the wireless client does not yet have a connection to the network and therefore cannot access a Web page or other resource in order to check for certificate revocation.

Troubleshooting Password-Based Validation

Troubleshooting password validation with PEAP-MS-CHAP v2 authentication consists of verifying the wireless client's user name and password credentials and the computer certificates of the NPS servers.

Validating the Wireless Client's Credentials

When you are using PEAP-MS-CHAP v2 for authentication, the name and password as sent by the wireless client must match the credentials of a valid account. The successful validation of the MS-CHAP v2 credentials by the NPS server depends on the following:

- The domain portion of the name corresponds to a domain that is either the domain of the NPS server or a domain that has a two-way trust with the domain of the NPS server.
- The account portion of the name corresponds to a valid account in the domain.
- The password is the correct password for the account.

To verify user account credentials, have the user of the wireless client log on to his or her domain using a computer that is already connected to the network, such as with an Ethernet connection (if possible). This process demonstrates whether there is a problem with the user's credentials or if the problem lies in the configuration of the authentication infrastructure.

Validating the NPS Server's Certificate

For the wireless client to validate the certificate of the NPS server for PEAP-MS-CHAP v2 authentication, the following must be true for each certificate in the certificate chain sent by the NPS server:

The current date must be within the validity dates of the certificate.

- When certificates are issued, they are issued with a valid date range, before which they cannot be used and after which they are considered expired.

The certificate has a valid digital signature.

- CAs digitally sign certificates they issue. The wireless client verifies the digital signature of each certificate in the chain, with the exception of the root CA certificate, by obtaining the public key from the certificate's issuing CA and mathematically validating the digital signature.

Additionally, the NPS server computer certificate must have the Server Authentication EKU (OID 1.3.6.1.5.5.7.3.1). To view the EKU for a certificate in the Certificates snap-in, in the contents pane, double-click the certificate, and then on the Details tab, click the Enhanced Key Usage field.

Finally, to trust the certificate chain offered by the NPS server, the wireless client must have the root CA certificate of the issuing CA of the NPS server certificate installed in its Trusted Root Certification Authorities Local Computer store.

For additional requirements for the computer certificate of the NPS server, see the section "Requirements for PKI" in this chapter.

Chapter Summary

Deploying a protected wireless network solution involves configuration of Active Directory, PKI, Group Policy, and RADIUS elements of a Windows-based authentication infrastructure. Once deployed, ongoing maintenance consists of managing wireless APs and their configuration for changes in infrastructure servers and updating and deploying wireless profiles. Common problems with wireless connections include the inability to connect due to an authentication or authorization failure and the inability to reach intranet resources from the wireless client.

Additional Information

For additional information about wireless support in Windows Vista and Windows Server 2008, see the following:

- Windows Server 2008 Help and Support
- Microsoft Wireless Networking (*http://www.microsoft.com/wifi*)

For additional information about Active Directory, see the following:

- Chapter 9, "Authentication Infrastructure"
- Windows Server 2008 Help and Support
- Windows Server Active Directory (*http://www.microsoft.com/ad*)

For additional information about PKI, see the following:

- Chapter 9, "Authentication Infrastructure"
- Windows Server 2008 Help and Support
- Public Key Infrastructure for Windows Server (*http://www.microsoft.com/pki*)
- Microsoft Windows Server 2003 PKI and Certificate Security (*http://www.microsoft.com/mspress/books/6745.aspx*)

For additional information about Group Policy, see the following:

- Chapter 9, "Authentication Infrastructure"
- Windows Server 2008 Help and Support
- Windows Server Group Policy (*http://www.microsoft.com/gp*)
- Microsoft Windows Group Policy Guide (http://www.microsoft.com/mspress/books/8763.aspx)

For additional information about RADIUS and NPS, see the following:

- Chapter 9, "Authentication Infrastructure"
- Windows Server 2008 Help and Support
- Network Policy Server (http://www.microsoft.com/nps)

For additional information about NAP and 802.1X Enforcement, see the following:

- Chapter 14, "Network Access Protection Overview"
- Chapter 15, "Preparing for Network Access Protection"
- Chapter 17, "802.1X Enforcement"
- Windows Server 2008 Help and Support
- Network Access Protection (*http://www.microsoft.com/nap*)