Microsoft Solutions for Security

Securing Wireless LANs with PEAP and Passwords

Microsoft®

Table of Contents

Chapter 1: Securing Wireless LANs with PEAP and Passwords 1
  Introduction 1
  Solution Overview 2
    Appendixes 4
  Style Conventions 5
  Support and Feedback 5
    Support 5
    Give Us Your Feedback 6

Chapter 2:Planning a Wireless LAN Security Implementation 7
  Overview 7
  Chapter Prerequisites 7
  How Wireless LAN Security Works 8
    How 802.1X with PEAP and Passwords Works 8
  Target Organization Profile 11
    Organization Layout 11
    IT Environment 12
  Design Criteria 13
  WLAN Architecture 15
    Network Design 15
    IAS Server Placement 16
    IAS Software and Hardware Requirements 20
    IAS Configuration 21
    Obtaining Certificates for IAS Servers 25
    WLAN Clients 27
    Migration from an Existing WLAN 29
  Scaling for Larger Organizations 30
    IAS Server Placement 30
    Multiple Domains 31
    PKI Architecture 32
  Variations on the Solution Architecture 33
    Bootstrapping Client Computers 36
    SOHO Environments 37
  Summary 37
  References 38

Chapter 3: Preparing Your Environment 41
  Overview 41
  Chapter Prerequisites 41
  IT Infrastructure Prerequisites and Assumptions 41
  Preparing for Implementation 42
    Permissions Needed 42
    Tools Needed 43
  Installing the Solution Tools 43
    Using the Scripts 44
  Setting up Your Network and Directory Infrastructure 45
    Configuring the Network 45
    DHCP 46
    DNS 46
    Active Directory 46
  Preparing Your Servers 48
    Operating Systems Supported 48

Hardware Guidelines ... 49
Obtaining and Installing Supporting Software ... 49
Server Security Configuration ... 51
Server Security Updates ... 54
Summary ... 56
References ... 57

Chapter 4: Building the Network Certification Authority ... 59
Overview ... 59
Chapter Prerequisites ... 60
Preparing for Implementation ... 60
Permissions Needed ... 60
Tools Needed ... 60
Certification Authority Parameters ... 61
Checking Readiness for Installation ... 61
Installing Certificate Services ... 62
Installing the Certificate Services Software Components ... 62
Verifying the CA Installation ... 63
Configuring the CA ... 64
Configuring the CA Properties ... 64
Importing the Automatic Certificate Request GPO ... 65
Verifying CA Configuration ... 66
Summary ... 66
References ... 67

Chapter 5: Building the Wireless LAN Security Infrastructure ... 69
Overview ... 69
Chapter Prerequisites ... 70
Preparing for Implementation ... 70
Permissions Needed ... 70
Tools Needed ... 70
IAS Parameters ... 70
Checking Readiness for Installation ... 71
Validating the IAS Environment ... 71
Verifying DHCP Settings ... 72
Installing IAS ... 72
Installing the IAS Software Components ... 72
Verifying the Installation ... 73
Registering IAS in Active Directory ... 73
Configuring the Primary IAS Server ... 73
Automatically Enrolling for an IAS Server Certificate ... 74
Configuring the First IAS Server ... 74
Deploying Settings to Multiple IAS Servers ... 77
Replicating Settings from the First IAS Server ... 78
Configuring Wireless Access Points ... 80
Adding the Access Points as RADIUS Clients to IAS ... 80
Configuring the Wireless Access Points ... 83
Replicating RADIUS Client Configuration to Other IAS Servers ... 87
Summary ... 88
References ... 88

Chapter 6: Configuring the Wireless LAN Clients ... 91
Overview ... 91
Chapter Prerequisites ... 91
Preparing for Implementation ... 91
Tools Needed ... 92

WLAN Client Parameters 92
Allowing Users and Computers to Access the WLAN 92
Controlling WLAN Access Using Security Groups 93
Configuring Windows XP WLAN Clients 93
Install any Required Patches and Updates 94
Creating the WLAN Settings GPO 94
Deploying the WLAN Settings 96
Verifying Application of WLAN Group Policy 96
Verifying the Root CA Certificate on the Client 97
Verifying the Connection to the WLAN 97
Configuring Pocket PC 2003 Clients 98
Preparing the Pocket PC Device 98
Making the CA Certificate Available 98
Configuring the Pocket PC 99
Verifying the Pocket PC Connection to the WLAN 100
Summary 100
References 101

Chapter 7: Testing the Secure Wireless LAN Solution 103
Introduction 103
Knowledge Prerequisites 103
How Microsoft Tested the Solution 103
Test Network Layout 104
Verifying Your Implementation 105
Scenario 1: Verifying IAS Server Certificate Deployment 105
Scenario 2: Verifying the Root CA Certificate on the Windows XP Wireless Client 106
Scenario 3: Verifying User Authentication to the Wireless Network 106
Scenario 4: Verifying Computer Authentication to the Wireless Network 107
Scenario 5: Verifying Pocket PC Authentication to the Wireless Network 107
Scenario 6: Blocking a WLAN Client Using IAS Remote Access Policy 107
Scenario 7: WLAN Access Denied if the User is not a Member of WLAN Access Groups . 108
Scenario 8: Verifying IAS Service Failover 108
Scenario 9: Wireless Client Roving Between Access Points and Re-Authenticating to WLAN 109
Scenario 10: Re-authentication of Wireless Client Due to IAS Session Time-out 109
Scenario 11: E-mail Alert for IAS Backup Failure 109
Scenario 12: E-mail Alert for CA Service Failure 110
Test Tools 111
Summary 111

Chapter 8: Maintaining the Secure Wireless LAN Solution 113
Introduction 113
Overview 113
Chapter Prerequisites 113
Essential Maintenance Tasks 114
Initial Setup Tasks 114
Maintenance Tasks 115
Tools and Technology Required 115
Operating the WLAN Infrastructure 116
Operational Tasks 116
Monitoring 118
Managing Changes 123
Support Tasks 128
Optimization Tasks 129
Troubleshooting 131
Troubleshooting Procedures 131

    Troubleshooting Tools and Techniques 141
  Summary 147
  References 148

Appendix A: Using PEAP in the Enterprise 149
  What You Need From the EAP–TLS Solution 149
    Chapter 1—Overview 150
    Chapter 2—Deciding on a Secure Wireless Networking Strategy 151
    Chapter 3—Secure Wireless LAN Solution Architecture 151
    Chapter 4—Designing the Public Key Infrastructure 151
    Chapter 5—Designing a RADIUS Infrastructure for Wireless LAN Security 151
    Chapter 6—Designing Wireless LAN Security Using 802.1X 151
    Chapter 7—Implementing the Public Key Infrastructure 151
    Chapter 8—Implementing the RADIUS Infrastructure for Wireless LAN Security 152
    Chapter 9—Implementing Wireless Security Using 802.1X 152
    Chapters 10, 11, and 12—Operating the Solution 152
    Chapter 13—Test Guide 152
    Scripts 152

Appendix B: Using WPA in the Solution 153
  Using WPA in Place of WEP 153
    Creating an IAS Remote Access Policy for WLAN with WPA 153
    Manually Configuring Windows XP WLAN Settings for WPA 154
    Configuring Pocket PC 2003 for WPA 155
  Migrating from WEP to WPA 155
  References 156

Appendix C: Supported OS Versions 157

Appendix D: Scripts and Support Files 161
  Introduction 161
    Disclaimer 161
  Structure of the Scripts 161
    Job Output 163
    Executing the Jobs 164

1

Securing Wireless LANs with PEAP and Passwords

Introduction

Today, wireless technology is a hot topic of debate in the business world; most organizations either have already deployed wireless local area networks (WLAN) or are involved in discussions on pros and cons of wireless technology. The productivity improvements perceived by users and the attractiveness of low maintenance networking for information technology (IT) departments are undeniable. However, serious security concerns have made the majority of IT heads cautious about, if not downright hostile toward, the idea of introducing WLANs into their organizations. At the same time, the solutions proposed by analysts and network vendors to address these concerns have seemed overly complex and costly to deploy.

Securing Wireless LANs with PEAP and Passwords is the second Microsoft® security solution for WLANs. It is a companion to the first solution, *Securing Wireless LANs —a Certificate Services Solution*. Whereas the first solution was aimed at large organizations, the second is considerably simpler and easier to deploy and is designed for small and medium–sized organizations. The primary technological difference between the two solutions is that the first solution uses public key certificates to authenticate users and computers to the WLAN whereas the second uses user name and password authentication. Other distinguishing features of this solution are that it uses existing (rather than new) server hardware, employs a simpler administrative delegation model, and automates many more of the configuration tasks using scripts and predefined settings.

The documentation for this solution has two important characteristics, which distinguish it from general product documentation of Microsoft Windows® operating system and many of the technical white papers available from Microsoft. The first is the *prescriptive* nature of the guidance; where design choices were available, decisions were taken based on knowledge gained from internal deployment as well as customer feedback received by Microsoft. The solution is based on these best practices and built and tested in Microsoft labs to ensure that the solution works as intended. The second characteristic is that it is an *end–to–end* solution encompassing the complete lifecycle of designing and planning, building, testing and managing the solution.

As detailed in later chapters, the solution is based on the Institute of Electrical and Electronic Engineers (IEEE) 802.1X standard and requires a RADIUS (Remote Authentication Dial–In User Service) infrastructure. It uses a flexible architecture that can be adapted for a range of organizations starting from those with only a few tens of users to those with several thousand users. The solution was built and tested using Microsoft Windows® XP clients, Microsoft Pocket PC 2003 clients, and Microsoft Windows Server™ 2003 servers.

Solution Overview

This guidance is divided into four sections, each of which corresponds to a phase in the life cycle of the solution. These phases are planning, implementing, testing, and operating. These phases are further divided into chapters.

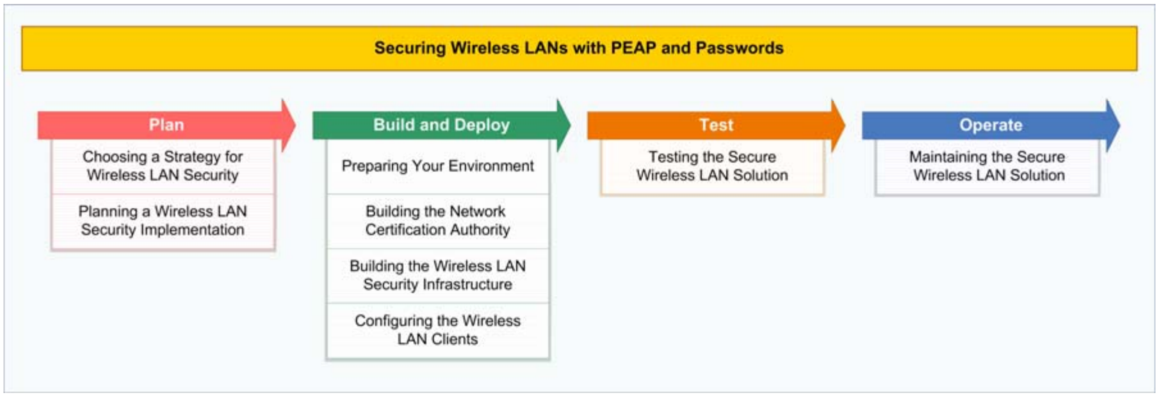
Securing Wireless LANs with PEAP and Passwords
Plan
Choosing a Strategy for Wireless LAN Security
Planning a Wireless LAN Security Implementation
Build and Deploy
Preparing Your Environment
Building the Network Certification Authority
Building the Wireless LAN Security Infrastructure
Configuring the Wireless LAN Clients
Test
Testing the Secure Wireless LAN Solution
Operate
Maintaining the Secure Wireless LAN Solution

Figure 1.1
Overview of Securing Wireless LANs

The planning section consists of an introduction, "Choosing a Strategy for Wireless LAN Security”, and Chapter 2, "Planning a Wireless LAN Security Implementation.” The next four chapters make up the build and deploy section. These chapters provide instructions for implementing the RADIUS servers using Windows Server 2003 Internet Authentication Service (IAS), and deploying the wireless clients and supporting infrastructure. Each chapter provides detailed procedures on installing and configuring the software components and integrating them into the solution. The chapters also include verification procedures that help minimizes errors.

The testing section has one chapter, which explains how to confirm that the solution is working correctly before it is deployed. The operating section also has a single chapter; this explains how to operate, monitor, change, and troubleshoot all the components of the solution.

A set of tools and scripts accompany the guidance and are used for automating many of the implementation and operations tasks.

The following section gives a more detailed description of each chapter.

Choosing a Strategy for Wireless LAN Security

This document serves as an introduction to the two WLAN security solutions described earlier. Its objective is to help you select the right strategy for the security infrastructure for your wireless network. It describes the business reasons that drive the adoption of WLAN technology and the security concerns surrounding it. It discusses the different options available for addressing these security concerns and outlines a solution based on strong authentication and network data protection. It also contains a discussion on the relative merits of the different approaches to securing WLANs including native WLAN security solutions, virtual private networks (VPN), and IP security.

Chapter 1: Securing Wireless LANs with PEAP and Passwords

Chapter 1 is this current chapter and gives an overview of the content of the solution guidance.

Chapter 2: Planning a Wireless LAN Security Implementation

This chapter describes the architectural design of the wireless LAN security solution. It covers the following topics:

- How a WLAN solution based on 802.1X and Protected Extensible Authentication Protocol (PEAP) works.
- A description of the target organization for this solution and the key design criteria for the solution.
- Developing a WLAN security solution design based on the requirements of the target organization.
- Describing how this basic design can be scaled for much larger organizations.
- Discussing variations on the design to accommodate requirements outside the core solution such as introducing VPN or wired 802.1X networking.

The chapter concentrates on the design of a RADIUS infrastructure (using IAS, the RADIUS implementation included with Windows Server) to provide strong authentication and key management services. The chapter also includes a discussion of the wireless clients supported by the solution and the certificate requirements.

Chapter 3: Preparing Your Environment

This chapter focuses on the underlying information technology (IT) infrastructure needed to support this WLAN solution. It describes the preparation of Microsoft Active Directory® active directory, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) services, and underlying network requirements. It also includes procedures to apply security settings and install required security updates to the servers used in the solution.

Chapter 4: Building the Network Certification Authority

This chapter describes how to install a simple Certification Authority (CA) on a domain controller to provide certificates for the IAS servers. The procedures to do this are largely automated using scripts included with the guidance. The CA built for this solution is dedicated to the specific task of issuing certificates to the IAS servers and, as such, requires little or no ongoing maintenance.

Chapter 5: Building the Wireless LAN Security Infrastructure

This chapter gives instructions on how to deploy your WLAN security components, the IAS servers and the wireless access points (AP). It includes step–by–step guidance on installing IAS on a domain controller (or member server), configuring IAS settings and policies, setting up wireless APs to use the IAS servers, and replicating IAS settings between the IAS servers.

Chapter 6: Configuring the Wireless LAN Clients

This chapter contains the procedures to configure the clients supported by the solution. The three main sections of the chapter focus on controlling user and computer access to the WLAN, configuring the group policy settings for Windows XP WLAN clients, and manually configuring WLAN settings for Pocket PC 2003 clients.

Chapter 7: Testing the Secure Wireless LAN Solution

This chapter is derived from the test plan used by the Microsoft team when testing this solution. The build chapters (3 to 6) contain regular verification procedures used throughout the build process to verify that things are progressing correctly. This chapter supplements those procedures with a set of extra tests that you should carry out prior to deploying the solution in production.

Chapter 8: Maintaining the Secure Wireless LAN Solution

This chapter focuses on keeping the WLAN security infrastructure running properly. The first part of the chapter includes the key operational tasks that you need to maintain the system. These are divided into different categories covering: everyday maintenance tasks, monitoring and alerting; introducing changes into the environment; optimizing performance; and resolving problems. The final troubleshooting section includes a series of troubleshooting flowcharts, tables, and procedures along with detailed descriptions of a number of troubleshooting tools and techniques that you can use to help you diagnose and fix problems.

Appendixes

Appendix A: Using PEAP in the Enterprise

This solution was designed for small and medium businesses. This contrasts with the certificate–based WLAN solution (mentioned earlier) which was designed for an enterprise–level organization. However, a WLAN solution using PEAP with passwords can also be used by large organizations.

This appendix shows how you can adapt the enterprise–oriented guidance in the certificate–based WLAN solution to deploy a WLAN solution based on PEAP with passwords.

Appendix B: Using WPA in the Solution

This appendix provides information about the status of support for WiFi Protected Access (WPA) security and about how you can use WPA in place of dynamic WEP (Wired Equivalent Privacy) data protection. This solution was designed to support WPA, and WPA is referred to throughout the guidance. However, support for WPA was still not universal when this solution was being developed, therefore WPA was not used as the default option.

Appendix C: Supported Operating System Versions

This appendix comprises a table showing the operating system versions that are supported for wireless clients and for various server roles in this solution. It is intended to answer questions about whether alternative versions of Windows and other platforms can be used in the various roles of the solution.

Appendix D: Scripts and Support Files

The procedures in the implementation and operations chapters use a number of scripts and other support files. This appendix describes the scripts and how they work. This information is also provided in the SecuringWirelessLANs.rtf file included with the scripts.

Style Conventions

The following table describes style conventions used in this guidance.

Table 1.1: Style Conventions

Element	Meaning
Bold font	Characters that are typed exactly as shown, including commands and switches. User Interface (UI) elements in text that is prescriptive are also bold.
Italic font	Italic font is used in two special contexts: –Where italic fonts are used within the main body of the text, they indicate the title of another document. –Where italic fonts are used within commands or code (or text referring to a command or code), they indicate a placeholder for variables where specific values need to be supplied. For example, *Filename.ext* indicates that you should replace the italicized *Filename.ext* with the file name of your choice. Italic font is also occasionally used to provide emphasis to normal text.
Screen Text	For text displayed on the screen (for example, the output from a command–line tool) and for commands that need to typed in at the command line. Some commands do not fit within the page margins. Where this occurs, the command text is wrapped onto multiple lines with subsequent lines indented (this is indicated by a note following the command).
`Monospace font`	Code samples and contents of configuration files.
%SystemRoot%	The folder in which the Windows Server operating system is installed.
Note	Alerts the reader to supplementary information.
Important	Alerts the reader to supplementary information that is essential to the completion of the task.
Caution	Alerts the reader to situation where failure to take or avoid a specific action could result in the loss of data.
Warning	Alerts the reader to situation where failure to take or avoid a specific action could result in physical harm to the user or hardware.

Support and Feedback

Support

For further help in implementing the technologies discussed in this solution, you may contact your local Microsoft office or a Microsoft Services partner.

- To find your local Microsoft office, go to the following URL and select the relevant country/region
  http://www.microsoft.com/worldwide/.

- To find a Microsoft partner in your region, see in the “Services” section of the Microsoft Resource Directory, at the following URL:
  http://directory.microsoft.com/ResourceDirectory/Solutions.aspx.

- For more information about how the Windows Server 2003 components used in this solution are supported, including escalation paths, support offerings, resources, and support levels, see the following URL:
  http://support.microsoft.com.

Give Us Your Feedback

Microsoft would like your feedback on this material. In particular, please provide answer to the following questions:

- How useful was the information provided?
- Were the step–by–step procedures accurate?
- Were the chapters readable and interesting?
- Overall, how would you rate the solution?

Your feedback may be sent to the following e-mail address:
SecWish@Microsoft.com.

2

Planning a Wireless LAN Security Implementation

Overview

This chapter describes the overall design of the secure wireless local area network (WLAN) solution. It aims to give you a thorough understanding of the design of the solution and the reasons for designing it that way. It should also give you enough information to help you adapt the design to the particular needs of your organization.

The chapter begins with a description of how 802.1X and Protected Extensible Authentication Protocol (PEAP) work to secure access to the network. This is followed by a description of the target organization for the solution and explores some of their key requirements.

The middle portion of the chapter describes the design of the WLAN solution including: the network design; Internet Authentication Service (IAS) server placement; selection of hardware and software; obtaining certificates; and client configuration. How to migrate from an unsecured WLAN to 802.1X and PEAP is also outlined.

The sections towards the end of the chapter deal with variations on the basic solution design. The most important of these design variations is how to scale the solution for use in larger organizations, which is discussed at some length. Other design options covered are:

- Reusing the IAS infrastructure for wired LAN security
- Using IAS for remote access authentication
- Deploying WLANs in SOHO environments

Chapter Prerequisites

As part of planning for your secure WLAN implementation you need to ensure that you have the right skill sets available in your organization and that you involve the right people in the decisions affecting the deployment.

To get the best out of this chapter, it would be helpful if you were familiar with the following topics:

- Networking concepts particularly Wireless LANs.
- Microsoft® Windows® 2000 or Windows Server™ 2003.

- Microsoft Active Directory® directory service concepts, including Active Directory domains and forests, management tools, use of Group Policy, and manipulation of users, groups, and other Active Directory objects.
- Certificate services and public key infrastructure (PKI) concepts.
- General security concepts such as authentication, authorization and encryption.
- Windows security features such as users, groups, auditing, and access control lists (ACL).
- Application of security settings using Group Policy.

Note: Although this solution can be implemented without in-depth technical knowledge, you should ideally have a Microsoft Certified Systems Engineer (MSCE) certification or equivalent knowledge and experience.

How Wireless LAN Security Works

Different methods for securing WLANs were discussed at some length in the introductory document, “Choosing a Strategy for Wireless LAN Security”. The discussion focused on the use of strong authentication to the WLAN using 802.1X and encrypting the network traffic using dynamic Wired Equivalent Privacy (WEP) or WiFi Protected Access (WPA). The following are the key points from that discussion:

- The original 802.11 WLAN security scheme, known as Wired Equivalent Privacy (WEP), has serious security deficiencies that allow an attacker to discover the network key and break on to the network. This scheme is known as "Static WEP" in this because of its use of a fixed network access and encryption key shared between all members of the WLAN.
- Use of the IEEE 802.1X gives a strong access control mechanism for the WLAN. This must be coupled with a secure Extensible Authentication Protocol (EAP) method. The choice of EAP method defines the type of credentials that can be used to authenticate users and computers to the WLAN.
- Microsoft supports and recommends the use of PEAP with MS-CHAP v2 for password authentication and EAP-TLS for certificate authentication.
- PEAP is a means of protecting another EAP method (such as MS-CHAP v2) within a secure channel. The use of PEAP is essential to prevent attacks on password–based EAP methods.
- Strong data protection of the WLAN traffic can be provided by either dynamic WEP or WPA. Master encryption keys for data protection are generated as part of the 802.1X authentication process (although dynamic WEP and WPA use these keys differently).
- The distinction between static WEP and dynamic WEP is crucial. Dynamic WEP uses the same encryption algorithms as static WEP but continually refreshes the encryption keys, therefore defeating known attacks on static WEP. Dynamic WEP only refers to the network data protection mechanism, network authentication is handled separately by 802.1X.

How 802.1X with PEAP and Passwords Works

For password-based WLAN authentication, Microsoft supports the use of PEAP with MS-CHAP v2. Figure 2.2 illustrates how 802.1X with PEAP and MS-CHAP v2 works.

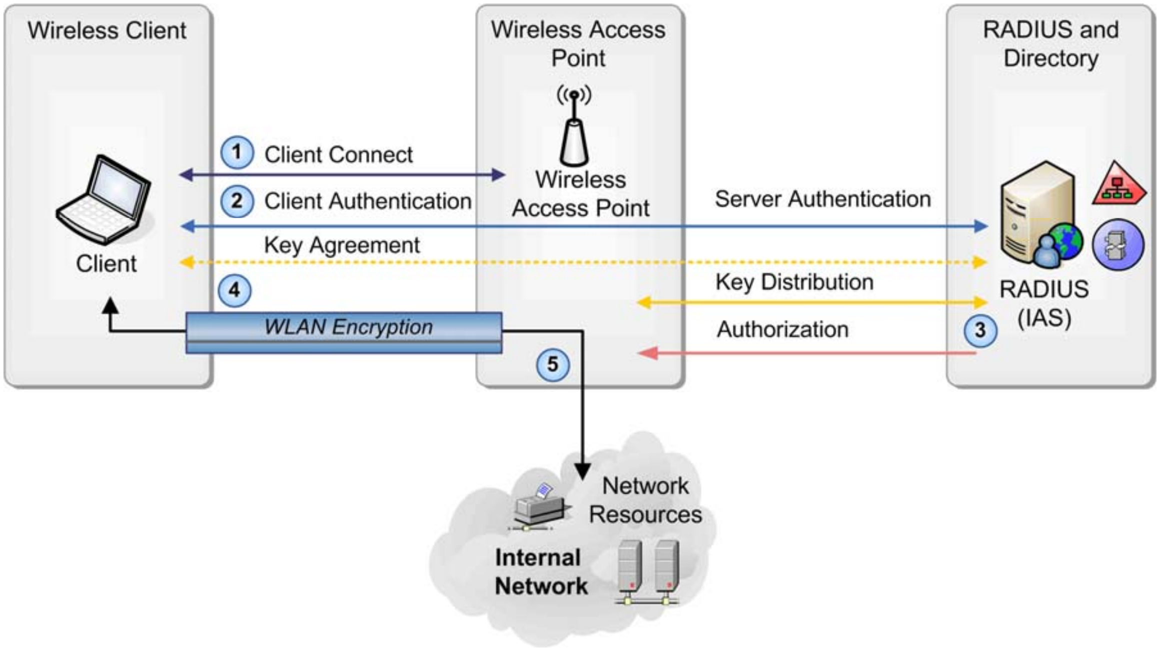

Figure 2.1

a. 802.1X and PEAP authentication to the wireless LAN

The figure shows the following four main components:

- **Wireless client:** This is a computer or device running an application that requires access to network resources. The owner of the credentials that are used to authenticate the client to the network can be a user or a computer. The client must have a WLAN network adapter that supports 802.1X and dynamic WEP or WPA encryption. The client is also referred to as the station (STA) in many network standards documents.

  Before the client can be granted access to the WLAN, it must agree on a set of credentials with the authentication service (the RADIUS server and directory) in some out–of–band operation. In this case, the domain accounts of the user and computer are created prior to connecting to the WLAN. The client knows its password and the domain controller (the directory) is able to verify the password. The client must also be preconfigured with the correct WLAN settings, which include the WLAN name and the authentication method to use.

Note: Strictly speaking, only one set of credentials (either the user or the computer) need to be agreed out-of-band. For example, you can connect the WLAN using the user credentials and then join the computer to the domain. However, this solution assumes that both user and computer accounts exist prior to accessing the WLAN.

- **Wireless access point (AP):** The wireless AP is responsible for controlling access to the WLAN and bridging a client connection to the internal LAN. It must support 802.1X and dynamic WEP or WPA encryption. In network standards terminology, the AP fills the role of the Network Access Service (NAS).

  The wireless AP and the RADIUS server also have a shared secret to enable them to securely identify each other.

- **The RADIUS server and directory:** the RADIUS server uses the directory to verify the credentials of WLAN clients. It makes authorization decisions based on a network access policy. It may also collect accounting and audit information about client access to the network. This is referred to as the authentication service (AS) in network standards terminology.

- **The internal network:** This is a secure network to which the wireless client application needs to gain access.

The following steps describe how the client makes a request and is granted access to the WLAN and thus the internal network. These step numbers correspond to the numbers in figure 2.1.

1. When the client computer is in range of the wireless AP, it tries to connect to the WLAN that is active on the wireless AP and identified by its Service Set Identifier (SSID). The SSID is the name of the WLAN and is used by the client to identify the correct settings and credential type to use for this WLAN.
2. The wireless AP is configured to allow only secured (802.1X authenticated) connections. When the client tries to connect to it, the AP issues a challenge to the client. The AP then sets up a restricted channel, which allows the client to communicate only with the RADIUS server (blocking access to the rest of network). The RADIUS server will only accept a connection from a trusted wireless AP; that is, one which has been configured as a RADIUS client on the IAS server and provides the shared secret for that RADIUS client.

   The client attempts to authenticate to the RADIUS server over the restricted channel using 802.1X. As part of the PEAP negotiation the client establishes a Transport Layer Security (TLS) session with the RADIUS server. Using a TLS session as part of PEAP serves a number of purposes:

   - It allows the client to authenticate the RADIUS server; this means that the client will only establish the session with a server holding a certificate that is trusted by the client.
   - It protects the MS-CHAP v2 authentication protocol against packet snooping.
   - The negotiation of the TLS session generates a key that can be used by the client and RADIUS server to establish common master keys. These keys are used to derive the keys used to encrypt the WLAN traffic.

   Secured within the PEAP channel, the client authenticates itself to the RADIUS server using the MS-CHAP v2 EAP protocol. During this exchange, the traffic within the TLS tunnel is only visible to the client and RADIUS server and is never exposed to the wireless AP.
3. The RADIUS server checks the client credentials against the directory. If the client is successfully authenticated, the RADIUS server assembles information that allows it to decide whether to authorize the client to use the WLAN. It uses information from the directory (such as group membership) together with constraints defined in its access policy (for example, the times of day that WLAN access is allowed) to either grant or deny access to the client. The RADIUS relays the access decision to the AP.

   If the client is granted access, the RADIUS server transmits the client master key to the wireless AP. The client and AP now share common key material that they can use to encrypt and decrypt the WLAN traffic passing between them.

   When using dynamic WEP to encrypt the traffic, the master keys are directly used as the encryption keys. These keys need to be changed periodically to thwart WEP key recovery attacks. The RADIUS server does this by regularly forcing the client to re–authenticate and generate a new key set.

   If WPA is used to secure the communication, the master key material is used to derive the data encryption keys, which are changed for each packet transmitted. WPA does not need to force frequent re–authentication to ensure key security.

4. The AP then bridges the client WLAN connection to the internal LAN, allowing the client to talk freely to systems on the internal network. The traffic sent between the client and AP is now encrypted.
5. If the client requires an IP address, it can now request a Dynamic Host Configuration Protocol (DHCP) lease from a server on the LAN. Once the IP address has been assigned, the client can begin communicating normally with systems on the rest of the network.

Computer and User Authentication to the WLAN

The process just described illustrates how a client (a user or a computer) successfully connects to the WLAN. Microsoft Windows® XP authenticates both the user and the computer independently. When computer first starts up, it uses its domain account and password to authenticate to the WLAN. The authorization of the computer to the WLAN follows all of the steps outlined in the previous section. Having the computer connect to the WLAN using its own credentials permits it to be managed even when no user is logged on. For example, group policy settings can be applied and software and patches distributed to the computer.

When a user logs on to the computer, the same authentication and authorization process is repeated, but this time with the user's name and password. The user’s session replaces the computer WLAN session; this means that the two are not active simultaneously. It also means that an unauthorized user cannot use an authorized computer to access the WLAN.

Note: Windows XP allows you to override this behavior and specify that either only the computer or user credentials are used. These are not recommended configurations. The former allows users to connect to the WLAN without authorization. The latter prevents the computer from connecting to the WLAN until a user logs on, which will interfere several computer management functions.

Target Organization Profile

This solution is designed for a small business of 100–200 people. Although the organization is fictitious, its characteristics and requirements are derived from extensive real–world research. These real–world requirements have helped shape the style and scope of the guidance as well as the choices made in the design.

It is important to understand that this solution is not restricted to organizations of this size. The simplicity of the design and the scalability of the components used mean that the same PEAP–based WLAN solution can be easily scaled for much larger (with thousands of users) and much smaller organizations. By understanding the characteristics of the target organization, you will be better placed to understand the assumptions of the design and adapt them to your own organization.

Using the solution in larger organizations is covered in the "Scaling for Larger Organizations" section of this chapter. For very smaller organizations, all of the required components can be installed on a single existing server.

Organization Layout

The physical and information technology (IT) layout of the organization is shown in the following figure.

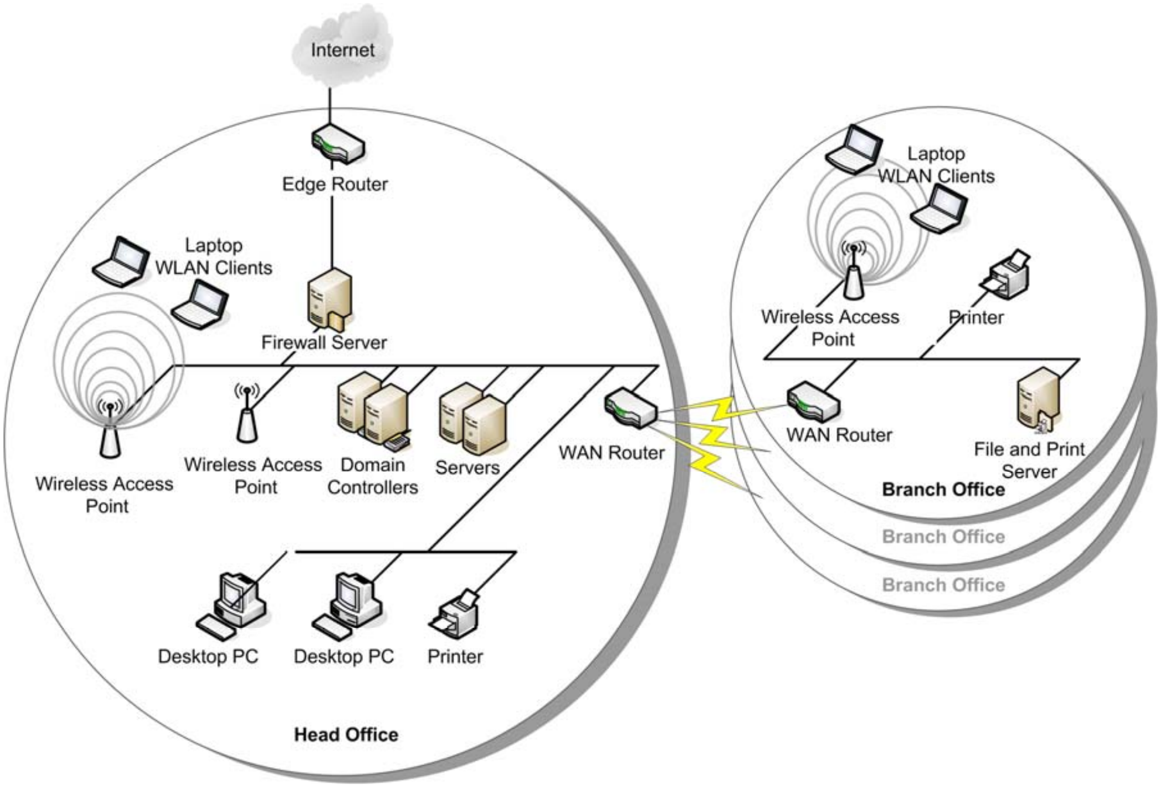

Figure 2.2
b. The physical and IT layout of the target organization

There is a single large head office, which houses most of the IT systems and the majority of the users. All Active Directory domain controllers are located here. The head office has a connection to the Internet through a firewall server. There are a number of WLAN clients and wireless APs connected to the internal network.

There are also one or more outlying offices with very few local IT services beyond network connectivity to the head office. There are a small number of clients (possibly all wireless) at this office and it frequently receives visitors from head office who bring their WLAN clients to be able to connect back to their applications and data at the head office.

The wide area network (WAN) connectivity between offices is provided either by private lines (for example a T1—1.5Mbps) or by DSL Internet connections and a virtual private network (VPN) router–to–router link across the Internet. The WAN connection is typically not resilient to failure.

Note: If the WAN connection between offices is provided by a VPN connection across the Internet, each office will typically have a firewall protecting it from threats on the Internet. The presence of this firewall is not relevant to the WLAN discussion and has been omitted to aid clarity.

IT Environment

The Active Directory of this organization is a single domain forest with at least two domain controllers. It authenticates users to the domain and provides directory and authentication services to several applications such as Microsoft Exchange Server and Outlook® for e–mail. The domain controllers have recently been upgraded from Windows 2000 Server to Windows Server 2003, Standard Edition. The domain controllers also run additional services such as Domain Name System (DNS), DHCP, and Windows Internet Name Service (WINS) for a few legacy applications.

The IT systems are predominantly Microsoft technologies, with Windows XP on client computers and Windows Server 2003 on server systems. There are also a number of servers running Windows 2000, which the company plans to upgrade as application testing and support allow. The organization has begun to invest in mobile systems such as Windows XP, Tablet Edition, and Pocket PC 2003 particularly for its sales, distribution, and warehouse staff.

Key server applications include Microsoft Exchange Server, SQL Server (running several line–of–business applications), Internet Information Services (IIS), and Windows SharePoint™ Team Services.

Applications are deployed to client computers using Active Directory group policy. Operating system patches are deployed using Microsoft Software Update Service (SUS) and the Windows AutoUpdate service.

System monitoring is done directly on the server systems by reviewing Windows event logs, performance logs, and application logs daily. Critical alerts for hardware and software are sent to the IT administrator through e–mails and alerts on the system consoles.

The organization has two full–time IT personnel, who look after the IT planning, service delivery, and day–to–day support. Both the IT manager and the IT support engineer have latest MCSE certifications and a number of years of experience in IT.

Design Criteria

The organization described in the previous section will typically have the following types of criteria for a WLAN solution. These criteria have been extended to cover a broad category of organizations. The design presented in the rest of the chapter explicitly uses these criteria.

Table 2.1: WLAN Solution Design Criteria

Design Factor	Criteria
Security Requirements	**–Robust authentication and authorization of wireless clients.** **–Robust access control to permit network access to authorized clients and to deny any unauthorized access.** **–High strength encryption (128–bit) of wireless network traffic.** **–Secure management of encryption keys.**
Scalability—Min/Max users supported	**25 to 5,000 or more WLAN users** **See Table 2.2 for authentication loads for different sizes of WLAN.**
Scalability—Number of sites supported	Basic: **Single large site with local domain controllers and IT services; one or more small sites with no domain controllers. Minimum users required are 25.** High end: **Single central site with multiple domain controllers; large offices with single domain controller and/or resilient WAN connectivity to head office; multiple small offices with no domain controller,**

Design Factor	Criteria
	probably no WAN resilience. Maximum users allowed are 5000. For use with larger organizations, refer to Appendix A, "Using PEAP in the Enterprise".
Availability Requirements	Use of multiple wireless APs, IAS, or domain controllers gives WLAN resilience to single component failure for larger offices. Small office WLANs are vulnerable to WAN failure unless redundant connectivity is installed.
Platform Support	Server platforms: **Windows Server 2003, Standard Edition or Enterprise Edition (for IAS and Certification Authority (CA) installation). Standard edition supports maximum of 50 wireless APs (RADIUS clients) per server.** Client platforms: **Windows XP Professional or Tablet Edition; Pocket PC 2003.**
Extensibility (reuse of solution components for other applications)	Other network access applications (remote access VPN, 802.1X wired network access, and firewall authentication) can be supported by same authentication infrastructure.
IT Organization Requirements	Installation and management of solution requires IT professional with latest MSCE certification or equivalent knowledge and 2 to 3 years experience in IT industry.
Manageability Requirements	The solution will require minimal management to maintain healthy operation. Alerts are sent through e-mail and/or Windows event log (or modified to trigger other alter types). IAS component can be monitored by Windows monitoring solution (using event logs and performance counters), by RADIUS logging and by Simple Network Management Protocol (SNMP) management system.
Standards Conformance	The solution supports the following standards: –IEEE 802.11 (a, b, or g) network standards. –IEEE 802.1X authentication with PEAP and MS-CHAP v2. It can be used with other EAP methods such as certificate-based EAP-TLS and PEAP-EAP-TLS. –Dynamically keyed WEP and WPA WLAN protection. Future capabilities and standards (for example, 802.11i). –RADIUS support for RFC 2865 and 2866.

1.

The following table gives an indication of the WLAN authentication requirements for different sizes of organization. The "New Authentications per second" is part of the steady load and assumes an average of four new full authentications per user per day as users rove between wireless APs. The "Peak New Authentications per second" column indicates the type of load expected when all users authenticate over a 30 minute period (for example at the start of the day). The "Re-authentications per second" column shows the number of periodic re-authentications to force the renewal of dynamic WEP keys.

Table 2.2: WLAN Authentication Requirements

Number of WLAN Users	New Authentications per Second	Peak New Authentications per Second	Re–authentications per Second
100	> 0.1	0.1	0.1
1000	0.1	0.6	1.1
10,000	1.4	5.6	11.1

2.

These figures are referred to later in the chapter when discussing IAS server sizing.

WLAN Architecture

This section covers the architecture of the solution.

Network Design

The following figure illustrates the basic network layout for the head office.

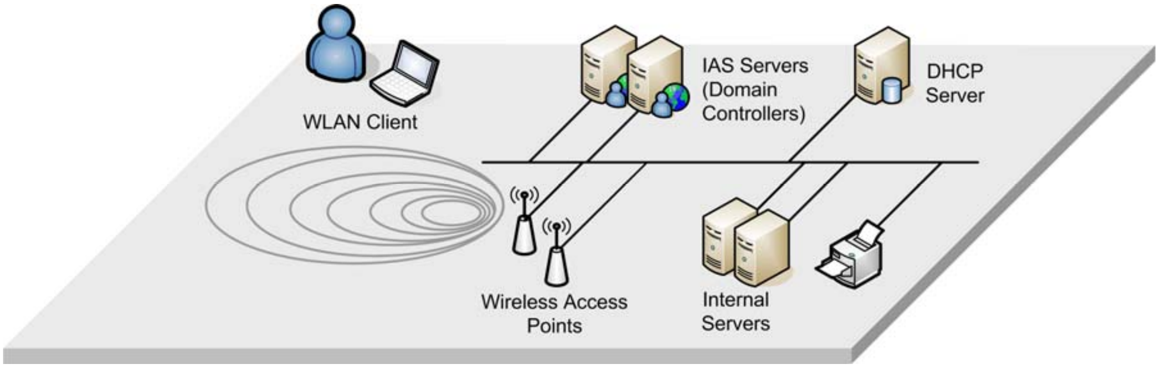

Figure 2.3

c. The network layout for the head office

The figure shows wireless clients, two or more wireless APs, two IAS servers running on Active Directory domain controllers, a DHCP server, and other network connected servers, clients, and devices. With the exception of the WLAN clients, all items are connected on a single LAN using one or more layer 2 switches. A single subnet is used for the entire internal network at this site. There are routed connections (not shown in the figure) through the firewall to the Internet and other offices.

Larger organizations are more likely to have a routed environment within a single site. Although this does not make any difference to the authentication infrastructure, it may have an impact on how the wireless APs are connected to the rest of the network. To make it easier for users to rove between multiple APs across a site, it is a normal practice to place all the wireless APs and WLAN clients on the same IP subnet. This allows users to rove between wireless APs but still keep the same IP address. A detailed discussion of this topic is beyond the scope of this guide. It is covered in more detail in the "Deploying a Wireless LAN" chapter of the *Windows Server 2003 Deployment Kit.*

In your network design, you must ensure the following:

- The wireless APs have connectivity to both primary and secondary IAS servers. If the APs are on a different VLAN/subnet from the IAS servers, traffic must be routable between these subnets.
- The WLAN clients must have connectivity to DHCP servers. If the servers are not on the same subnet, you need to have DHCP/BOOTP relay agents to forward the client DHCP request to a DHCP with a scope defined for that subnet. The clients

will, of course, also need connectivity to their normal network services such as domain controllers, file servers, and so on.

Selection of Wireless Network Hardware

You should ensure that your wireless APs and wireless network adapters support the following:

- 128-bit WEP encryption (if using dynamic WEP) or TKIP encryption (RC4) or AES encryption (if using WPA).
- 802.1X Authentication.
- Dynamic Key Update (WEP encryption only).
- WPA Support (even if you are using dynamic WEP, you should have a clear commitment from vendor to provide firmware update to provide WPA support.)

You should have sufficient wireless APs to provide coverage for WLAN clients across the physical locations that you need to support. You should also plan the wireless AP placement so that there is adequate backup coverage in all locations in case a wireless AP fails. Wireless AP placement is covered in more detail in the "Deploying a Wireless LAN" chapter of the *Windows Server 2003 Deployment Kit,* also listed in the “References” section at the end of this chapter. You should also read the article "Recommendations for IEEE 802.11 Access Points" referenced at the end of this chapter.

IAS Server Placement

The goal of IAS server placement is to achieve a resilient WLAN service while keeping implementation and management costs low. A WLAN service that is resilient to a single component failure has the following characteristics:

- All physical zones where you need WLAN coverage must have two or more wireless APs in range.
- Each wireless AP must be able to communicate with a backup IAS server in the event that its primary IAS server fails or the network connection to this server fails.
- The services on which IAS and the WLAN clients are dependent (for example, Active Directory, DHCP, and DNS) must also provide resilience.

The second of these is the most significant for planning IAS server placement. In this solution, IAS is on existing domain controllers. This provides the highest performance configuration together with relatively low implementation and management costs. As a general recommendation for organizations of all sizes, you should deploy IAS to every site that has a domain controller (although you may not need to install IAS on every domain controller).

The following figure illustrates the placement of IAS servers in the organization. IAS is deployed on two existing domain controllers in the head office. The network CA (refer to the section "Obtaining Certificates for IAS Servers" later in this chapter) is also installed on one of these domain controllers. All APs in the head office are configured to use these IAS servers.

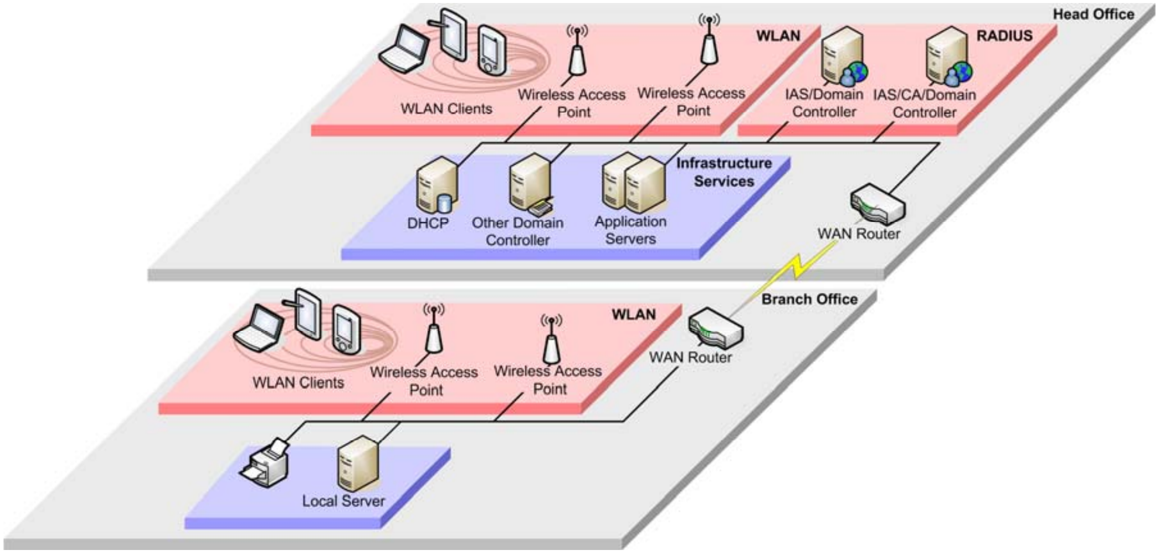

Figure 2.4

d. *The head office and branch office infrastructure*

The organization has a small branch office with no local domain controller. The wireless APs in this site use the two IAS servers in the head office for all authentication requests. This means that users will be unable to authenticate to the WLAN if the WAN connection to head office fails. This may be an unacceptable risk for many organizations.

To resolve this, you should either install redundant WAN connectivity or install a local IAS and domain controller. Although this might seem like an unreasonable cost for this type of office, WAN failure will also cause most other network services to fail (for example, local file servers) without access to a domain controller. Rectifying this will therefore benefit the reliability of these services as well as the local WLAN. Deploying domain controllers to branch offices is discussed in the section "Scaling for Larger Organizations", later in the chapter.

For small offices where WAN connectivity is highly unreliable and deploying a local domain controller is not feasible, you may decide to deploy a standalone WLAN. For more information on this, you should read the section "SOHO Environments" later in the chapter.

Assignment of APs to RADIUS Servers

You must assign all your wireless APs to IAS servers. Each wireless AP requires a primary and a secondary RADIUS server. This allows the wireless AP to use the secondary RADIUS server in the event that the primary server has failed or is not contactable. This arrangement is shown in the following figure.

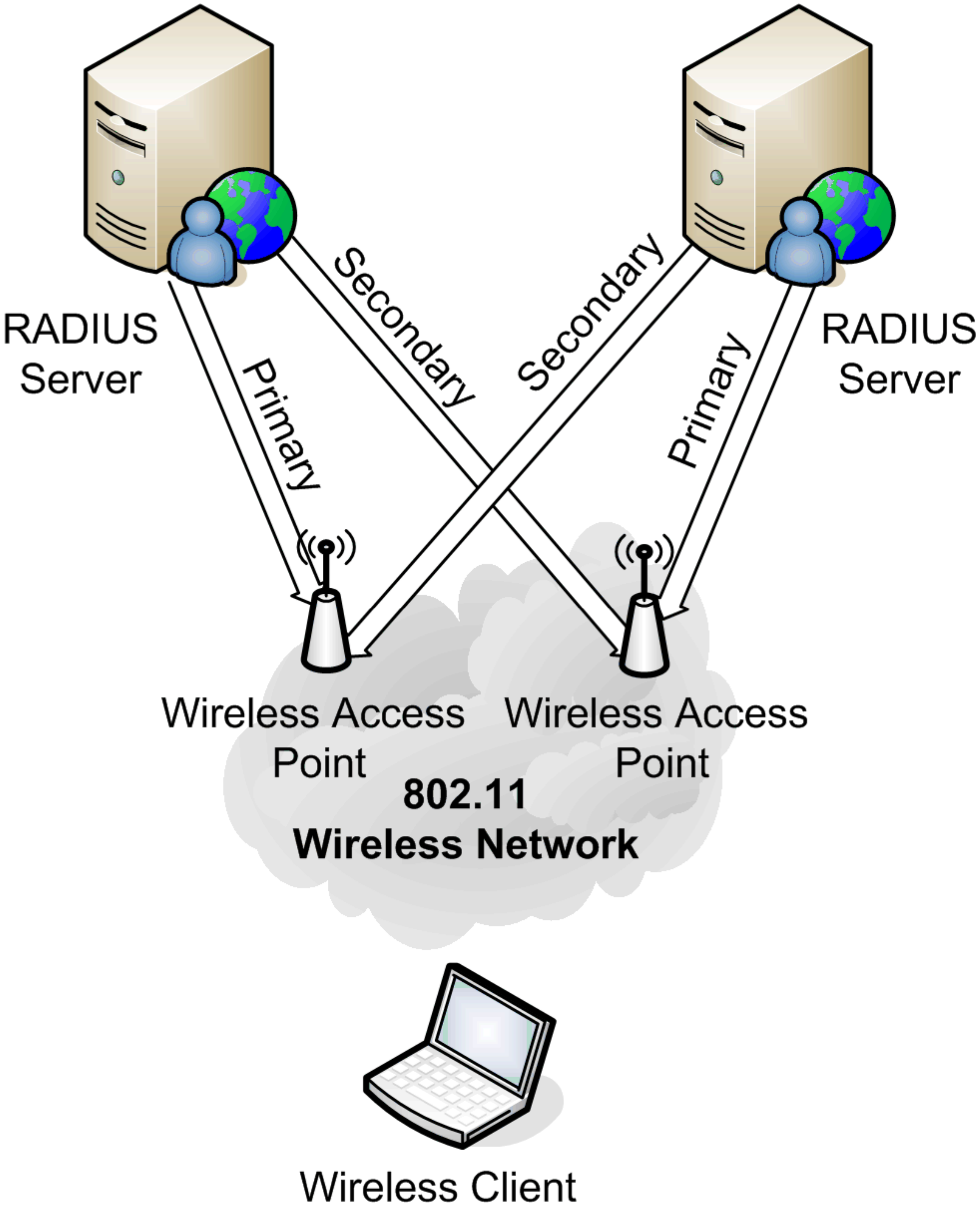

Figure 2.5

e. Balancing AP between primary and secondary IAS servers

The figure shows how each of the wireless APs is configured with different primary and secondary RADIUS servers. This allows load balancing between the servers. Wireless APs in sites with no local IAS server will follow the same pattern using the IAS servers in the head office as primary and secondary RADIUS servers.

For wireless APs in sites with only one local IAS server, the local server should always be the primary server and the server in the head office (or other suitable location where there is reliable connectivity to an IAS server) should be the secondary server. This is illustrated in the following figure.

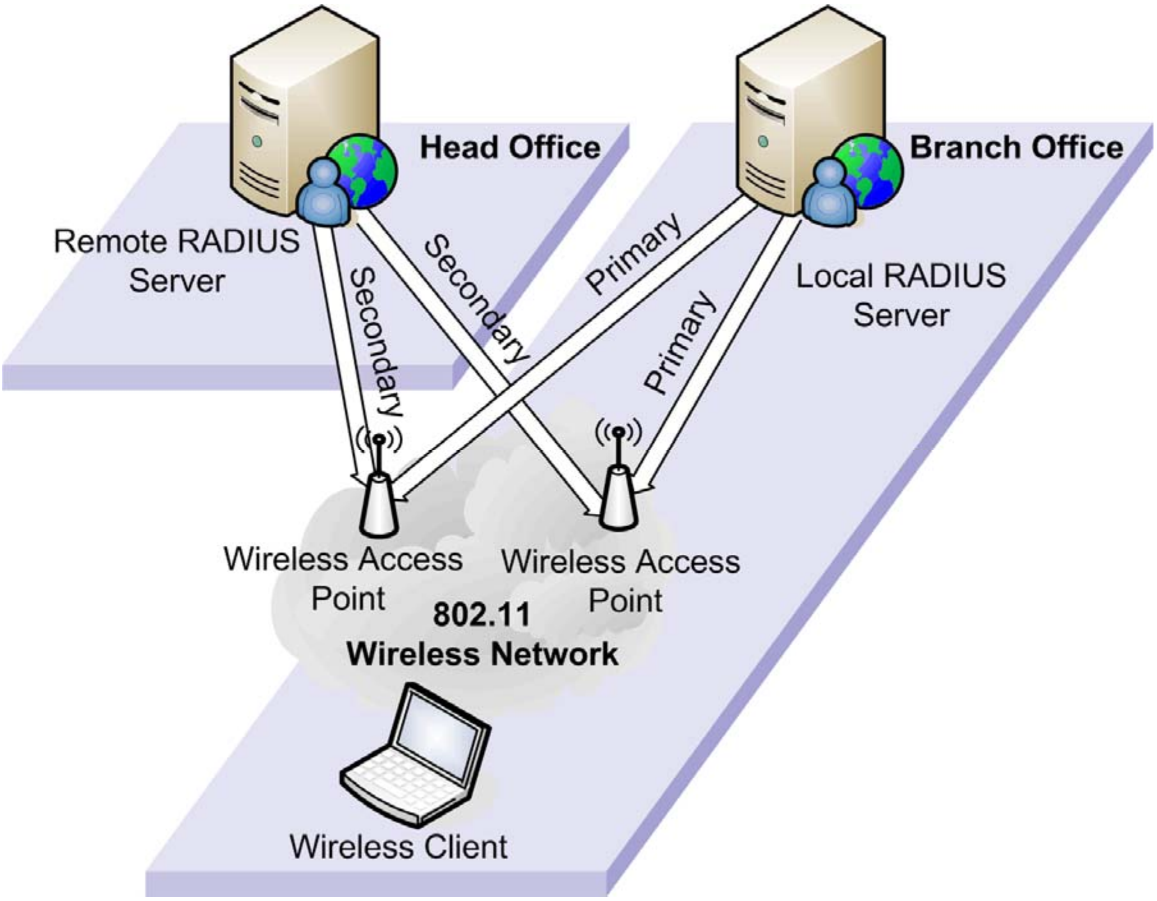

Figure 2.6
f. *Configuring APs to use local and remote IAS servers*

If you have many APs, you should carefully document the assignment of APs to IAS servers. You can use this record to ensure that every AP has been assigned a primary and a secondary server and that the load from APs is evenly balanced across the available servers.

Note: All wireless APs will failover to the secondary IAS server when the primary IAS server is not available. However, most APs do not automatically revert to using the primary when it becomes available again (they will only fall back if the secondary subsequently fails). This is not a major problem where both IAS servers are at the same location; it will simply make load across the servers uneven. However, where the secondary IAS is remote, a temporary failure of the primary may leave all APs authenticating to the secondary over a non–optimal WAN link.

If your APs do not automatically revert to their designated primary server, you may need to manually reset the APs so that they start using the local IAS server when it recovers after a failure. Transient network conditions can also cause APs to failover to their secondary RADIUS servers, so you may need to occasionally check the authentication request events in the IAS server application logs to spot any APs using the wrong IAS.

Co-location of IAS with Domain Controllers

In this solution, IAS is installed on existing domain controllers. This keeps the costs of implementation low and gives a performance improvement over using IAS on a separate member server. The performance gain occurs because IAS can communicate with the Active Directory on the same computer without incurring any network delay.

You should be aware of some caveats of installing IAS on domain controllers. While these will not be of concern to many organizations, you may want to consider them before proceeding:

- You will not be able to have a single configuration for all of your domain controllers unless, of course, you opt to install IAS on all domain controllers.
- You will not be able to enforce separation between IAS administration and domain administration. Installing IAS on domain controllers means that the IAS Administrators need to be members of the built-in domain Administrators group as well.
- High load on the domain controller functions will adversely affect the performance of IAS and vice versa. You may want to put these on separate servers to have more control over their individual performance and operation of these services.

IAS Software and Hardware Requirements

For a target organization of 100 to 200 users, it is unlikely that IAS load on servers will ever be an issue as long as you are using the recommended hardware specification for Windows Server 2003. However, for larger organizations, this may be a consideration, particularly if they are running IAS on existing domain controllers.

The load on the IAS will be affected by:

- Number of users and devices requiring RADIUS authentication.
- Choice of authentication options such as EAP type and the re-authentication frequency.
- Whether RADIUS logging is enabled.

You can use the figures given in table 2.2, in earlier "Design Criteria" section, to estimate the number of authentications per second that you can expect from a given user population. You should consider the steady state load when users are authenticating normally and the 'worst case' load during peak times. Extrapolating the figures from this table, 200 users generate a steady state load of less than one full authentication every 50 seconds and one fast re–authentication every ten seconds. These are such small numbers that the only really significant figure is how long it takes to authenticate all users following an outage — when all users need to connect back to the WLAN immediately. This is a much more extreme peak than the start-of-day logon, which will tend to spread over 30 minutes or more.

Authentication options have a significant effect on IAS server load. Protocols such as PEAP perform a CPU–intensive public key operation upon initial log on; although for subsequent re-authentications, cached session information is used, allowing what is known as a "fast reconnect". If you are using dynamic WEP, the clients will re-authenticate every 15–60 minutes to generate new encryption keys. However, with WPA you need to enforce re-authentication much less frequently, typically every 8 hours.

The following table shows the approximate number of authentications per second for IAS on an Intel Pentium 4 2 GHz server running Windows Server 2003 with Active Directory on a separate server.

Note: The information in the following table was derived from tests done by Microsoft Solutions for Security. It is provided without warranty of any kind and should only be used as a guideline for capacity planning purposes and not for performance comparisons.

Table 2.3: Authentications per Second

Authentication Type	New Authentications	Fast Reconnect Authentications
PEAP authentications per second	**36**	**166**
Time to authenticate 200 users	**6 sec**	**2 sec**
Time to authenticate 1000 users	**30 sec**	**7 sec**

3.

These figures were calculated with RADIUS logging enabled and with Active Directory running on a separate server; both of these factors reduce the performance of IAS, so these figures can be considered a pessimistic estimate.

As these figures show, this type of server will allow 200 WLAN users to authenticate to the network in six seconds and 1000 users in 30 seconds.

Using Windows Server Standard or Enterprise Edition

This solution uses Windows Server 2003, Standard Edition for all IAS servers; this keeps the cost of server licenses low and allows you to deploy on existing servers whether they be Standard or Enterprise Edition.

IAS in Windows Server 2003, Standard Edition has the limitations that each server can support only 50 RADIUS clients and two RADIUS server routing groups.

Note: RADIUS clients are not the same as WLAN clients. RADIUS client refers to wireless APs and also other network access servers, such as VPN servers and firewalls that make use of RADIUS authentication services.

For the target organization of 1 to 200 users, a maximum of 50 APs per server is more than sufficient. For larger organizations this limit may be significant particularly for large offices, or where many satellite offices feed into one or two hub IAS servers.

Assuming 15 users per wireless AP, this means that a single IAS server on Windows Server 2003, Standard Edition could support approximately 750 users. This calculation takes into account the total number of APs that will use a server as a primary or a secondary RADIUS server; therefore, two servers will support 50 APs and not 100. If any of your IAS servers need to support more than 50 APs, you need to use Windows Server 2003, Enterprise Edition. You can, of course, also mix and match the two editions by using Windows Server 2003, Enterprise Edition for large offices and hub offices, and Windows Server 2003, Standard Edition for smaller offices.

IAS Configuration

IAS settings can be broken down into four major categories:

- IAS Server settings
- RADIUS Logging configuration
- Remote Access Policies
- Connection Request Policies

These categories are described in detail in the following subsections. All these settings are common to all of the IAS servers used in this solution; this allows the settings to be configured on one IAS server and copied to the others. This technique is used in Chapter 5, “Building the WLAN Security Infrastructure” to ensure that the IAS settings are consistent between all servers in your organization.

In addition, each IAS server will also have one or more wireless APs configured as RADIUS clients. RADIUS clients were described in the earlier section "Assignment of APs to RADIUS Servers". The set of RADIUS clients is usually different for each server and therefore they are not replicated between the servers in the same way as the other settings.

IAS Server Settings

This category includes:

- Logging of authentication requests to the Windows event log. Logging of both successes and failures is enabled in this solution.

> **Note:** Request logging is covered in the "RADIUS Logging" section later in this chapter.

- The User Datagram Protocol (UDP) ports that the IAS server listens on for RADIUS authentication and accounting requests. This solution uses the default RADIUS ports 1812 and 1813 for authentication and accounting, respectively.

RADIUS Policies

IAS policies control the authentication and authorization of accounts to the network. There are two types of policies:

- Remote Access Policy (RAP).
- Connection Request Policy (CRP).

The RAP controls how or whether a connection is authorized to the network. A RAP contains a set of filter conditions that determine whether that policy applies to a given connection request. Some examples of filter conditions are: specifying the Windows security group of which a client must be a member, specifying the connection type (such as Wireless or VPN) of the requesting client, and specifying the time of day that the client is attempting to connect. Each RAP has a policy action, which is set either to *allow* or *deny* a connection request. Connection requests matching the RAP condition filter will be allowed or denied access to the network according to the policy action setting.

A RAP also contains a set of parameters that apply to an allowed connection, known as the RAP profile. These parameters include the authentication methods that are acceptable for this connection, how an IP address will be assigned to the client, and the amount time for which the client can remain connected before re–authentication is required. There can be multiple RAPs on an IAS; each connection request is evaluated against them (in order of priority) until a matching RAP either allows or denies the request.

The RAP in this solution is configured as shown in the following table.

Table 2.4: Remote Access Policy Configuration

Configuration Item	Setting
Policy Name	**Allow Wireless LAN Access**
Policy Type	**Allow**

Configuration Item	Setting
RAP Conditions	
NAS-Port-Type matches	**IEEE 802.11 Wireless** **Other Wireless**
Windows Group matches	**Wireless LAN Access**
RAP Profile	
Dial-in constraints — Client Timeout	**60 minutes (dynamic WEP)** **8 hours (WPA)**
IP Address assignment	**Server settings determine IP assignment**
IP Filtering	**None**
Authentication	**All disabled apart from EAP**
Authentication—EAP Type used	**Protected EAP (PEAP)**
Authentication—PEAP EAP type used	**EAP MS-CHAP v2**
Authentication—Fast Reconnect	**Enabled**
RADIUS Attributes	**Ignore-User-Dialin-Properties = "True"** **Termination Action = "RADIUS-Request"**

4.

The condition filter matches all wireless clients and all members of the domain group Wireless LAN Access. Parameters that are not relevant to WLAN access, such as Multilink and Microsoft Point-to-Point Encryption (MPPE) encryption settings, are not included in the table. For more details on the use of security groups with the RAP, refer to the “WLAN User and Computer Administration Model” section later in this chapter.

The Dial-in constraints—Client Timeout setting can have an impact on the security and the reliability of the solution. Reasons for using different values to those given in the table are discussed in the "Security Options for Dynamic WEP" section later in the chapter.

The RADIUS attribute "Ignore-User-Dialin-Properties" is used to bypass per user control of network access permissions. See the "WLAN User and Computer Administration Model" section for an explanation of per user and per group access control.

A connection request policy controls whether to process the request at a particular RADIUS server or send it to another RADIUS server (called RADIUS proxy). RADIUS proxies are typically used where the RADIUS server does not have the information to process the request itself and must forward it to an authoritative RADIUS server, for example, to a server in another Active Directory forest. RADIUS proxies are not used in this solution and are outside the scope of this guide.

For more information about remote access and connection request policies, and the use of RADIUS proxies, see the "References" section at the end of the chapter.

RADIUS Logging

You can configure IAS servers to log two types of optional information:

- Successful and rejected authentication events.
- RADIUS authentication and accounting information.

Successful and rejected authentication events generated from WLAN devices and users can be recorded in the Windows Server 2003 System Event Log on the IAS server. Authentication Event Log information is most useful for troubleshooting authentication issues, although this information may also be used for security auditing and alerting purposes.

Initially, you should keep success and reject event logging enabled but you may consider disabling success events once the system has stabilized. Successful WLAN access events will bloat the System Event Log but may be needed for audit purposes.

If you use a monitoring and alerting tool such as Microsoft Operations Managager (MOM), you should consider adding a rule to alert on IAS authentication failure events in the System Event Log. Alternatively, you could use an event log query tool such as eventquery.vbs to check the event log for authentication failures (see the "Eventquery.vbs" entry in the online help). Single events are usually insignificant but a series of such events can indicate an attempted break-in.

IAS also has the ability to record authentication and network access session information in the form of RADIUS request logs. You normally use RADIUS logging either when you need to charge for network usage (for example, as an Internet service provider (ISP), you need to charge based on connection time) or where you need specialized security audit information (although, for most purposes this is already covered by the authentication events logged to the event log).

For more information on RADIUS logging, refer to the ”References” section at the end of the chapter.

IAS Security

You should treat IAS with similar security precautions as you use with a domain controller. Secure control of your network is dependent on the security of your IAS infrastructure. There are several simple measures, which you can implement to improve the security of IAS:

- Use strong passwords for your RADIUS clients (wireless APs). The solution includes scripts to generate true random passwords to make dictionary attacks difficult.
- Enable RADIUS Message Authenticator for all RADIUS clients to prevent the IP addresses of wireless APs from being spoofed. It is enabled in this solution.
- Ensure that your server security settings are appropriate. This is covered in Chapter 3, “Preparing Your Environment.”
- Ensure that your servers are patched with the latest security hotfixes and that you maintain up-to-date patches on an ongoing basis. This is also covered in Chapter 3, “Preparing Your Environment.”
- Ensure that you are using strong domain account settings. In particular, you should ensure that strong passwords and regular password changes are enforced. You may also consider enabling domain account lockout to block password guessing attacks. However, you should only enable account lockout if you have the support resources to unlock accounts for users in a timely fashion.
- Consider using IPSec to secure the RADIUS traffic and strengthen mutual authentication between your wireless APs and IAS servers. However, not all wireless APs support the use of IPSec for this.

For more information on IAS security measures, see the “References” section at the end of this chapter.

WLAN User and Computer Administration Model

Access to the WLAN in this solution is controlled using domain security groups. Although it is possible to use the dial–in properties of domain user objects to allow and deny access to individuals, this is tedious to administer for many users.

This solution uses a very simple scheme of allowing all domain users and computers access to the WLAN. For many organizations, controlling access through domain membership is a strong enough control and minimizes additional management overhead associated with the WLAN. However, to give more control to organizations that require it, security groups can be used to define who is allowed to access the WLAN.

As described in the section "RADIUS Policies," the IAS remote access policy uses a filter condition that grants WLAN access to all members of the Wireless LAN Access group. The following table shows the membership of the Wireless LAN Access group.

Table 2.5: Wireless Access Groups to Allow All Users and Computers

Top Level Universal Group (Granted Access in RAP)	First Level Members (Domain Global Groups)	Second Level Members (Domain Global Groups)
Wireless LAN Access	Wireless LAN Users	Domain Users
	Wireless LAN Computers	Domain Computers

5.

The group in the first column, Wireless LAN Access, has two members listed in the second column namely, Wireless LAN Users and Wireless LAN Computers. These "First Level" groups themselves have members (shown in the third column — Second Level Members") namely, the Domain Users and Domain Computers groups respectively. This arrangement of nested groups allows all users and computers in the domain to connect to the WLAN.

If allowing all users and computers to access the WLAN is overly permissive for your organization, you can remove either or both Domain Users and Domain Computers from these groups. You will then need to add the specific user and computer accounts or groups to the Wireless LAN groups. The following table illustrates how to use the Wireless LAN Access group structure in this manner.

Table 2.6: Wireless Access Groups to Allow Selected Users and Computers

Top Level Universal Group (Granted Access in RAP)	First Level Members (Domain Global Groups)	Second Level Members (Domain Global Groups)
Wireless LAN Access	Wireless LAN Users	User1 User2 User3
	Wireless LAN Computers	Computer1 Computer2 Computer3

6.

For more information on the use of these security groups in a multidomain forest, refer to the "Scaling for Larger Organizations" section later in this chapter.

Obtaining Certificates for IAS Servers

The IAS servers need to have certificates to authenticate the WLAN clients. Server certificates are required to create the TLS encrypted tunnel between IAS servers and clients. TLS helps protect the authentication exchange between the server and clients.

Note: TLS is an RFC standard based on the similar Secure Sockets Layer version 3.0 (SSL 3.0). Both are commonly used to secure Web traffic as part of the Hypertext Transfer Protocol, Secure (HTTPS).

Embedded CA vs. Commercial CA

To provide these certificates, you have the choice to either install a CA yourself or buy the certificates from a commercial certificate provider. Both options are valid and choosing one over the other creates no real technical difference to the WLAN solution.

The major pros and cons to using in–house CA compared to buying certificates from a commercial provider are summarized in the following table.

Table 2.7: Pros and Cons of Using Your Own CA vs. Commercial Certificates

In-house CA	Commercial CA
No per certificate cost	**Per certificate cost**
CA software to be installed and managed	**No server software**
Automatic enrollment and renewal	**More complex enrollment process, manual installation of certificates**

7.

The balance of the argument depends on how complex and costly it is to manage your own CA. If the cost of setting up a local CA is low and the management is simple, it is often a more attractive proposition than purchasing external certificates.

This solution uses a simple internal CA to provide the certificates. The terms "embedded CA" and "network CA" have been used in this guide to indicate that it is a special purpose CA, which is essentially invisible to users and administrators and which issues certificates of a single type. The limited functionality of the CA in this solution means that it can be installed and used with little or no user or management intervention. For example, in this solution, the CA can issue a certificate with a lifetime of 25 years; therefore, you will not have to renew it during the lifetime of the solution. Automatic enrollment and renewal of the IAS server certificates means that there is no manual certificate distribution to perform.

Contrast this with using external certificates. You must remember to renew the certificates of all IAS servers every year or two years. Each time you have to manually create the certificate request on each IAS server, send the request to the commercial CA then retrieve and manually install the issued certificate. Failure to do this will prevent users from connecting the WLAN. For many organizations the management overhead of this is far more onerous than the simple internal CA described used in this solution.

Limitations of the Solution CA

This solution uses a special CA configuration to issue certificates to the IAS servers. It was only designed to meet this specific need and is not suitable as a general purpose certification authority.

Digital certificates are used in many applications, such as secure e-mail and Web browsing, IP Security (IPSec), Virtual Private Networks (VPN), Encrypting File System (EFS), and others. Each of these applications has its own security requirements. Your organization will have its own unique security requirements with respect to these applications. For these reasons, Microsoft strongly recommends not attempting to use the solution CA for any other purpose.

If you plan to use these or other certificate applications, design your certificate infrastructure around their requirements. Things that you need to consider include:

- The solution CA is a self-signed root CA, so you cannot revoke it (you have to revoke the issued certificates in the case of CA compromise).
- Industry or country-specific regulations may require you to use a multitier CA hierarchy for some or all certificate types.
- Microsoft does not recommend installing a CA on a domain controller for high-security certificate uses.

For more information about the detailed planning required to design a more generic PKI architecture, see Chapter 4, "Designing the Public Key Infrastructure," in the companion solution, *Securing Wireless LANs—A Certificate Services Solution*.

You should also keep in mind that there are a number of constraints due to the CA being installed on the Standard Edition of Windows Server 2003. Although adequate for this solution, the Standard Edition supports a limited set of functionality compared to Windows Server 2003, Enterprise Edition. The salient features that are not available in Windows Server 2003, Enterprise Edition include:

- **Autoenrollment of certificates to both computers and users:** The Automatic Certificate Request Service (as used in Windows 2000 Server and Windows Server 2003, Standard Edition) only supports automatic enrollment of computer certificates. User certificates cannot be enrolled automatically.
- **Version 2 certificate templates:** Many certificate types used by Windows Server 2003 and Windows XP use the advanced features of version 2 templates. However, a CA based on Windows Server 2003, Standard Edition cannot issue certificates in version 2 templates.
- **Editable certificate templates:** Version 1 templates cannot be modified or created to produce new certificate types.
- **Archival of keys is not supported**.

If you require any of these features, you need a CA based on the more advanced capabilities of Windows Server 2003, Enterprise Edition. For a detailed description of the differences between Enterprise and Standard Edition, see the paper titled "PKI Enhancements in Windows XP Professional and Windows Server 2003" listed in the “References” section at the end of the chapter.

If you do not have clear requirements for other types of certificates at present, however, you can deploy the CA described in this solution without closing your options in the future. At a later stage, if you identify other requirements for certificates, you can deploy a more sophisticated PKI alongside this solution. You are then free to either run them side by side or migrate to issuing all certificates from the new PKI.

WLAN Clients

The WLAN solution supports several, different types of WLAN client either explicitly or implicitly. This solution supports Windows XP, Professional Edition, Windows XP, Tablet Edition, and Pocket PC 2003 clients. For specific guidance on how to configure and use these clients with the solution, refer to chapter 6, “Configuring the WLAN Clients”. The guide does not cover using other types of clients that support 802.1X with PEAP-MS-CHAP v2. Although some other types of clients will work (Windows 2000 Professional, for example), this guide has no instructions on how to configure them and the Microsoft Solutions for Security team has not tested them with this solution.

Windows XP

Windows XP, Professional Edition and Windows XP, Tablet Edition are fully supported in this solution. All Windows XP clients must be updated with Service Pack 1 or later. The computers must be members of the same domain as the IAS servers or members of another domain within the same forest. Domain membership is required so that the computers can authenticate themselves to the WLAN and can download the WLAN settings specified in Group Policy.

Computer authentication to the WLAN is used when no user is logged on to the computer. This allows the computer to obtain Group Policy object (GPO) settings, run startup scripts, and have patches downloaded to it. It is also required during the initial stages of user log on. The user cannot start to authenticate to the WLAN until after the user profile is loaded; therefore log on scripts, other GPO settings, and roaming profiles will fail if the computer does not have an existing connection to the network before the user logs on.

Windows XP computers that are not domain members may still be used with the solution, with the following caveats:

- You will have to configure the WLAN client settings manually.
- Computer authentication to the WLAN is difficult to achieve.
- User authentication to the WLAN requires a separate user name and password prompt into which the user must type their domain (WLAN) credentials.

Microsoft also strongly recommends enabling the personal firewall on all client computers using wireless.

Pocket PC 2003

Pocket PC 2003 supports 802.1X and PEAP, however, you may have to obtain updates from the vendor of your device and Microsoft to get full WLAN functionality. It is also possible to use versions of Pocket PC earlier than 2003 but Microsoft did not provide built-in support for 802.1X for earlier versions. You may be able to obtain specific support from your Pocket PC device vendor or use WLAN client software from a third party.

Pocket PC systems have no concept of a computer domain account and are always authenticated to the WLAN using user credentials. Normally a connection to the WLAN will require a user to type their domain user name and password each time. It is possible to save the credentials so that the device connects automatically but this is not recommended unless you have very strong security features on the Pocket PC device.

In addition, Pocket PCs do not understand Group Policy so their WLAN settings cannot be set automatically using this. You have to set the WLAN configuration manually.

Other 802.1X Clients

Clients other than Windows XP and Pocket PC 2003 may work with this solution if they support 802.1X and PEAP-MS-CHAP v2. Windows 2000 clients are supported using the Windows 2000 Microsoft 802.1X Authentication Client. Details on how to obtain the Windows 2000 Microsoft 802.1X Authentication Client are included in the references at the end of this chapter. Windows clients other than Windows 2000 (such as Windows® NT 4.0, Windows 9*x* and Windows® Me) are supported with a client available through Microsoft Premier Support. You may also be able to obtain client for these and other platforms from non−Microsoft network software vendors.

You should also consult Appendix C, "Supported Windows Versions."

WPA Support

The WLAN solution described here supports the use of WPA WLAN protection in place of dynamic WEP. WPA is always preferred over WEP because it provides better key management and implements a stronger network encryption algorithm. WPA also supports the use of AES encryption, if the hardware (wireless APs and network adapters) provide the necessary support.

Although WPA provides a number of advantages over dynamically keyed, there are some caveats over its use. These include:

- GPO support for configuring WPA settings on WLAN clients will not be available until Windows Server 2003 Service Pack 1.
- Client support for systems other than Windows XP may not be available. Although Microsoft is likely to provide WPA support for Pocket PC 2003, Windows 2000 and other Microsoft clients may not be supported (non-Microsoft vendors may provide WPA support for these clients).
- It may not be possible to upgrade the existing WLAN equipment (wireless APs and client network adapters) to support WPA. The cost of buying and deploying new hardware may also be prohibitive.

GPO and Pocket PC 2003 support for WPA will appear soon, making WPA the option of choice. Until then, dynamic WEP coupled with 802.1X authentication continues to provide a very high level of protection for WLANs and is the default choice for this solution. For more information on WPA, see the “References” section at the end of this chapter.

Migration from an Existing WLAN

If you have an existing wireless network in place, you should plan a migration strategy upfront to ensure minimal disruption to users and the environment.

Many organizations have 802.11–based WLANs operating without network authentication or encryption. Other organizations have implemented static WEP using shared key encryption often combined with Media Access Control (MAC) address filtering.

The process of migrating from either of these scenarios to an 802.1X secured WLAN involves the following steps:

1. **Deploy certificates to IAS Servers:** For details on how to deploy certificates to an IAS server, refer to chapter 4, “Building a Certification Authority”, of this guidance.
2. **Configure the wireless network remote access policies on the IAS servers:** Steps for configuring a wireless remote access policy are described in Chapter 5, “Building the WLAN Security Infrastructure”, of this guidance.
3. **Deploy a WLAN configuration for the new WLAN to client computers:** The new 802.1X−enabled network needs a new network Service Set Identifier (SSID). The network settings for the new WLAN can then be deployed by Active Directory GPO. WLAN group policy should be deployed well in advance of wireless AP reconfiguration to ensure that mobile computers with only occasional LAN access receive the configuration. This is described in Chapter 6, “Configuring WLAN Clients.”
4. **Configuration of wireless APs to require 802.1X security:** This is usually best done site by site, (for example, by building or campus) and it is either performed out of hours or with adequate warning to users about possible WLAN outage. You should create RADIUS client entries for the IAS for all APs on the site, configure the APs with the addresses of the IAS servers for the AP's RADIUS entries, and finally, switch the AP over to allow only 802.1X authenticated clients. To facilitate

rollback, you may want to back up the wireless AP settings before starting this step, so that they can be restored in an emergency.

This type of rollout minimizes the disruption to users and allows you to rollback a site easily, if anything goes wrong. There will inevitably be some problems experienced by users during the switch over, so you should keep the users informed about the migration and be prepared to handle more support calls than normal.

As with all migration strategies, careful planning and testing is essential. The steps involved in configuring client computers and wireless APs can cause disruption to the environment if they are not tested thoroughly to iron out nascent problems.

Detailed planning of migration from unsecured and static WEP WLANs or from proprietary WLAN security schemes are not included in this guidance. All these are similar in principle and follow the pattern above. However, if you require more assistance with your migration planning, see your Microsoft partner or contact your local Microsoft subsidiary who will put you in touch either with a Microsoft partner in your area or with Microsoft Consulting Services.

Scaling for Larger Organizations

This section describes some of the key considerations for using this solution in a large organization (one with several thousand users, for example). The use of PEAP and password authentication in the enterprise is detailed in Appendix A, “Using PEAP in the Enterprise.”

IAS Server Placement

As you increase the number of locations where you support WLANs, you need to decide how these wireless APs will be serviced by IAS servers. There are essentially two approaches:

- **Use a small number of central IAS servers:** Use a small number of central IAS servers to handle all WLAN authentication traffic (two are likely to be sufficient). You need to ensure that the WAN connections between your outlying offices and the IAS servers are resilient.
- **Distribute IAS servers to each office:** There is a lower limit to the size of an office where this makes economic sense but, as a rule of thumb, any office that is large enough to have its own domain controller can have IAS locally (usually installed on the domain controller).

Although the investment in network resilience may seem an expensive option, you need to weigh this against the administration cost of managing many distributed IAS servers. Even if IAS is installed on the same physical server as an existing domain controller there will be some cost of managing each IAS instance. In practice, most large organizations will use a hybrid of the two in the following ways:

- Centralize IAS servers and invest in WAN resilience wherever possible.
- Distribute IAS to offices where WAN resilience is not achievable or is prohibitively expensive.
- Use pre–shared key (PSK) WPA WLANs for very small offices with poor connectivity or for employees’ home offices.

The centralized IAS strategy was illustrated in the "IAS Server Placement" section, earlier in this chapter. The use of a local domain controller and IAS in a branch office is shown in the following figure. This shows a larger outlying office that is linked by a WAN to the Head Office shown in the figure 2.4 earlier.

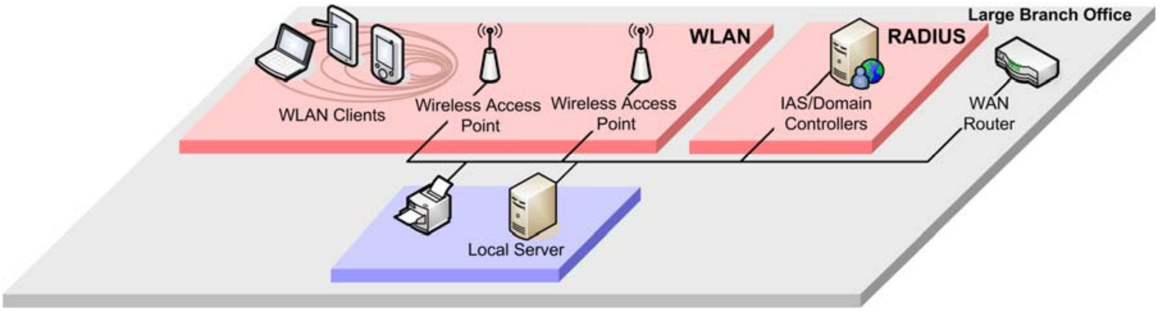

Figure 2.7

g. Larger branch office with local domain controller and IAS

In this site, the APs are configured to use their local IAS server as the primary RADIUS server and one of the IAS servers in head office as the secondary RADIUS server. This means that WLAN clients can be authenticated, even if the local IAS server or WAN connectivity fails.

However, if you have resilient WAN connectivity (for example, multiple WAN links with different providers), there is little to be gained by deploying additional servers at branch offices; it only adds complexity and additional management overhead.

Multiple Domains

The basic solution design scales transparently to multi–domain forests. The key points to consider while using the solution with multiple domains are as follows:

- IAS servers must be registered in each domain that has users or computers that will be accessing the WLAN. For details, refer to Chapter 5, “Building the WLAN Security Infrastructure.”
- The GPOs for server settings and automatic certificate request settings must be imported into every domain in which IAS servers are installed. The steps to do this are detailed in Chapter 3, “Preparing Your Environment” and Chapter 4, “Building a Certification Authority.”
- The GPO that controls client computer WLAN settings must be created in each domain where there are client computers that will access the WLAN. For more details on this, refer to Chapter 6, “Configuring WLAN Clients.”
- The security groups used by IAS to filter remote access policies need to be configured to support multiple domains.

The first three items are mostly self-explanatory and the steps for configuring these for multiple domains are covered in later chapters. The use of the security groups is slightly more complex and is covered in detail in the following section.

Use of Security Groups in Multiple Domains

The following table shows how you can organize the security groups described in the "WLAN User and Computer Administration Model" section in a multidomain forest.

Table 2.8: Wireless Access Groups to Allow All Users and Computers

Top Level Universal Group (Granted Access in RAP)	First Level Members (Domain Global Groups)	Second Level Members (Domain Global Groups)
RootDom\Wireless LAN Access	UserDom1\Wireless LAN Users	UserDom1\Domain Users
	UserDom2\Wireless LAN Users	UserDom2\Domain Users
	UserDom3\Wireless LAN Users	UserDom3\User1 UserDom3\User2 UserDom3\User2
	UserDom1\Wireless LAN Computers	UserDom1\Domain Computers
	UserDom2\Wireless LAN Computers	UserDom2\Domain Computers
	UserDom3\Wireless LAN Computers	UserDom3\HR Computers UserDom3\Finance Computers

8.

The table shows the same group nesting arrangement as the tables in the "WLAN User and Computer Administration Model" section. The members of the group listed in the first column are shown in the second column; the members of the groups listed in the second column are shown in the third column.

The example in the table uses fictitious names. For example, RootDom is the name of the domain where IAS servers are installed and UserDom1 and UserDom2 are other domains containing users and computers to be granted WLAN access.

In the example shown, all users and computers from UserDom1 and UserDom2 are implicitly granted access to the WLAN because the Domain Users and Domain Computers groups from those domains are members of the Wireless LAN Users and Wireless LAN Computers groups for the same domain. However, the users from UserDom3 are individually added to the Wireless LAN Users group of UserDom3. The computers are granted access by using business unit security groups (for example, all computers in the HR department).

The global groups for each domain, namely, Wireless LAN Users and Wireless LAN Computers, are then added as members of the universal group Wireless LAN Access. All members of this latter group are granted access to the WLAN in the IAS remote access policy.

PKI Architecture

As mentioned in the earlier section "Obtaining Certificates for IAS Servers," many applications can utilize certificates. It is important to note that while appropriate for this solution, a standalone CA is unlikely to meet the more varied needs of larger organizations. Before implementing the CA described in this guidance, ensure to carefully consider other uses for certificates that you might have in the future, as well as alternate PKI architectures more appropriate for these scenarios.

To read about PKI planning in more detail, refer to Chapter 4, "Designing the Public Key Infrastructure" in the companion solution, *Securing Wireless LANs—A Certificate Services Solution*. Although more sophisticated than the CA in this guide, the PKI discussed in that solution is still relatively simple: it uses only two CAs, for example. However, it is designed to be a foundation for a much broader range of certificate needs.

If you decide against implementing a more sophisticated PKI such as this, you can still use the guidance given in Chapter 4 of this guide, “Building a Certification Authority.” However, you should consider making the following changes to the instructions provided in that chapter:

- Install the CA on its own server instead of installing on a domain controller.
- Use Windows Server 2003, Enterprise Edition, to give you more flexibility in the future.
- Instead of using the automatic certificate request service, use Windows Server 2003 autoenrollment. For instructions on how to use autoenrollment, see the product documentation for Windows Server 2003 Enterprise Edition.
- Use the "RAS and IAS Server" certificate template or create a customer certificate type for the IAS server certificates instead of using the "Computer" template.

Note: "RAS" in the certificate template name stands for Remote Access Service.

Guidance for how to do these is given in the “Public Key Infrastructure” section of the Windows Server 2003 product documentation and in Chapter 4, "Designing the Public Key Infrastructure," Chapter 7, "Building the Public Key Infrastructure," and Chapter 9 "Implementing Wireless LAN Security" in the companion solution, *Securing Wireless LANs—A Certificate Services Solution*.

Variations on the Solution Architecture

This section discusses variations to the core design. The following subsections look at alternatives to the default security settings of the solution, using the IAS servers for wired and remote access authentication, creating guest WLANs for visitors and deploying WLANs to very small environments such as home offices.

Security Options for Dynamic WEP

The "How 802.1X with PEAP and Passwords Works" section earlier in this chapter discussed the use of dynamic WEP encryption in the solution. The security of dynamic WEP relies on its ability to renew the encryption keys at regular intervals to thwart known attacks on the WEP protocol. IAS ensures that the keys for each wireless client are renewed at a set interval by using a client session time-out, which forces the client to re-authenticate to the WLAN.

Reducing the session time-out value increases security but may reduce reliability and performance. A 60 minute time-out gives adequate security for most circumstances and certainly for 11 Mbps 802.11b networks. Normally, wireless clients will never transmit enough data in 60 minutes to allow a WEP key to be recovered by an attacker.

The latest research indicates that static WEP keys can be recovered by capturing between 1 and 5 million network packets encrypted with the same key. This is documented in the technical paper “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP” by Adam Stubblefield, John Ioannidis and Aviel D. Rubin of AT&T Labs—see the reference at the end of this chapter).

Note: The figure of 1 million packets was obtained from testing static WEP WLANs using relatively weak keys (a "user–memorable passphrase") and is not directly applicable to dynamic WEP WLANs. Unlike typical static WEP WLANs, dynamic WEP uses strong random encryption keys and renders one of the key optimizations used by the authors much less effective. Nevertheless, it is good security habit to err on the side of caution and use the pessimistic figure of 1 million packets to assess the security threat to dynamic WEP WLANs.

One million packets typically equates to around 500 MB of data (assuming an average packet size of 500 bytes). For the encrypted data to be secure, the session time-out needs to be set so that it forces each client's key to be renewed before the client sends more than this amount of data.

For typical client network usage, such as e-mail, Web browsing, and file sharing, average data transfer rates are 160 Kbps or less. At this transfer rate, assuming 500 bytes packet size, it would take approximately 7 hours for an attacker to accumulate enough data to recover the client’s current encryption key.

Note: In laboratory conditions, 500 Mb could be transmitted in much less than 7 hours; around 10 minutes on a11 Mbps WLAN or less than 3 minutes on a 54 Mbps WLAN. However, this assumes a single client having exclusive use of the WLAN and streaming unacknowledged UDP packets in one direction. This scenario, or anything near it, is extremely unlikely for a real world WLAN.

A 60 minute session time-out is more than adequate for most organizations. This means that an average client would transmit around 150,000 packets before each key refresh; nearly an order of magnitude less than the 1 million packet threshold required for WEP key cracking. However, you may want to use a shorter time-out value for one or more of the following reasons:

- If you have wireless clients that send or receive large amounts of data over the WLAN in relatively short time periods, you should set the time-out to a shorter duration than the time it takes a single client to send and receive 75 MB (this is less than 20 percent of the amount of data required to recover a WEP key, so has a large safety margin).
- If you use 802.11a or 802.11g 54 Mbps WLANs, it is easier to transmit larger numbers of packets in a given time. You may want to reduce the session time–out to 15 minutes on these faster WLANs.
- If the capabilities of WEP key cracking techniques improve significantly, less data will be needed to recover the WEP keys. For example, if a new cryptanalytic technique is discovered that allows keys to be recovered with only 100,000 packets, you would need to lower the session time-out to prevent wireless clients reaching this limit before their encryption keys are renewed.
- If you have specialist security needs, you may wish to reduce the time-out below the threshold at which even theoretical attacks on WEP would be successful (10 minutes or 3 minutes as described in the previous note). However, you need to weigh this decision against the caveats described later in this section. If the data is sensitive enough to require this level of precaution, you should seriously consider using only WPA data protection on the WLAN and using IP security to help protect the data when traveling over wired LANs.

There are two main disadvantages to reducing session time-out:

- **Lower WLAN reliability:** Very short WLAN session time-outs could cause clients to fail re-authentication and disconnect from the WLAN if communication with a domain controller or IAS server was lost temporarily.
- **Increased load on IAS servers:** The shorter the time-out, the more often the client needs to re-authenticate with an IAS server and domain controller. As a result, the load on IAS servers and domain controllers will increase. Because IAS caches client authentication sessions the load increase will normally be significant

only for organizations with a very large number of wireless clients or when using extremely short session time-out values.

Other Network Access Services

The RADIUS design used in this solution can provide authentication, authorization, and accounting services for other network access servers such as 802.1X wired network authentication and VPN and remote access authentication.

802.1X Wired Network Authentication

802.1X wired network authentication is the simplest such application requiring no modification of the basic RADIUS design. Organizations that have a widely-distributed wired network infrastructure may find it difficult to control unauthorized use of the corporate network. For example, it is often difficult to prevent visitors plugging in laptops or employees adding unauthorized computers to the network. Some parts of the network, such as data centers, may be designated high security zones and only authorized devices should be allowed on these networks; this could even mean the exclusion of employees with corporate computers.

How a wired network access solution would integrate with the design is illustrated in the following figure.

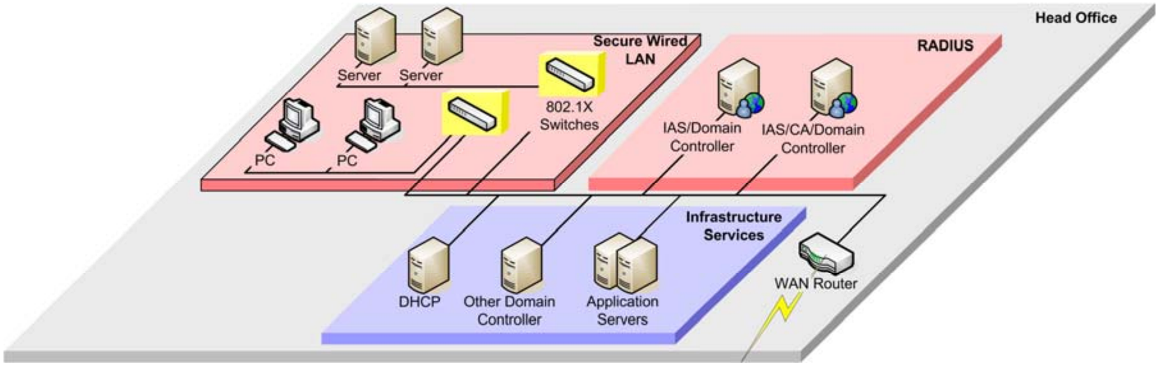

Figure 2.8

h. *Using 802.1X wired authentication*

The bold–edged box represents the 802.1X wired components and the other boxes contain the relevant services. Compare this figure to figure 2.4. Only the head office is shown in this figure.

802.1X−capable network switches play an identical role to the wireless APs in the core solution and can take advantage of the same RADIUS infrastructure to authenticate clients and selectively authorize access to the appropriate network segment. This has the obvious advantages of centralizing account management in the corporate directory while still retaining network access policies under the control of the network security administrator.

VPN and Remote Dial–Up Authentication

Another network access service that could use the RADIUS components is VPN and remote dial-up. Particularly in larger organizations, it is likely that some additions would need to be made to the design as it stands, such as the addition of RADIUS proxies. The extended solution is shown in the following figure.

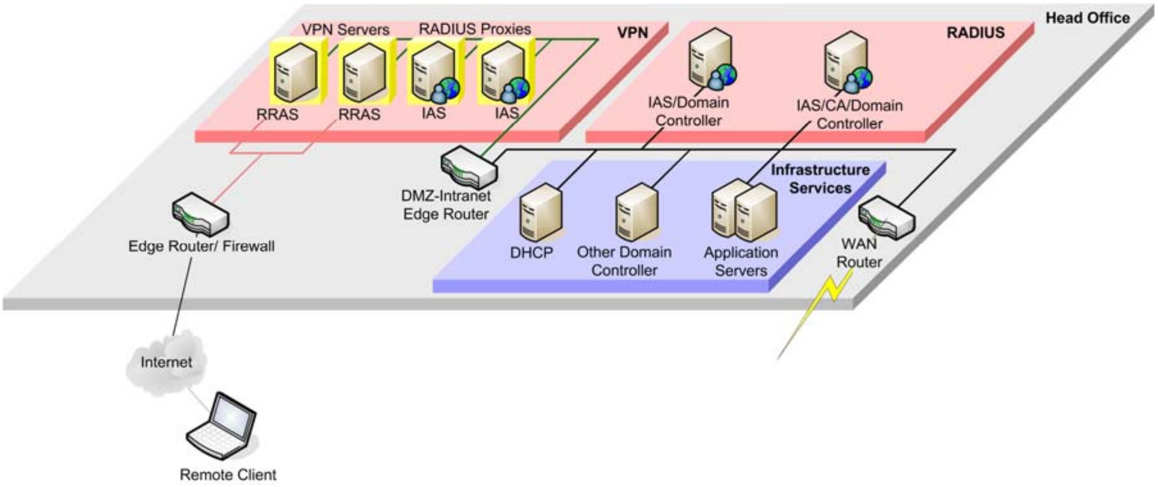

Figure 2.9

i. *Extension of the RADIUS component to support VPN*

The VPN servers, in this variant, play the same functional role as the wireless APs in the core design. They pass the clients' authentication requests to the RADIUS infrastructure. It is possible to have the RADIUS requests passed directly to the internal IAS servers. However, many organizations like to add an additional layer of RADIUS proxies providing an extra security layer and routing the requests to the internal IAS servers.

As with wired network security, this solution brings the same advantages of reusing existing infrastructure and centralizing account management. Further enhancements are possible, such as using smart card-based user authentication. The internal remote access VPN solution from Microsoft for the company's own staff uses virtually the same VPN and RADIUS architecture with smart cards for user authentication.

Dial-up remote access works in a similar way by using the dial-up server capability instead of the VPN functions of Windows Server Routing and Remote Access.

A major advantage that using IAS brings to both VPN and Remote Dial-up is the ability to use Windows Server 2003 Network Access Quarantine Control. Quarantine Control uses capabilities of the Routing, Remote Access Server (RAS) and Windows enhanced remote access client (Connection Manager) to allow and deny access based on the security state of the client computer. It works by performing checks on the client at connect-time; for example, ensuring that the client has up-to-date antivirus software, or that it is running a corporate-approved operating system build. If the client fails these checks, the RADIUS server denies it access to the network. Therefore, even a properly authenticated user and computer may be denied access if they present a possible security threat to the company network.

To learn more about the quarantine feature of Windows Server 2003, see the references at the end of the chapter.

Bootstrapping Client Computers

Most wireless capable computers also have a wired network interface. This makes it relatively easy for the clients to join the domain and download WLAN settings prior to connecting to the WLAN. However, this may not always be the case. Already, handheld devices have only wireless, and do not have wired network adapters. This presents the problem of bootstrapping a client prior to connecting to the WLAN because it does not have the settings and credentials that it needs to connect to the WLAN.

This problem becomes even more difficult if an organization decides to use both wired and wireless 802.1X security, because a client cannot connect to a wired LAN without first having the correct credentials and settings.

There are two main approaches to bootstrapping a client computer if you cannot use a wired LAN to retrieve settings and credentials; these are:

- Using a guest LAN and using an alternative authenticated connection (for example a VPN connection) to obtain credentials and settings.
- Manually configuring clients.

Microsoft currently supports only the second option. Microsoft will be releasing a wireless provisioning service that will be suitable for using a "guest" WLAN to bootstrap the client computer WLAN configuration. Until then, manual configuration is a simple way to achieve this. To configure the client computer settings and join it to the domain, the person configuring the computer needs to be a member of the local Administrators group on the computer.

► **To bootstrap a computer using manual configuration:**

1. Manually configure WLAN settings for the correct WLAN SSID.
2. Connect to WLAN using a valid user domain credentials. You will not be able to connect using the computer account until the computer is joined to the domain.
3. Join the computer to the domain and then restart it.
4. After rebooting, the client will be able to connect to the WLAN using the computer account and will download the WLAN GPO settings. These settings will simply overwrite the manually configured settings.
5. Both the user and the computer can now connect to the WLAN.

SOHO Environments

You may need to deploy WLANs to locations where it is not possible or practical to authenticate users using your IAS infrastructure. For example, home offices for users who regularly work from home or small offices with very unreliable or low bandwidth connectivity to the main corporate network.

Previously the only solution to this was to configure static WEP security and hope that no one was determined enough to bother to attack your WLAN. A far better solution is to use WPA in PSK mode. All Wi-Fi certified wireless APs now ship with WPA security although older APs may not support this. You should ensure that your APs support WPA PSK because of the additional security value that it brings. Unlike static WEP, the WPA authentication key is not recoverable from the encrypted traffic; therefore, it is much more difficult for an attacker to break on to the network. You should also ensure that your users are trained to use strong WPA keys and to change them regularly and that understand the security implications of not doing so. To implement WPA PSK, you need a wireless AP, wireless network adapters, and a client operating system (such as Windows XP) that supports WPA. You do not need a RADIUS server or other server infrastructure.

Summary

This chapter began with a description of how 802.1X wireless LAN security works. To provide focus for the design, a picture of the target organization for solution was given along with the organization's key design criteria for the WLAN solution. Following this, the main aspects of the chosen WLAN design were discussed. The design covered the network, IAS server placement and IAS configuration, the use of certificates, and the different types of wireless clients. The key points on migration from an existing WLAN were also outlined.

The two sections at the end of the chapter discussed important variations to the basic design. Firstly, how to scale the solution for larger organizations was described, along with instructions on how to deal with the main points of divergence from the core solution. This was followed by illustrations of how to use the same basic authentication infrastructure to support other network services such as remote access, VPN, and wired network security; and how to deal with the sticky problems of bootstrapping clients and deploying WLANs to SOHO environments.

The next chapter begins the implementation of the solution by helping you prepare your network, Active Directory, and server security for deployment of WLAN components.

References

This section provides references to important supplementary information or other background material relevant to the content of this chapter.

- For more details on 802.1X Authentication, see "IEEE 802.1X Authentication for Wireless Connections" at the following URL:
  http://www.microsoft.com/technet/columns/cableguy/cg0402.asp
- For more information on how PEAP with passwords works, see "PEAP with MS-CHAP Version 2 for Secure Password–based Wireless Access" at the following URL:
  http://www.microsoft.com/technet/columns/cableguy/cg0702.asp
- For more details on 802.1X authentication; the interaction between clients, wireless APs, and RADIUS servers; as well as recommendations for features that should be supported on wireless APs; see "Recommendations for IEEE 802.11 Access Points" at the following URL:
  http://www.microsoft.com/whdc/hwdev/tech/network/802x/AccessPts.mspx
- For more information on wireless LAN design including providing DHCP services and wireless AP layouts, see the "Deploying a Wireless LAN" chapter in the *Windows Server 2003 Deployment Kit* at the following URL:
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/DNSBM_WIR_OVERVIEW.asp
- For more information on Securing IAS, see the Windows Server 2003 product documentation at the following URL:
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_ias_security.asp
- For more information on Certificate Services features available in Windows Server 2003, Enterprise Edition, see the paper "PKI Enhancements in Windows XP Professional and Windows Server 2003" at the following URL:
  http://www.microsoft.com/technet/prodtechnol/winxppro/plan/pkienh.asp

  Note: This article was written before the release of Windows Server 2003 and uses the terms Windows .Net Server, Advanced Server, and Standard Server to refer to Windows Server 2003, Enterprise Edition, and Standard Edition respectively.

- For more information on Microsoft 802.1X Authentication Client for Windows 2000, see the Knowledge base article “Using 802.1x Authentication on Computers Running Windows 2000” at the following URL:

http://support.microsoft.com/default.aspx?scid=313664

- For more information on “Wi-Fi Protected Access (WPA) Overview" and "WPA Wireless Security Update” in Windows XP, see the following URLs:

  http://www.microsoft.com/technet/columns/cableguy/cg0303.asp

  http://support.microsoft.com/default.aspx?kbid=815485

- For a discussion of the security concerns with WEP, see the “Weaknesses in the Key Scheduling Algorithm of RC4” technical paper by Scott Fluhrer, Itsik Mantin, and Adi Shamir and the “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP” technical paper by Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. You should consider that these papers are discussing the security of static WEP; therefore, the conclusions drawn are not directly applicable to dynamic WEP WLANs. For the "Weaknesses in the Key Scheduling Algorithm of RC4", see the following URL:

  http://www.crypto.com/papers/others/rc4_ksaproc.pdf

- For the “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP” AT&T Technical Report, see the following URL:

  http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

- For more information on deployment of wireless LANs and remote access VPNs within Microsoft, see "Mobility: Empowering People through Wireless Networks" and "Securing Remote Users at Microsoft" at the following URLs:

  http://www.microsoft.com/technet/itsolutions/msit/security/secwlan.asp

  http://www.microsoft.com/resources/casestudies/casestudy.asp?casestudyid=13787

- For more information on network access quarantine control, see the papers "Network Access Quarantine Control in Windows Server 2003" and "Planning for Network Access Quarantine Control" at the following URLs:

  http://support.microsoft.com/default.aspx?scid=818747

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs

  /deployguide/dnsbf_vpn_aosh.asp

- For information on using WPA to secure SOHO WLANs, see "WPA Wireless Security for Home Networks" at the following URL:

  http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp

3

Preparing Your Environment

Overview

This chapter helps you to prepare your information technology (IT) environment for the deployment of the security infrastructure for your wireless local area network (WLAN). The principal tasks in preparing the environment include:

- Preparing your Microsoft® Active Directory® directory service domain by creating required security groups.
- Preparing your servers for installing Internet Authentication Service (IAS) and Certificate Services. This task involves the following three sub tasks:
  - Applying security settings to the servers.
  - Installing required tools on the servers.
  - Updating the servers to ensure that they have no known security vulnerabilities.

Chapter Prerequisites

Before proceeding with this chapter, you should have a thorough understanding of the architecture and design of this solution, which is described in Chapter 2, “Planning a Wireless LAN Security Implementation.“ In addition, you should be familiar with the installation and administration of Microsoft Windows® 2000 Server or Microsoft Windows Server™ 2003. Familiarity with the following topics will also be helpful:

- Active Directory concepts including Active Directory structure and management tools; management of users, groups, and other Active Directory objects; and use of Group Policy.
- Windows system security related topics including security concepts such as users and groups, auditing of access control lists (ACL), and application of security settings using Group Policy.
- Windows Scripting Host and Microsoft Visual Basic® Scripting Edition (VBScript) language.

IT Infrastructure Prerequisites and Assumptions

This chapter and the remaining chapters of this guide are based on the following assumptions about your IT infrastructure; although some of these may be implemented as part of this solution. Many of these assumptions are not rigid requirements; where valid alternative configurations exist, they are indicated in the guidance.

- An Active Directory forest using Windows 2000 Server or Windows Server 2003 domain controllers, with all WLAN users as members of a domain within the same forest.

Note: The domain controllers on which IAS and Certificate Services are installed must be running Windows Server 2003.

- Two or more servers running Windows Server 2003, Standard Edition (Windows Server 2003, Enterprise Edition is also supported) on which solution components are installed.
- These servers have enough capacity to run IAS and Certificate Services in addition to any existing services and applications. Certificate Services is installed only on the first server.
- IAS will be installed on existing domain controllers. This is optional, you can install IAS on a domain member server.
- Certificate Services will be installed on a domain controller. Optionally, you can install Certificate Services on a domain member server.
- You have access to Windows Server 2003 installation media.
- The domain into which IAS will be installed is running in Windows 2000 native mode. This is optional.
- An installed or planned wireless LAN infrastructure consisting of multiple wireless access points (AP). The design of the WLAN infrastructure and related issues such as placement of wireless APs and channel selection are outside the scope of this guidance.
- The entire organization is assumed to have less than 50 APs.
- One or more outlying offices with no local domain controllers (and no IAS servers), but with clients who require connections to the WLAN.

Though the solution has been built to this specific profile, the basic design can adapt to many other configurations, such as branch offices with local domain controllers, or installation into multidomain forests. The impact of alternative valid configurations, wherever applicable, is noted in the guidance.

Preparing for Implementation

Permissions Needed

To carry out the procedures given in this chapter you must use an account that is a member of the Administrators group for the domain that contains the servers. By default, the built–in Administrator account of the domain is a member of the Administrators group, however, you can use any other account that is a member of this group.

Note: This guidance is based on the assumption that you are installing Certificate Services and IAS on a domain controller. If you are installing these on servers other than domain controllers, the account that you use need only be member of the local Administrators group on each of the servers.

Tools Needed

You need the following tools to carry out the procedures given in this chapter:

Table 3.1: Tools Needed

Tool	Description	Source
WLAN Solution Scripts	The set of scripts and tools supplied with this solution.	Installation details given in this chapter.
Group Policy Management Console	Advanced management tool for Group Policy objects (GPOs), which allows you to import and export GPOs.	Can be downloaded from the Microsoft.com site. Installation details given in this chapter.
CAPICOM	System library that allows certificate and security operations to be scripted.	Can be downloaded from Microsoft.com site. Installation details given in this chapter.
DSACLs.exe	A command–line tool, which allows permissions to be set on Active Directory objects.	Windows Server 2003 installation CD. Installation details given in this chapter.
Active Directory Users and Computers	Microsoft Management Console (MMC) tool used to manage Active Directory users, groups, computers, and other Active Directory objects.	Installed as part of Windows Server 2003.

Installing the Solution Tools

A number of scripts and tools are supplied with this guidance to help simplify configuration and operation of this solution. You must install these scripts and tools on each of the IAS servers. Some of these scripts are required during ongoing operations (as described in Chapter 8, “Maintaining the Secure Wireless LAN Solution”); therefore, you should not delete them after completing the installation. By default, the scripts are installed into the C:\Program Files\Microsoft\Microsoft WLAN-PEAP Tools folder.

▸To install the scripts and tools on each server

1. Copy the **PEAPWLAN.msi** file supplied with the solution to the server.
2. From **Windows Explorer** double-click the **PEAPWLAN.msi** file to start the installation, and then click **Next** to start the installation.
3. If you want to install the scripts to a location other than the default C:\Program Files\Microsoft\Microsoft WLAN-PEAP Tools folder, specify the location.
   You will be asked whether to install the scripts for just your account or for all users. Click **All Users**, click **Next** to continue, and then click **Next** again to confirm.
4. After completing the installation, setup displays the **Tools Readme** file. This file contains an important disclaimer and a brief description of the scripts that have been installed. You should read this before continuing. Click **Next** to proceed, and then click **Finish** to complete the installation.

To enable easier access to these scripts, you can create a shortcut to open a command shell in the folder where the scripts are stored.

▸To create a shortcut to the MSS WLAN tools

1. From **Windows Explorer** navigate to the **MSS WLAN Tools** folder, the default location is C:\Program Files\Microsoft\Microsoft WLAN-PEAP Tools.
2. Double-click the batch script **CreateShortcut.cmd** file. This creates a shortcut named MSS WLAN Tools on your desktop.
3. You may want to move or copy this shortcut to your **Start** menu.

Using the Scripts

The scripts are written in Windows Scripting Host using the VBScript language. All the scripts work in a similar way. They should be run by using the two batch files (MSSSetup.cmd and MSSTools.cmd) rather than executing them directly. The batch files simplify the syntax of the scripts.

Most of the scripts take a single parameter, which specifies the function to be performed. Some scripts take additional parameters (these are explained in the guidance as required). The scripts are run from the folder in which they are installed; that is, from a command shell with the current working directory set to the tools installation folder.

The scripts produce the following different types of outputs:

- Message boxes that display information or alert text, prompt for a decision or prompt for input.
- Detailed progress information sent to a scrollable window as the script runs. If the script encounters an error, it displays error information in the window. When the script run completes, you are prompted to close the window or to keep it open for later inspection (for example, you may want to keep the window open to investigate errors).
- For many tasks, the detailed progress information is also written to a log file (%systemroot%\debug\ MSSWLAN-Setup.log). This is intended to be used for troubleshooting and auditing the installation. All the installation and configuration tasks as well as the export and import of IAS settings are recorded in this log. For security reasons, the tasks that generate the RADIUS secrets (passwords) for the wireless APs are not logged.

Setting up Your Network and Directory Infrastructure

Configuring the Network

You should connect the components to the network as shown in the following figure or according to the specific requirements of your network.

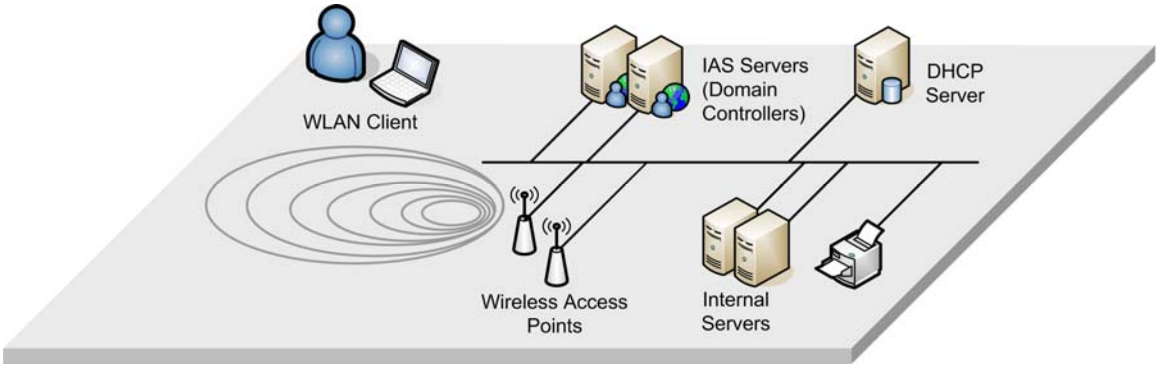

Figure 3.1
Simple WLAN network configurations

This figure shows the simplest configuration possible where the IAS servers, the APs, and the rest of your internal network are connected to the same LAN. In larger installations, the network is, typically, segmented into multiple virtual LANs (VLAN) that are connected using routers or layer 3 switches. The precise configuration will vary enormously depending on your organization's individual requirements; a detailed discussion of this topic is outside the scope of this guidance.

For more information on the network configuration for a WLAN infrastructure, see the “Deploying Wireless LANs” chapter of the *Windows Server 2003 Deployment Kit*.

Configuring the IP Network

The solution is largely independent of the VLAN and subnet arrangement. As discussed in Chapter 2, “Planning a Wireless LAN Security Implementation,” you can choose to have your wireless clients on a different VLAN from the rest of the network. However, this solution has only been tested for the simplest case; that is for a given site, the wireless clients are placed on the same LAN as the rest of the network and share the same IP subnet.

If you choose to have your wireless clients on a separate VLAN, you must allocate a separate IP subnet for the wireless clients and link the wireless VLAN to the rest of your network using a router or a layer 3 switch. For more complex environments, there are advantages to configuring separate subnets for your WLAN clients at each physical site. These advantages include:

- You can keep separate Dynamic Host Configuration Protocol (DHCP) scopes for wired and wireless clients; this allows you to set a much shorter lease time for WLAN clients.
- If you have a routed environment with multiple subnets on the same site, allocating a single subnet for all WLAN clients at that site allows these clients to roam between APs while keeping the same IP address.
- You can use the WLAN subnet to define an Active Directory site and associate specific Group Policy settings with that site. However, you cannot use this

mechanism to apply the GPO WLAN client settings described in Chapter 6, "Configuring the Wireless LAN Clients" because these settings need to be applied to the clients before they are able to successfully connect to the WLAN.

DHCP

IP addresses and IP network information need to be allocated to the WLAN clients. This solution uses the Windows DHCP service to do this; therefore a DHCP service must be available for use by the WLAN clients.

You need to allocate a separate DHCP scope for each subnet where you will be deploying clients. For example, if you have two separate sites with a routed wide area network (WAN) connection between them, you must create a DHCP scope for each subnet. If you are allocating separate subnets for your WLAN and wired LAN clients, you need to configure a separate scope for each WLAN subnet. Moreover, if you have routed connections between your APs and DHCP servers, you need to configure DHCP relay agents on the routers or install the Windows DHCP Relay Agent on a server on the same subnet as the APs.

For higher availability, you should consider a resilient DHCP configuration using split-scopes, clustered DHCP, or standby DHCP configurations. For more information about these, see the "Deploying DHCP" chapter of the *Windows Server 2003 Deployment Kit*.

DNS

Active Directory depends on a properly functioning Domain Name System (DNS) service. This solution is based on the assumption that such a service is in place and operational. You will have installed DNS as part of the Active Directory installation process or have configured it separately.

Active Directory

This solution has been designed and tested using the following Active Directory configuration:

- A single-domain Active Directory forest.
- Windows Server 2003 domain controllers (newly installed, not upgraded from Windows 2000 domain controllers).
- A domain functional level of Windows 2000 native mode.

In many cases, it is possible to use other configurations of Active Directory; for example, using multiple domains or using Windows 2000 domain controllers. Where these configurations are supported by Microsoft, additional guidance on using these is given in the text. However, these alterative configurations do not form part of the core, tested solution.

Requirements for All Versions of Active Directory

A native mode domain allows you to create Active Directory universal security groups. Using universal groups makes managing multidomain network access policies easier. However, for single domain deployments, this setting is academic. The installation scripts check whether the domain is in native mode or not. If the domain is in native mode, the script will make use of universal groups but otherwise it will only use global groups.

Active Directory must have a Windows Server 2003 schema. This is needed to support the Wireless Network Policies GPO Settings. There is no requirement for a specific

Active Directory forest functionality level. In this solution, the default Windows 2000 forest functionality level is assumed.

For more information about the concepts of domain and forest mode, see the references at the end of this chapter.

Using Windows 2000 Domain Controllers

In this solution, IAS and Certificate Services are installed on Windows Server 2003 systems. No guidance is given for using the Windows 2000 versions of these components. If you are using Windows 2000 domain controllers and are not planning to upgrade any of them to Windows Server 2003 you must upgrade the schema to Windows 2003 level. For more information about upgrading your schema, see the reference at the end of the chapter.

If this solution is to be used in a domain or forest using Windows 2000 domain controllers, you must ensure that these domain controllers have Windows 2000 Service Pack 3 (SP3) or later applied. The service pack is required to ensure that the domain controllers support Lightweight Directory Access Protocol (LDAP) signing. This is a security enhancement required by Windows Server 2003 CAs and Windows XP clients that use automatic certificate enrollment.

Verifying the Security of the Domain Account Policies

This solution relies on user and computer passwords for authenticating users and computers to the WLAN. It is, therefore, extremely important that you do not allow use of weak or blank passwords. Easily predictable passwords will make it simple for an attacker to break on to your WLAN. Because the same passwords are used to authenticate the user or computer to the domain, this will allow the attacker access to all your network resources as well.

The easiest way of eliminating weak passwords is to set strong password policies in the Default Domain Policy GPO. You should also enforce periodic expiry of passwords, minimum password age, and password history check (to ensure that users are not reusing the same password).

Warning: You should warn your users and administrators before changing the domain password policy. To avoid frustration and confusion among your users, it is a good idea to inform them early about the new password policy that you plan to adopt, together with instructions on choosing good passwords.

For recommendations on best practices for your domain password policy, see the *Windows Server 2003 Security Guide*. Reference for this document is provided at the end of this chapter.

Creating Security Groups

Use the procedure given later in this section to create security groups in Active Directory for use in this solution. The groups created are listed in the following table and, where indicated, their membership is populated. By default, these groups are created in the Users container.

Table 3.2: Security Groups and Memberships

Security Group	Purpose	Group Type	Members
Wireless LAN Users	Specifies which users can authenticate to the WLAN.	Global	Domain Users
Wireless LAN	Specifies which computers	Global	Domain Computers

Security Group	Purpose	Group Type	Members
Computers	can authenticate to the WLAN.		
Wireless LAN Access	This group is used in the RADIUS access policy to control access to the WLAN.	Universal	Wireless LAN Users Wireless LAN Computers.
Wireless LAN Computer Settings	Specifies which computers receive WLAN settings from group policy.	Domain Local	Wireless LAN Computers.

▸ To create and populate security groups

1. Open a command shell using the **MSS WLAN Tools** shortcut.
2. At the command prompt, type *MSSSetup CreateWLANGroups,* and then press **ENTER**.

Important: If you have moved the Domain Users and Domain Computers groups from their default location in the Users container they will not be added to the Wireless LAN Users and Wireless LAN Computers groups respectively. In this case, you must add them to these groups manually.

Note: If you install this solution in a mixed mode domain, the Wireless LAN Access group will be created as a Domain Global group instead of a Universal group. This means that you need to create one of these groups in each domain, if you are to install this solution into a multi–domain forest (this task is described in Chapter 2, "Planning a Wireless LAN Security Implementation.")

If you are installing this solution in multiple domains, you need to create the Wireless LAN Users and Wireless LAN Computers global groups in each domain and add them to the Wireless LAN Access group. You also need to create a Wireless LAN Computer Settings domain local group in each domain where you have WLAN clients and add the Wireless LAN Computers universal group as a member.

Preparing Your Servers

This section covers server–specific configuration. You need to perform most of the following procedures for each server that you plan to install as IAS server. The procedure in the "Server Security Configuration" section is the only exception because, even though the security settings are applied to each server, this procedure has to be executed only once per domain. The settings are then automatically applied to others servers in the domain.

Operating Systems Supported

This solution has been built and tested using Windows Server 2003, Standard Edition for all server components. However, the guidance and installation scripts are the same for Windows Server 2003, Enterprise Edition.

You should read the "Using Windows Server Standard or Enterprise Edition" section in Chapter 2, "Planning a Wireless LAN Security Implementation" before deciding whether you need to use Windows Server 2003, Enterprise Edition or not. Use of Windows Server 2003, Standard Edition places limitations on the functionality of Certificate Services and the number of wireless APs that IAS can support, either or both of which may be unacceptable for large organizations.

This solution has not been designed to support earlier versions of Windows Server and has not been tested with any of them. The Windows 2000 Server versions of IAS and Certificate Services may work for some or all of the server roles in this solution but guidance on how to do this is outside the scope of this documentation.

Hardware Guidelines

The first server that you install will run Certificate Services as well as IAS. Certificate Services requires minimal resources in this solution. However, you should ensure that the load that IAS places on the server does not negatively affect the performance of the domain controller functions of the server. This is unlikely to be the case in any but the very largest IAS implementations. If necessary, you should add an additional domain controller to the same Active Directory site to compensate for this.

If you plan to enable RADIUS logging, you should allocate a separate physical disk for the logs.

Table 3.3: Recommended Minimum Hardware for IAS Server

Item	Requirement
CPU	Single CPU 733 MHz or better
Memory	256 MB
Network interfaces	Single network adapter
Disk storage	IDE or SCSI RAID Controller 2 x 18 GB (SCSI) or 2 x 20 GB (IDE) configured as RAID 1 volume Local removable media storage (CD−RW or tape for backup), if no network backup facility is available 1.44 MB disk drive for data transfer.

You should read the "IAS Software and Hardware Requirements" section in Chapter 2, ”Planning a Wireless LAN Security Implementation,” for a further discussion of hardware performance requirements.

Obtaining and Installing Supporting Software

This section lists the additional software needed on your servers. It also describes how to obtain and install the software.

Group Policy Management Console

Group Policy Management Console (GPMC) is used to install and configure the Group Policy Objects (GPOs) used by the solution. The GPMC only needs to be installed on the first server on which IAS is installed; its installation on subsequent IAS servers is optional.

Note: Installation of the GPMC changes the user interface of Active Directory Users and Computers slightly on the server on which GPMC is installed. For more information on using the GPMC and downloading, see the reference at the end of this chapter.

▸ To install the Group Policy Management Console

1. Download the **Gpmc.msi** installation file from the Microsoft Download Center.
2. Ensure that you are logged on as a member of the domain Administrators group (or the local Administrators group of the computer on which you are installing the GPMC, if you are not installing it on a domain controller).

3. From **Windows Explorer** double-click the **Gpmc.msi** installation file.
4. Follow the setup wizard prompts to install the GPMC; accept all defaults.

Important: You should install GPMC in the Program Files folder (although it does not matter which drive this is on). You should also use the default installation folder —GPMC—within Program Files (if you change the folder name, you must update the name of the folder that you used to install GPMC in the Constants.txt file). Later procedures use some of the tools installed by GPMC and if you install it elsewhere they will be unable to locate the GPMC tools.

Windows Server 2003 Support Tools

Some of the Windows Support Tools are used by the configuration scripts and procedures in this solution. You should install these from the Windows Server 2003 installation media. These are needed by the CA installation and configuration scripts so you must install them on the on the server on which Certificate Services is to be installed. They are not required on the other servers although you may wish to install them there.

▸ To install the Windows Server 2003 support tools

1. Ensure that you are logged on as a member of the domain Administrators group (or the local Administrators group of the computer on which you are installing the support tools, if you are not installing it on a domain controller).
2. Insert the **Windows Server 2003 installation CD** (or connect to the installation source if you are installing from the network or other media).
3. From **Windows Explorer**, navigate to the installation media drive (CD drive or a floppy drive), and then to the **\support\tools\supptools.msi** file. Double-click the file to begin the installation.
4. Follow the setup wizard prompts to install the support tools, and accept the license agreement and the default installation folder.

CAPICOM

CAPICOM is a scriptable interface to a set of Windows security functions known as the CryptoAPI (CAPI). CAPICOM is needed for the Certificate Services health monitoring scripts and to generate the RADIUS secrets used to authenticate the wireless APs. You should install CAPICOM version 2.0 or later on all IAS servers in your organization.

You can find the latest version CAPICOM 2.0 at the Microsoft Download Center (see the "References" section at the end of this chapter).

The CAPICOM distribution file does not contain an automated setup; therefore you should use the batch script, InstCAPICOM.cmd (supplied with this solution). If you wish to perform these steps manually, you can copy the commands from the batch script.

▸ To install CAPICOM

1. Download the **CAPICOM** distribution file, **CCR2INST.exe**, from the Microsoft Download Center and copy it to a temporary folder on the server.
2. Ensure that you are logged on as a member of the domain Administrators group (or the local Administrators group of the computer on which you are installing CAPICOM, if you are not installing it on a domain controller).
3. Open a command shell using the **MSS WLAN Tools** shortcut.
4. At the command prompt, type:

   InstCAPICOM [d:]PathtoCCDistFile\CCR2INST.EXE, and then press **ENTER**.

Note: Replace *[d:]PathtoCCDistFile* with the full path (including the drive letter, if on a different drive) of the folder to which you copied the CAPICOM distribution file.

Microsoft Baseline Security Analyzer (MBSA)

This tool is required to verify that the operating system security updates are current and to detect possible problems with the security configuration of the servers. You need to use version 1.1.1 or later of MBSA to scan Windows Server 2003 systems. You can find the latest version of MBSA at the Microsoft Download Center.

▸ To install MBSA

1. Download the **mbsasetup.msi** installation file from the Microsoft Download Center.
2. Ensure that you are logged on as a member of the domain Administrators group (or the local Administrators group of the computer on which you are installing MBSA, if you are not installing it on a domain controller).
3. From **Windows Explorer**, navigate to the **mbsasetup.msi** file, and then double-click it.
4. Follow the setup wizard prompts to install the MBSA; accept all defaults.

Server Security Configuration

This section describes how to apply security policies and other security measures to Windows Server 2003 prior to installing IAS and Certificate Services.

This solution is designed to be installed on existing servers (typically domain controllers). The security settings used in this section are intentionally conservative because of the danger of security settings conflicting with installed applications and services that may be already running on the server.

Using the Windows Server 2003 Security Guide

Windows Server 2003 has strong default security settings. For most organizations, these settings provide good protection for their systems if combined with an effective update maintenance process (for more details on update maintenance, see the "Server Security Updates" section later in this chapter). However, you should also consider the recommendations described in the *Windows Server 2003 Security Guide*. This guide defines security settings appropriate for different server roles.

Servers used in this solution carry out several of server roles defined in the *Security Guide*; the "Domain Controller" and "RADIUS Server" roles for most servers; and, in the case of the first server, the "Certification Authority" role as well. For each role, the guide defines a security template with all the security settings appropriate to that role. For a server with multiple roles, you must therefore apply a combination of the security templates corresponding each of the server's separate roles. On your servers, you may also have other infrastructure services such as DNS, DHCP, and Windows Internet Naming Service (WINS), in which case you need to include the security templates appropriate to these roles as well. For instructions on how to do this, see the *Windows Server 2003 Security Guide*.

Warning: The security setting templates in the *Windows Server 2003 Security Guide* explicitly disable a number of services not required by the defined server roles. If you have any other applications or services running on the servers, you must test these applications to ensure that the security templates do not disable services or change any security settings on which your applications or services are dependent. Instructions on combining roles and changing settings to accommodate other applications are also included in the *Windows Server 2003 Security Guide*.

Applying Security Settings

Unlike most of the other procedures in the "Preparing Your Servers" section of this chapter, this procedure does not need to be carried out on each server. Instead, the settings are imported into a GPO in Active Directory and then applied globally to all the servers.

There are only two types of security settings applied in this solution. The first type is applied to configure all required services to start automatically (in case these are stopped or disabled by any other security policy applied to the computer). The second type is applied to change the audit policy so that audit failures for common events (such as logon) are also captured to the security log.

The following table lists the services set to start automatically.

Table 3.4: Windows Services Enabled by Policy

Service	Policy Setting
Certificate Services	Automatic
Internet Authentication Service	Automatic
Microsoft Software Shadow Copy Provider	Automatic
Removable Storage	Automatic
Task Scheduler	Automatic
Volume Shadow Copy	Automatic

The following table lists the audit categories where failure auditing is enabled in addition to the default success auditing.

Table 3.5: Audit Policy Settings

Audit Policy	Setting
Audit Account Logon Events	Success/Failure (default is Success only)
Audit Account Management Events	Success/Failure (default is Success only)
Audit Logon Events	Success/Failure (default is Success only)
Audit Policy Change Events	Success/Failure (default is Success only)

Enabling the audit settings shown in the table will increase the storage requirements for the security log. You should ensure that the event logs are set to adequate sizes on your domain controllers. The default size of event log for Windows Server 2003 are more than adequate but Windows 2000 used default sizes that were normally far too small for practical use (these settings may still be in effect if you have upgraded from Windows 2000). In Chapter 5, “Building the Wireless LAN Security Infrastructure,” you will see how the IAS servers are configured to log all successful and failed WLAN connections to the Windows system log. You should ensure that security and system logs are set to adequate sizes on all domain controllers. Windows Server 2003 uses 16 MB for the system and application logs and 128 MB for the security log: these are appropriate values for this solution.

Importing the Security Settings GPO

The following procedure imports the settings described in the previous section into the domain but does not apply them to any server.

▸ To install the security settings GPO into your domain

1. Open a command shell using the **MSS WLAN Tools** shortcut.
2. At the command prompt, type the following command to import the GPO called IAS Server Security Policies into the domain:

   MSSSetup ImportSecurityGPO, and then press **ENTER**.

Applying Security Settings to All Domain Controllers

In this procedure the security settings are applied to all the domain controllers (with or without IAS installed). This should not have an adverse effect on domain controller functions or any other applications or services running on them because there are no settings in the GPO that disable any functionality. If you do not want to apply these settings to all of you domain controllers see the procedure immediately following this one.

To apply the settings to all domain controllers, you need to link the imported GPO to the Domain Controllers organizational unit (OU). GPO is linked manually because of the danger of overwriting GPO settings already configured in your domain.

▸ To apply the security settings to all domain controllers

1. Click **Start,** click **All Programs**, click **Administrative Tools**, and then **Group Policy Management** to start the **GPMC**.
2. Navigate to the **Domain Controllers** OU in the left pane and click it.

   This OU should appear immediately beneath the domain object.
3. Right-click the OU name, and then click **Link an Existing GPO…**.
4. In the list of GPOs, click **IAS Server Security Policies**, and then click **OK** to return to the main GPMC window.
5. In the right pane, ensure that the **Linked Group Policy Objects** tab is selected, and then click the **IAS Server Security Policies** GPO.
6. Click the double up-arrow symbol immediately to the left of this list to move this GPO to the highest priority.

   This ensures that the required services will remain enabled regardless of other security policies applied to the domain controllers.
7. Close the **GPMC**.

   The security settings will be applied to the servers at the next GPO refresh interval (the default refresh interval is 5 minutes for domain controllers).

Applying Security Settings Only to IAS Servers

If you do not want the security settings to be applied to all domain controllers (or if you have chosen not to install IAS on the domain controllers), you can create a separate OU for IAS servers and then apply the GPO to that OU. If you are not installing IAS on domain controllers, you should create the IAS servers OU in some other part of the domain.

▸ To apply the security settings only to the IAS servers

1. Click **Start,** click **All Programs**, click **Administrative Tools**, and then **Group Policy Management** to start the **GPMC**.
2. Navigate to the **Domain Controllers** OU in the left pane and click it.

   This OU is immediately beneath the root of the domain.

3. Create a new child OU beneath this OU by right-clicking the **Domain Controllers** OU name, and then selecting **New Organizational Unit** from the pop-up menu.
4. Type a name for the OU when prompted, for example, *IAS Servers*.
5. Right-click this OU and click **Link an Existing GPO…**.
6. Select **IAS Server Security Policies** in the list of GPOs, and then click **OK** to return to the main GPMC window.
7. Close the **GPMC**.
8. Move the computer object of each combined domain controller and IAS server from the **Domain Controllers** OU to the new child OU.
   The security settings will be applied to the servers at the next GPO refresh interval (the default refresh interval is 5 minutes for domain controllers and 90 minutes for other computers).

Note: If you are installing the IAS servers in multiple domains, you need to repeat the installation and linking of GPOs for each domain in the forest.

Verifying the Security Settings

▸ To verify that the security settings have been applied

1. From a command shell, at the command prompt, type:

   gpupdate /force, and then press **ENTER**.
2. Check the **Application Event** log for events from the **SceCli** source (this may take a few seconds to appear). There should be an event ID 1704 logged. The text of the event should read as follows:

   ```
   Security policy in the Group policy objects has been applied
   successfully.
   ```

Server Security Updates

In contrast to the GPO security settings, you need to check and apply security updates on every server. If you have relatively few servers to manage, you can use manual procedures. If you have many servers and do not already have an automated update maintenance system, manually checking for and applying updates on all servers will be an extremely tedious task. Instead, you should consider automating the application of security updates using Microsoft Software Update Service (SUS) or Microsoft Systems Management Server (SMS) 2003. For more information on the use of these to manage security updates, see the *Microsoft Guide to Security Patch Management*.

Checking Current Security Updates

There are two main ways of checking the currency of the security updates on your server, namely Windows Update and MBSA. There are also tools, which perform similar functions, from vendors other than Microsoft.

Windows Update

Windows Update is an online service designed primarily for use by small businesses and home users (there is, however, no restriction on who can use this service). Because Windows Update requires a live connection to the Internet, you must not use this service without protecting your server with a firewall.

For more information on Windows Update, see the references at the end of this chapter.

Microsoft Baseline Security Analyzer

MBSA is a security evaluation tool, which checks systems for a variety of security problems including missing updates. For more information on MBSA, see the references at the end of this chapter

▸ To check installed security updates using MBSA

1. If your server does not have connectivity to the Internet, you must obtain the current version of the MBSA security database each time prior to running the check. This is an XML file, **msecure.xml**, which can be downloaded from the URL given at the end of this chapter. Copy this file to the folder where MBSA was installed (the default folder is C:\Program Files\Microsoft Baseline Security Analyzer).
2. To check the current update status of the server, at the command prompt, type:

   Mbsacli /hf –v, and then press **ENTER**.
3. Make a note of security updates that are missing. These are displayed as follows:

   ```
   * WINDOWS SERVER 2003, STANDARD EDITION GOLD
   Note          MS03-030    819696
   Please refer to Q306460 for a detailed explanation.
   ```
4. For each missing security update, you can obtain the associated security update by using your Web browser to access the related Microsoft Knowledge Base article. Type the following URL into your browser:

   http://support.microsoft.com/default.aspx?kbid=XXXXXX

   Note: You should replace XXXXXX with the Knowledge Base article number(s) listed in the MBSA output (for example 819696 in the example above).
5. Install each update according to the instructions in the Knowledge Base article.

Using MBSA to Check Other Security Issues

Apart from checking that security updates are current, you should use MBSA to check for other potential security problems on your server. To do this, run the graphical version (from the **Start** menu), perform a scan of the server, and act on any warnings.

In particular, you should watch for any user accounts detected as having blank, weak, or nonexpiring passwords. However, do not alter the settings of any built-in accounts such as krbtgt.

Unless you have changed the default Internet Explorer security zone settings on your servers, you can ignore MBSA warnings about nonstandard settings. The default settings for Windows Server 2003 are stronger than the Internet Explorer zones settings which MBSA is checking against.

The procedure given in this chapter only covers running MBSA to scan the local machine, procedure for running it to scan computers over the network is beyond the scope of this guidance. For further details on the use of MBSA, see the reference at the end of the chapter.

Managing and Installing Updates on Your Servers

Comprehensive coverage of automated on–going updates management is beyond the scope of this guidance. However, you should be aware of the three main ways in which you can perform ongoing management of system updates using Microsoft technology.

AutoUpdate

AutoUpdate is a service built into Windows servers and clients that allows each computer to check for and download any important security hotfixes as they are released by Microsoft. You have the option to have the updates automatically installed. This requires that each computer has Web (HTTP) access. The earlier caution about ensuring that you have adequate firewall protection in place for each device (see the "Windows Update" section) applies here as well.

For more information about AutoUpdate, see the reference at the end of this chapter.

Software Update Service

Software Update Service (SUS) builds on the AutoUpdate service. It removes the requirement for each computer to connect to the Internet, by centralizing the update checking and downloading functionality in one or more central computers. The administrator can then approve or reject downloaded updates at the SUS server(s). All approved updates are retrieved by all the other computers in the organization. These computers use the AutoUpdate service to check and download updates from the SUS server(s) instead of the Windows Update site.

For guidance on how to deploy SUS, see *Patch Management Using Microsoft Software Update Services*. The URL to obtain this document is given at the end of this chapter.

Update Management with Microsoft Systems Management Server

Using Microsoft SMS 2003, you can completely automate the delivery of service packs, security updates, and software updates. Using SMS 2000 with the Software Update Services Feature Pack integrates the features of SUS with the wider capabilities of SMS. Both SMS 2000 and SMS 2003 include the ability to schedule MBSA scans of your organization's computers. For more information about the use of SMS, see the following papers:

- *Patch Management Using Microsoft Systems Management Server 2003*
- *Patch Management Using Microsoft Systems Management Server 2.0*

URLs to obtain these documents are provided at the end of the chapter.

Summary

This chapter provided guidance on preparing your network, Active Directory, domain controllers, and other elements of your environment for the installation of a secure WLAN infrastructure. The scripts used to configure this solution were installed together with a number of supporting tools. Security groups used by this solution were created in the domain, and security settings were imported and applied to your servers. Finally, the currency of security updates on the servers was examined and, if necessary, corrected.

The next chapter covers installation of Certificate Services on the first server installed to create the network CA.

References

This section provides references to important supplementary information or other background material relevant to the content of this chapter.

- The "Deploying Wireless LANs" chapter in the Windows Server 2003 Deployment Kit, is available at the following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/DNSBM_WIR_OVERVIEW.asp

- For information about Active Directory domain functional levels and instructions on how to change between them, see the following sections of the Windows Server 2003 product documentation available at the following URLs.

  - This section describes the different domain and forest levels:

    http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_levels.asp

  - This section describes changing the domain and forest level:

    http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_changedomlevel.asp

- For detailed information on upgrading a Windows 2000 Active Directory Schema to Windows Server 2003 level, see the ADPrep documentation page at the following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/adprep.asp

- For detailed information on downloading and using the Group Policy Management Console, see the following URL:

  http://go.microsoft.com/fwlink/?LinkID=8630

- For downloading Version 2.0.0.3 of CAPICOM, see to the following URL:

  http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6

  However, you should search for "CAPICOM" from the following URL to ensure that you are getting the latest version:

  http://www.microsoft.com/downloads

- For instructions on downloading and using the Microsoft Baseline Security Analyzer (MBSA), see the following URL:

  http://www.microsoft.com/technet/security/tools/tools/mbsahome.asp

- The latest Microsoft Patch database (mssecure.xml), in the form of a signed CAB file, can be downloaded from the following URL:

  http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab

- The Windows Server 2003 Security Guide is available at the following URL:

  http://go.microsoft.com/fwlink/?LinkId=14845

- For Windows Update, see the following URL:

  http://v4.windowsupdate.microsoft.com/en/default.asp

- For more information on using AutoUpdate, see article at following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/autoupdate_top.asp

- See the Patch Management, Security Updates, and Downloads pages at the following URL: http://www.microsoft.com/technet/security/topics/patch/secpatch/default.asp
- The URL above provides links to the following and other relevant guides:
    - Patch Management Using Microsoft Software Update Services
    - Patch Management Using Microsoft Systems Management Server 2003
    - Patch Management Using Microsoft Systems Management Server 2.0

4

Building the Network Certification Authority

Overview

This chapter guides you through installing and configuring Microsoft® Windows Server™ 2003 Certificate Services. Certificate Services is an optional component of Windows Server 2003 and is not installed by default.

An installation of Certificate Services is referred to as a Certification Authority (CA). Only one CA is required for the *Securing Wireless LANs with PEAP and Passwords* solution. This CA will be used to issue certificates to the Internet Authentication Service (IAS) servers (discussed in the subsequent chapters of this solution).

The goal of this chapter is to provide you with a very simple, special purpose CA. Unlike most CAs, it will be used to issue only one type of certificate—server certificates for the IAS servers used in the solution. For this reason, it has been designed to be extremely simple to install, configure, and manage. It is important to note that if your organization plans on using certificates for additional purposes, such as IPSec or VPN in the future, Microsoft recommends considering a more robust Public Key Infrastructure (PKI) architecture for your environment. See the planning materials referenced in Chapter 2, "Planning a Wireless LAN Security Implementation," for more details.

The information in this chapter is limited to the implementation instructions for the CA. This chapter does not explain any of the general concepts of PKI, or any of the implementation details of Microsoft Certificate Services other than what is necessary to complete the installation. It also does not address using this CA to issue any types of certificates other than the server authentication certificates for IAS.

This chapter is based on the assumption that you do not currently have a PKI in your organization. If you do have one, it may be possible to issue certificates to the IAS servers from this rather than installing the CA described in this chapter. However, guidance on how to do this or how to install this CA into your existing PKI is outside the scope of this solution.

Instead of installing your own CA, you can obtain certificates from a commercial CA such as VeriSign or Thawte. For a discussion on the relative merits of installing your own CA versus buying certificates from an external provider, see the "Obtaining Certificates for IAS Servers" section in Chapter 2, “Planning a Wireless LAN Security Implementation.” This chapter does not include any guidance on obtaining and using certificates from a commercial CA. At the end of the chapter, however, there is a reference to a Microsoft document that describes this process.

Chapter Prerequisites

In addition to the prerequisites listed in Chapter 3, “Preparing Your Environment,” you should be familiar with Certificate Services and PKI concepts (although in-depth knowledge is not required).

Before implementing the instructions in this chapter, you need to read and implement the guidance provided in Chapter 3, “Preparing Your Environment.” You should also have read the design and planning information in Chapter 2, “Planning a Wireless LAN Security Implementation,” and have a thorough understanding of the architecture and design of the solution.

Preparing for Implementation

Permissions Needed

To carry out the procedures in this chapter, you need to log on with an account that is a member of the following groups:

- The **Domain Admins** group for the domain into which you are installing the CA.
- The **Enterprise Admins** group of the Microsoft Active Directory® directory service forest.

By default, the built-in Administrator account of the forest root domain (the first domain created in the forest) is a member of both these groups, but you may use any other account with the same group memberships.

Note: If you are not installing the CA into the forest root domain, and the forest is a Windows 2000 Active Directory (or has been upgraded from a Windows 2000 Active Directory), the account used for the installation will also need to be a member of the forest root domain.

Tools Needed

You need the following tools to carry out the procedures in this chapter.

Table 4.1: Tools Needed to Build and Install a CA

Tool	Description	Source
MSS Secure WLAN Tools	The set of scripts and tools supplied with this solution.	Installation steps provided in Chapter 3.
Group Policy Management Console (GPMC)	Advanced management tool for import and export of Group Policy objects (GPOs).	Installation steps provided in Chapter 3. Can be downloaded from Microsoft.com.
CAPICOM	System library that allows scripting of certificate and security operations.	Installation steps provided in Chapter 3. Can be downloaded from Microsoft.com.
DSACLs.exe	A command line tool that allows permissions to be set on Active Directory objects.	Installation steps provided in Chapter 3. Available as part of Windows Server 2003

Tool	Description	Source
		installation CD.
Active Directory Users and Computers	A Microsoft Management Console (MMC) tool that is used to manage Active Directory users, groups, and computers as well as other Active Directory objects.	Installed as part of Windows Server 2003.
Certification Authority administrative tool	An MMC tool that is used to manage the CA.	Installed as part of Certificate Services installation on Windows Server 2003.

9.

Certification Authority Parameters

The following table lists the parameters that are used for installing and configuring the CA in this solution. These parameters are all set in the PKIparams.vbs script file and may be modified there if required.

Table 4.2: CA Settings Used in the Solution

CA Configuration Parameter	Setting
Drive and path of Certificate Services request files	C:\CAConfig
Length of CA key	2048 bits
Validity period of CA certificate	25 years
Maximum validity period of certificates issued by CA	2 years
CRL publishing interval for CA	7 days
CRL overlap period (that is, the time between a new CRL being published and an old CRL expiring)	4 days
Delta–CRL publishing disabled	0
Certificate templates available on the CA	Computer (Machine)

10.

Note: The validity period of the CA is set to a large value to avoid the administrative overhead of having to renew the CA certificate periodically. Unlike the certificates issued to computers and users, CA certificates cannot be renewed automatically and if the CA certificate is not renewed before it expires, all certificates issued by the CA will fail.

Important: The settings listed in the previous table were used in the internal testing of this solution and are known to work as documented. Many of these values can be changed, but you should do this only if you fully understand the purpose of a particular setting and the implications of changing it.

Checking Readiness for Installation

Before installing Certificate Services on your server, you must ensure that the domain is contactable and that the required tools have been installed.

To check the server prior to installation of the CA

1. Log on to the server where you intend to install the CA (and the first instance of IAS server (using an account with appropriate administrative permissions).

2. Click the **MSS WLAN Tools** shortcut to open a command shell, then at the command prompt, type:

   MSSsetup CheckCAenvironment

   The name of the domain into which you are installing the CA is shown in a distinguished name (DN) format (for example, dc=Treyresearch, dc=net), which is equivalent to a Domain Name System (DNS) format (Treyresearch.net).
3. If the domain name is correct, click **OK**. If it is incorrect, click **Cancel**, log on to the correct domain, and then repeat steps 1 and 2.

The script checks for the following:

- Active Directory domain controller can be contacted.
- CAPICOM is installed.
- GPMC is installed.
- DSACLs.exe is installed and accessible.

If any problem is detected, you are notified with an error logged to the script console window. You should investigate and correct this error before continuing.

Installing Certificate Services

This section describes how to install Certificate Services to create a CA. The CA is installed as an Enterprise Root CA.

Installing the Certificate Services Software Components

You must install the CA software components using the supplied script. This script uses the Windows Optional Components Installation Manager to install the CA, building all required configuration files as it runs. To perform the installation, use the Windows Server 2003 installation CD (or the network path to a Windows installation source.

Caution: If a CA was previously installed, or if you are trying to reinstall the CA, you must first remove the existing installation. Before removing the CA, ensure that it is not in use by other applications.

Use **Add/Remove Windows Components** of the **Add/Remove Programs** applet in **Control Panel** to remove Certificate Services.

▸ **To install Certificate Services**

1. Use the **MSS WLAN Tools** shortcut to open a command shell.
2. At the command prompt, type the following to install the Certificate Services software components.

   MSSsetup InstallCA, and then press **ENTER**.
3. When prompted, type a name for the CA.

   Make the name descriptive and unique for your organization (for example, Trey Research Network CA).
4. To confirm the name, click **OK**.

   To edit the name, click **No**.

   To stop the installation, click **Cancel**.

The script builds the installation parameter files. When this is completed, you are prompted to continue with the installation.

5. Click **OK** to proceed or click **Cancel** to stop the installation.

Note: If you cancel the installation here, the configuration file — CAPolicy.inf — and the optional components parameter file — OC_CertSrv.txt — will be left in the Windows folder and the current working folder respectively. These files can be modified and used in a custom installation if you do not want to accept the solution defaults.

6. After the confirmation message displays telling you that the installation is complete, click **OK**.

Verifying the CA Installation

You can verify successful completion of the Certificate Services installation using the following procedure.

▸ **To verify correct installation of the CA**

1. Use the **MSS WLAN Tools** shortcut to open a command shell.
2. At the command prompt, type:

   MSSsetup VerifyCAInstall, and then press **ENTER**.
   The certificate viewer displays the CA certificate.
3. Click the **General** tab of the certificate, and then verify that the displayed values match those in the following table.

Table 4.3 CA Certificate Properties

Certificate Attribute	Required Setting
Issued to	The name of the CA as entered during installation.
Issued by	The name of the CA as entered during the installation.
Valid from…to…	The interval specified here should be 25 years.

11.

4. Click the **Certification Path** tab and verify that only one certificate displays in the certification path field. The certificate status should display **The Certificate is OK**.
5. Click **OK** to close the certificate viewer.

If any of the previous values are not what you expected, you restart the Certificate Services installation.

Note: If you need to rerun the CA installation, you must first remove the installed Certificate Services as described earlier.

Configuring the CA

After the CA is installed, you must run some additional scripts to configure some of the remaining CA parameters.

Configuring the CA Properties

This procedure sets a number of parameters on the CA, which govern how it behaves. Some of these parameters are set during the CA installation while others must be set after the installation. The values of these parameters are specified in the "Certification Authority Parameters" section earlier in this chapter. The script used in this procedure configures the CA properties as listed in the following table.

Table 4.4: CA Configuration Properties

CA Property	Description of Setting
CRL Distribution Point (CDP) URLs	Specifies the locations from which a current certificate revocation list (CRL) can be obtained. In this solution only a Lightweight Directory Access Protocol (LDAP) URL is used. It contains the LDAP path for the CRL published to Active Directory.
Authority Information Access (AIA) URLs	Indicates the location from which a CA certificate can be obtained. As with the CDP, only the LDAP URL pointing to Active Directory is used.
Validity Period	Indicates the maximum validity period for issued certificates (this is different from the validity period of the CA certificate itself, which is set during installation).
CRL Period	Indicates the frequency of CRL publication.
CRL Overlap time	Indicates the overlap time between issuing of a new CRL and expiry of the previous CRL.
Delta-CRL Period	Indicates the frequency of delta-CRL publication. (On this CA, delta-CRLs are disabled.)
CA Auditing	Indicates the CA auditing settings. (All auditing is enabled by default.)

12.

Note: Many of these parameters affect the configuration of the CA's CRL. A CRL is a list of certificates that were issued by the CA but were subsequently canceled (or revoked) by the administrator. Even though you are unlikely to ever need to revoke any certificates while managing this solution, many applications rely on being able to read a current CRL to check the revocation status of a certificate (even though the CRL might be empty). If the application cannot find a CRL, it may reject the certificate.

▸ **To configure the CA properties**

1. Use the **MSS WLAN Tools** shortcut to open a command shell.
2. At the command prompt, type the following to configure the CA components:

   MSSsetup ConfigureCA, and then press **ENTER**.

   During the configuration, the script pauses for 20 seconds to wait for a task to complete on the CA. You do not need to respond to the pop-up messages announcing this delay.
3. Click **OK** to dismiss the message.

If the script reports an error, investigate the reason by tracing through the log file (%systemroot%\debug\MSSWLAN-Setup.log) and rerun the configuration script after correcting the problem.

Note: You can rerun this configuration script as many times as required.

Importing the Automatic Certificate Request GPO

This procedure imports the IAS Certificate Autoenrollment Policy GPO that is preconfigured to allow automatic issuance of certificates to the IAS servers in the domain. It uses a feature called the Automatic Certificate Request Service (ACRS).

ACRS should not be confused with the Autoenrollment capabilities in Windows Server 2003, Enterprise Edition, although the two perform similar functions. It is a more limited service than Autoenrollment and was first used in Windows 2000. It only allows *computer* (not user) certificates to be enrolled and works only with version 1 certificate templates. However, ACRS is adequate for the limited certificate usage in this solution, and using it allows the CA to be installed on (the less expensive) Standard Edition of Windows Server 2003.

Important: If there are multiple domains in your Active Directory forest, you need to repeat this procedure for each domain in which you install an IAS server.

The script used in the following procedure imports a preconfigured GPO with a policy to automatically enroll certificates. The GPO specifies the predefined "Computer” certificate type as the type to enroll. The script then applies security permissions to the GPO so that only members of the RAS and IAS Servers group are affected (the default setting is to apply GPOs to all authenticated users and computers).

Note: In some contexts, the Computer certificate template may be referred to as the Machine template. "Machine" is the internal name of the template, whereas "Computer" is its display name.

► **To install the Automatic Certificate Request GPO into your domain**

1. Use the **MSS WLAN Tools** shortcut to open a command shell.
2. At the command prompt, type the following to import the IAS Certificate Autoenrollment Policy GPO into the domain:

   MSSsetup ImportAutoenrollGPO, and then press **ENTER**.

Next, you must link this GPO to the domain so that the GPO settings will be applied to the IAS servers. This is given as a manual procedure to allow you to control the process of linking the GPO. Automating this step would run the risk of overwriting existing GPO link settings in your domain.

► **To apply the Automatic Certificate Request GPO**

1. Click **Start**¸ click **All Programs**, click **Administrative Tools**, and then **Group Policy Management** to start the **GPMC**.
2. In the left pane of the **GPMC**, navigate to the domain object corresponding to your domain.

   The domain object is located under the top level **Domains** container and has the same name as the DNS name of your domain.
3. Right-click the domain object, and then select **Link an Existing GPO…**.

4. From the list of GPOs, select **IAS Certificate AutoEnrollment Policy**.
5. Click **OK** to return to the main **GPMC** window.
6. In the right pane, click the **Linked Group Policy Objects** tab, and then select the **IAS Certificate AutoEnrollment Policy** GPO.
7. Close the **GPMC**.

   The automatic certificate request settings will be applied to your servers only after they are added as members of the RAS and IAS Servers group. This is covered in a procedure in the next chapter.

Important: If your domain is in mixed mode and you are installing IAS on member servers (rather than on domain controllers), the RAS and IAS Servers local group will not be visible on the member servers. This will prevent the ACRS GPO from being applied to these servers and hence, stop the certificate enrollment for these servers. To avoid this, create a domain global group, add the IAS member server accounts to this group, and add this group to the GPO access control list (ACL), granting it **Apply** and **Read** permissions.

Verifying CA Configuration

The following procedure confirms that you have configured the CA correctly. The script verifies that:

- The CA has the correct validity period (for issued certificates).
- The CRL publishing period is correct.
- The CA has the Computer certificate template assigned.
- The Automatic Certificate Request (Autoenrollment) GPO has been successfully imported into the domain.

These values are checked against the settings stored in the PKIParams.vbs file. The script does not check for absolute values; it only checks if the settings have been configured on the CA correctly.

▸ **To verify the CA configuration**

1. Use the **MSS WLAN Tools** shortcut to open a command shell.
2. AT the command prompt, type the following to configure the CA components:

   MSSsetup VerifyCAConfig, and then press **ENTER**.

If the script output shows any failures, you should retrace the steps in this chapter and rectify the indicated problems.

Summary

This chapter guided you through the installation process of a special purpose CA to issue server certificates to IAS servers. The CA configuration used is designed to be extremely low maintenance and therefore, should require minimum management in the future. However, the operational and support information that you may require is included in Chapter 8, "Maintaining the Secure Wireless LAN Solution."

You are now ready to install the IAS servers. This will be covered in Chapter 5, “Building the Wireless LAN Security Infrastructure."

References

This section provides references to important supplementary information or other background material relevant to the content of this chapter.

- For introduction to PKI concepts and the features of Windows 2000 Certificate Services, see the paper entitled, “An Introduction to the Windows 2000 Public-Key Infrastructure,” available at the following URL:

  http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/pkiintro.asp

- For introduction to PKI concepts and the features of Windows 2000 Certificate Services, see the paper entitled, “An Introduction to the Windows 2000 Public-Key Infrastructure,” available at the following URL:

  http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp

- For background product documentation that discusses key concepts and administration tasks, see the "Certificate Services" section in the Windows Server 2003 product documentation available at the following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/SE_PKI.asp

- For guidance on how to obtain and use certificates from a commercial CA, see the article "Obtaining and Installing a VeriSign WLAN Server Certificate for PEAP-MS-CHAP v2 Wireless Authentication," available at the following URL:

  http://download.microsoft.com/download/9/f/d/9fd73f17-2fdf-4409-b2d2-31437c7f29f3/WLANCertEnroll.doc

5

Building the Wireless LAN Security Infrastructure

Overview

This chapter provides guidance on the installation and configuration of Internet Authentication Service (IAS) to provide Remote Access Dial-In User Service (RADIUS) services to a wireless local area network (WLAN), and the configuration of wireless access points (APs) to use the IAS RADIUS services.

The principal topics in the chapter are as follows:

- Preparing for and installing IAS
- Configuring the first IAS server
- Replicating settings to other IAS servers
- Adding wireless APs as RADIUS clients of IAS
- Configuring the wireless APs

The procedures in this chapter are less automated than the procedures in the earlier chapters. Although IAS is configurable programmatically, many settings cannot be configured using Windows® Scripting Host or available command-line tools. Compiled application code is usually less accessible to non-developers than scripts. So, where a procedure was not scriptable, the manual steps to complete that procedure were used. If you want to automate the configuration of IAS using the Server Data Objects interface, refer to MSDN® at http://msdn.microsoft.com. For the exact location of the information on the subject, see the references at the end of this chapter.

The configuration steps in this chapter are largely manual; however, there are some positive aspects to this. First, the IAS administration interface is easy to use and is often driven by configuration wizards. Second, you will normally perform the configuration steps only on one server and then replicate these settings to the other IAS servers using simple commands. Third, performing these steps manually helps you to learn more about the installation and configuration of IAS. This last point is more relevant here than for the other components of the solution. IAS is the hub around which the rest of the solution revolves, so it is desirable to have some experience of administering and configuring it.

Chapter Prerequisites

Before implementing the instructions provided in this chapter, you should have read and implemented the procedures in Chapter 3, "Preparing Your Environment" and Chapter 4, "Building a Network Certification Authority." You should have also read Chapter 2, "Planning a Wireless LAN Security Implementation," and understood the architecture and design of this solution.

In addition, it will help if you are familiar with following topics:

- IAS and RADIUS
- WLAN concepts

Preparing for Implementation

Permissions Needed

To carry out the procedures in this chapter, you need to log on with an account that is a member of the Administrators group for the domain into which you are installing the IAS servers.

Note: If you are not installing IAS on domain controllers, you will only need to be a member of the local Administrators group on each IAS server to install and configure IAS. You will also need to have permissions to modify the membership of the RAS and IAS Servers group for the domain into which you are installing IAS server.

Tools Needed

The following tools are needed to perform the procedures in this chapter.

Table 5.1: Tools Needed

Tool	Description	Source
MSS Secure WLAN Scripts	The set of scripts and tools supplied with this solution.	Provided in the Chapter3, "Preparing Your Environment."
Internet Authentication Service	Microsoft® Management Console (MMC) tool used to manage IAS policies and settings.	Provided as part of Windows Server™ 2003.
Active Directory Users and Computers	MMC tool used to manage the Microsoft Active Directory® directory service users, groups, computers, and other Active Directory objects.	Provided as part of Windows Server 2003.

13.

IAS Parameters

The following table lists the main parameters used in the installation and configuration of the IAS server.

Table 5.2: IAS Server Configuration Parameters

Configuration Item	Setting
IAS Logging to Windows Event Log	
Rejected Authentication Requests	Enabled
Successful Authentication Requests	Enabled
IAS RADIUS Logging	Disabled
Remote Access Policy	
Remote Access Policy Name	Allow Wireless LAN Access
Security group to grant access to	Wireless LAN Access
EAP Type used	Protected Extensible Authentication Protocol (PEAP)
PEAP EAP type used	EAP MS-CHAP v2
Fast Reconnect	Enabled
Remote Access Policy Profile	
Minutes clients can be connected (Session-Timeout)	60 minutes This may be reduced to 15 minutes for 54 Mbps 802.11a/g WLANs
RADIUS Attributes	Ignore-User-Dialin-Properties = "True" Termination Action = "RADIUS-Request"
Connection Request Policy	
Policy Name	Use Windows authentication for all users
Policy Conditions	Day-and-Time-Restrictions = All times

14.

Important: These settings were used in the internal testing of this solution and are known to work as documented. Although many of these can be set to other values, you should do this only if you are confident that you fully understand the purpose of a particular setting and the implications of changing it.

Checking Readiness for Installation

IAS is dependent on correct network and Active Directory configuration and connectivity. Several tools are required for the successful installation and maintenance of IAS.

Validating the IAS Environment

Before installing IAS on the server, you must run a series of checks to ensure that a domain controller is contactable and that all the required tools have been installed as per the procedures described in Chapter 3, "Preparing Your Environment." The following procedure uses a script to perform these checks automatically for you.

▸ **To check the IAS environment**

1. Open a command shell using the **MSS WLAN Tools** shortcut on the server on which you want to install IAS.
2. Run the following command:

```
MSSSetup CheckIASEnvironment
```

3. The script confirms the name of the domain to which this server belongs. Click **OK** to accept.

4. After completing the checks, a dialog box displays indicating success or failure of each check. Click **OK** to close the dialog box.
5. If all the checks completed successfully, continue with the next procedure. Otherwise, check the setup log (**%systemroot%\debug\MSSWLAN-Setup.log**) to investigate the cause of the failure and rectify the problem before rerunning the script.

Verifying DHCP Settings

Dynamic Host Configuration Protocol (DHCP) will be used to assign IP addresses to the WLAN clients automatically. Ensure that the DHCP scopes assigned at each site have enough IP addresses to cover the maximum number of WLAN clients that may be active at the site. If the scope is shared with wired clients, it must be large enough to accommodate both sets of clients.

Organizations with large numbers of WLAN clients or which have WLAN clients that regularly move from site to site, should configure separate scopes for WLAN clients. Having separate scopes allows you to specify very short lease times for these clients (for example, eight hours or less) and hence helps prevent transient WLAN clients quickly exhausting the available IP addresses. To do this, place the WLAN clients on a separate subnet from the rest of the site network, and configure a router or layer 3 switch to connect the subnets.

For smaller or relatively static environments, sharing an IP subnet and a single DHCP scope between wired and WLAN clients is quite acceptable.

For more information, see the "Deploying a Wireless LAN" chapter of the *Windows Server 2003 Deployment Kit*. The reference for this is given at the end of this chapter.

Installing IAS

This section describes how to install IAS on your server.

Installing the IAS Software Components

You can install the IAS software components using a script provided with this guidance. This script uses the Windows Optional Components Installation Manager to install IAS, and builds all the required configuration files as it runs.

▸ **To install IAS**

1. Open a command shell using the **MSS WLAN Tools** shortcut.
2. Run the following command to install the IAS software components:

```
MSSetup InstallIAS
```

3. The script then builds the installation parameter file. When this is complete, you are prompted to continue with the installation. The Windows Server 2003 installation CD (or network path containing the Windows installation source) is required to complete the installation. Click **OK** to proceed or **Cancel** to stop the installation before it is finished.

Note: If you choose to cancel the installation, the IAS optional components parameter file (OC_IAS.txt) will be left in the current working folder. This can be modified and used in your custom installation if you do not want to accept the solution defaults.

---

4. When the installation completes, a confirmation message will be displayed. Click **OK**.

Verifying the Installation

To verify the installation, click **Start,** point to **All Programs,** point to **Administrative Tools,** and click on **Internet Authentication Service**. IAS should be shown as installed and running on the server.

Registering IAS in Active Directory

Each IAS server needs to be registered in Active Directory. Registering means adding the IAS server computer account to the RAS and IAS Servers security group, which ensures that IAS servers have permission to read the remote access properties of user and computer accounts in Active Directory.

You can register your servers in one of the following ways:

- By adding these servers manually into the group (using **Active Directory Users and Computers**).
- By using the **Register with Active Directory** item on the **Action** menu of the **Internet Authentication Service** MMC.
- By using the **Netsh** command.

The last method (using **Netsh** command) is shown here because it is simple to script and allows the server to be registered in other domains.

▸ **To register IAS in the default domain**

1. Log on to the IAS server and open a command shell using the **MSS WLAN Tools** shortcut.
2. Run the following command:

```
netsh ras add registeredserver
```

If you have multiple domains, perform the following procedure for each domain that has users or computers that will be authenticated by this IAS server. For example, if your IAS servers are installed in domain A and you have WLAN users in domain B, you must register the IAS servers in domain B as well as domain A. To do this, you need to have permission to modify the RAS and IAS Servers group membership in the target domain.

▸ **To register IAS in domains other than the default domain**

1. At the command prompt, run the following command, replacing *DomainName* with the name of the domain in which the IAS server needs to be registered:

```
netsh ras add registeredserver domain = DomainName
```

Note: Alternatively, add the IAS server computer object directly into the RAS and IAS Servers security group in the target domain using **Active Directory Users and Computers**.

Configuring the Primary IAS Server

This section provides guidance on configuring the first IAS server. Subsequent IAS servers will be configured by replicating the settings from this server using the procedures described later in the chapter.

Automatically Enrolling for an IAS Server Certificate

Chapter 4, "Building the Network Certification Authority," provided the steps for installing a Group Policy object (GPO) to allow members of the RAS and IAS Servers group to enroll computer certificates automatically. The registration of the IAS server in Active Directory causes the server account to be added to this group. However, the server needs to be restarted for the computer to have this group membership added to its logon token and be able to enroll a certificate successfully.

Note: Just as with users, computers do not receive changed group membership in their logon session access token until they log on to the domain again. For computers, this occurs at boot time.

Before continuing with the next procedure, restart the server.

Warning: Before restarting the server, ensure that no tasks are being performed on this server. If the server is a domain controller, ensure that another domain controller is available to users before restarting this one. You should also avoid restarting during a critical system task such as server backup.

Verifying IAS Server Certificate Deployment

After restarting the server, ensure that the IAS server certificate has been successfully enrolled.

- **To verify the IAS server authentication certificate**

1. Open a command shell using the **MSS WLAN Tools** shortcut.
2. Run the following command to open the **Certificates** MMC:

```
ComputerCerts.msc
```

3. In the console tree, double-click **Certificates (Local Computer)** and then double-click **Personal**. Next, click **Certificates**.
4. You should see at least one certificate with the name of this server in the **Issued To** column and the name of your certification authority (CA) in the **Issued By** column. Scroll across the list (to the right) to view the **Certificate Template** column. You should see the value **Computer** for this certificate in this column.

   Note: If this is the first IAS server and it is being installed on the same server as the CA, you will also see another certificate with the name of the CA in both columns; this is the self-signed CA certificate.

   ---

5. If the required certificate does not appear in the **Certificates** MMC snap-in, select **Certificates (Local Computer)** from the console tree (in the left pane), click **All Tasks** from the **Action** menu, and then click **Automatically Enroll Certificates**. Then refresh the view of the **Certificates** MMC.

Configuring the First IAS Server

The configuration of all the IAS servers will be largely identical in this solution (though the set of wireless APs installed on each server will usually be different for each server). To keep the configuration synchronized between servers, and to minimize the effort of managing multiple servers, you will perform the majority of configuration tasks on the first installed IAS server and then replicate this server's settings to other IAS servers in the organization.

During the procedures in this section, you will configure the following types of setting on the first IAS server:

- Logging of Requests
- Remote Access Policy
- Connection Request Settings

Later, these settings will be replicated to the other IAS servers. You must also add a RADIUS client entry to IAS for each wireless AP served by that IAS server (this is covered in the "Configuring Wireless Access Points" section, later in this chapter).

Configuring Logging to Windows Event Logs

IAS logs significant system-level events such as service startup and shutdown and problems such as configuration errors and service failures to the Windows system log. It can also optionally log successful and failed authentication attempts.

To enable IAS logging of authentication requests

1. To open the **Internet Authentication Service** MMC, click **Start,** point to **All Programs,** point to **Administrative Tools,** and click **Internet Authentication Service**.
2. Right-click **Internet Authentication Service (local)** and then select **Properties**.
3. Ensure that the **Rejected authentication requests** and **Successful authentication requests** are both enabled.
4. Click **OK**.

Configuring Logging of Authentication and Accounting Requests to RADIUS Logs

IAS can also log authentication and accounting information to RADIUS logs. IAS does not create RADIUS logs by default and RADIUS logging is not enabled in this solution in order to minimize management overhead.

If you require RADIUS logging for security auditing or accounting purposes, either or both types of request logs can be enabled. IAS can write these logs to text files or to a SQL database. You can use these logs as input to security monitoring systems to help you track potential security violations. More rarely, organizations use the accounting logs for billing purposes although this is typically confined to commercial Internet and other Network service providers. If you want to implement RADIUS logging or simply read more about it, see the references at the end of this chapter.

Note: You should not enable RADIUS authentication and account logging unless you have a specific need for it. It can degrade server performance and the log files also need regular housekeeping to ensure that they do not fill the server disks.

Creating an IAS Remote Access Policy for WLAN

Perform the following procedure to create a remote access policy on the IAS server.

To create a remote access policy in IAS

1. Open the **Internet Authentication Service** MMC by clicking **Start,** pointing to **All Programs,** pointing to **Administrative Tools,** and clicking **Internet Authentication Service**.
2. Right-click the **Remote Access Policies** folder and then click **New Remote Access Policy**. Click **Next** to continue.

3. Select **A typical policy for a common scenario** as the way you want to set up the policy and name it **Allow Wireless LAN Access**. Click **Next**.
4. Select **Wireless** for the access method.
5. Select the **Group** option for **Grant access based on**, and type in (or browse for) the Wireless LAN Access security group. Click **Next** to continue.
6. Select **Protected EAP (PEAP)** from the list of EAP types.
7. Click the **Configure…** button. The IAS server certificate issued earlier should be displayed in the **Certificate Issued** field (if not, select it from the list of available certificates). **Secured Password (EAP MSCHAPv2)** should be displayed in the list of **EAP Types**. Check the **Enable Fast Reconnect** check box.

Important: If you are using Pocket PC 2003 Wireless clients, you must not check the **Enable Fast Reconnect** check box unless you have a version of Pocket PC that supports this option (see the Knowledge Base article reference at the end of this chapter). If you enable Fast Reconnect, the Pocket PC clients will not be able to reconnect to the network after their initial authentication times out.

8. Click **OK** and then **Next.** Click **Finish** to complete the procedure.

Important: The new **Allow Wireless LAN Access** policy can coexist with other remote access policies that you have created or with the default remote access policies. However, you must ensure that any other default remote access policies are either deleted or listed below (at a lower priority) the **Allow Wireless LAN Access** policy in the **Remote Access Policies** folder of IAS.

Modifying the WLAN Access Policy Profile Settings

The **New Remote Access Policy** wizard (as used in the previous procedure) creates a valid remote access policy but the following two settings need to be configured manually. The first setting adds the RADIUS attribute **Ignore-User-Dialin-Properties**. This tells IAS to ignore the remote access permission setting specified on the **Dial-In** tab of the Active Directory user object. It also prevents IAS from sending this information in the RADIUS responses to the wireless APs because this can sometimes cause compatibility problems.

The second category allows the IAS server to terminate the client connection after a specified time-out and force the client to re-authenticate. These settings are particularly important when using dynamic Wired Equivalent Privacy (WEP) data protection (the default for this solution). The session time-out controls the frequency at which new network data encryption keys are generated.

Note: Wi-Fi Protected Access (WPA) has its own mechanism to generate new keys for each transmitted packet. The following discussion is not applicable to WPA WLANs.

The session time-out value is a tradeoff between security and reliability. 60 minutes time-out gives adequate security for most circumstances and certainly for 11 Mbps 802.11b networks. Normally, wireless clients will never transmit enough data in 60 minutes to allow a dynamic WEP key to be recovered by an attacker. Faster WLANs using the 802.11a or 802.11g 54 Mbps standards allow more data to be transmitted in a given time; you should consider using a 15 minute time-out for faster WLANs. However, using a shorter value can reduce WLAN reliability and increase the load on the IAS servers.

You should read the section "Security Options for Dynamic WEP" in Chapter 2, “Planning a Wireless LAN Security Implementation” for a more detailed discussion on setting the client session time-out.

You must configure the value for client session timeout and the **Termination-Action** attribute of RADIUS to the required value so that the IAS server can force the client to re-authenticate at the required interval. For more information about remote access policy settings, see the "RADIUS Policies" section of Chapter 2, "Planning a Wireless LAN Security Implementation."

- **To modify the wireless access policy profile settings**

1. In the **Internet Authentication Service** MMC, right-click **Allow Wireless LAN Access** policy and select **Properties**. Then click **Edit Profile**.
2. Click the **Dial-in Constraints** tab, then select the **Minutes clients can be connected (Session-Timeout)** option and type **60** (minutes) as the value if you are using an 802.11b (11 Mbps) WLAN or **15** (minutes) for a higher speed 802.11a or g (54 Mbps) WLAN.

> **Note:** If you are using WPA WLAN protection in place of dynamic WEP, set this value to eight hours. A setting of eight hours will ensure that clients have valid up-to-date credentials for a reasonable length of time. At the same time, it ensures that a client cannot remain connected for excessive periods after its account has been disabled. However, in very high security environments where you need to minimize the delay between disabling an account and forcing the client off the network, this value may be reduced to one hour.

3. Click the **Advanced** tab, add the **Ignore-User-Dialin-Properties** attribute, and set it to **True.** Then add the **Termination-Action** attribute and set it to **RADIUS Request**.

Verifying the Connection Request Policy for WLAN

The default IAS connection request policy is configured to instruct IAS to authenticate users and computers directly against Active Directory. Perform the following steps to verify the configuration of the default connection request policy.

- **To verify configuration of the default connection request policy**

1. Open the **Internet Authentication Service** MMC; navigate to the folder **Connection Request Processing\Connection Request Policies** and right-click **Use Windows authentication for all users** connection request policy. Then select **Properties**.
2. Verify that the policy conditions contains **Date-And-Time-Restrictions matches “Sun 00:00-24:00; Mon 00:00-24:00; Tue 00:00-24:00; Wed 00:00-24:00; Thu 00:00-24:00; Fri 00:00-24:00; Sat 00:00-24:00.”**
3. Click the **Edit Profile** button and ensure that **Authenticate requests on this server** is selected on the **Authentication** tab.
4. Ensure that no rules are specified on the **Attribute** tab.

Deploying Settings to Multiple IAS Servers

After configuring the primary IAS server, you can replicate this configuration to the other IAS servers.

Follow the procedures earlier in this chapter for "Installing IAS" and "Registering IAS in Active Directory" on each of your additional servers. You should also carry out the procedure for "Verifying IAS Server Certificate Deployment" to ensure that a certificate has been enrolled by each of the new servers. Having done this, you are ready to export the IAS settings from the first server and import them into your other servers as described in the procedures in the following section.

Important: You can only replicate settings to other Windows Server 2003 IAS servers. Using these procedures, you cannot replicate settings from Windows Server 2003 to Windows 2000 versions of IAS.

Replicating Settings from the First IAS Server

You can use the **Netsh** command to export portions of IAS configuration to text files. The scripts used in the following procedures make use of Netsh.exe to export settings from and import them into an IAS server.

The following categories of IAS settings can be separately exported from and imported into an IAS server:

- Server settings
- Logging configuration
- Remote access policies
- Connection request policies
- RADIUS clients
- Full configuration (this includes all the above)

Exported settings are stored in text files, however the data is encoded. These text files can be used to transfer common configuration settings across multiple IAS servers to ensure consistent configuration and speedy deployment.

Most of the configuration categories will be common to IAS servers in a similar role (the exception typically being the RADIUS clients' category). In this solution, the IAS servers will be authenticating only WLAN clients. If you are planning to use one or more of the IAS servers differently, (for example, to authenticate remote access clients) you need to configure and replicate settings of those servers independently or perform the configuration manually. Otherwise, you risk overwriting and losing policy and other configuration settings.

You should perform configuration of the following items only on the first IAS server (as described in the earlier section "Configuring IAS").

- Server configuration
- Logging settings
- Remote access policies
- Connection request polices

Using the procedures in this section will export these settings and replicate them to other IAS servers.

Tip: To help you track changes to the IAS configuration, include a version number in the name of the remote access policy. Each time you change the IAS settings, update the name to include a new version number. This will make it is easier to track changes across the IAS servers and see that they are all using the same settings.

Designate your first IAS server as the "master" IAS server. Then use the following procedures to replicate the settings from this server to the other IAS servers in your organization. The replication of RADIUS client settings is detailed in the "Replicating RADIUS Client Configuration to Other IAS Servers" section later in this chapter.

Note: The "Master" designation has no special meaning to IAS. It is only used to indicate which server you will use to make the initial configuration changes before they are replicated to the other IAS servers.

Exporting Settings from the Master IAS Server

This procedure saves the current IAS server settings to disk files.

► **To export the IAS configuration to disk files**

1. Log on to the primary IAS server and open a command shell using the **MSS WLAN Tools** shortcut.
2. If required, identify a folder to store the output files or insert a blank, formatted floppy disk into the server's drive.
3. Run the following command to export the IAS configuration:

   ```
   MSSTools ExportIASSettings [/path:OutputFolder]
   ```

   OutputFolder is an optional parameter used to specify the folder to which the exported files will be written. The path needs to be in quotes if it contains embedded spaces. This folder, if specified, must exist otherwise the files are written to the current directory.
4. The script will create the following files:
   - IAS_Server_Settings.txt
   - IAS_Logging.txt
   - IAS_Rem_Access_Policies.txt
   - IAS_Con_Request_Policies.txt
5. Store the files to import them into the other servers.

Importing Settings to Other IAS Servers

This procedure uses the settings files exported in the previous procedure to configure other IAS servers with identical settings. This procedure does not import the RADIUS clients, which is covered in a later section.

Warning: The import of IAS settings to an IAS server will overwrite all existing IAS settings on that server (with the exception of the RADIUS client information). If you have created different settings on any server (for example, different remote access policies to support virtual private network (VPN) clients), do not use this procedure to import the IAS WLAN settings to that server. Instead, configure the settings manually using the procedures described in the "Configuring the Primary IAS Server” section earlier in this chapter.

To import IAS configuration from disk files

1. Log on to the target IAS server and open a command shell using the **MSS WLAN Tools** shortcut.
2. Identify the folder containing the configuration files previously exported from the master IAS server.
3. Run the following command to import the IAS configuration:

   ```
   MSSTools ImportIASSettings [/path:IntputFolder]
   ```

   InputFolder is an optional parameter used to specify the folder where the script will look for the settings files to import. The path needs to be in quotes if it contains embedded spaces. If no folder is specified, the files are expected to be in the current directory.

You should verify that the settings have been imported correctly by opening the **Internet Authentication Service** MMC and checking the remote access and connection request policy settings.

Configuring Wireless Access Points

This section describes how to add wireless APs as RADIUS clients of the IAS servers.

Adding the Access Points as RADIUS Clients to IAS

You must add wireless APs as RADIUS clients to IAS before they are allowed to use RADIUS authentication and accounting services. For more information on how to allocate wireless APs to different IAS servers, see the procedures in Chapter 2, "Planning a Wireless LAN Security Implementation."

The wireless APs at a given location will typically be configured to use an IAS server at the same location for their primary RADIUS server and another IAS server at the same or a different location as the secondary RADIUS server. The terms "primary" and "secondary" here do not refer to any hierarchical relationship, or difference in configuration, between the IAS servers themselves. The terms are relevant only to the wireless APs, each of which has a designated primary and secondary (or backup) RADIUS server. Before you configure your wireless APs, you must decide which IAS server will be the primary and which will be the secondary RADIUS server for each wireless AP.

The following procedures describe adding RADIUS clients to two IAS servers. During the first procedure, a RADIUS secret is generated for the wireless AP; this secret, or key, will be used by IAS and the AP to authenticate each other. The details of this client along with its secret are logged to a file. This file is used in the second procedure to import the client into the second IAS.

Important: You must not use this first procedure to add the same client to two IAS servers. If you do this, the client entries on each server will have different RADIUS secret configured and the wireless AP will not be able to authenticate to both servers.

Adding Access Points to the First IAS Server

This section describes the adding of wireless APs to the first IAS server. A script is supplied to automate the generation of a strong, random RADIUS secret (password) and add the client to IAS. The script also creates a file (defaults to Clients.txt) that logs the details of each wireless AP added. This file records the name, IP address, and RADIUS secret generated for each wireless AP. These will be required when configuring the second IAS server and wireless APs.

If you prefer to add the clients manually, follow the "Generating the client's entries for wireless APs" procedure later in this chapter, to generate secrets for the wireless APs.

Important: The RADIUS clients are added to IAS as "RADIUS Standard" clients. Although this is appropriate for most wireless APs, some APs may require that you configure vendor–specific attributes (VSA) on the IAS server. You can configure VSAs either by selecting a specific vendor device in the properties of the RADIUS clients in the **Internet Authentication Service** MMC or (if the device is not listed) by specifying the VSAs in the IAS remote access policy. For more information on configuring VSAs in IAS, see the references at the end of this chapter.

In addition, refer to your wireless AP documentation for information regarding VSA requirements on RADIUS servers.

▸ **To add a RADIUS client to the first IAS server**

1. Log on to the IAS server where you want to add the wireless APs and open a command shell using the **MSS WLAN Tools** shortcut.
2. If there is an existing RADIUS–clients output file in the current directory (or if you specify an existing file in the path parameter), the new client entry will be appended to that file. If you do not want this to happen, please remove the existing file or specify an alternative file name in the command.
3. Run the following command to add a wireless AP to IAS:

   MSSTools AddRADIUSClient [**/path:***OutputFile.txt*]

   Note: The *path* parameter is optional. You can specify the name of the file (plus optional folder path) in which the output from the command will be stored. The path needs to be in quotes if it contains embedded spaces. If no path parameter is specified, the command will save the output in the file Clients.txt in the current directory.

4. When prompted, type a name for the wireless AP. This should be a user-friendly reference in the **Internet Authentication Service** MMC; it does not need to be the name given to it in the wireless AP configuration. Use a Domain Name System (DNS) name or any other string.
5. Type the IP address of the wireless AP (in decimal dotted notation, for example, 10.20.1.153).
6. A password is automatically generated for the client (this password is a randomly generated cryptographic string of 23 printable characters used by IAS and the wireless AP to authenticate each other). These settings are used to add the RADIUS client to IAS. The name, IP address, and secret are also appended to the output file (default is Clients.txt) in the current directory. The output file is a comma–delimited text file with one RADIUS client on each line, so it can be easily used in scripts or imported and manipulated using a tool such as Microsoft Excel.
7. Repeat steps 3 to 6 for all other wireless APs that you want to add to this IAS server.

Later, you will use the output file for reference while setting the RADIUS secrets on the wireless APs. For more information, see the "Configuring the Wireless Access Points" section later in this chapter.

Important: Do not leave the RADIUS clients output file on the server. It contains the RADIUS client secrets in unencrypted form. After adding the wireless APs, you should move the file to a floppy disk or other writable, removable media and store it in a secure place.

The "Adding a RADIUS client to the first IAS server" procedure described above uses a sample tool included with this solution (AddRADIUSClient.exe*)*. This tool is a simple Visual Basic.NET application, which uses the Server Data Objects interface to configure an IAS server. You can use it to write your own script to add clients to IAS server.

This tool is not supported by Microsoft and has not been thoroughly tested. However, the source code of this application is included should you need to examine or modify it before using it.

Note: Unlike most of the scripts used in the setup procedures, this script does not write progress details to the MSSWLAN-setup.log log file. The reason for this is to prevent the RADIUS client secrets being stored there and posing a security risk. However, the progress details are logged to the screen.

Scripting the Addition of Access Points to IAS Server (Alternative Procedure)

If you do not want to add the wireless APs to the IAS server interactively using the previous procedure, you can just generate the RADIUS client entries output files for each wireless AP without adding them to IAS. You can then use the "Importing the RADIUS clients to the second IAS server" procedure described later in this section to import the RADIUS client entries into both the first IAS server and the second IAS server. Because you can script this whole operation, you may prefer to add your RADIUS clients this way if you have to add a large number of wireless APs.

Important: This procedure is an alternative method for adding RADIUS clients in a scripted rather than an interactive fashion. If you have followed the previous procedure "Adding a RADIUS client to the first IAS server," you do not need to follow this procedure.

Use the following procedure to generate strong RADIUS secrets. The script, like the previous procedure, uses a CryptoAPI function to generate a truly random value for each RADIUS secret. This ensures that the values are sufficiently strong to defeat password guessing or dictionary attacks.

► **To generate the clients entries file for wireless APs**

1. Open a command shell using the **MSS WLAN Tools** shortcut.
2. Run the following command. Substitute a user-friendly name of the wireless AP for the *ClientName* parameter and the IP address of the wireless AP for *IPAddress*. (You can optionally provide an alternative file name and path to specify where the output is to be saved. If no path parameter is specified, the output is saved to the file Clients.txt in the current working folder.) If the output file already exists, the new value will be appended to it. If it does not exist, the file will be created.

   ```
   MSSTools GenRADIUSPwd /client:ClientName /IP:IPaddress
   [/path:path\filename]
   ```

   The "client" and the "path" parameters can include embedded spaces; if either does, you must enclose the parameter in quotes. The command may be shown wrapped on to multiple lines but you should type it on a single line.

3. Repeat step 2 for all wireless APs for which you need to generate RADIUS secrets. Each client entry will be appended to the output file (default is Clients.txt). The file is a comma-delimited text file with one RADIUS client on each line, so it can be easily used in scripts or imported and manipulated using a tool such as Microsoft Excel.

Caution: Do not leave the output file on the server. It contains the RADIUS client secrets in plaintext. After adding the wireless APs, you should move the file to a floppy disk or other writable, removable media and store it in a secure place.

Note: Unlike most of the scripts used in the setup procedures, this script does not write progress details to the MSSWLAN-setup.log log file. This is to prevent the RADIUS client secrets being stored there and posing a security risk. However, the progress details are logged to the screen.

Importing the Access Points into the Second IAS Server

After adding the wireless APs to the first IAS server, you need to add them to a second server before configuring the wireless APs to use RADIUS.

- **To import the RADIUS clients to the second IAS server**

1. Copy the clients output file created in the previous procedures (for security reasons, remove this file from the first IAS server altogether—it is no longer required there).
2. Verify that the file contains the correct entries by opening and viewing in Notepad or Microsoft Excel. (This is important because the file might contain old entries left over from a previous run of the procedure). Remove any unnecessary client entries.
3. Run the following command to import these clients into the second IAS server:

```
MSSTools AddSecRADIUSClients [/path:InputFile.txt]
```

Note: The *path* parameter is optional. You can use a different path parameter to read the input from a different file or folder. The path needs to be in quotes if it contains embedded spaces. If no parameter is specified, the command will look for and read input from the file Clients.txt in the current directory.

4. The script will reject any malformed client entries in the file and display the number of successful and failed entries when completed.
5. Verify that the clients have been added correctly by opening the **Internet Authentication Service** MMC and looking at the **RADIUS Clients** folder.

Note: Unlike most of the scripts used in the installation and configuration of the solution, this script does not write progress details to the MSSWLAN-setup.log file. The reason for this is to prevent the RADIUS client secrets being stored there and posing a security risk. However, the progress details are logged to the screen.

Configuring the Wireless Access Points

Having added RADIUS clients entries for the wireless APs to IAS, you now need to configure the wireless APs themselves. You must add the IP addresses of the IAS servers and the RADIUS client secrets that each AP will use to communicate securely with the IAS servers. Every wireless AP will be configured with a primary and secondary (or backup) IAS server. You should perform the procedures in this section for the wireless APs at every site in your organization. For more information on how to allocate wireless

APs to your IAS servers, please refer to Chapter 2, "Planning a Wireless LAN Security Implementation."

The procedure for configuring wireless APs varies depending on the make and model of the device. However, wireless AP vendors normally provide detailed instructions for configuring their devices. Depending on the vendor, these instructions may also be available online.

Prior to configuring the security settings for your wireless APs, you must configure the basic network settings. These will include but are not limited to:

- IP Address and subnet mask of the wireless AP
- Default gateway
- Friendly name of the wireless AP
- Wireless Network Name (SSID)

This list will include a number of other parameters that affect the deployment of multiple wireless APs: settings that control the correct radio coverage across your site for example, 802.11 Radio Channel, Transmission rate, and Transmission power, and so forth. Discussion of these parameters is outside the scope of this guidance. Use the vendor documentation as a reference when configuring these settings or consult a network services supplier. For more information on deploying wireless APs, see the references at the end of this chapter.

The guidance in this chapter assumes that you have set these items correctly and are able to connect to the wireless AP from a WLAN client using an unauthenticated connection. You should test this before configuring the authentication and security parameters listed in the following sections.

Enabling Secure WLAN Authentication on Access Points

You must configure each wireless AP with a primary and a secondary RADIUS server. The wireless AP will normally use the primary server for all authentication requests, and switch over to the secondary server if the primary server is unavailable. As discussed in Chapter 2, "Planning a Wireless LAN Security Implementation," it is important that you plan the allocation of wireless APs and carefully decide which server should be made primary and which should be made secondary. To summarize:

- In a site with two (or more) IAS servers, balance your wireless APs across the available servers so that approximately half of the wireless APs use server 1 as primary and server 2 as secondary, and the remaining use server 2 as primary and server 1 as secondary.
- In sites where you have only one IAS server, this should always be the primary server. You should configure a remote server (in the site with most reliable connectivity to this site) as the secondary server.
- In sites where there is no IAS server, balance the wireless APs between remote servers using the server with most resilient and lowest latency connectivity. Ideally, these servers should be at different sites unless you have resilient wide area network (WAN) connectivity.

The following table lists the settings that you need to configure on your wireless APs. Although the names and descriptions of these settings may vary from one vendor to another, your wireless AP documentation helps you determine those that correspond to the items in the table.

Table 5.3: Wireless Access Point Configuration

Item	Setting
Authentication Parameters	
Authentication Mode	802.1X Authentication
Re-authentication	Enable
Rapid/Dynamic Re-keying	Enable
Key Refresh Time-out	60 minutes
Encryption Parameters (these settings usually relate to static WEP encryption)	(Encryption parameters may be disabled or be overridden when rapid re–keying is enabled)
Enable Encryption	Enable
Deny Unencrypted	Enable
RADIUS Authentication	
Enable RADIUS authentication	Enable
Primary RADIUS authentication server	Primary IAS IP Address
Primary RADIUS server port	1812 (default)
Secondary RADIUS authentication server	Secondary IAS IP Address
Secondary RADIUS server port	1812 (default)
RADIUS authentication shared secret	**XXXXXX** (replace with generated secret)
Retry Limit	5
Retry timeout	5 seconds
RADIUS Accounting	
Enable RADIUS accounting	Enable
Primary RADIUS accounting server	Primary IAS IP Address
Primary RADIUS server port	1813 (default)
Secondary RADIUS accounting server	Secondary IAS IP Address
Secondary RADIUS server port	1813 (default)
RADIUS accounting shared secret	**XXXXXX** (replace with generated secret)
Retry Limit	5
Retry timeout	5 seconds

15.

Important: The **Key Refresh Time-out** is set to 60 minutes for use with dynamic WEP. The **Session Timeout** value set in the IAS remote access policy is the same or shorter than this. For more information, see the earlier section "Modifying the WLAN Access Policy Profile Settings." Whichever of these has the lower setting will take precedence, so you only need to modify the setting in IAS. If you are using WPA, you should increase this setting in the AP to eight hours. Consult your vendor's documentation for more information.

Use the same RADIUS secrets generated in the "Adding a RADIUS client to the first IAS server" procedure to add wireless APs to IAS. Although you may have not yet configured a secondary IAS server as a backup to the primary server, you can still add the server's IP address to the wireless AP now (to avoid having to reconfigure it later). Configuring additional IAS servers is discussed in a later section of this chapter.

Depending on the wireless AP hardware model, you may not have separate configurable entries for Authentication and Accounting RADIUS servers. If you have separate configurable entries, set them both to the same server unless you have a specific reason for doing otherwise.

The RADIUS retry limit and timeout values given in the table are common defaults but these values are not mandatory.

Note: If you are currently using wireless APs with no security enabled or only static WEP, you need to plan your migration to an 802.1X–based WLAN. For more information about migration from an existing wireless network, see the "Migration from an Existing WLAN" section of Chapter 2, "Planning a Wireless LAN Security Implementation."

Additional Settings to Secure Wireless Access Points

In addition to enabling 802.1X parameters, you should also configure the wireless APs for highest security. Most network hardware is supplied with insecure management protocols enabled and administrator passwords set to well-known defaults, which poses a security risk. You should configure the settings listed in the following table; however, this is not an exhaustive list. You should consult your vendor's documentation for authoritative guidance on this topic. When choosing passwords and community names for Simple Network Management Protocol (SNMP), use complex values that include upper and lowercase letters, numbers, and punctuation characters. Avoid choosing anything that can be guessed easily from information such as your domain name, company name, and site address.

Table 5.4: Wireless Access Point Security Configuration

Item	Recommended Setting	Notes
General		
Administrator password	XXXXXX	Set to complex password.
Other management passwords	XXXXXX	Some devices use multiple management passwords to help protect access using different management protocols; ensure that all are changed from the defaults to secure values.
Management Protocols		
Serial Console	Enable	If no encrypted protocols are available, this is the most secure method of configuring wireless APs although this requires physical serial cable connections between the wireless APs and terminal and hence cannot be used remotely.
Telnet	Disable	All Telnet transmissions are in plaintext, so passwords and RADIUS client secrets will be visible on the network. If the Telnet traffic can be secured using Internet Protocol security (IPsec) or SSH, you can safely enable and use it.
HTTP	Disable	HTTP management is usually in plaintext and suffers from the same weaknesses as unencrypted telnet. HTTPS, if available, is recommended.
HTTPS (SSL or TLS)	Enable	Follow the vendor's instructions for

Item	Recommended Setting	Notes
		configuring keys/certificates for this.
SNMP Communities		SNMP is the default protocol for network management. Use SNMP v3 with password protection for highest security. It is often the protocol used by GUI configuration tools and network management systems. However, you can disable it if you do not use it.
Community 1 name	XXXXXX	The default is usually "public." Change this to a complex value.
Community 2 name	Disabled	Any unnecessary community names should be disabled or set to complex values.

16.

You should not disable SSID (WLAN network name) broadcast since this can interfere with the ability of Windows XP to connect to the right network. Although disabling the SSID broadcast is often recommended as a security measure, it gives little practical security benefit if a secure 802.1X authentication method is being used. Even with SSID broadcast from the AP disabled, it is relatively easy for an attacker to determine the SSID by capturing client connection packets. If you are concerned about broadcasting the existence of your WLAN, you can use a generic name for your SSID, which will not be attributable to your organization.

Replicating RADIUS Client Configuration to Other IAS Servers

Typically, the wireless APs in a given site are serviced by an IAS server at that site. For example, the site A IAS server services wireless APs in site A, while the site B server services wireless APs in site B and so on. However, other server settings such as the remote access policies will often be common to many IAS servers. For this reason the export and import of RADIUS client information is handled separately by the procedures described in this section.

Although you will find relatively few scenarios where replicating RADIUS client information is relevant, it is useful in certain circumstances (for example, where you have two IAS servers on the same site acting as primary and secondary RADIUS servers for all wireless APs on that site).

▸ **To export the RADIUS client settings to a file**

1. Log on to the source IAS server and open a command shell using the **MSS WLAN Tools** shortcut.
2. If required, identify a folder to store the output file or insert a blank, formatted floppy disk into the server's drive.
3. Run the following command to export the RADIUS client configuration:

   ```
   MSSTools ExportIASClients [/path:OutputFolder]
   ```

   OutputFolder is an optional parameter used to specify the folder where the output file will be written. If this parameter is not supplied, the output file is written to the current directory. If this parameter is supplied, the folder must exist.
4. The script creates the file IAS_Clients.txt.

Caution: You must remove this file from this server and store in a secure place since it contains the RADIUS secrets for all wireless APs configured on the server. After exporting the RADIUS client settings, you can import them into the other servers. You will typically do this to create a secondary server for a given set of wireless APs.

► **To import RADIUS client settings from a file:**

1. Log on to the target IAS server and open a command shell using the **MSS WLAN Tools** shortcut.
2. Identify the folder (or floppy disk) where the exported RADIUS secrets file IAS_Clients.txt is stored.
3. Run the following command to import the RADIUS client configuration:

   MSSTools ImportIASClients [**/path:***InputFolder*]

   InputFolder is an optional parameter used to specify the folder where the file will be read from. This folder must exist if specified. If no folder is specified, the file is assumed to be in the current directory

---

Warning: If you have copied the IAS_Clients.txt file to the target server, you must remove it from this server and store in a secure place, because it contains the RADIUS secrets for all wireless APs configured on this server.

Importing RADIUS client information is not an additive process. The imported RADIUS client settings will overwrite any existing client entries that you have on the server.

You can create a more flexible method of importing RADIUS clients by using the AddRADIUSClient.exe tool supplied with this solution. This allows you to script the selective addition of RADIUS clients to different servers.

Summary

This chapter provided guidance on the following topics:

- How to install and configure the first IAS server.
- How to install additional IAS servers and how to replicate the configuration to them from the first server.
- How to add wireless APs to IAS as RADIUS clients.
- How to configure your wireless APs to use the IAS servers and how to change the default settings to improve their security.

You are now ready to configure your WLAN clients. Information on how to accomplish this is covered in Chapter 6, “Configuring the Wireless LAN Clients."

You should read Chapter 8, "Maintaining the Secure Wireless LAN Solution." This chapter contains essential information about keeping your RADIUS infrastructure running in a secure and reliable manner.

References

This section provides references to important supplementary information or other background material relevant to the content of this chapter.

- The "Internet Authentication Service" section of the Windows Server 2003 product documentation at the following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_IAStopnode.asp

- For more information on deploying IAS, see the "Deploying IAS" chapter of the *Windows Server 2003 Deployment Kit* at the following URL:
  http://go.microsoft.com/fwlink/?LinkId=4716
- For more information on programming IAS using the Server Data Objects interface, see the "Server Data Objects" page on MSDN at the following URL:
  http://msdn.microsoft.com/library/en-us/sdo/sdo/server_data_objects_.asp
- For more information on IAS and RADIUS logging, see the "Remote Access Logging" section in the IAS product documentation at the following URL:
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_ias_log_conc.asp
- For more information on Pocket PC support for PEAP Fast Reconnect, see the article 827824, "FIX: Wireless Clients Cannot Connect When the PEAP Fast Reconnect Authentication Option is Turned On" in the Microsoft Knowledge Base at the following URL:
  http://support.microsoft.com/default.aspx?scid=kb;en-us;827824
- For more information on configuring specific RADIUS support for APs, see the "Vendor-Specific Attributes" page in the IAS product documentation at the following URL:
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_ias_attributes_conc_top.asp
- For more information on deploying a WLAN, see the "Deploying a Wireless LAN" chapter of the *Windows Server 2003 Deployment Kit* at the following URL:
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/DNSBM_WIR_OVERVIEW.asp
- For more information on Windows XP wireless technology, see the *Windows XP Wireless Deployment Technology and Component Overview* white paper at the following URL:
  http://www.microsoft.com/windowsxp/pro/techinfo/administration/networking/default.asp

6

Configuring the Wireless LAN Clients

Overview

This chapter provides guidance on configuring and deploying the network settings for your wireless local area network (WLAN) clients and connecting the clients to the WLAN. It includes procedures for connecting Microsoft® Windows® XP (Professional and Tablet Edition) and Pocket PC 2003 clients to the WLAN.

The chapter also provides details on verifying security group memberships for WLAN users and computers, configuring the WLAN settings using Group Policy for Windows XP clients, and procedures for configuring Pocket PC clients.

Chapter Prerequisites

In addition to the prerequisites described in Chapter 3, “Preparing Your Environment,” you should be familiar with the following topics:

- Windows XP configuration and driver installation.
- Pocket PC 2003 configuration and use.

You should have read and implemented the guidance provided in Chapter 3, “Preparing Your Environment,” Chapter 4, “Building the Network Certification Authority,” and Chapter 5, “Building the Wireless LAN Security Infrastructure.” In addition, you should also have read the design and planning information provided in Chapter 2, “Planning a Wireless LAN Security Implementation” and understood the architecture and design of the solution.

Preparing for Implementation

To carry out the Group Policy configuration procedures in this chapter, you need to log on with an account that is a member of the Domain Admins group for the domain into which you are installing the WLAN settings. By default, the built-in Administrator account of the domain is a member of this group but you may use any other account with the same group membership.

To carry out the Windows XP client computer verification procedures you need to be a member of the local Administrators group for that computer.

Tools Needed

The following table lists the tools that are required for implementing the procedures in this chapter.

Table 6.1: Tools Needed

Tool	Description	Source
Group Policy Management Console (GPMC)	Advanced management tool for import and export of Group Policy objects (GPO).	Installation steps provided in Chapter 3, "Preparing Your Environment."
Active Directory Users and Computers	A Microsoft Management Console (MMC) tool for managing Microsoft Active Directory® directory service users, groups, and computers and other Active Directory objects.	Installed as part of Windows Server™ 2003.

17.

WLAN Client Parameters

The following table lists some of the main parameters used in this chapter.

Table 6.2: WLAN Client Settings

Configuration Item	Setting
Group to allow WLAN access	Wireless LAN Access
Group to allow WLAN access for users	Wireless LAN Users
Group to allow WLAN access for computers	Wireless LAN Computers
WLAN GPO name	WLAN Client Settings
GPO filtering security group	Wireless LAN Computer Settings
Wireless network policy name	Windows XP WLAN Client Settings (Protected Extensible Authentication Protocol (PEAP)-Wired Equivalent Privacy (WEP))
WLAN network name (SSID)	*LucerneWLAN* (change this to your WLAN service set identifier (SSID))
Extensible Authentication Protocol (EAP) type	PEAP
PEAP authentication method	Secured Password (EAP-MSCHAP v2)
PEAP fast reconnect	Enabled

18.

The values shown in italic font need to be replaced with setting values that are relevant to your environment.

Allowing Users and Computers to Access the WLAN

You can control user and computer access to a network access server (such as a wireless access point (AP)) by setting the dial-in permission on the domain account of the user or computer. This was the method used by Windows NT® 4.0 to control user access to the Remote Access Service (RAS). However, controlling network access for a large number of users with this method is extremely cumbersome. Moreover, it is an "all-or-nothing" setting, which means that you cannot allow virtual private network (VPN) access while simultaneously blocking WLAN access for a given user.

Internet Authentication Service (IAS), with Windows 2000 and Windows Server 2003, allows you to control access to network services using Active Directory security groups associated with a remote access policy. This method is more flexible and much easier to manage because it allows you to use group memberships to govern access to a network service.

Controlling WLAN Access Using Security Groups

Access to the WLAN is controlled by the IAS Remote Access Policy (RAP). The RAP for this solution was configured in Chapter 5, “Building the Wireless LAN Security Infrastructure.” This policy includes a filter to allow access to the WLAN only to members of the Wireless LAN Access security group.

Wireless LAN Access is not populated with user and computer accounts directly. It has two security groups as members—Wireless LAN Users and Wireless LAN Computers. The solution makes Domain Users and Domain Computers members of these groups, respectively, which allows all users and computers to connect to the WLAN by default. The background to this topic is discussed in the "WLAN User and Computer Administration Model" section in Chapter 2, “Planning a Wireless LAN Security Implementation.”

Using Security Groups for More Granular Control

Allowing all users and computers access to the WLAN is a very simple administration model, but you may need to exert more control over which users and computers can access the WLAN. To do this, you must remove Domain Users and Domain Computers from Wireless LAN Users and Wireless LAN Computers, respectively. You can then add the specific users and computers to which you want to grant access as members of these groups.

Avoid adding users and computers directly to Wireless LAN Access, because it is a universal group and, therefore, its membership is published to the forest-wide global catalog. Being published to the global catalog means that any changes to its membership will be replicated to all domain controllers in the organization. Adding users and computers to the domain-specific groups (Wireless LAN Users and Wireless LAN Computers) limits the replication changes to just the domain controllers within a single domain.

Note: Pocket PCs do not have Active Directory computer accounts, and therefore you do not need to add them to Wireless LAN Computers. They only use the user account to authenticate to the WLAN; therefore, only the account of the Pocket PC user is significant.

Users receive changed group membership information only at logon. Therefore, your users will need to log off and log on again after you create and populate the WLAN access groups. Similarly, client computers must be restarted after any changes to their group memberships.

Configuring Windows XP WLAN Clients

In this section, you will learn how to configure WLAN client settings for Windows XP. The procedures described here will enable you to configure PEAP password authentication using dynamically keyed Wired Equivalent Privacy (WEP) for data protection. The settings can be applied to both Windows XP Professional and Windows XP Tablet Editions.

For instructions on how to configure Wi-Fi Protected Access (WPA) data protection and key management, see Appendix B, "Using WPA in the Solution."

Install any Required Patches and Updates

You should ensure that all relevant patches and updates have been applied to the client computers, including:

- Critical security patches.
- Windows XP service packs (Service Pack 1 or later).
- Windows XP WPA client (if required).
- WLAN-related Windows patches (for example, the Wireless Update Rollup Package for Windows XP—see Knowledge Base article 826942. This package is highly recommended unless Windows XP SP2 is installed).
- Updated WLAN drivers from your network adapter or computer vendor.

Creating the WLAN Settings GPO

To automate the delivery of WLAN client settings, you can use Active Directory Group Policy. The Group Policy Editor in Windows Server 2003 includes a collection of settings called Wireless Network Policy, which allows you to set client settings that are specific to your WLAN.

Important: It is assumed that the client computers are joined to the domain and are able to connect to a wired LAN so that they can receive the WLAN client settings.

You can create GPOs either by using GPMC or by using **Active Directory Users and Computers**.

Important: The Wireless Network Policy GPO settings will not appear in the GPO Editor if you are editing the GPO from a Windows 2000 or Windows XP system. You must edit these settings from a Windows Server 2003 system or a system with the Windows Server 2003 administration tools installed. However, the settings work with both Windows 2000 and Windows Server 2003 domain controllers. These settings are not present in the local policy object of any version of Windows.

► **To create a WLAN Client GPO using GPMC**

1. Open the GPMC and select the domain object of the domain you are configuring.
2. Right-click the domain and select **Create and Link a GPO Here…**

   Note: The GPO is linked at the domain level; therefore, the settings will be available to all computers in the domain. If you prefer, you can restrict the scope of the GPO by linking it to a lower-level organizational unit (OU).

3. When prompted for the name, type **WLAN Client Settings**.
4. In the right pane, double-click the newly created **WLAN Client Settings** GPO. The right pane now displays the properties of the GPO.
5. Click the **Scope** tab. In the **Security Filtering** list, select **Authenticated Users** and delete it using the **Remove** button.
6. Click **Add…** to add a different group.
7. Type (or browse for) **Wireless LAN Computer Settings**.

Note: The effective membership of the Wireless LAN Computer Settings group is the Domain Computers group; Domain Computers is a member of Wireless LAN Computers which in turn is a member of the Wireless LAN Computer Settings group. The GPO at the domain level (refer to step 1) allows all computers in the domain to receive WLAN client settings. If you want to restrict the settings to a smaller subset, remove Domain Computers from the Wireless LAN Computers group membership.

8. Click the **Details** tab and select **User configuration settings disabled** from the **GPO Status** drop-down list. Click **OK** to confirm.
9. Right-click the GPO in the left pane and select **Edit**… to edit the GPO settings.
10. When the GPO Editor opens, navigate to **\Computer Configuration\Windows Settings\Security Settings\Wireless Network (IEEE 802.11) Policies**.
11. Select the **Wireless Network (IEEE 802.11) Policies** object from the navigation pane and then select **Create Wireless Network Policy** from the **Action** menu.
12. Use the wizard to name the policy as **Windows XP WLAN Client Settings (PEAP-WEP)**. Leave the **Edit properties** check box selected and then click **Finish** to close the wizard.
13. Click the **Preferred Networks** tab and then click **Add…** to add a new preferred network.
14. In the **Network Name (SSID)** field, type the name of your wireless network.
15. In the **Description** field, type a description of the network.

Note: If you have an existing WLAN and you intend to run this side by side with the 802.1X-based WLAN of this solution, you must use a different SSID for the new WLAN.

16. Click the **IEEE 802.1x** tab and select **Protected EAP (PEAP)** from the **EAP Type** drop-down list.
17. Click the **Settings…** button to modify the PEAP settings. From the **Trusted Root Certification Authorities** list, select the root CA certificate for the CA that you had installed in Chapter 4, “Building the Network Certification Authority.”

Important: If you ever need to reinstall your CA from scratch (not just restore from backup), edit the GPO and select the root CA certificate for the new CA.

18. Select **Secured Password (EAP-MSCHAP v2)** in **Select Authentication Method** and then select the **Enable Fast Reconnect** option.
19. Close each properties window by clicking **OK**.
20. Close the GPO Editor and the GPMC.

To create the GPO using **Active Directory Users and Computers** (if you have not installed the GPMC), substitute the following steps for steps 1 to 10 in the previous procedure.

► **To create a GPO using Active Directory Users and Computers**

1. Open **Active Directory Users and Computers** and select the domain object.
2. Right-click the domain object and select **Properties**.
3. Click the **Group Policy** tab and then click the **New…** button.
4. Type **WLAN Client Settings** for the GPO name.

5. Click the **Properties** button and then click the **Security** tab.
6. Select **Authenticated Users** from the **Group or User Names** list and click the **Remove** button.
7. Click **Add…** and type (or browse for) **Wireless LAN Computer Settings**. Click **OK**.
8. With the **Wireless LAN Computer Settings** group name in the **Group or User Names** list highlighted, click **Read** and **Apply Group Policy** permissions in the **Allow** column of the **Permissions** list.
9. Click the **General** tab and click **Disable User Configuration settings**. Click **Yes** to any warning messages.
10. Click **OK** to apply the changes and close the GPO properties window.
11. Click the **Edit** button to edit the policy and navigate to **\Computer Configuration\Windows Settings\Security Settings\Wireless Network (IEEE 802.11) Policies.**
12. Repeat steps 11 to 20 of the previous procedure.

Deploying the WLAN Settings

If you are migrating from an existing WLAN (unsecured, static WEP or other type), you should deploy WLAN Group Policy settings for the new 802.1X-based network several days, or even weeks, in advance of configuring 802.1X settings on your wireless access points and activating the new WLAN. Doing so will provide the client computers with ample opportunity to download and apply the **WLAN Client Settings** Group Policy, even if they only connect to the wired LAN occasionally.

You can also apply the Group Policy settings to your client computers before a WLAN network adapter is installed and configured by Windows. The WLAN settings will be ignored until a valid WLAN network adapter is installed. Once the network adapter is installed, it will automatically be configured with the WLAN Group Policy settings.

Verifying Application of WLAN Group Policy

To verify correct application of the WLAN GPO settings, you need to log on to a client computer. The Domain Computers group is a member of the Wireless LAN Computer Settings security group, which is used to filter which computers receive the WLAN settings in the WLAN Client Settings GPO. All domain computers should therefore have received these GPO settings. You may need to restart the computer if it has not been restarted since the creation of the Wireless LAN Computer Settings group.

Note: You must have a WLAN network adapter installed on the computer to view the wireless network settings.

▸ **To verify successful deployment of the WLAN settings**

1. Log on as a member of the local Administrators group on a client computer.
2. Double-click the **Network Connections** folder in **Control Panel**.
3. View the properties of the **Wireless Network Connection** icon that corresponds to your wireless card. On the **Wireless Networks** tab, you should see your new wireless network SSID (name) under **Preferred Networks**.
4. Select the new wireless SSID and click **Properties** to view the settings and verify that they match those chosen in the WLAN Group Policy.
5. If the SSID does not appear under **Preferred networks** or the network settings shown for this SSID do not match the settings configured in the WLAN Group

Policy, close all Wireless Networks dialog boxes and run the following command from the command prompt.

```
Gpupdate /force
```

After a minute or two, reinspect the settings. If the settings still do not appear, refer to the “Troubleshooting” section in Chapter 8, “Maintaining the Secure Wireless LAN Solution.”

Verifying the Root CA Certificate on the Client

To authenticate to the IAS server using PEAP, the clients need to have the certificate for the network CA (installed using the guidance provided in Chapter 4, “Building the Network Certification Authority”) in their Trusted Root CA store. This certificate was published to Active Directory as part of the CA installation. All members of your Active Directory forest will automatically download and install this certificate in their Trusted Root CA store.

▸ **To verify that the root CA certificate has been installed**

1. Log on as Administrator to the client computer.
2. Run MMC.exe (from the **Start, Run…** menu option or a command shell).
3. From the **File** menu of the MMC, select **Add/Remove Snap-in…**
4. On the **Add/Remove Snap-in** window, click the **Add…** button. Select the **Certificates** item from the list of available snap-ins.
5. Select **Computer Account** and then click **Next**.
6. Click **Finish**.
7. Close the **Add Standalone Snap-in** and the **Add/Remove Snap-in** windows.
8. In the left pane, navigate to Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates.
9. Locate the certificate for your CA. (It will be listed under the name you gave during the CA installation.)
10. If the certificate does not appear in the list, open a command shell and type the command:

    ```
    Gpupdate /force
    ```

11. Return to the **Certificates** management console. Right-click the **Certificates (Local Computer)** node, select **Refresh** and then check for the CA certificate again.

    If the certificate still does not appear, see the “Troubleshooting” section in Chapter 8, “Maintaining the Secure Wireless LAN Solution.”

Verifying the Connection to the WLAN

Having verified the WLAN GPO settings and the root CA certificate, you can now test the connection to the WLAN using a client computer.

▸ **To test the connection to the WLAN**

1. As a domain user with authorized access to the WLAN, log on to a client computer that has a WLAN card installed and is not connected to the wired network. By default, all domain users have access to the WLAN.

Note: If the WLAN is not working at this point and the user does not have cached credentials on the computer, the logon will fail.

---

2. From the command prompt, use the **ping** command to verify network connectivity to another computer on the network.

   If the **ping** command (or logon) fails, see the “Monitoring Client Connection to the WLAN” subsection of the “Troubleshooting” section in Chapter 8, “Maintaining the Secure Wireless LAN Solution.”

For more information on testing procedures for WLAN clients, see Chapter 7, “Testing the Secure Wireless LAN Solution.”

Configuring Pocket PC 2003 Clients

Pocket PC 2003 has full support for 802.1X WLAN networks using either PEAP (with passwords) or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) (with certificates). However, Pocket PC 2003 is a modular operating system and the vendor of the handheld device can choose whether or not to include this facility; therefore, you should not assume that all Pocket PC 2003 devices are WLAN-capable. Leading vendors of these devices provide 802.1X WLAN-capable systems either with built-in WLAN hardware or with an add-on WLAN network adapter. This section describes the configuration of the generic Pocket PC WLAN interface and is based on the HP IPAQ 5550 Pocket PC. However, some vendors implement their own WLAN drivers and interfaces. The following instructions may not be correct for these latter devices and you should follow the instructions provided by your device vendor.

Some Pocket PC device vendors also offer 802.1X WLAN support on Pocket PC 2002. Pocket PC 2002 has not been tested with this solution. You should consult your vendor's Web site for details of their Pocket PC 2002 support for WLAN.

Preparing the Pocket PC Device

Before configuring the device, you should obtain and install any relevant updates for your Pocket PC available from its vendor, including:

- Read-only memory (ROM) updates. (These may contain a variety of updates including drivers.)
- Network driver updates.
- Other WLAN or network updates that are relevant to 802.1X networking.

Important: Before installing the updates, you should carefully read the documentation accompanying each of them. Some updates may be incompatible with others or with what you are trying to achieve. For example, HP has published an update for the IPAQ 555x series to support Cisco LEAP but this update is incompatible with their 802.1X WLAN driver update and will prevent PEAP from working.

Making the CA Certificate Available

You need to install the CA certificate of your network CA into the Trusted Root CA store of all Pocket PCs that need to connect to the WLAN. To do this, you must export the certificate from the CA and make it available for Pocket PC users or information technology (IT) staff.

► **To export the CA certificate**

1. Log on to the CA server and open a command shell.
2. Run the following command to export the CA certificate to a file:

```
certutil –ca.cert rootca.cer
```

You can specify a path to the Rootca.cer file if you want to save it in a different folder. (You need to enclose the path and file name in quotes if it contains embedded spaces.)

3. Copy the certificate file to a file share or Web server directory so that users can easily download it when required for the Pocket PC installation.

Configuring the Pocket PC

You must configure each Pocket PC with the CA certificate and WLAN settings before it can be connected to the WLAN. You need some means of copying the certificate file to the Pocket PC. This procedure assumes the use of ActiveSync® connection established using a docking cradle, Infrared, or Bluetooth connection. You can also use removable media (such as a Compact Flash, Secure Digital, or Multimedia Card) to transfer the certificate file, or use an unauthenticated WLAN connection to allow the Pocket PC to download the certificate from a Web site. You can also send the certificate to the user in e-mail, allow them to synchronize (to transfer the e-mail to Pocket Outlook®), and then have the use execute the attached certificate file.

► **To import the CA certificate to the Pocket PC**

1. Connect the Pocket PC to a host computer using ActiveSync (you may need to establish an ActiveSync partnership to do this) and your preferred connection method.
2. From the host computer, use the ActiveSync **Explore** option to open a folder window on the device; it should open the **My Documents** folder.
3. Obtain the CA certificate file from its published location and copy it to the **My Documents** folder. You can ignore the warning about file conversion. You can now disconnect the device from the ActiveSync connection.
4. On the Pocket PC, locate the CA certificate file using **File Explorer** and double-tap the file.
5. You will be asked whether you want to install the certificate. Verify that the CA name matches the name of your network CA and tap **Yes** to install it.

   You can verify successful installation of the certificate by selecting **Settings**, **System**, **Certificates**, and then clicking the **Root** tab.

► **To configure the 802.1X WLAN settings on the Pocket PC**

1. If the WLAN adapter is not already enabled on the device, enable it using either a hardware switch or a software tool.
2. If a pop-up message displays indicating that a new network has been found, select **Work** as the location to which the WLAN will connect you. Then tap **Settings**.
   If the pop-up message does not appear (because the WLAN had been previously detected), perform the following steps:
   - Tap the **Connectivity** icon (two arrows pointing in opposite directions) on the Pocket PC title bar and tap **Settings**.
   - Tap the **Advanced** tab and then tap the **Network Card** button.
     On the **Wireless** tab, you should see your WLAN SSID in the list of available wireless networks (if there are any other WLANs in range, their names may appear here).
   - Tap the name of your WLAN in the list.
3. On the **General** tab, select **Work** from the **Connects to:** list.
4. On the **Authentication** tab, select the following options:

- **Data encryption (WEP Enabled)**
- **The Key is provided for me automatically**
- **Enable network access using IEEE 802.1X**

Clear the **Network Authentication (Shared mode)** option.

5. In the **Extensible Authentication Protocol Type:** list, select **PEAP**.
6. Tap **OK** to close the WLAN settings screen.
7. When prompted to enter domain credentials to connect to the WLAN, type the name, password, and domain of a user who is authorized to connect to the WLAN.

Warning: You should select the **Save Password** option only if a strong security mechanism, such as fingerprint scanning or strong password access, is implemented to help protect the device from unauthorized use. Remember that the user credentials are used to authenticate to domain resources as well as the WLAN. If they are compromised, they will allow an intruder to access all your internal network resources over the WLAN without detection.

8. If you navigated to the WLAN settings through the **New Network** popup in step 2, tap the **Connectivity** icon on the title bar of the Pocket PC and tap **Settings** to open the **Connections Settings** screen.
9. Tap the **Advanced** tab and then the **Network Card** button. (You will already be at this screen if you did not navigate through the **New Network** popup in step 2.)
10. In the **Wireless Networks** list, you should see the name of the WLAN that you just configured. The status should be **Connected**; if it is not, tap and hold the name and tap **Connect**. (You may be prompted to enter the user credentials again.)
11. If the WLAN is now shown as **Connected**, tap **OK** to close the **Configure Wireless Networks** and the **Connections Settings** screens.

Note: If you are going to give these instructions to the Pocket PC users to configure their own devices, they can enter their own domain credentials when prompted. However, if the IT support engineers are preconfiguring the Pocket PCs for the users, you need to provide the engineers with valid domain accounts (with access to the WLAN); it is especially important that *they* do not select the **Save Password** option when using such accounts. The users should then be instructed to enter their own credentials when they first connect using the Pocket PCs.

Verifying the Pocket PC Connection to the WLAN

You can verify that the Pocket PC has successfully connected to the WLAN in a number of ways. The simplest way is to connect to an application on the network, such as a Web site. (You may need to configure a proxy server on the device if the Web server is not on the LAN.)

If the connection fails, see the “Troubleshooting” section in Chapter 8, “Maintaining the Secure Wireless LAN Solution.”

Summary

This chapter dealt with the configuration of WLAN network settings for Windows XP and Pocket PC clients. It provided guidance on using security groups to control access to the WLAN, configuring Group Policy to deploy WLAN settings to Windows XP clients, and configuration steps for Pocket PC 2003 clients.

References

This section provides references to important supplementary information or other background material relevant to the content of this chapter.

- For more information on administering WLAN access by user and by security group, see the "Introduction to remote access policies" topic in the Windows Server 2003 product documentation, which is available at the following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_rap_intro.asp

- For more information on the Wireless Update Rollup Package for Windows XP, see the following URL:

  http://support.microsoft.com/default.aspx?scid=826942

- For more information on configuring WLAN network settings using Group Policy, see the "Define Active Directory–based wireless network policies" topic in the Windows Server 2003 product documentation, which is available at the following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/wireless_definepolicy_inGP_topnode.asp

- You can get more technical information on the WLAN support in your Pocket PC from the device vendor. For more technical information, see the "Windows CE .NET Wireless Technology Overview" on the Microsoft Developer Network at the following URL:

  http://msdn.microsoft.com/library/en-us/wcemain4/html/cmconwindowscenetwirelesstechnologyoverview.asp

7

Testing the Secure Wireless LAN Solution

Introduction

The primary objective of this chapter is to provide the reader with guidance on testing their own deployment of the *Securing Wireless LANs with PEAP and Passwords* solution. The recommendations given in this chapter are based on the experience gained by Microsoft® in testing this solution.

The first part of this chapter describes the testing process used by Microsoft. The second part covers the test scenarios that you can use to verify your solution before implementing it in the production environment. The test scenarios given in this chapter supplement the verification testing procedures included in chapters 3 through 6.

Knowledge Prerequisites

Operational knowledge of the following areas will be helpful in testing this solution:

- Public Key Infrastructure (PKI) concepts and Microsoft Certificate Services.
- Internet Authentication Service (IAS) server (RADIUS server).
- Installation of wireless network adapter drivers and configuration of wireless network settings in Microsoft Windows® XP.
- Use and configuration of Pocket PC 2003.
- The Microsoft Active Directory® directory service (including Active Directory structure and management tools; working with users, groups, and other Active Directory objects; and Group Policy).
- Microsoft Windows® Scripting Host and Microsoft Visual Basic® Scripting Edition (VBScript) language (these will be helpful in customizing or using the scripts and tools provided with this guidance).

How Microsoft Tested the Solution

The Microsoft test team focused on verifying the solution profile described in Chapter 2, "Planning a Wireless LAN Security Implementation". Following are the main characteristics of the profile:

- A single-domain Active Directory forest containing two domain controllers with the domain functional level of Windows 2000 native mode.

- Domain controller servers were installed on Windows Server™ 2003, Standard Edition.
- Windows XP Service Pack 1 Professional and Tablet Editions and Pocket PC 2003 (Hewlett Packard IPAQ 5550) were used as wireless clients.
- IAS was installed on the domain controllers.
- The Certification Authority (CA) server was installed on one of the domain controllers.
- The network at the head office site was on a single local area network (LAN); the branch office site was on a separate LAN.
- Dynamic Wired Equivalent Privacy (WEP) was used for WLAN data protection rather than WPA.
- The remote branch office had only wireless access points (APs) as infrastructure and latency was introduced in the connection to the head office to simulate a DSL or cable modem type of connection.

This profile does not cover all possible configurations of the solution (such as scaling to larger organization sizes); however, it ensures that all components of the configurations have been tested. The architectural changes required to scale this profile to that of an organization with 5000 users are relatively minor.

Note: The testing described here only includes the verification of the solution performed by Microsoft. It does include the extensive product testing carried out by the Microsoft product groups; the solution testing is additional to this.

Test Network Layout

The test lab environment was based on the network design described in Chapter 2, “Planning a Wireless LAN Security Implementation”. The following figure shows the physical layout of the lab instance, which has the simplest network configuration described in Chapter 2.

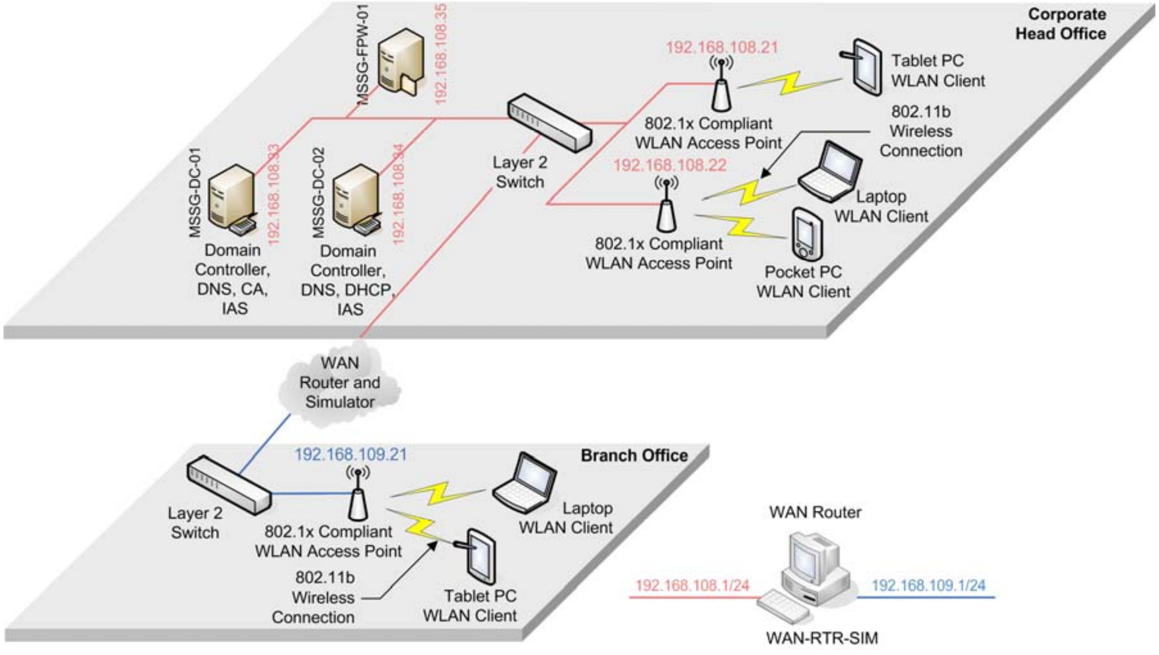

Figure 7.1

Test lab network architecture

The head office network was on a single network with the wireless clients and domain servers on single subnet. The branch office site had a separate network and was on a different subnet. The router linking the head office and branch office included simulated WAN latency and bandwidth restriction. The wireless APs were sufficiently spaced out so that users could rove between them.

Although a single, unsegmented LAN was used for testing, you may want to segregate your internal network using different subnets, virtual LANs (VLANs), and switches to better manage network performance and security.

Once the base network consisting of domain controllers, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), file, print, and Web services with static wireless WEP was developed, the implementation guidance given in chapters 3 through 6 was used to install and configure each component. These chapters include verification procedures, which were all performed as described. A larger suite of tests was performed before, during, and after the build. The most important test scenarios used are included in the next section; you can use them to test your implementation of the solution.

The built solution, the build and operating scripts, and the documentation were subjected to three rounds of testing and the issues were raised as bugs. Testing was considered complete and successful when all the bugs were resolved.

Verifying Your Implementation

This section describes the principal test scenarios used by Microsoft to test the solution.

These test scenarios are not exhaustive; you may develop your own scenarios based on the requirements of your organization. Some verification scenarios described in previous chapters have been repeated in this chapter for completeness. You should have read the previous chapters before you use these scenarios for testing. In case the test fails in any of the scenarios, see the "Troubleshooting" section in Chapter 8, "Maintaining the Secure Wireless LAN Solution" to diagnose and resolve the test failures.

Scenario 1: Verifying IAS Server Certificate Deployment

This scenario verifies that once the IAS servers are built and configured, they will receive the server authentication certificate auto–enrolled from the network CA.

Execution Details

1. Open a command shell using the MSS WLAN Tools shortcut.
2. Run the following command to open the **Certificates** MMC:
   ```
   ComputerCerts.msc
   ```
3. In the console tree, double-click **Certificates (Local Computer)** and then double-click **Personal**. Next, click **Certificates**.
4. You should see at least one certificate with the name of the IAS server in the **Issued To** column and the name of your CA in the **Issued By** column. Scroll the list (to the right) and verify that the value in the **Certificate Template** column is **Computer** for this certificate.
5. If the required certificate does not appear in the **Certificates** MMC, select **Certificates (Local Computer)** from the console tree in the left pane, click **All Tasks** from the **Action** menu, and then click **Automatically Enroll Certificates**. Then refresh the view of the **Certificates** MMC.

Scenario 2: Verifying the Root CA Certificate on the Windows XP Wireless Client

This scenario verifies that a valid wireless Windows XP client receives the network CA's Root Certificate in its Trusted Root Certification Authorities store. This certificate is downloaded and added to the store when the Group Policy is updated.

Execution Details

1. Log on to the client computer as an Administrator.
2. Select **Start, Run…** type **`MMC.exe`** and press **Enter**.
3. From the **File** menu of the MMC, select **Add/Remove Snap-in…**
4. In the **Add/Remove Snap-in…** window, click the **Add…** button. Select the **Certificates** item from the list of available snap-ins.
5. Select **Computer Account** and then click **Next**.
6. Click **Finish**.
7. Close the **Add Standalone Snap-in** and the **Add/Remove Snap-in…** windows.
8. In the left pane, navigate to Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates.
9. Locate the certificate for your CA. (It should be listed under the name you gave your CA during installation.)
10. If the certificate does not appear in the list, run the following command at a command prompt:

    ```
    Gpupdate /force
    ```
11. Return to the **Certificates** MMC. Right-click the **Certificates (Local Computer)** node, select **Refresh**, and then check for the CA certificate again.

Scenario 3: Verifying User Authentication to the Wireless Network

This scenario is the most important test scenario. It verifies that a WLAN user is able to successfully authenticate and connect to the network after the solution is installed and configured.

Execution Details

1. Ensure that a particular domain user is a member of the Wireless LAN Users group or the Domain Users group (which is a member of the first group).
2. Have the user log on to a client computer that has a WLAN card installed and is not connected to the wired network. The user should give the domain credentials during logon.
3. Open **Network Connections** panel from the **Control Panel**, and check the status of **Wireless Network Connections**. It should show the **Authentication Succeeded** status for the wireless connection.
4. From the command prompt, use the ping command to verify network connectivity to another computer on the network.
5. On the IAS server, open **Event Viewer**. The **System** event log should contain an Information type IAS log of Event ID 1. Browse through the description of the log; it should have user's authentication details.

Scenario 4: Verifying Computer Authentication to the Wireless Network

This scenario verifies that a computer is authenticated to the network when the user is not logged in.

Execution Details

1. Ensure that the computer account is a member of the Wireless LAN Computers group or the Domain Computers group (which is a member of the first group).
2. Restart the computer after ensuring that it has a WLAN card installed and is not connected to the wired network.
3. At the logon prompt, do not login and keep the machine idle for a few minutes.
4. On the IAS server, open **Event Viewer**. The **System** event log should contain an Information type IAS log of Event ID 1 for the computer hostname. Browse through the description of the log; it should have the computer authentication details.

Scenario 5: Verifying Pocket PC Authentication to the Wireless Network

This test scenario verifies that a user can successfully log on to the WLAN network from a Pocket PC device.

Execution Details

1. Ensure that a particular domain user is a member of the Wireless LAN Users group or the Domain Users group (which is a member of the first group).
2. Enable the wireless connection on the Pocket PC and configure the 802.1X settings on the Pocket PC following the guidance provided in Chapter 6, “Configuring the Wireless LAN Clients.”
3. Select and hold your network name in the list of wireless networks till it displays an option to connect. Choose **Connect** to connect.
4. When prompted to enter domain credentials at the **Network Log On** screen, type the name, password, and domain of the user.
5. If authentication is successful, the network status icon will not have a cross sign. Verify the status by opening **Internet Explorer** from **Start** menu and browsing any intranet Web site.
6. On the IAS server, open **Event Viewer**. The **System** event log should contain an Information type IAS log of Event ID 1. Check the description of the log; it should have user’s authentication details.

Scenario 6: Blocking a WLAN Client Using IAS Remote Access Policy

This scenario is based on the guidance provided in Chapter 8, “Maintaining the Secure Wireless LAN Solution.” An administrator, if required, can block a user’s wireless access to the network using the Deny Remote Access policy (this procedure is detailed in the ”Denying WLAN Access to a User or Computer” section of Chapter 8). You should configure the Deny Remote Access policy on the IAS servers before you execute this test scenario.

Execution Details

1. Ensure that a particular computer account is a member of the Deny Wireless LAN Users group.

2. Have the user log on to a client computer that has a WLAN card installed and is not connected to the wired network. User should enter the domain credentials at logon.
3. The user should not be able to log on to the domain; they should see an “access denied” message.
4. On the IAS server, open **Event Viewer**. The **System** event log should contain a Warning type IAS log of Event ID 2. Browse through the description of the log; it should have the user’s authentication failure details.

Scenario 7: WLAN Access Denied if the User is not a Member of WLAN Access Groups

This test case verifies that a user is denied wireless access to the network if he/she is not a member of the Wireless LAN Users group. This is an alternate method of blocking user’s wireless access to the network.

Execution Details

1. Open the **Active Directory Users and Computers** console from **Administrative Tools** panel.
2. Remove the Domain Users group from the Wireless LAN Users group, or remove a particular user if you are adding users directly to the Wireless LAN Users group.
3. Have the user log on to a client computer that has a WLAN card installed and is not connected to the wired network. User should enter the domain credentials at logon.
4. The user should be unable to log on to the network and should see an “access denied” message.
5. On the IAS server, open **Event Viewer.** The **System** event log should contain a Warning type IAS log of Event ID 2. Browse through the description of the log; it should have the user’s authentication failure details.

Scenario 8: Verifying IAS Service Failover

This test scenario verifies availability of IAS service to the wireless clients when one of the IAS servers becomes unavailable. Such failures should not result in disruption of network connectivity for the wireless clients. This important test scenario verifies that the APs switch over to secondary IAS servers when the primary IAS server becomes unavailable.

Execution Details

1. Open the **IAS** MMC on the primary IAS server of your network and click the server name. Then stop the IAS service by clicking the **Stop** button on the menu bar.
2. Using a domain user account with authorized access to the WLAN, log on to the network using a wireless connection.
3. The user should be able to successfully authenticate and connect to the network. Verify this by opening the **Network Connections** panel from the **Control Panel**, and check status for **Wireless Network Connections**. The status should show **Authentication Succeeded** for the wireless connection.
4. From the command prompt, use the **ping** command to verify network connectivity to another computer on the network.
5. On the secondary IAS server, open **Event Viewer**. The **System** event log should contain an Information type IAS log of Event ID 1. Browse through the description of the log; it should have user’s authentication details.

Scenario 9: Wireless Client Roving Between Access Points and Re-Authenticating to WLAN

This scenario verifies that the wireless clients can roam between APs, which results in re-authentication (or Fast Reconnect, if enabled). It is important that this scenario is tested before deploying the solution in the production environment. This test verifies that the wireless network connectivity is seamless for users.

Execution Details

1. Using a domain user account with authorized access to the WLAN, log on to the network using a wireless connection. Ensure that the network connection was successful.
2. On the IAS server, open **Event Viewer**. The **System** event log should contain an Information type IAS log of Event ID 1. Browse through the description of the log; it should have the user's authentication details.
3. From the user's authentication details, note the IP Address of the AP to which the user is connected. The value is shown in the **Client-IP-Address** field.
4. Perform roaming with your machine to another location so that the client is in close proximity with a neighboring AP and far from the AP to which it was connected.
5. This should cause your Windows XP client to perform a re-authentication and get connected to the new AP.
6. On the IAS server, open **Event Viewer**. The **System** event log should contain an Information type IAS log of Event ID 1. Browse through the description of the log; it should have the user re-authentication details and the **Client-IP-Address** field should have the IP of the new AP.

Scenario 10: Re-authentication of Wireless Client Due to IAS Session Time-out

This scenario verifies the dynamic WEP key rotation configured in the IAS Connection Request Policy. The test verifies that the client(s) are re-authenticated periodically (after the configured time duration) so that their WEP keys keep changing.

Execution Details

1. Using a domain user account with authorized access to the WLAN, log on to the network using a wireless connection. Ensure that the network connection was successful.
2. On the IAS server, open **Event Viewer**. The **System** event log should contain an Information type IAS log of Event ID 1. Browse through the description of the log; it should have the user's authentication details.
3. Leave the client connected to the network for a time period more than one hour. You can start a continuous ICMP request to another computer on the network to confirm that the connection is active.
4. After about an hour's time period, open the **Event Viewer** and check the **System** event log. It should contain an Information type IAS log of Event ID 1. Browse through the description of the log; it should have the user re-authentication details.

Scenario 11: E-mail Alert for IAS Backup Failure

This test case verifies that e-mail alerts are properly configured for the IAS servers as documented in this solution. When properly implemented, these alerts significantly improve the manageability of the IAS service, which is critical for wireless network connectivity. Ideally, this test should be performed after implementation to confirm that the notification services are running properly.

To test this scenario, an IAS backup failure is simulated to generate the required e-mail alerts. The steps for configuring IAS backup as required in this scenario are given in Chapter 8, “Maintaining the Secure Wireless LAN Solution.” You should have read Chapter 8 and configured the necessary scripts before executing this test case.

Execution Details

1. Open a command shell using the MSS WLAN Tools shortcut.
2. Edit the **Constants.vbs** file and set the **ALERT_EMAIL_ENABLED** parameter to **True**.
3. Configure the **ALERT_EMAIL_RECIPIENTS** parameter with the e-mail addresses of the persons who need to be alerted.
4. Configure the **ALERT_EMAIL_SMTP** parameter with the SMTP server’s IP address or DNS name.
5. Run the following IAS backup command to some non-existent folder:

   ```
   MSSTools BackupIAS /path:C:\IncorrectIASpath.
   ```
6. On the IAS server, open **Event Viewer**. The **Application** event log should contain an Error type IAS Operations log of Event ID 211.
7. The persons identified for alerts should receive an e-mail alert.

Scenario 12: E-mail Alert for CA Service Failure

This test case is similar to the IAS backup failure alert test case. It verifies that the e-mail alerts are sent to the concerned administrative people if the CA service fails.

The steps for configuring CA backup as required in this scenario are given in Chapter 8, “Maintaining the Secure Wireless LAN Solution.” You should have read through Chapter 8 and configured the necessary scripts before executing this test case.

Execution Details

1. Open a command shell using the MSS WLAN Tools shortcut.
2. Edit the **Constants.vbs** file and set the **ALERT_EMAIL_ENABLED** parameter to **True**.
3. Configure the **ALERT_EMAIL_RECIPIENTS** parameter with the e-mail addresses of the persons who need to be alerted.
4. Configure the **ALERT_EMAIL_SMTP** parameter with the SMTP server’s IP address or DNS name.
5. Open **Certification Authority** from **Administrative Tools** panel. Click the CA name, and select **Action**, **All Tasks,** and then **Stop service**.
6. Open the **Services** MMC from the **Administrative Tools** panel.
7. Right-click **Certificate Services** and select **Properties**. Change **Startup** type to **Disable** and click **OK** to close.
8. Run the following CA command:

   ```
   MSSTools CheckCA
   ```
9. On the CA server, open **Event Viewer**. The **Application** event log should contain an Error type CA Operations log of Event ID 1.
10. The persons identified for alerts should receive an e-mail alert when the CA service fails.
11. Revert the **Certificate Services Startup** type to **Automatic** in the **Services** MMC.

12. Start the service on the **Certification Authority** MMC by clicking the **Start** button on the menu bar.

Test Tools

The following tools were used during the testing of this solution. Some of these tools are also used during the building and maintaining phases:

1. **Certutil:** This is a multipurpose tool used to configure CA; dump and display CA configuration information; back up and restore CA components; and verify certificates, key pairs, and certificate chains.
2. **Dcdiag:** This tool analyzes the state of domain controllers in a forest or enterprise.
3. **Event Log Viewer:** This tool monitors and captures logs related to applications, security, and the system.
4. **Group Policy Management Console:** This tool is used to view and edit Group Policy objects in Active Directory.
5. **NetMon:** This utility captures and filters frames from network traffic to and from the computer on which it is installed. This tool is not directly required but it is useful for debugging authentication issues. This tool can be installed from **Control Panel** by selecting **Add/Remove Components**, **Windows Components**, **Management and Monitoring Tools,** and then **Network Monitor Tools**.
6. **Netsh:** This is a command-line scripting utility that allows you to display or modify, either locally or remotely, the network configuration of a computer that is currently running. This is a multipurpose tool used for IAS-related operations.
7. **Windows Backup:** This is the backup and restore tool supplied with Windows that performs backup and restore operations on files, folders, and system state. This tool can be run either through a wizard or a command line.
8. **PerfMon:** This tool allows you to view system performance logs, alerts, and counters. You can use this tool to monitor the performance of your IAS.
9. **Ping:** This tool verifies IP-level connectivity to another TCP/IP computer by sending ICMP Echo Request messages. Corresponding Echo Reply messages that are received are displayed along with round-trip times.
10. **Schtasks:** This tool schedules commands and programs to run periodically or at a specified time. It adds and removes tasks from the schedule, starts and stops tasks on demand, and displays and changes scheduled tasks.

Most of these tools are installed automatically when the Windows operating system is installed. Installation of the other tools is covered in Chapter 3, "Preparing Your Environment."

Summary

This chapter covered the testing of the secure WLAN solution. The first part briefly described the parameters used by Microsoft when testing this solution during development. The second part provided instructions on how to perform some of the most important test scenarios used for testing this solution. These test scenarios allow you to verify the correct operation of your own WLAN security infrastructure prior to its deployment in a production environment.

8

Maintaining the Secure Wireless LAN Solution

Introduction

This chapter covers the operational procedures involved in managing the *Securing Wireless LANs with PEAP and Passwords* solution. The chapter contains guidance on the key operational and support tasks that you need to perform to maintain the wireless local area network (WLAN) security infrastructure, including the Internet Authentication Service (IAS) servers, certification authority (CA), wireless access points (APs), and the WLAN clients. However, this chapter does not include guidance on general network management or the management of aspects other than security services; for example, network traffic analysis and optimization.

Overview

The major sections in this chapter are:

- **Essential Maintenance Tasks:** This section lists the key tasks that you need to perform to set up the management system (for example, configuring backup jobs) and the list of tasks that you need to perform regularly to maintain the system (for example, weekly housekeeping tasks).
- **Operating the WLAN Infrastructure:** This section is primarily a reference section that details the different types of tasks you need to perform to maintain the WLAN security infrastructure. Subsections include information about standard operational tasks, implementing changes, support tasks, and optimization tasks.
- **Troubleshooting:** This section contains procedures and flowcharts that can help you troubleshoot common problems you may encounter with your WLAN infrastructure. It also includes descriptions of useful troubleshooting tools and procedures to enable logging for different components.
- **References:** This section lists sources of supplementary information referred to in the text.

Chapter Prerequisites

You should be familiar with the administration of Microsoft® Windows® Server™ 2003 or Windows® 2000 Server. The following areas are especially relevant:

- Basic operations and maintenance of Microsoft Windows Server 2003, including the use of tools such as Event Viewer, Computer Management, and NTBackup.
- IAS.
- Certificate Services.
- The Microsoft Active Directory® directory service (including Active Directory structure and tools), management of users, groups, and other Active Directory objects, and use of Group Policy.
- Windows system security concepts such as users, groups, auditing, access control lists (ACL), the use of security templates, and the application of security templates using Group Policy or command-line tools.
- Wireless LAN and general network concepts.
- An understanding of Windows Script Host and knowledge of the Microsoft Visual Basic® Scripting Edition (VBScript); this knowledge will help you to understand and use the scripts supplied with the solution.

In addition, you should have read the following chapters and have a thorough understanding of the architecture and design of the solution:

- Chapter 2, "Planning a Wireless LAN Security Implementation"
- Chapter 3, "Preparing Your Environment"
- Chapter 4, "Building the Network Certification Authority"
- Chapter 5, "Building the Wireless LAN Security Infrastructure"
- Chapter 6, "Configuring the Wireless LAN Clients"

Essential Maintenance Tasks

This section lists the key tasks that you must perform to successfully operate your WLAN infrastructure. These tasks can be divided into two categories:

- Initial setup tasks
- Ongoing maintenance tasks

This section also lists the tools and technologies used in the procedures in this chapter.

Initial Setup Tasks

The following table shows the tasks that must be performed to put the WLAN security infrastructure into production.

Table 8.1: Initial Setup Tasks

Task Name	*Section*
Configuring the IAS Backup	*Operational Tasks*
Configuring Alert Types	*Monitoring*
Enabling Monitoring of IAS	*Monitoring*
Enabling Monitoring of the CA	*Monitoring*

Maintenance Tasks

The following table shows the tasks that must be performed regularly to keep your LAN security infrastructure operating correctly. You can use this table for planning the required resources and the operational schedule for administering the system.

Table 8.2: Maintenance Tasks

Task Name	Frequency	Section
Testing the Backups	6 months	Operational Tasks

Tools and Technology Required

The following table lists the tools or technologies required for the procedures described in this chapter.

Table 8.3: Required Technology

Item Name	*Source*
Active Directory Users and Computers Management Console (MMC)	*Windows Server 2003*
Certification Authority MMC	*Windows Server 2003*
Certutil.exe	*Windows Server 2003*
DCDiag.exe	*Windows Server 2003 Support Tools*
DSquery.exe	*Windows Server 2003*
Event Viewer	*Windows Server 2003*
Group Policy Management Console (GPMC)	*Web download from Microsoft.com*
MSS WLAN Tools	*Scripts installed as part of this solution*
Netdiag.exe	*Windows Server 2003 Support Tools*
Performance Monitor	*Windows Server 2003*
PKI Health	*Windows Server 2003 Resource Kit*
Removable media for backing up Root CA	*CD-RW or Tape*
SchTasks.exe	*Windows Server 2003*
Text editor	*Notepad — Windows Server 2003*
Windows Backup	*Windows Server 2003*
Windows Task Scheduler Service	*Windows Server 2003*

Table 8.4: Recommended Technology

Item Name	*Source*
E-mail infrastructure—for operational alerts	*SMTP/POP3/IMAP server and client, such as Microsoft Exchange Server and Microsoft Outlook®*
Operational Alert Console	*Microsoft Operations Manager or other service monitoring system*
Operating system update distribution	*Microsoft Systems Management Server (SMS) or Microsoft Software Update Services*

Operating the WLAN Infrastructure

This section includes the major tasks that you need to perform to maintain the WLAN security infrastructure.

Operational Tasks

Operational tasks include jobs that need to be done at regular intervals to keep the WLAN infrastructure functioning correctly.

Backing up IAS and the Certification Authority

You need to perform regular backups of the IAS servers, including the IAS server running the CA. IAS requires a special procedure to export its settings to a file, which can then be backed up with a normal file backup. You can back up Certificate Services using Windows system state backup, which is available in the Windows Backup tool. You should establish adequate backup procedures on all the servers on which IAS is running.

The following two procedures are not mutually exclusive; you need to configure both an IAS backup and a server backup.

Configuring the IAS Backup

You need to create a folder with restricted permissions into which the IAS configuration will be exported each night. You also need to create a scheduled job that will run the IAS configuration backup every night (the backup script does not require IAS to be shut down during the backup operation). If the backup succeeds, an event is written to the Windows Application log. An error event will be logged in the case of a backup failure.

Caution: The IAS backup files include all of the RADIUS client secrets. This is highly sensitive information, so you should be careful to store this backup data securely.

▸ **To configure the IAS backup**

1. Open a command shell on the server using the **MSS WLAN Tools** shortcut and use the following command to create a folder to save the IAS settings:

   ```
   md c:\IASBackup
   ```

   (The IAS configuration is typically less than 100 KB and can be saved to the system drive, as shown.)

2. Use the following command to set permissions for the folder so that only administrators and backup operators can read and modify its contents:

   ```
   cacls c:\IASBackup /G system:F administrators:F "Backup
   Operators":C
   ```

   (This command may wrap to more than one line here, but you should enter it as a single line.)

3. Test the backup by issuing the following command:

   ```
   "C:\Program Files\Microsoft\Microsoft WLAN-PEAP
   Tools\msstools.cmd" BackupIAS /path:C:\IASBackup
   ```

   (This command may wrap to more than one line here, but you should enter it as a single line. "**Microsoft WLAN-PEAP Tools**" contains two embedded spaces; one after "Microsoft" and the other after "WLAN-PEAP.")

   Note: If the backup is successful, an event will be written to the Windows Application log and to the screen; otherwise, error events will be logged.

   ---

4. Create a scheduled task that will run the IAS configuration export every night. For example, the following command schedules the job to run at 10:00 P.M. every night:

```
SCHTASKS /Create /RU system /SC Daily /TN "IAS
Backup" /TR "\"C:\Program Files\Microsoft\Microsoft WLAN-
PEAP Tools\msstools.cmd\" BackupIAS /path:C:\IASBackup"
/ST 22:00
```

(This command may wrap to more than one line here, but you should enter it as a single line. "**Microsoft WLAN-PEAP Tools**" contains two embedded spaces; one after "Microsoft" and the other after "WLAN-PEAP.")

Note: Enclosing the path to the msstools.cmd script file within backslashes (\) ensures that the double quotation marks (“) do not get interpreted and stripped from the command by the Windows command shell. The command that gets passed to and stored by the task scheduler is as shown in step 3.

Taking Server Backups

Having set up a scheduled task to back up IAS configuration to disk, you must also configure a regular backup of the server system state and the exported IAS configuration files to a removable medium or to a network location. The simplest way to do this is to use the built-in Windows Backup tool. If you use a different backup system, you must establish whether it includes the functionality equivalent to the Windows system state backup (you should be able to find this out from your backup system's documentation). A system state backup (or equivalent) is essential to properly back up Active Directory and Certificate Services keys and certificate databases.

If your backup software does not have Windows system state backup functionality, you can perform the following steps:

- Configure Windows Backup to perform a system state backup to a file on the server (you must ensure that you have enough disk space for this because a system state backup will be 500 MB or larger). See the Windows Backup online help for details on how to do this.
- Configure your backup software to copy the system state backup file as well as the IAS backup file described in the previous procedure.

You should do the following to ensure safe and consistent backups:

- Schedule the different backup operations so that they do not overlap; otherwise, you run the risk of corrupting the backup data.
- Start the server and system state backup at least 10 minutes after the start time of the IAS backup.
- If you are performing separate system state and server file backups, allow at least one hour for the system state backup to complete before starting the server file backup.
- Always store a recent copy of the backup data at a physical location other than that of the backed up server. This will help you recover the server in the event that all computer equipment at the site is destroyed or becomes inaccessible.

Caution: This backup data is very sensitive because it contains the RADIUS secrets for all APs on this server, all of the private key material for the CA, and the Active Directory database. You must transport and store the backup media securely because unauthorized access to this data could compromise the security of your entire organization.

Testing the Backups

You can test system backups adequately only by restoring them to a test server and verifying that the restored server functions as expected. A system state backup must be restored to a system that has a disk layout identical to that of the backed up server. For example, Windows must be installed in the same path on the test restore server as on the backed up server and the drive layout for storing Windows files (such as paging files) should be identical for the two servers.

Important: To help avoid name and IP address clashes between the test restore server and the original server, the test server should be kept offline from the time when the system state restore is started.

▸ **To restore the server**

1. Prepare a restore server on to which you want to restore the backed up data. On the restore server, you need to use the same edition of Windows Server 2003 used on the backed up server. (You must also install the solution scripts on this server. For more information, see the "Installing the Solution Tools" section in Chapter 3, "Preparing Your Environment.")
2. If you are using a separate system state backup and file backup, use your backup software to restore the system state backup file and the IAS settings backup file from the backup medium to the server. The IAS settings should be restored to the same path: C:\IASBackup.
3. Run the Windows Backup utility and select the restored system state backup file. You need to be a member of a group that has Backup and Restore rights on the computer (such as Backup Operators or Administrators).
4. Click **Restore**.
5. Restart the system.
6. Verify that everything functions as expected after the restart and that the Active Directory and Certificate Services have started without error (you should expect to see errors in the event logs due to the fact that the server is not connected to the network).
7. Use the **MSS WLAN Tools** shortcut to open a command shell. Restore the IAS configuration by running the following command:

```
MSSTools RestoreIAS /path:C:\IASBackup
```

8. Verify that the IAS settings have been restored by opening the IAS management console and checking the RADIUS clients and Remote Access Policies folders.

Monitoring

This section describes monitoring the IAS and CA components of the WLAN security infrastructure. It does not include any guidance on monitoring the wireless APs or other network devices, nor does it include general advice on monitoring Windows servers. Information on monitoring Windows servers is available from the "References” section at the end of the chapter.

Most of the procedures in this section use automated monitoring scripts supplied with the solution. If these scripts detect a failure, they will trigger an alert and, in some cases, attempt to recover from the failure.

Configuring Alert Types

Any alerts from the monitoring scripts can be sent to the Windows Application event log or to one or more e-mail recipients (or both). Before enabling the monitoring tools, you need to specify the alert types that you want. In addition, if you have opted to send e-mail alerts, you need to provide the e-mail addresses of the recipients and the name of the e-mail server to which you want to send the messages.

To specify these parameters, you need to edit the constants.vbs file. The relevant sections from this file are shown here, with items that you may want to change shown in *Italics*:

```
'Alerting parameters
CONST ALERT_EMAIL_ENABLED = FALSE     'set to enable/disable e-mail
CONST ALERT_EVTLOG_ENABLED = TRUE     'set to enable/disable eventlog entries
' set to comma-separated list of recipients to get e-mail alerts
CONST ALERT_EMAIL_RECIPIENTS  = "Admin@woodgrovebank.com,Ops@woodgrovebank.com"
'SMTP server to use (use DNS name or IP address)
CONST ALERT_EMAIL_SMTP  = "mail.woodgrovebank.com"
```

Monitoring IAS

IAS will record many different events in the Windows System log. These include service start and stop notifications (and any associated errors or warnings) and notifications of authentication attempts. (Authentication request log entries are described in detail in the "Troubleshooting” section later in this chapter.)

Enabling Monitoring of IAS

The solution includes a simple script that monitors the responsiveness of IAS. The script checks to see if IAS process is running. If it is, the script tries to query IAS using the **Server Data Objects** interface. If either of these checks fails, the script issues an alert.

Note: The monitoring script does not check for successful RADIUS authentication—it only checks the general responsiveness of the IAS process. To check end-to-end RADIUS operations, you need a RADIUS client to emulate the wireless APs relaying the WLAN client request.

The following procedure describes how to configure the monitoring script to run as a scheduled task so that it automatically alerts you if IAS stops responding. However, because the script is running on the server itself, it will obviously not alert you if the server as a whole has failed; therefore, you must also monitor your servers to ensure that they are alive and responding. You need to carry out the following procedure to configure the script to run as a scheduled task on each IAS server.

Every time an error is detected, an alert is sent by e-mail (if e-mail alerts have been configured) and an event is written to the Application log (see the table in the next section for details of the event types logged). In contrast to the CA monitoring script, no attempt is made to correct problems by restarting IAS. Because IAS, unlike a CA, is needed continuously to authenticate WLAN clients, allowing the monitoring script to blindly restart IAS may cause problems rather than resolve them. Instead, you should watch for any alerts generated by the script and perform a proper diagnosis of the cause of the alert before attempting to repair the problem manually.

To configure IAS monitoring

1. Open a command shell using the **MSS WLAN Tools** shortcut.
2. Run the following command to schedule the script to run every hour starting at 1:30 A.M. (it runs 30 minutes past the hour to offset it from the IAS backup job).

```
SCHTASKS /Create /RU system /SC Hourly /TN "IAS
Check" /TR "\"C:\Program Files\Microsoft\Microsoft WLAN-
PEAP Tools\msstools.cmd\" CheckIAS" /ST 01:30
```

(This command may wrap to more than one line here, but you should enter it as a single line. "**Microsoft WLAN-PEAP Tools**" contains two embedded spaces; one after "Microsoft" and the other after "WLAN-PEAP.")

Note: Enclosing the path to the msstools.cmd script file within backslashes (\) ensures that the double quotation marks (") do not get interpreted and stripped from the command by the Windows command shell. Using backslash (\) before the quotes (") ensures that the command that gets passed to and stored by the task scheduler is as shown in step 2.

IAS Events Logged by the MSS Scripts

The monitoring script and the IAS backup script log the following types of events to the event log.

Table 8.5: IAS Events Returned by IAS Tools Scripts in This Solution

IAS Event	Significance	Event Category	Event Source	Event ID
IAS Backup OK	*Backup of IAS configuration to file succeeded.*	*Information*	*IAS Operations*	*210*
IAS Invalid Backup Path	*Backup failed because invalid destination path was specified.*	*Error*	*IAS Operations*	*211*
IAS No Access to Backup Path	*Backup failed because backup files could not be written to the destination path specified.*	*Error*	*IAS Operations*	*212*
IAS Restore OK	*IAS settings successfully restored from the saved configuration.*	*Information*	*IAS Operations*	*220*
IAS Restore Failed	*Restoration of IAS settings failed.*	*Warning*	*IAS Operations*	*221*
IAS Policy Query Failed	*IAS could not be contacted using Server Data Objects interface. IAS may not be running.*	*Error*	*IAS Operations*	*230*

IAS Event	Significance	Event Category	Event Source	Event ID
IAS No Policies Detected	*IAS does not contain any remote access policies.* *This should never occur on a normally configured IAS server and probably indicates an IAS or a network problem.*	*Error*	*IAS Operations*	*231*
IAS Not Installed	*IAS is not installed on the computer.*	*Error*	*IAS Operations*	*232*
IAS Had Stopped	*The IAS service was not running but was started successfully.*	*Warning*	*IAS Operations*	*233*
IAS Not Running	*An attempt to start the IAS service failed.*	*Error*	*IAS Operations*	*234*

Monitoring the Certification Authority

The CA requires relatively little attention beyond monitoring for general server health and performing adequate backup. In this solution, the CA is only required for the relatively rare tasks of issuing certificates to new IAS servers and renewing existing certificates once a year. The CA, therefore, is not normally a critical service.

The CA also publishes a list of certificates that have been revoked by the administrator. This list, known as a Certificate Revocation List (CRL), is published weekly to the Active Directory. This CA will only issue a small number of certificates, so the CRL will also be small and will typically be empty. Despite this, it is essential that the CRL is published to Active Directory in a timely manner so that the applications can check on the revocation status of any certificates issued by the CA. For example, the CA itself needs to check the revocation status of any certificate it issues before sending it to the certificate requestor.

The CA monitoring script checks that the CA is responding to requests and that a valid CRL is available in Active Directory. If either of these checks fails, the script attempts to restart the CA. In case of a CRL failure, it also tries to publish a new CRL. If a failure is detected even after these recovery attempts, an alert is generated that is sent as an e-mail message to the configured e-mail account and is written to the event log.

Enabling Monitoring of the Certification Authority

The following procedure describes how to configure the monitoring script to run as a scheduled task so that it will automatically alert you and attempt recovery if an error is encountered. This script needs to be run only on the CA server.

▸ **To configure the CA monitoring script**

1. Open a command shell using the **MSS WLAN Tools** shortcut.

2. Run the following command to schedule the script to run every hour starting at 1:20 A.M. (it is scheduled to run 20 minutes past the hour to offset it from other scheduled tasks).

   ```
   SCHTASKS /Create /RU system /SC Hourly /TN "CA Check"
   /TR "\"C:\Program Files\Microsoft\Microsoft WLAN-PEAP
   Tools\msstools.cmd\" CheckCA" /ST 01:20
   ```

   (This command may wrap to more than one line here, but you should enter it as a single line.)

   Note: Enclosing the full path of the msstools.cmd script file within backslashes (\) ensures that the double quotation marks (“) do not get interpreted and stripped from the command by the Windows command shell. The path stored by the task scheduler must be enclosed in quotes if it includes any embedded spaces (such as in "Program Files"). Using a backslash (\) before the quotes (“) ensures that the path stored by the task scheduler is enclosed in double quotation marks.

Certification Authority Events Logged by the MSS Scripts

The CA monitoring script logs the following events to the event log.

Table 8.6: CA Events Returned by the CA Monitoring Script in This Solution

CA Event	Significance	Event Category	Event Source	Event ID
CRL expired	*A valid CRL is not accessible—this is currently causing a loss of service.*	*Error*	*CA Operations*	*20*
CRL overdue	*The CRL is still valid but a new one is overdue and should have been published.*	*Error*	*CA Operations*	*21*
CRL cannot be retrieved from Active Directory	*A CRL is not available at a published CRL distribution point. This may be causing loss of service.*	*Error*	*CA Operations*	*22*
Certificate Services service not responding: *Event ID 1—Client Interface offline* *Event ID 2—Admin Interface offline*	*Certificate Services remote procedure call (RPC) interface is offline—certificates cannot be issued. May require service restart.*	*Error*	*CA Operations*	*1 and 2*
Other event	*CA monitor script execution failure.*	*Error*	*CA Operations*	*100*

Managing Changes

The tasks in this section relate to changes that you may need to make to the configuration of your WLAN security infrastructure.

Windows Security Update Management

Both IAS and Certificate Services updates are included in the base service packs and patches for Windows Server 2003; you do not need to update these components separately.

You should read through the guidance and follow the references given in the "Server Security Patching" section in Chapter 3, “Preparing Your Environment.”

Managing Changes on Your IAS Servers

Chapter 5, “Building the Wireless LAN Security Infrastructure,” recommended that you nominate one of your IAS servers as the "master" server; the server on which you will make all IAS configuration changes (see the "Deploying Settings to Multiple IAS Servers" section in Chapter 5). These changes will then be replicated to the other servers in your organization, using automated export and import of the IAS configuration database to ensure consistent settings throughout your IAS infrastructure.

The set of RADIUS clients (the wireless APs) configured on each IAS, however, are not normally replicated. The Wireless APs supported by each server may vary substantially and rarely will two IAS servers have exactly the same set of clients (this can be the case if you have two central IAS servers to service all wireless APs in your organization, for instance).

Backing up IAS Settings Prior to Making Changes

Even though you have scheduled backups of your servers every night, it is a good idea to perform a manual backup of IAS prior to making changes on your servers. This will allow you to roll back any changes and restore the server state immediately prior to the changes made. The following procedure uses the backup script to export server configuration, policies, log settings, and RADIUS clients.

► **To backup the IAS configuration**

1. Open a command shell on the server using the **MSS WLAN Tools** shortcut and use the following command to create a folder to save the IAS export file:

   ```
   md c:\IASSaveState
   ```

   (The IAS configuration is typically less than 100 KB and can be saved to the system drive, as shown in the example. However, any path can be used as long as it is used consistently in this and the subsequent commands.)

2. Run the following commant to set permissions for the folder so that only administrators and backup operators can read and modify its contents:

   ```
   cacls c:\IASSaveState /G system:F administrators:F "Backup Operators":C
   ```

   (This command may wrap to more than one line here, but you should enter it as a single line.)

3. Run the backup script to export the IAS settings by issuing the following command:

   ```
   MSSTools BackupIAS /path:C:\IASSaveState
   ```

Replicating Settings to Other IAS Servers

You should establish your own repeatable procedure to ensure that the settings from your master server are replicated to all other IAS servers in your organization. This may involve instructing local support staff to import the settings. More often, this will be performed remotely by copying the configuration files and using a Remote Desktop session to run the configuration import script.

To replicate the settings to other IAS servers, follow the procedures described in the "Replicating Settings from the First IAS Server" section in Chapter 5, “Building the Wireless LAN Security Infrastructure.”

Note: You might find it useful to embed a version number in the Remote Access Policy name so that it is easy to check that all IAS servers have same settings version.

Adding IAS Servers to Your Environment

Before installing a new IAS server, you should identify the wireless APs that will be configured as clients of this server, following the guidelines provided in Chapter 2, “Planning a Wireless LAN Security Implementation.” You will also need another IAS server configured as the secondary RADIUS server to provide the APs with resilience in case of server failure. If you are reconfiguring the existing APs to use this new server, you must carefully plan the migration to avoid disruption of service for your users during the AP switchover. Normally, as long as an AP has at least one active authentication RADIUS server, there will be no disruption.

► **To install IAS on a new server**

1. Follow the guidelines in Chapter 3, "Preparing Your Environment" to prepare your server.
2. Follow the instructions included in the "Installing IAS" and the "Registering IAS in Active Directory" sections in Chapter 5, "Building the Wireless LAN Security Infrastructure."
3. To replicate changes from your master IAS server to the new server, follow the "Replicating Settings from the First IAS Server" procedure described in Chapter 5, "Building the Wireless LAN Security Infrastructure."
4. Finally, add the RADIUS client entries for the wireless APs to IAS and configure the Wireless APs to use the new IAS server.

Adding a Wireless Access Point to the Network

To add a new wireless AP, you need to complete the following two tasks:

1. Add the AP as a RADIUS client to a primary and a secondary IAS server.
2. Configure the AP to use the IAS servers as primary and secondary RADIUS servers.

The IAS servers you choose as primary and secondary RADIUS servers will depend on the network location of the AP. Ideally, choose a primary IAS server that is on the same LAN as the AP or at least has reliable connectivity to the AP. Choose a secondary IAS server that has reliable connectivity to the AP. For more information, see the guidance provided in the "Assignment of APs to RADIUS Servers" section in Chapter 2, “Planning a Wireless LAN Security Implementation.”

Once you have identified suitable IAS servers for the AP, carry out the following procedures. These are the same as the procedures given for adding an AP to IAS in Chapter 5, "Building the Wireless LAN Security Infrastructure.”

To add an AP to the network

1. To add the AP as a RADIUS client to the primary IAS, follow the procedure described in the "Adding APs to the First IAS Server" section in Chapter 5, “Building the Wireless LAN Security Infrastructure.”
2. To add the AP as a RADIUS client to the secondary IAS, follow the procedure described in the "Importing the APs into the Second IAS Server" section in Chapter 5, “Building the Wireless LAN Security Infrastructure.”
3. Configure the AP by following the guidance provided in the “Configuring the Wireless Access Points" section in Chapter 5, "Building the Wireless LAN Security Infrastructure."

Removing a Wireless Access Point

You might need to remove a wireless AP from the network if you are relocating or reorganizing your sites. You should always remove RADIUS client entries from IAS if they are no longer in use.

To remove a wireless AP from the network

1. Identify the primary and secondary IAS for the AP to be removed.
2. Use the **Internet Authentication Service** MMC to delete the RADIUS client entry for the AP. (Verify that the RADIUS client IP matches the IP address of the decommissioned AP; do not rely on the name of the RADIUS client.)
3. Repeat step 2 on the secondary IAS server.

Granting WLAN Access to a User or Computer

If you have followed the default setup for this solution, all users and computers in the domain in which you installed the IAS servers will automatically have access to the WLAN. This is because the Domain Users and Domain Computers groups are members of the Wireless LAN Users and Wireless LAN Computers groups, respectively. These groups are, in turn, members of the Wireless LAN Access group, which is used by the IAS remote access policy to grant access to the WLAN.

Controlling Access for Members of the Same Domain

If you want to explicitly control which users and computers can connect to the WLAN, you should use security groups to manage their access. You should remove the Domain Users and Domain Computers groups from the Wireless LAN Users and Wireless LAN Computers groups, respectively. In their place, add the specific users and computers to which you want to grant access to the WLAN.

This changes the solution default so that the WLAN is inaccessible to everyone unless access is explicitly granted by adding someone to a security group. This is a more precautious approach than "allow by default" and is normally preferred by organizations with high security needs. It may also be useful in other cases where only a limited number of people are allowed access to the WLAN; for example, during the pilot phase of a larger rollout.

To enable WLAN access for a user or computer in the same domain

1. Using **Active Directory Users and Computers**, add the user or computer account to the Wireless LAN Users or Wireless LAN Computers group.
2. If you are adding a user, ask the user to log off and log on again. If you are adding a computer, reboot the computer.
3. Verify that the user or computer can access the WLAN.

Controlling Access for Members of Another Domain

If you have a multi-domain forest, you may want to enable users and computers from other domains to use the WLAN. For this, you need to be logged on using an account that is one of the following:

- An administrator of both domains
- An account that has permissions to create groups in the other domains and permissions to modify the membership of the Wireless LAN Access group in your home domain (that is, the domain into which the IAS servers are installed).

▶ **To grant WLAN access to the users and computers from other domains**

1. Log on with an account that has permissions to create groups in the domain containing the users and computers that you want to grant access to the WLAN (the target domain).
2. Open **Active Directory Users and Computers** and focus on a domain controller for the target domain.
3. Create a domain global group named Wireless LAN Users in the target domain.
4. Create a domain global group named Wireless LAN Computers in the target domain.
5. Log on with an account that has permissions to modify the membership of the Wireless LAN Access group in the home domain. Using **Active Directory Users and Computers**, find the Wireless LAN Access group and open it to edit its properties. From the **Membership** tab of the group properties, add the Wireless LAN Users and Wireless LAN Computers groups from the target domain as members of this group.
6. Identify the users from the target domain who require WLAN access. Add their accounts to the Wireless LAN Users group in that domain. Likewise, add the required computer accounts from the target domain to the Wireless LAN Computers group in that domain. Alternatively, you can add Domain Users and Domain Computers to these groups to allow all members of the target domain to access the WLAN.

Denying WLAN Access to a User or Computer

The default for this solution is to allow access to the WLAN to all users and computers in the domain into which you installed the IAS servers. They are granted access automatically because they are members of the Domain Users and Domain Computers groups, respectively. This can be problematic if you need to block WLAN access for individual users or computers. You must not remove users or computers from the built-in Domain Users and Domain Computers groups. Use one of the following strategies instead:

- If the user has left the organization (or, in the case of a computer, it has been lost or stolen), you can disable the Active Directory account of that user or computer.
- Manage access by using the Remote Access Permissions on the user or computer account object to allow or deny access. This was discussed briefly in the "Allowing Users and Computers to Access the WLAN" section in Chapter 6, “Configuring the Wireless LAN Clients.”
- If you want to remove WLAN access from a user or computer but continue to allow the account to be used for normal domain access and other network access you need to either use a selective access WLAN model or implement a remote access "Deny" policy. The option you choose will depend on whether you want WLAN

access to be granted by default or you want to deny access by default and grant WLAN access to only specified users.

- Using specific group memberships to implement a selective access policy was described earlier in the chapter in the "Granting WLAN Access to a User or Computer" procedure. You can deny access to the WLAN simply by removing a user or computer from the relevant security group.
- Creating an IAS remote access policy to deny access to selected groups is described in the following procedure "Controlling WLAN Access Using a Deny Policy."

Important: You should not remove users or computers from the Domain Users or Domain Computers groups, respectively. Although it is technically possible, doing this will prevent the user or computer account from functioning correctly in normal domain use.

Controlling WLAN Access Using a Deny Policy

If you want to allow access by default but be able to deny access to individual users and computers by exception, you need to create a "Deny" Remote Access Policy in IAS.

▸ **To create a Deny Remote Access Policy**

1. In **Active Directory Users and Computers**, create a universal group named Deny Wireless LAN Access.
2. Create domain global groups Deny Wireless LAN Users and Deny Wireless LAN Computers and add them as members of the Deny Wireless LAN Access group.
3. Log on to the master IAS server that you use to edit global IAS settings (these settings will be replicated to the other IAS servers later).
4. In the **Internet Authentication Service** MMC, right-click the **Remote Access Policies** folder and select **New Remote Access Policy…**
5. Select **Set up a Custom Policy** and type **Deny Wireless LAN Access** for the policy name. Click **Next** to continue.
6. Click **Add…** to add a policy condition and select **Windows–Groups** from the list and click **Add...**
7. Click **Add…** to add a security group. Type (or browse for) the Deny Wireless LAN Access group and click **OK**.
8. Click **Add…** to add another policy condition and select **NAS-Port-Type** from the list and click **Add...**
9. From the list of **Available types**, select **Wireless - IEEE 802.11** and click **Add >>**. Then select **Wireless – Other** and click **Add >>** to add them to the **Selected types** list. Click **OK** to complete and click **Next** to continue.
10. Select **Deny remote access permission** and click **Next** to continue.
11. At the **Profile** screen, click **Next** to skip and then click **Finish** to complete.
12. The **Deny Wireless LAN Access** policy should be created at the top of the list (highest priority) of policies (or at least above the Allow Wireless LAN Access policy). If it is not, right-lick the policy name and click **Move Up** until it is higher in the list than the **Allow Wireless LAN Access** policy.
13. Use the procedures described earlier to replicate the new settings to the other IAS servers in your organization.

Any users or computers that you add to the Deny Wireless LAN Users or Deny Wireless LAN Computers groups will be refused access to the WLAN. However, this setting will only take effect the next time the denied user logs on or the denied computer is restarted.

Support Tasks

This section covers common tasks that you need to perform to recover from problems in your WLAN security infrastructure. Many of these tasks are referenced by the “Troubleshooting” section included in this chapter.

Restoring an IAS Server Configuration from Backup

IAS policies and settings are stored in the IAS configuration database. They can be restored independently of the rest of the system settings. You should schedule the IAS backup task to backup IAS settings to the C:\IASBackup folder every night. For more information on this topic, see the "Configuring the IAS Backup" procedure in the "Operational Tasks" section of this chapter. If you need to undo changes made that day, you can restore settings from the backup files (in C:\IASBackup) created the previous night or from the "rollback" backup made prior to the making changes. For further details, see the "Backing up IAS Settings Prior to Making Changes" procedure in the "Managing Changes" section.

If you need to restore an earlier version of the settings, you must recover the exported IAS settings from the server backup.

Warning: This procedure will restore all IAS settings including RADIUS clients, overwriting any existing settings on the server. The backup that you are attempting to restore should be one that was taken from the same server.

▸ **To restore the IAS settings**

1. If the IAS setting backup files that you want to use are not on the server, you must restore them from backup media. Be sure to select only the files in the IASBackup folder to restore. Do not restore System State unless you also want to revert to earlier system-wide settings.
2. Use the **MSS WLAN** Tools shortcut to open a command shell. Restore the IAS configuration by running the following command:

```
msstools RestoreIAS /path:C:\IASBackup
```

3. Verify that the IAS settings have been restored by opening the IAS management console and checking the RADIUS clients and Remote Access Policies folders.

If, for some reason, you do not have a usable backup of this system, you can export the settings from another IAS server and import them to this server. Typically, IAS servers in the same role will share the same configuration settings but will have a different set of RADIUS clients, so you should not use this procedure to restore the settings from another server. Instead use the "Replicating Settings from the First IAS Server" procedure described in Chapter 5, “Building the Wireless LAN Security Infrastructure.”

Important: You must ensure that the restored system is patched up to date. Restoring from an old backup may mean that patches previously applied have been rolled back.

Restoring Full Server Configuration from Backup

Procedures for restoring the server will vary depending on the choice of backup system. The following is based on the assumption that you have backed up the system by performing Windows system state backup to a file, followed by a file backup of this file and other required files.

▸ **To restore the server**

1. Depending on the state of the server, you may need to prepare the server from scratch; for example, if a severe hardware failure has destroyed the server system disks. Otherwise, you can perform a restore directly to it without reinstalling the operating system.
2. If you are using separate system state backup and file backup, use your backup software to restore the system state backup file and the IAS settings backup file from the backup medium to the server. The IAS settings should be restored to the same path, which is C:\IASBackup.
3. Run the Windows Backup utility and select the restored system state backup file. You need to be a member of the group, that has Backup and Restore rights on the server (such as Backup Operators or Administrators).
4. Click **Restore**.
5. Restart the system.
6. Verify that everything performs as expected and that Active Directory and Certificate Services, if installed, have started without error.
7. Use the **MSS WLAN Tools** shortcut to open a command shell. Restore the IAS configuration by running the following command:

```
MSSTools RestoreIAS /path:C:\IASBackup
```

8. Verify that the IAS settings have been restored by opening the IAS MMC and checking the RADIUS clients and Remote Access Policies folders.

Important: If IAS is running on a domain controller, restoring a system state backup will also restore the backed up version of the Active Directory database on that server. However, any changes made to Active Directory after the backup was made will be replicated to the restored server at the next Active Directory replication cycle.

Optimization Tasks

This section covers the tasks that are relevant for optimizing the running of the IAS infrastructure.

Determining Maximum Load on the IAS Server

This section provides information on the likely maximum load on the IAS server.

Performance is rarely an issue for IAS servers that are properly sized and configured. IAS servers are under most load during peak times such as morning hours when many users simultaneously log on, shortly after a major network outage, or during a RADIUS server failure when wireless APs failover to a backup server.

The following table gives an indication of the WLAN authentication requirements for different sizes of organization.

Table 8.7: WLAN Authentication Requirements

Number of WLAN Users	New Authentications per Second	Peak New Authentications per Second	Re-authentications per Second
100	> 0.1	0.1	0.1
1000	0.1	0.6	1.1

Number of WLAN Users	New Authentications per Second	Peak New Authentications per Second	Re-authentications per Second
10,000	1.4	5.6	11.1

The New Authentications per Second column is a part of the steady load; you can assume an average of four new full authentications as users rove between wireless APs. The Peak New Authentications per Second column indicates the type of load expected when all users require authentication over a 30 minute period (for example, at the start of the day). The Re-authentications per Second column shows the number of authentications with fast reconnect caused by IAS forcing a session time-out after 15 minutes. (Although a 60 minute time-out is the solution default, 15 minutes is used here to give a worst-case figure.) You should assess these figures against your own organization's requirements to determine the type of load that you need to support.

Internal tests by Microsoft show that IAS can handle a high load on modest server hardware. The load serviced by IAS is best represented by the number of Extensible Authentication Protocol (EAP) authentications per second. The following table shows the results from an IAS server running on an Intel Pentium 4 2GHz server running Windows Server 2003.

The tests were conducted with RADIUS logging enabled (to a separate disk) and with IAS on a separate server from the Active Directory domain controller; therefore, these figures should be regarded as a worst case. The default configuration for this solution is to have logging disabled and IAS housed on the same server as the domain controller. Both of these items will improve authentication throughput.

Note: This information is provided without warranty of accuracy and should only be used as a guideline for capacity planning purposes and not for performance comparisons.

Table 8.8: Sample IAS Server Capacity Measurements

Authentication Type	Authentications per Second
New Protected Extensible Authentication Protocol (PEAP) authentications	*36*
New PEAP authentications with TLS/SSL offload card support	*50*
Authentications with fast reconnect	*166*

IAS can be configured to generate disk-based RADIUS logs containing varying amounts of RADIUS request information. If you choose to enable RADIUS logging, you should consider the overhead that this will place on the servers, particularly on the disk subsystems. Slow disk throughput will act as a bottleneck on IAS performance and will delay IAS RADIUS responses to APs, leading to protocol time-outs and unnecessary failover of APs to secondary RADIUS servers. If you expect a high load (you can use the figures in the previous tables as a guideline) and are going to enable RADIUS logging, you should ensure that IAS is configured to write RADIUS logs to a high performance disk that is separate from the Windows system drive and page file drive.

Enabling Windows Server 2003 IAS tracing features (as described in the "Enabling and Disabling Tracing on the IAS Server" section in this chapter) will also generate additional load on IAS servers. This may be required occasionally to troubleshoot network access issues but should not be enabled permanently. Nevertheless, you may want to ensure that your IAS servers have some additional headroom to allow tracing to be used for limited periods of time and still service the production load.

Other Optimization Measures

For other IAS optimization guidelines, see the "Designing an Optimized IAS Solution" section in the "Deploying IAS" chapter of the *Windows Server 2003 Deployment Kit*.

Troubleshooting

This section contains procedures and techniques that will help you diagnose and fix problems with the wireless LAN solution.

Troubleshooting Procedures

The following procedures help you identify the possible causes of a problem and the action to take to resolve the problem. This section is organized hierarchically. The first procedure "Determining the Kind of Problem” will point you to one of several procedures, each of which drills down into detailed troubleshooting steps. These procedures, in turn, may point you to further troubleshooting procedures that focus on particular components of the solution.

Each of these procedures is described in detail later in this chapter (some are given in the pictorial form; others, for which the text description is too lengthy for a figure, are presented in tables or text). Some of the procedures make use of the "Troubleshooting Tools and Techniques" section of this chapter. You should familiarize yourself with that section to use the troubleshooting procedures effectively.

Important: These diagnostic procedures do not cover every eventuality. Where the recommended investigation steps do not lead you to the source of the problem, you should backtrack and follow the other diagnostic procedures given here. Sometimes, the full extent or nature of symptoms is not apparent and may point you in the wrong direction. For example, a single user may be the only person in an office to report a problem that affects the whole office. Although the table points to diagnostic procedures related to a single client failure, other procedures are probably more appropriate.

You should also consult the WLAN and IAS troubleshooting documents listed at the end of the chapter.

Determining the Type of the Problem

Start by classifying the type of problem that you are experiencing, using the following flowchart. The diamonds represent questions or decision points and the rectangles represent the diagnosis of the problem and indicate the name of the procedure to follow.

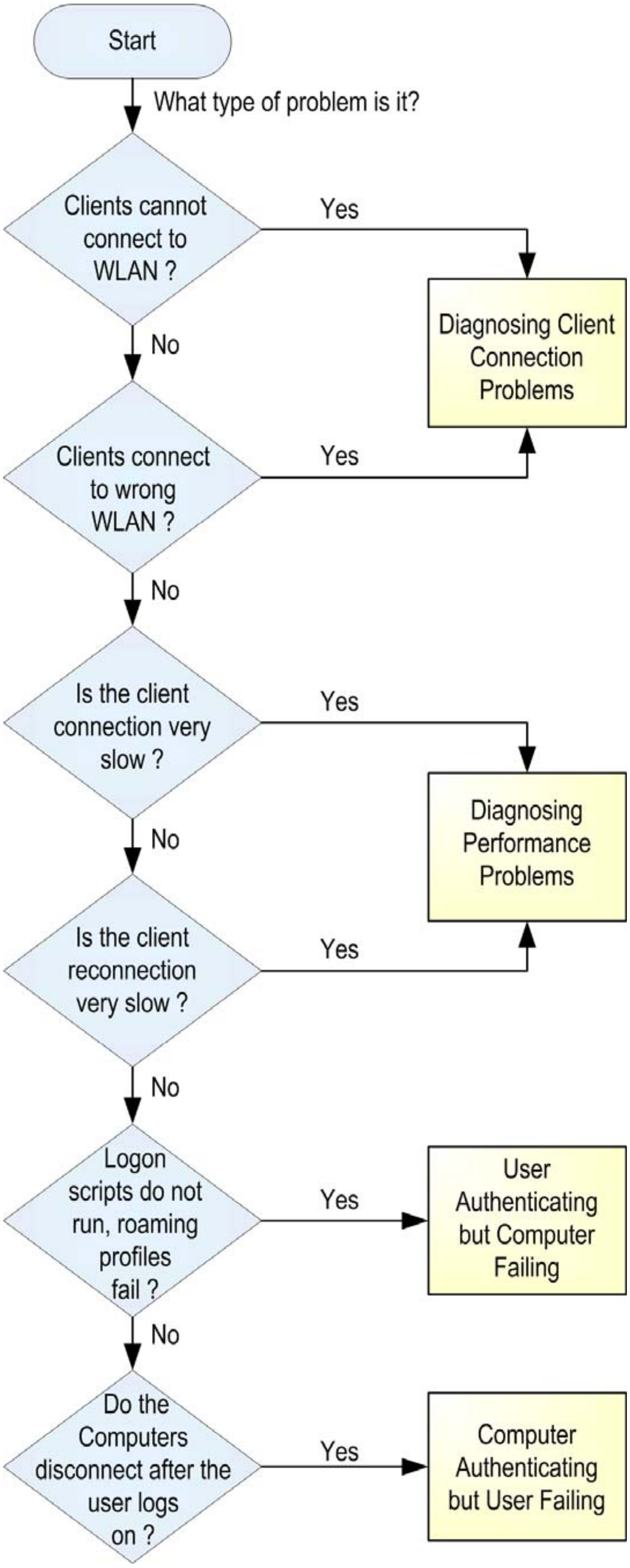
Start
What type of problem is it?
Clients cannot connect to WLAN ?
Yes
No
Diagnosing Client Connection Problems
Clients connect to wrong WLAN ?
Yes
No
Is the client connection very slow ?
Yes
No
Diagnosing Performance Problems
Is the client reconnection very slow ?
Yes
No
Logon scripts do not run, roaming profiles fail ?
Yes
No
User Authenticating but Computer Failing
Do the Computers disconnect after the user logs on ?
Yes
Computer Authenticating but User Failing

Figure 8.1

Determining the type of problem

Diagnosing Client Connection Problems

The following table categorizes different types of connection problems based on the number and location of clients affected. The Likely Problem(s) column indicates the factors that are most likely to produce the shown symptoms. The Diagnostic Procedures to Follow column lists the diagnostic procedures that you should try first to diagnose the problem. Each of these procedures is described in detail later in this chapter.

Table 8.9: Who is Unable to Connect to the WLAN?

Symptom	Likely Problem(s)	Diagnostic Procedures to Follow
A single client	*Computer configuration or user/computer account.*	*Check User/Computer Account* *Check Client Computer*
Several clients at one site	*Misconfiguration of one or more APs.*	*Check Wireless AP configuration*
Whole of a site (local IAS)	*Misconfigured or malfunctioning IAS server onsite; Active Directory replication problems preventing local domain controller receiving correct information; malfunctioning IAS server coupled with WLAN connectivity problem.*	*Check Active Directory and Network Services* *Check IAS* *Check WAN Connectivity*
Whole of a site (no local IAS)	*WLAN connectivity problem; Active Directory replication problems (if local domain controller).*	*Check WAN Connectivity*
All clients in all sites	*Organization-wide configuration (client settings Group Policy object (GPO), RAP groups, certificate renewal failures.*	*Check Active Directory and Network Services ("Check WLAN settings GPO" and "Check Active Directory Groups" checks)* *Check the CA* *Check IAS*

Diagnosing Performance Problems

This section focuses on performance problems associated with the WLAN security infrastructure. General wireless and wired network performance problems are not dealt with in this chapter.

Table 8.10: Performance Problems

Symptom	Possible Solution

Symptom	Possible Solution
Authentication delay affecting many users	*IAS server heavily loaded, check performance monitor.*
	Authentication across a slow WLAN link (even if you have a local IAS check that APs have not failed over to the remote IAS).
	Delays with a Dynamic Host Configuration Protocol (DHCP) server issuing an IP address can affect total connection time.
Re-authentication delay when roaming between APs	*A delay of a few seconds is normal when switching between APs.*
	If a client goes out of range of an AP (and stays out of range longer than 10 seconds), it can take up to 60 seconds for re-authentication to start after coming back in range of an AP. This happens because the Windows WLAN client, when disconnected from a WLAN, only polls for WLANs every 60 seconds.
WLAN network throughput is low	*This symptom may be due to too many clients using too few APs, incorrect AP placement, weak radio signal caused by obstruction or excessive distance.* *All these are aspects of the WLAN network design and are outside the scope of this documentation. You should consult your vendor or solution provider for advice.* *For more information, see the "Deploying a Wireless LAN" chapter of the* Windows Server 2003 Deployment Kit*.*

User Authenticating but Computer Failing

This solution uses both user authentication and computer authentication to the WLAN. The computer domain credentials are used to authenticate to the WLAN when no user is logged on to the computer. When a user logs on, the user's credentials are then used to re-authenticate to the WLAN. This arrangement allows the computer to communicate with the WLAN when no one is logged on and enables the computer to be managed remotely, to download server GPO settings, and so forth.

When a user logs on to a WLAN computer, there is a slight delay while the user is authenticating to the WLAN. Until the user is properly authorized to connect, the computer's authenticated WLAN session is still active. However, if the computer was unable to authenticate to the WLAN, this delay means that there is no network connectivity at the start of the user's logon session.

This can cause a number of subtle problems. For example, roaming user profiles will fail to load, some computer GPO settings will not be applied, and user logon scripts and GPO-based software deployments (which run very early in the logon process) will fail.

To determine the cause of the failure of computer authentication, you should follow the "Check User/Computer Account" procedure later in this guide.

Computer Authenticating but User Failing

Unlike the previous case, this problem is immediately obvious and will be reported by the affected users straight away. To determine the cause of failing user authentication, you should follow the "Check User/Computer Account" procedure.

Diagnostic Procedures

The following section provides the detailed troubleshooting steps referred to in the previous sections.

Check User/Computer Account

The following flowchart helps you in diagnosing the cause of a user or computer authentication failure.

Note: The arrow shaped box in the flowchart indicates that you should refer to the "Check Client Computer" procedure, as specified in the box.

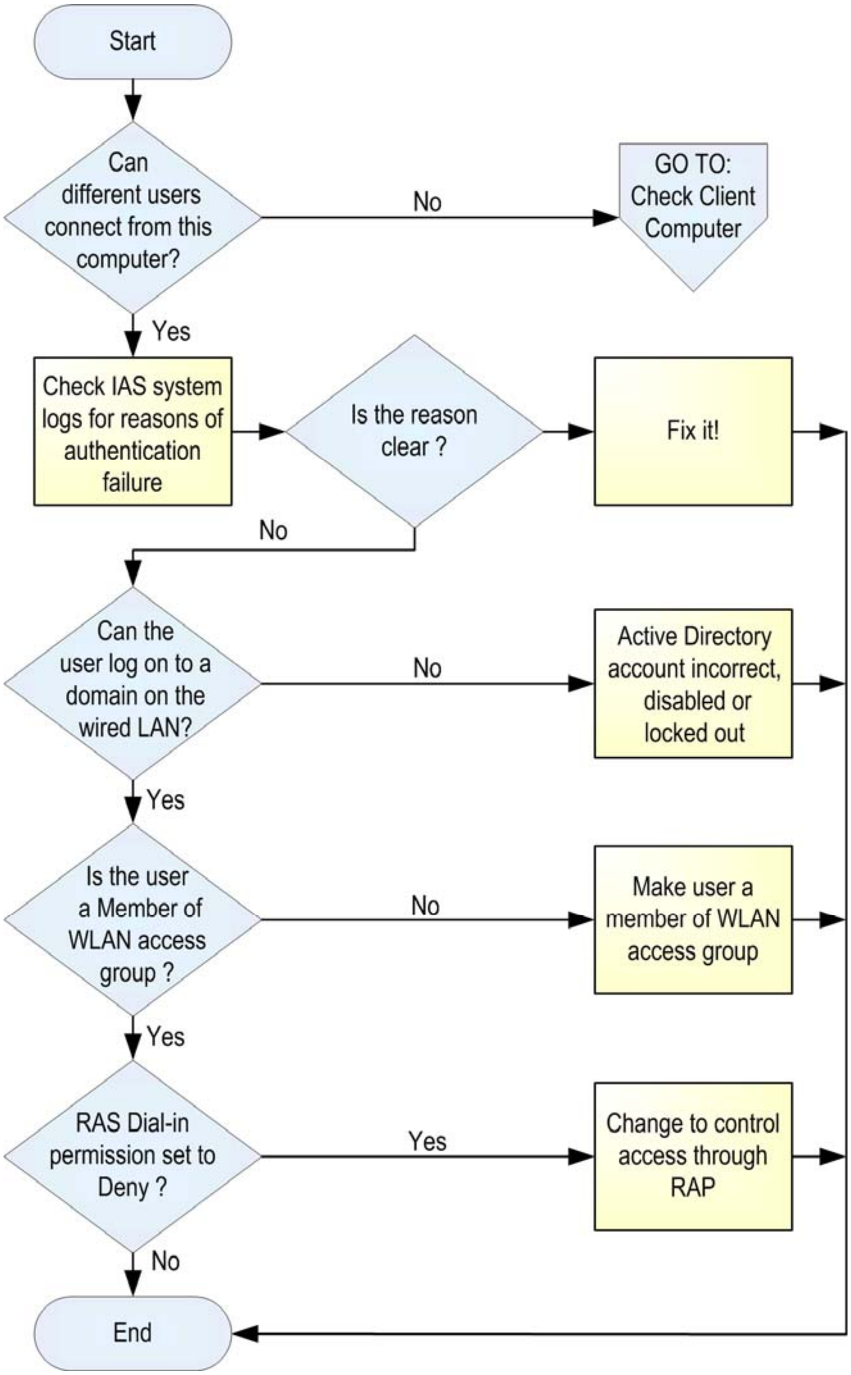
Start
Can different users connect from this computer?
No
GO TO: Check Client Computer
Yes
Check IAS system logs for reasons of authentication failure
Is the reason clear ?
Fix it!
No
Can the user log on to a domain on the wired LAN?
No
Active Directory account incorrect, disabled or locked out
Yes
Is the user a Member of WLAN access group ?
No
Make user a member of WLAN access group
Yes
RAS Dial-in permission set to Deny ?
Yes
Change to control access through RAP
No
End

Figure 8.2

Checking the user or computer account

Check Client Computer

The following flowchart helps you diagnose problems with the client computer.

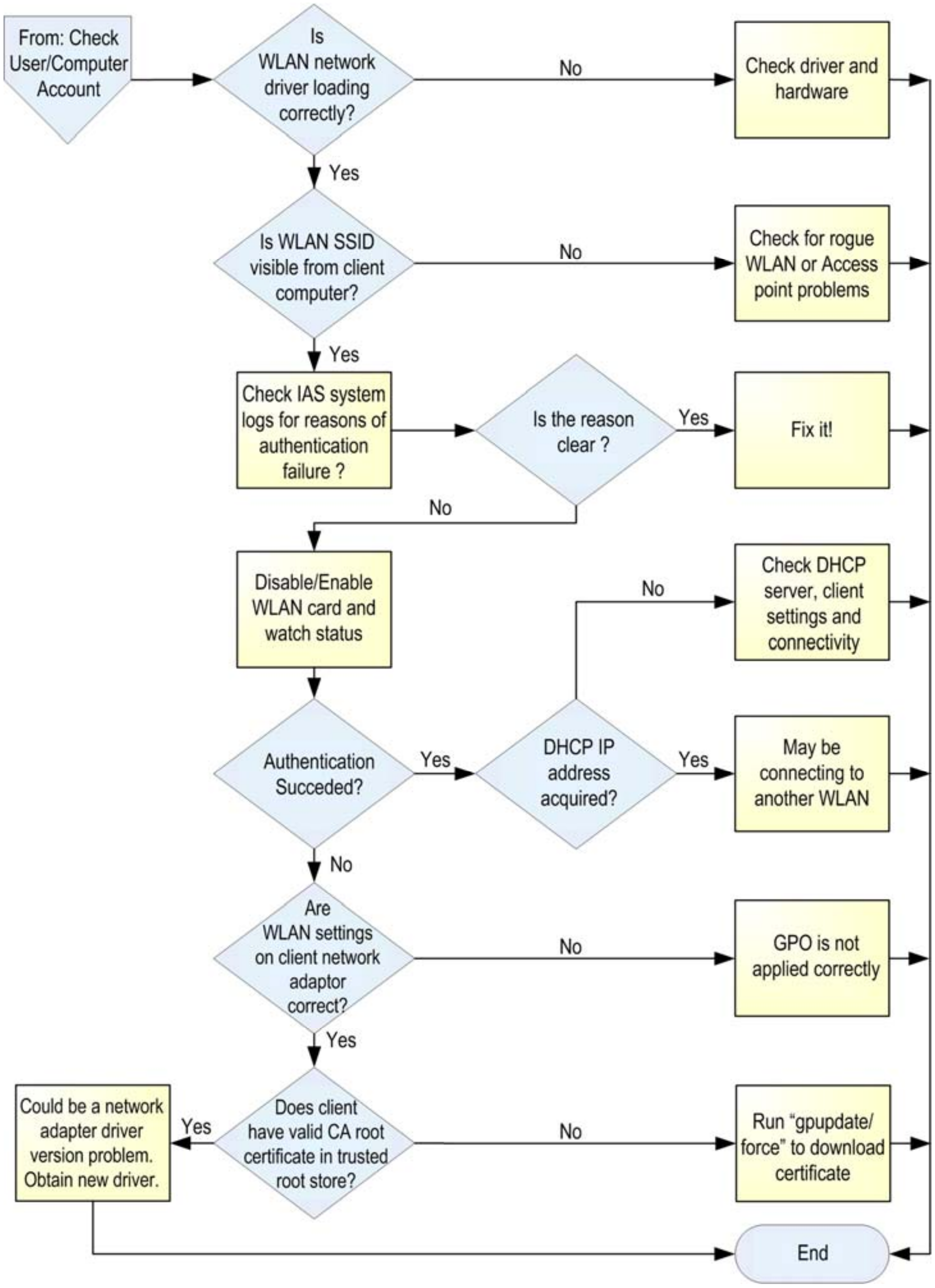
From: Check User/Computer Account
Is WLAN network driver loading correctly?
No
Check driver and hardware
Yes
Is WLAN SSID visible from client computer?
No
Check for rogue WLAN or Access point problems
Yes
Check IAS system logs for reasons of authentication failure ?
Is the reason clear ?
Yes
Fix it!
No
Disable/Enable WLAN card and watch status
No
Check DHCP server, client settings and connectivity
Authentication Succeded?
Yes
DHCP IP address acquired?
Yes
May be connecting to another WLAN
No
Are WLAN settings on client network adaptor correct?
No
GPO is not applied correctly
Yes
Could be a network adapter driver version problem. Obtain new driver.
Yes
Does client have valid CA root certificate in trusted root store?
No
Run "gpupdate/ force" to download certificate
End

Figure 8.3

Checking the client computer

Note: The arrow shaped box in the flowchart is a link from the "Check User/ Computer Account" procedure.

The status of the WLAN card (as required by the "Disable/Enable WLAN card and watch status" step shown in the flowchart) can be seen in the **Details** pane of the Network

Connections folder (in **Control Panel**). When you enable the card, you should see the card status stepping through the following phases:

- Connecting
- Authenticating
- Acquiring IP Address (unless this is statically assigned)

Monitoring the point at which this process fails is one of the most useful diagnostic procedures.

Check IAS

The following table lists a series of checks to be performed if you suspect that an IAS server is causing problems.

Table 8.11: IAS Diagnostic Checks

Check	Detail
IAS is running	*Open the **Computer Management** MMC and navigate to **Services**. Ensure that IAS is in the running state.*
IAS basic network configuration	*Run the **netdiag** command to check if there are any errors in the network configuration of the IAS sever.*
IAS server has current server certificate	*Open the **Certificates** MMC and look in the \Certificates (Local Computer)\Personal\Certificates folder. There should be a certificate for the server in this folder with the following characteristics:* *-Current date is within validity period of certificate.* *-Subject Alternative Name matches Domain Name System (DNS) name of server.* *-Server Authentication is present in Extended Key Usage* *-Certificate Issuer is trusted (in **Trust Path** tab).* *-The certificate has not been revoked.* *View the profile settings of the IAS Remote Access Policy, click the **Authentication** tab, and view the 802.1X settings. The server certificate just described should be selected.*
IAS is a member of RAS and IAS Servers group in the domain	*The server needs to be a member of this group (normally added when IAS is registered in Active Directory).*
IAS Remote Access Policy or Connection Request Policy incorrect	*Check that policy settings (and version number, if you have included it) matches what you expect. If you are in doubt, redeploy the configuration from the "master" IAS.*
View IAS events in the system event log	*Look for errors or warning events from IAS in the system event log. Authentication failures will have a reason code indicating the cause of the problem.*
Enable IAS Tracing	*See the "Enabling and Disabling Tracing on the IAS Server" procedure in the "Troubleshooting Tools and Techniques" section later in this chapter.*
Enable Client Tracing	*See the "Enabling and Disabling Tracing on the Client Computer" procedure in the "Troubleshooting Tools and Techniques" section later in this chapter.*
Enable SChannel	*To diagnose certificate-related and TLS problems enable SChannel*

Check	Detail
logging	*logging. For more information, see the "Enabling SChannel Logging on the IAS Server" procedure in the "Troubleshooting Tools and Techniques" section later in this chapter. You can also enable SChannel logging on the client to acquire additional diagnostic information from the client side.*

Check the Certification Authority

The following table contains a series of checks, which you can perform to determine whether the CA is performing correctly.

Table 8.12: CA Diagnostic Checks

Check	Detail
Certificate Services is running	*Open the **Computer Management** MMC and navigate to **Services**. Ensure that Certificate Services is running.*
If TLS fails (shown in RASTLS tracing log or SChannel logging) or the CA does not issue certificates, check the CRL	*Run the command **msstools CheckCA** on the CA to check that a current CRL has been published and is accessible.* *If you are experiencing problems on particular IAS servers (or at particular sites), obtain the PKI Health Tool (from the* Windows Server 2003 Resource Kit*). This is an MMC tool that will show you if the server has any problems accessing a current CRL or CA certificate.*
If no certificates have been enrolled/renewed, check the Certificate autoenrollment GPO	*-Check that the Autoenrollment GPO is linked to the correct location (usually the domain).* *-Check that the GPO has the "Computer" template set as the type of certificate to be enrolled (in Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Automatic Certificate Request Settings**)**.* *-Check that the RAS and IAS Servers group has **Apply Policy and Read** permissions on the GPO and check that no Deny permissions could be overriding these (for example, Authenticated Users—Deny Read).*
Certificate templates	*The Computer template should be assigned to the CA (look at the Templates folder in the **Certification Authority** MMC).* *The Computer template should have **Enroll permission for RAS and IAS Servers** group (check that no Deny permissions are overriding this).*
CA DCOM interface remotely	*Run the following command from a remote IAS server to check that DCOM/RPC is functioning between the server and the CA:* ***certutil –ping –config*** CAHostName\CAName *where,* CAHostName *is the computer name of the CA server and* CAName *is the descriptive name given to the CA when you set it up (it will be the name shown as **Issued By:** on the **General** tab of any certificate issued by this CA).*

Check Active Directory and Network Services

The following table lists a series of checks that you can perform on Active Directory and other network components to determine whether they are performing correctly.

Table 8.13: Active Directory Diagnostic Checks

Check	Detail
Check communications with Active Directory from IAS	*Run the command **netdiag /test:ldap /test:trust** on the IAS server. This command will also check for DNS problems.*
Check WLAN security groups	*Check the memberships of the security groups used in this solution to control access to the WLAN. The default memberships are shown in the "Creating Security Groups" section in Chapter 3, "Preparing Your Environment."*
Check the client WLAN settings GPO	*Check that the settings in the WLAN settings GPO are correct, the GPO is linked to the correct OU (or domain), and the correct permissions have been applied to it. (See the "Creating the WLAN Settings GPO" section of Chapter 6, " Configuring the Wireless LAN Clients.")*
Check that Active Directory is replicating correctly	*Run the command **dcdiag /test:replications** from the IAS server where you are experiencing problems. (Even if IAS is not running on a domain controller, the dcdiag tool will check the domain controller being used by that instance of IAS.)*
Check DHCP Server	*Check that the DHCP server is running, a valid scope for the WLAN clients has been created and is active, and there is connectivity between the wireless APs and the DHCP server (more precisely, connectivity is required between the default virtual local area network (VLAN) of the APs and the DHCP server to allow the WLAN clients to acquire an IP lease).*

Check Wireless Access Point Configuration

The following table lists a series of checks that you can perform on the wireless APs to determine whether they are performing correctly.

Table 8.14: Wireless AP Diagnostic Checks

Check	Detail
Check AP IP configuration and connectivity with IAS	*Many APs have a basic connectivity test facility (such as ping). Try to ping both the primary and secondary IAS servers (alternatively, try to ping the AP from the primary and secondary IAS servers).*
Check AP RADIUS settings	*Check the IP address and port settings configured on the AP for the primary and secondary RADIUS servers. Ensure that these match the configuration on the IAS servers.*
Check RADIUS client entry on IAS server(s)	*Verify that the primary and secondary IAS servers have a RADIUS client entry for this AP. IAS will log an error to the System log if it receives a RADIUS request from a device that is not configured as a client.*
Check RADIUS client secret	*It may be difficult to verify the RADIUS client secret visually because it is sometimes not possible to view the RADIUS secret after it has been*

Check	Detail
	entered into the AP. If the value configured in the IAS RADIUS client entry differs from that configured on the AP, IAS will log an error to the System event log.
Check AP Firmware revision	*Verify that the firmware of the AP is up to date. Check the vendor Web site for updates.*
Check DHCP server	*Check that the DHCP server is running, a valid scope for the WLAN clients has been created and is active, and there is connectivity between the wireless APs and the DHCP server (more precisely, connectivity is required between the default VLAN of the APs and the DHCP server to allow the WLAN clients to acquire an IP lease).*

Check WAN Connectivity

WLAN failures may be caused by WAN connectivity problems between different components. The following table lists the items that are most likely to be the sources of problems.

Table 8.15: WAN Diagnostic Checks

Check	Detail
Wireless APs authenticating to remote IAS Servers	*Test simple connectivity between the AP and the primary and secondary IAS servers. Most APs have a simple* ***ping*** *or* ***traceroute*** *command for this purpose.* *If there are firewalls or routers filtering traffic between the sites in question, you must verify that RADIUS authentication and accounting traffic is permitted (requests plus replies on user datagram protocol (UDP) ports 1812 and 1813).*
Domain Controllers replicating across a WAN	*Replication problems between domain controllers may occur even where basic IP connectivity is present. Excessive latency may cause the RPC communications between the domain controllers to fail. You should test this using the dcdiag tool as described in the "Check Active Directory and Network Services" section earlier in this chapter.*
WLAN Client and DHCP Server	*Where the DHCP server is not on the same LAN as the APs and authenticated WLAN clients, you must configure a BOOTP/DHCP relay agent to forward the requests to the correct DHCP server on the remote network.*

Troubleshooting Tools and Techniques

This section describes some of the techniques and tools that will be useful during troubleshooting.

Checking Client Network Connections Folder Status

The Network Connections folder and the Windows XP system tray notification icons provide information about the state of the WLAN authentication.

In the Network Connections folder (in **Control Panel**), the status text under the wireless network adapter describes the current state of the connection. Highlighting the adapter displays additional information about the connection in the **Details** panel of the Network

Connections folder. Disabling and then re-enabling the adapter will display the status of the adapter as it tries to connect to and authenticate to the WLAN; this information can be useful when debugging client connection problems.

Right-click the adapter icon and click **Status** to see the WLAN signal strength (on the **General** tab) and the IP address details (on the **Support** tab).

Viewing IAS Authentication Events in the Event Log

Client authentication success and failure events, which are recorded in the System event log on the IAS servers, can be useful for troubleshooting. By default, event logging is enabled for successful and failed authentication requests. This setting can be changed from the **Service** tab for the IAS server properties in the **Internet Authentication Service** MMC.

Looking at these events is useful for troubleshooting authentication failures. The event types produced by IAS are listed in the following table.

Table 8.16: IAS Authentication Request Events

IAS Event	Significance	Event Category	Event Source	Event ID
Access Granted	*A user or computer was successfully authenticated and granted access to the WLAN.*	*Information*	*IAS*	*1*
Access Denied	*An access attempt was denied (reason shown in text of event).*	*Warning*	*IAS*	*2*
Discarded	*The access attempt was discarded because it timed out.*	*Error*	*IAS*	*3*

Each event contains detailed information about the authentication request including:

- Client name
- IP address and identifier of AP
- Client type (should be "Wireless-IEEE 802.11")
- Name of remote access policy
- Authentication and EAP type
- Reason code and description

If the authentication fails, the reason codes and descriptions will often indicate the precise problem (although the reason given can sometimes be misleading or ambiguous). The available reason codes are given in the following table.

Table 8.17: IAS Authentication Request Event Reason Codes

Reason Code	Description

Reason Code	Description
00	*Success*
01	*Internal error*
02	*Access denied*
03	*Malformed request*
04	*Global catalog unavailable*
05	*Domain unavailable*
06	*Server unavailable*
07	*No such domain*
08	*No such user*
16	*Authentication failure*
17	*Change password failure*
18	*Unsupported authentication type*
32	*Local users only*
33	*Password must change*
34	*Account disabled*
35	*Account expired*
36	*Account locked out*
37	*Invalid logon hours*
38	*Account restriction*
48	*No policy match*
64	*Dialin locked out*
65	*Dialin disabled*
66	*Invalid authentication type*
67	*Invalid calling station*
68	*Invalid dialin hours*
69	*Invalid called station*
70	*Invalid port type*
71	*Invalid restriction*
80	*No record*
96	*Session time-out*

In some cases, the information gleaned from the event log entries is not enough to diagnose the cause of the problem. In such cases you may need to enable tracing on the IAS client and the IAS server. These are described in the next procedures.

Enabling and Disabling Tracing on Client Computers

Windows supports detailed tracing information on most components to help with diagnosis of problems that may arise. Enabling tracing for a component causes diagnostic output to be written to text log files and provides a level of detail beyond that found in event logs.

To obtain detailed information about the WLAN authentication process, you must enable tracing for the EAP over LAN (EAPOL) and Remote Access Service-Transport Layer Security (RASTLS) components using the **netsh** command. After enabling tracing, try the authentication process again and examine the Eapol.log and Rastls.log files for indications of problems (these files are written to the %Systemroot%\Tracing folder).

To enable tracing on client computers

- Run the following commands:

```
netsh ras set tracing eapol enabled
netsh ras set tracing rastls enabled
```

To disable tracing on client computers

- Run the following commands:

```
netsh ras set tracing eapol disabled
netsh ras set tracing rastls disabled
```

Note: Tracing consumes significant system resources and creates log files which can grow rapidly. Be sure to disable tracing when troubleshooting is complete.

Enabling and Disabling Tracing on the IAS Server

Enabling tracing on IAS works in the same way as on the client.

You can use the **netsh** command to enable and disable tracing for a variety of different components related to network authentication. The most useful components to enable for tracing of 802.1X with PEAP authentication issues are the following:

- **IASSAM (the Iassam.log file in the %Systemroot%\tracing folder):** This is the most commonly used trace file for IAS issues as it describes functions related to cracking (translating between different formats) user names, binding to a domain controller, and verifying credentials. It is the "heart" of the IAS trace files and is usually required to debug any authentication related issues.
- **RASTLS (the Rastls.log file in the %Systemroot%\tracing folder):** This trace file is used for all EAP and PEAP related authentications. This log holds most of the vital debugging information; however, it is challenging to read and understand. Microsoft is planning to release documentation that will make this information easier to interpret.
- **RASCHAP (the Raschap.log in the %Systemroot%\tracing folder):** This trace file is used for all MS-CHAP v2 and other CHAP based password authentication operations.

Enabling tracing on the following IAS components is normally not required for troubleshooting 802.1X authentication but may be useful for troubleshooting other problems:

- **IASRAD (the Iasrad.log file in the %Systemroot%\tracing folder):** This logs all RADIUS protocol-related operations. It will describe the ports that the server is listening on and so forth. It may be useful for debugging wireless AP compatibility problems.
- **IASSDO (the Iassdo.log file in the %Systemroot%\tracing folder):** The IASSDO log deals with transactions from the user interface (UI) to the MDB files that store the server's configuration and dictionary. This log is used to troubleshoot any service or UI-related issues.

To enable tracing on the IAS server

1. Run the **netsh** command corresponding to the type of tracing information that you require. When troubleshooting 802.1X authentication issues, the IASSAM, RASTLS and RASCHAP logs will contain the most useful information.

```
netsh ras set tracing iassam enabled
netsh ras set tracing rastls enabled
netsh ras set tracing raschap enabled
netsh ras set tracing iasrad enabled
netsh ras set tracing iassdo enabled
```

   Alternatively, to enable tracing for all categories of network components, run the following command:

```
netsh ras set tracing * enabled
```

To disable tracing on the IAS server

1. Run one or more of the following **netsh** commands to disable tracing for the categories enabled in the previous procedure:

```
netsh ras set tracing iassam disabled
netsh ras set tracing rastls disabled
netsh ras set tracing raschap disabled
netsh ras set tracing iasrad disabled
netsh ras set tracing iassdo disabled
```

   Alternatively, to disable tracing for all categories of network component, run the following command:

```
netsh ras set tracing * disabled
```

Note: Since tracing consumes significant system resources, you should use it sparingly to help identify network problems. After the trace is captured or the problem is identified, you should disable tracing.

By default, IASSAM and RASTLS tracing logs are set to 1 MB only, which might cause valuable information to be overwritten in log files during heavy load. The following procedure sets the tracing logs to 10 MB. When a log file reaches the 10 MB limit is reached, it is renamed (to IASSAM.old and RASTLS.old) and a new log file created. This keeps a maximum of 20 MB of data on the server for each tracing type. You can repeat this for any of the tracing types by substituting the tracing category name (such as RASTLS and RASCHAP) for the "IASSAM" key name used in the procedure.

To set the IASSAM tracing log file to 10 MB

1. Start Regedit.exe.
2. Navigate to the following registry key: **HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing**
3. Find the subkey **IASSAM**. This should have a registry value **MaxFileSize** (a type of **REG_DWORD**). Edit this value and set the data value to be **0xA00000** (this is the hexadecimal representation of 10MB—the default being 0x100000). You can set this to a value other than 10 MB if you wish (although the logs will start to become unmanageable at sizes much larger than this).

Warning: Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should backup any valuable data on the computer.

Enabling SChannel Logging on the IAS Server

SChannel is a security support provider (SSP) that supports a set of Internet security protocols, such as Secure Sockets Layer (SSL) and Transport Level Security (TLS). If you suspect that there are problems related to the IAS server certificate, or if the RASTLS log indicates that there is some problem with creating the TLS session, you should enable SChannel logging on both the client and the server. Events are logged to the Security log.

Follow the same procedure for both client and server.

► **To enable SChannel logging**

1. Start Regedit.exe.
2. Navigate to the following registry key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\**
3. Enable detailed SChannel events by changing the value of **EventLogging** from **1** (**REG_DWORD** type, data **0x00000001**) to **3** (**REG_DWORD** type, data **0x00000003**).

Warning: Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should backup any valuable data on the computer.

When you finish troubleshooting, be sure to disable SChannel logging because this consumes significant system resources and will flood the event log with unwanted entries.

Pocket PC Diagnostic Tools

Windows XP has a range of network diagnostic tools. Pocket PCs, by contrast, have relatively few built into the base system. Your Pocket PC vendor, Microsoft, and other companies provide different types of tools to help you diagnose Pocket PC problems. Some examples include:

- **IP configuration and diagnostic tools:** Tools such as VXUtil or VXIPConfig from Cambridge Software.
- WLAN diagnostic tools provided by your Pocket PC vendor.

Summary

This chapter covered the following items needed to maintain the health of your WLAN security infrastructure:

- Identifying the essential maintenance tasks.
- Describing the operational, monitoring, support, changing, and optimization tasks related to this environment.
- Describing key troubleshooting procedures and techniques.

References

This section provides references to other sources of information that serve as a background to the guidance provided in this chapter.

- For more information on backing up and restoring Windows servers, see the Windows Server 2003 "Backing up and restoring data" page on Microsoft.com at:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/ctasks001.asp

- For more information on monitoring and management, see the "Microsoft Solutions for Management" page on Microsoft.com at:

  http://www.microsoft.com/technet/itsolutions/techguide/msm/default.mspx

- For more information on optimizing IAS, see the following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dnsbk_ias_rziy.asp

- For information on troubleshooting wireless network components, see the following URLs:

  http://support.microsoft.com/default.aspx?scid=313242

  http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifitrbl.asp

- For more information on troubleshooting IAS, see the following URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_ias_tshoot_node.asp

- For more information on IP configuration and diagnostic tools such as VXUtil or VXIPConfig, see the following URL:

  http://www.cam.com/windowsce.html

Appendix A

Using PEAP in the Enterprise

Microsoft® has produced two solutions for securing wireless local area networks (WLANs). The first solution *Securing Wireless LANs — a Certificate Services Solution* uses client certificates to authenticate wireless clients, and is primarily intended for large and enterprise organizations. The second solution, *Securing Wireless LANs with PEAP and Passwords* (the subject of this current guide), uses passwords and the Protected Extensible Authentication Protocol (PEAP) to authentication wireless clients. This latter guide was written primarily for small and medium organizations. However, there is nothing about PEAP that restricts its use to smaller organizations. Large and enterprise organizations can also use PEAP and password authentication to secure their WLANs.

If you are part of a large organization that is planning to implement PEAP with passwords, this appendix will show you how to use sections from both solutions to implement the solution. Both solutions use the same technical architecture and components so it is relatively simple to take the enterprise–focussed content from the first solution but replace the certificate authentication protocols with the PEAP and password protocols. The aim is to leave you with merged guidance that includes details relevant to an enterprise WLAN solution, such as advanced administrative delegation, RADIUS logging and server role separation, but using password authentication for your wireless clients.

Throughout this appendix, for reasons of brevity, the term "EAP–TLS solution" will be used to refer to the first solution *Securing Wireless LANs LANs — a Certificate Services Solution* and the term "PEAP solution" will refer to the second solution *Securing Wireless LANs with PEAP and Passwords*. Extensible Authentication Protocol–Transport Layer Security is the name of the client certificate based authentication protocol used in the first solution.

What You Need From the EAP–TLS Solution

Since the EAP–TLS solution guide was written for large organizations, it should be your primary reference. It includes planning, implementation, and operational details (such as delegated administration) that are likely to be of more interest to large organizations. Following the table is a list of the chapters of the EAP–TLS solution. For each chapter, a short description is given indicating whether the content from this solution relevant for the "merged" guidance or not. Where the content from the PEAP solution should be used in place of the EAP–TLS solution instructions this is highlighted

For reference, the mapping between chapters of the two solutions is shown in the following table. Due to the differences in scope and use of technology there is not a one–to–one mapping between the chapters.

Table A.1: Mapping of Chapters between EAP–TLS and PEAP Solutions

EAP–TLS Solution	PEAP Solution
Chapter 1—Overview	Chapter 1—Securing Wireless LANs with PEAP and Passwords
Chapter 2—Deciding on a Secure Wireless Networking Strategy	Introduction — Choosing a Strategy for Wireless LAN Security
Chapter 3—Secure Wireless LAN Solution Architecture	Chapter 2—Planning a Wireless LAN Security Implementation
Chapter 4—Designing the Public Key Infrastructure	
Chapter 5—Designing a RADIUS Infrastructure for Wireless LAN Security	
Chapter 6—Designing Wireless LAN Security Using 802.1X	
	Chapter 3—Preparing Your Environment
Chapter 7—Implementing the Public Key Infrastructure	Chapter 4—Building the Network Certification Authority
Chapter 8—Implementing the RADIUS Infrastructure for Wireless LAN Security	Chapter 5 — Building the Wireless LAN Security Infrastructure
Chapter 9—Implementing Wireless Security Using 802.1X	Chapter 6 — Configuring the Wireless LAN Clients
Chapter 10—Introduction to Operations Guide	Chapter 8 — Maintaining the Secure Wireless LAN Solution
Chapter 11—Managing the Public Key Infrastructure	
Chapter 12—Managing the RADIUS and WLAN Security Infrastructure	
Chapter 13—Test Guide	Chapter 7—Testing the Secure Wireless LAN Solution

19.

You should note that the EAP–TLS solution was intentionally structured to keep the Public Key Infrastructure (PKI), RADIUS, and WLAN components as independent of each other as possible to allow the reuse of these components in other applications. This means that there is some repetition in the EAP–TLS solution. For example, chapters on PKI and RADIUS both include server build instructions, since, in large organizations, it is possible that the installation of CAs and IAS servers is the responsibility of different groups within IT. Also, some of the logical steps through the design and implementation chapters may be misleading in the context of a PEAP solution. Therefore, you should read through the PEAP solution to obtain an overview of the whole process and then return to the EAP–TLS solution for specific design and implementation details.

The following sections contain the descriptions of how to use the chapters from the EAP–TLS solution in association with the chapters of the PEAP solution.

Chapter 1—Overview

Chapter 1 is an overview of the solution and contains short summaries of each of the chapters and appendixes in the guide. As you will be working primarily from the EAP–TLS guide, you should use chapter 1 from that solution.

Chapter 2—Deciding on a Secure Wireless Networking Strategy

The content of this chapter is very similar to the content of the Introduction, “Choosing a Strategy for Wireless LANs Security” of the PEAP solution. The introduction to the PEAP solution works as a preface to both the solutions, so you should use this instead of using Chapter 2 from the EAP–TLS solution.

Chapter 3—Secure Wireless LAN Solution Architecture

This chapter provides an architectural overview of the certificate–based WLAN solution, of all except the first of the following items are relevant:

- Description of how 802.1X with EAP–TLS (certificates) works. You should refer to the description provided in Chapter 2, “Planning a Wireless LAN Security Implementation” of the PEAP solution instead.
- Description of the target organization.
- List of the key solution design criteria.
- Illustration of how the different server components are used in different locations in the organization.
- Description of how the solution can be scaled.
- Examples of using elements of the solution to support other network applications such as 802.1X wired security and virtual private network (VPN).

The references to the certification authority (CA) may also be relevant for use in the next chapter.

Chapter 4—Designing the Public Key Infrastructure

This chapter contains a detailed description of the planning process for a simple PKI. The PEAP solution also contains instructions for a simple, single–purpose CA. Even though you will not need to issue certificates to your WLAN clients, you should consider using following this chapter to help design your PKI. The larger your organization, the more likely it is that you will have requirements for certificates other than simple network authentication. This chapter will help to design a more robust and flexible PKI than the one presented in the PEAP solution.

Chapter 5—Designing a RADIUS Infrastructure for Wireless LAN Security

You should follow the guidance provided in this chapter from the EAP–TLS solution.

Chapter 6—Designing Wireless LAN Security Using 802.1X

You should follow the guidance provided in this chapter from the EAP–TLS solution.

Chapter 7—Implementing the Public Key Infrastructure

This is only relevant if you have decided to implement a full featured PKI as described earlier. Otherwise follow Chapter 4, ”Building a Certification Authority” in the PEAP solution.

Chapter 8—Implementing the RADIUS Infrastructure for Wireless LAN Security

You should follow the guidance provided in this chapter. You should also read Chapter 5, "Building the Wireless LAN Security Infrastructure" from the PEAP solution for supplementary information.

Chapter 9—Implementing Wireless Security Using 802.1X

You should follow the instructions given in Chapters 5, "Building the Wireless LAN Security Infrastructure" and Chapter 6, “Configuring the Wireless LAN Clients” of the PEAP solution on how to configure the IAS remote access policy and the client Group Policy object (GPO) settings. Chapter 5 of the PEAP solution also contains useful details on configuring wireless AP settings and scripts to help automate the entry of RADIUS clients and replication of IAS settings that are not given in the EAP–TLS solution.

Chapters 10, 11, and 12—Operating the Solution

You should follow the guidance provided in these chapters of EAP–TLS solution. In addition, you should read the guidance provided in Chapter 7, “Maintaining the Secure Wireless LAN Solution” of the PEAP solution, on troubleshooting WLAN problems. There are detailed procedures and techniques given here that will provide useful supplement to the procedures in the EAP–TLS chapters.

Chapter 13—Test Guide

You should use the content from this chapter. If you have chosen not to implement a full PKI as described in Chapter 4, “Designing the Public Key Infrastructure” of EAP–TLS solution, ignore some of the PKI–related testing in this chapter.

Scripts

The scripts used in the PEAP solution were developed from the EAP–TLS solution scripts. However, although the PEAP scripts contain more functionality than the EAP–TLS scripts, they are not an exact superset. The EAP–TLS scripts contain more sophisticated CA monitoring functions for example. In most cases the scripts provided in the PEAP solution should be used but you may want to install the scripts for both solutions into separate folders and use each of them as appropriate. The scripts are only provided as basic samples to illustrate techniques so you should feel free to modify them to better match your needs.

Appendix B

Using WPA in the Solution

The wireless local area network (WLAN) solution described in this documentation works equally well with either dynamic Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) WLAN protection. The implementation differences between the two are minor and are documented in this appendix.

Currently, there are some potential difficulties with using WPA, which include:

- **Manual configuration of WPA settings:** The support for setting Windows® XP client WPA settings using group policy is not available in the versions of Windows® earlier than Windows Server™ 2003 Service Pack 1. Until Service Pack 1 is available and you have deployed it in your organization, you will have to configure your clients manually (there is no way to script WLAN settings for Windows XP). You need to install Service Pack 1 only on the server on which you are editing the WLAN settings Group Policy object (GPO); it is not required on the clients, domain controllers, or IAS servers.
- **Restricted availability of WLAN clients:** At the time of writing, Microsoft® only provides WPA support for Windows XP Service Pack 1 and later.
- **Availability of WPA compliant hardware:** Although WPA support is now mandatory for all Wi-Fi certified hardware, existing network equipment may need to be upgraded to support WPA. You will need to obtain firmware updates for any access points or network adapters that do not currently support WPA. In some (rare) cases, you may need to replace equipment if the manufacturer does not produce WPA updates.

Using WPA in Place of WEP

Although the majority of the guide is applicable to both WPA and dynamic WEP, there are two main points in the documentation where the instructions differ:

- The “Creating an IAS Remote Access Policy for WLAN” section in Chapter 5, “Building the Wireless LAN Security Infrastructure.”
- The “Creating the WLAN Settings GPO” section in Chapter 6, “Configuring the Wireless LAN Clients.”

Creating an IAS Remote Access Policy for WLAN with WPA

To use WPA WLAN protection in place of dynamic WEP, you should set the client session time–out value to 8 hours instead of 60 minutes. WPA has an in–built mechanism to generate new WLAN encryption keys, so it does not need to force the clients to re–authenticate frequently. Eight hours is a reasonable value to ensure that clients have valid up–to–date credentials (for example, it ensures that a client cannot remain connected for excessive periods after its account has been disabled). In very high security environments, you can reduce this time–out value, if needed.

In the "Modifying the WLAN Access Policy Profile Settings" section in Chapter 5, “Building the Wireless LAN Security Infrastructure,” use the following procedure to set the remote access policy profile settings:

- **To modify wireless access policy profile settings:**

1. In the Internet Authentication Service MMC, open the properties of the **Allow Wireless LAN Access** policy, and then click **Edit Profile**.
2. On the **Dial-in Contraints** tab, in the **Minutes clients can be connected (Session-Timeout)** field, type the value *480* (480 minutes or 8 hours).
3. On the **Advanced** tab, add the **Ignore-User-Dialin-Properties** attribute, set it to **True**, and then add the **Termination-Action** attribute and set it to **RADIUS Request**.

You also need to change the session time–out in the wireless access point (AP) to match (or exceed) the time–out value set in this procedure.

Manually Configuring Windows XP WLAN Settings for WPA

Until GPO support becomes available in Windows Server 2003 Service Pack 1, you must configure WPA settings on the client manually. WPA is supported on Windows XP Service Pack 1 with the WPA client download installed (or on Windows XP Service Pack 2).

Note: When GPO support becomes available, you can also use the following procedure to create a Wireless Network Policy using the same settings.

- **To manually configure WPA WLAN settings:**

1. Open the properties of the **Wireless Network** interface. If the WLAN is displayed in the **Available Networks** list, select it, and click **Configure…**, otherwise click **Add** (in the **Preferred Networks** section).
2. Type the WLAN name into the **Network Name (SSID)** field (if it is not already displayed there) and, in the **Description** field, enter a description of the network.

   Note: If you have an existing WLAN and you intend to run this side–by–side with the 802.1X–based WLAN of this solution, you must use a different Service Set Identifier (SSID) for the new WLAN. This new SSID should then be used here.

3. In the **Wireless Network Key** section, select **WPA** (not **WPA PSK**) as the **Network Authentication** type and **TKIP** as the **Data Encryption** type. (If your hardware supports it, you can choose the higher strength Advanced Encryption Standard (**AES)** in place of **TKIP**).
4. Click the **IEEE 802.1x** tab, and select **Protected EAP (PEAP)** from the **EAP Type** drop–down list.
5. Click the **Settings…** button to modify the PEAP settings. From the **Trusted Root Certificate Authorities** list, select the root CA certificate for the CA. (This is the CA that you installed to issue IAS server certificates—see Chapter 4 for more details).

Important: If you ever need to re–install your CA from scratch (not just restore from backup), you will need to edit the client settings and select the root CA certificate for the new CA.

---

6. Ensure that **Secured Password (EAP-MS-CHAP v2)** is selected in the **Select Authentication Method** and check the **Enable Fast Reconnect** option.
7. Close each properties window by clicking **OK**.

Configuring Pocket PC 2003 for WPA

WPA was not supported natively in Pocket PC 2003 at the time of writing; however, this may be implemented in the future. Support for WPA on Pocket PC may also be available from other vendors.

Migrating from WEP to WPA

If you have deployed a secure WLAN solution based on dynamic WEP and want to migrate to WPA, you need to follow the steps in this section. You must ensure that you have deployed WPA software support (for example, the Windows XP WPA component) and hardware support (AP firmware and network adapter driver updates) prior to the migration. References in this procedure to configuring WPA settings in GPOs are only valid when the GPO is edited from Windows Server 2003 Service Pack 1 or later. This service pack had not been released at the time of writing. If you are not using Windows Server 2003 Service Pack 1 or later, follow the instructions given in the “Manually Configuring Windows XP WLAN Settings” section in this appendix.

► **To migrate from WEP to WPA, if your APs support dynamic WEP and WPA simultaneously:**

1. Configure all wireless APs to support both dynamic WEP and WPA.
2. Create a new WLAN client settings GPO. Create a Wireless Network policy that configures the correct settings for WPA (refer to the procedure provided in the "Manually Configuring Windows XP WLAN Settings" section in this appendix). Then disable the existing WEP GPO and enable the WPA GPO so that all WPA settings are sent out to all clients. The clients will start using WPA on the WLAN following the next GPO refresh.

Note: If you are configuring your clients manually, you must disable the GPO that contains the WEP settings; if you do not do this, the manual WPA settings will be overwritten by the GPO.

---

3. Finally, you should update the IAS remote access policy session time–out and the client session time–out in the AP (as described in the "IAS Remote Access Policy" section earlier in this appendix).

► **To migrate from WEP to WPA, if your APs do not support simultaneous use of WEP and WPA:**

1. Create a new WLAN SSID for the WPA network.
2. Edit the client network settings GPO and add the new SSID using WPA parameters (as described in the "Manually Configuring Windows XP WLAN Settings" section earlier in this appendix). If you are configuring your clients manually, you should configure them with the new SSID and WPA settings for that SSID. Do not remove the settings for the old WEP SSID in either case.

3. Working site–by–site, reconfigure your APs from WEP to WPA support, changing the SSID of the AP. As you reconfigure each AP, the clients will switch to the new SSID and use WPA.
4. Once you have reconfigured all APs, you can update the remote access policies on all IAS servers. You need to increase the session time–out value in the remote access policy (from 60 minutes to 8 hours) and change the same setting in the wireless APs (as described in the "IAS Remote Access Policy" section in this appendix).
5. Once the migration is complete, you can remove the WEP SSID from the GPO.

References

This section provides references to important supplementary information or other background material relevant to this appendix.

- The Cable Guy — March 2003, Wi-Fi Protected Access™ (WPA) Overview, available at the following URL:

  http://www.microsoft.com/technet/columns/cableguy/cg0303.asp
- Microsoft Knowledge Base Article 815485, "Overview of the WPA Wireless Security Update in Windows XP," available at the following URL:

  http://support.microsoft.com/?kbid=815485
- Microsoft Press Pass Announcement on WPA Availability, available at the following URL:

  http://www.microsoft.com/presspass/press/2003/mar03/03-31WiFiProtectedAccessPR.asp
- "Wireless 802.11 Security with Windows XP" white paper available at the following URL:

Appendix C

Supported OS Versions

The following table shows the status of different Microsoft® Windows® operating system client and server versions. The table lists the role of the system within this solution, the different operating system versions that might be used in that role, and the support status of each operating system. The final column includes additional explanatory notes or caveats.

Table A.1: Support Status of Operating System Versions in the Solution

Role	Operating System Version	Support Status	Notes
Wireless client	Windows® XP with Service Pack 1 (Professional and Tablet Editions)	Solution Tested	
	Pocket PC 2003	Solution Tested	The implementation of 802.1X WLAN support may vary between Pocket PC device vendors. Wi–Fi Protected Access (WPA) is not yet available from Microsoft although may be supported by companies other than Microsoft.
	Windows 2000	Supported	Need to obtain 802.1X client from Microsoft.com. WPA support is not available from Microsoft although may be available from companies other than Microsoft.
	Microsoft Windows NT® 4.0 –Windows 9x	Supported	Need to obtain 802.1X client through Premier Support. WPA support is not available from Microsoft although may be available from companies other than Microsoft.
	Other platforms	Unknown—support may be available from	Clients need to support 802.1X and PEAP–MS–

Role	Operating System Version	Support Status	Notes
		companies other than Microsoft.	CHAP v2.
Certification Authority	Windows Server™ 2003, Standard Edition	Solution Tested	
	Windows Server 2003, Enterprise Edition	Supported	Enterprise Edition is a superset of Standard Edition.
	Windows 2000 Server	Supported	The certification authority (CA) features of Windows 2000 Server are very similar to that of Windows Server 2003, Standard Edition.
	CAs from companies other than Microsoft	Unknown	The CA must be able to generate server certificates for Internet Authentication Service (IAS). You have to manage the enrolment and renewal manually.
RADIUS Server	Windows Server 2003, Standard Edition	Solution Tested	Standard Edition only supports up to 50 wireless access points (APs).
	Windows Server 2003, Enterprise Edition	Supported	Enterprise Edition is a superset of Standard Edition, so all features required by the solution are included in both editions.
	Windows 2000 Server	Supported	Windows 2000 Internet Authentication Service (IAS) may be used for wireless 802.1X with PEAP. Requires installation of Windows 2000 802.1X client on IAS server. No wizard support for wireless remote access policy configuration.
	Other platforms	Not Supported	
Domain controllers	Windows Server 2003	Solution Tested	Universal groups require Active Directory® domain to be in Windows 2000 native mode or higher.
	Windows 2000 Server	Supported	Universal groups require Active Directory domain to be in Windows 2000 native mode or higher.
Infrastructure	Windows	Solution Tested	

Role	Operating System Version	Support Status	Notes
servers, Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP)	Server 2003		
	Windows 2000 Server	Supported	
	Other platforms	Unknown	DHCP, DNS, and management solutions provided by companies other than Microsoft should work with this solution as long as they fulfill the basic requirements for Windows client and Active Directory.

20.

The support status in the table is listed as one of the following:

- **Solution Tested:** The operating system version has been specifically tested to work as part of the solution. All product versions included in this category are also included in the next, "Supported" category.
- **Supported:** The Microsoft Windows product group has tested this operating system version and Microsoft fully supports its use in this configuration (although you may need to provide additional configuration or customization beyond what is included in the guidance for this solution). This version has not, however, been tested as part of this solution, which may mean that the solution guide does not include full installation and configuration details for that version.
- **Not Supported:** The operating system version will not work within the solution as described. It may be possible to configure the unsupported system to work correctly, but this is likely to involve a significant amount of effort.
- **Unknown:** The operating system version may work in this role, there is no technical reason for it not to work. However, this is subject to your own verification and testing.

Note: In the table, there are few rows in which no operating system versions (in the Operating System Version column) are shown against roles (in the Role column); in these cases, either the operating system does not work for that role (**Not Supported** status) or it is not known whether it will work (**Unknown** status).

Appendix D

Scripts and Support Files

Introduction

This appendix contains a brief description of the scripts and other support files supplied with the solution. Although fully functional and tested with the solution, the scripts have not been through an extensive quality control process. They are intended to illustrate techniques and provide the basis for your own administrative scripts. You should fully test the scripts in your environment before deploying them in production.

Disclaimer

The sample scripts are not supported under any Microsoft® standard support program or service. The sample scripts are provided AS IS without warranty of any kind. Microsoft further disclaims all implied warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The entire risk arising out of the use or performance of the sample scripts and documentation remains with you. In no event shall Microsoft, its authors, or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the sample scripts or documentation, even if Microsoft has been advised of the possibility of such damages.

Structure of the Scripts

The Microsoft Visual Basic® Scripting Edition (VBScript) files require some explanation to understand how they work together. Unlike many VBScript examples, the script files included with the solution contain multiple, often independent functions. To provide access to these different functions, these scripts use the "job" functionality of WSH. This allows several independent program functions to be contained in, and called from the same file by specifying a job name as a parameter to the script.

There are two Windows Script (.wsf) files, which contain the user interface to all of the different script operations. The .wsf files call a set of .vbs files which contain the code that actually does the work for a particular job.

You can call the job using the following syntax:

```
cscript //job:JobName WScriptFile.wsf
```

Where *JobName* is the name of the operation and *WScriptFile* is the name of the XML interface file for the script. An excerpt from one of the .wsf files, where the job ConfigureCA is defined, is as follows:

```
<?xml version="1.0" encoding="utf-8" ?>
<package xmlns="Windows Script Host">
        <job id="ConfigureCA">
                <description>Configures the CA registry parameters</description>
                <script language="VBScript" src="constants.vbs" />
                <script language="VBScript" src="pkiparams.vbs" />
                <script language="VBScript" src="helper.vbs" />
                <script language="VBScript" src="ca_setup.vbs" />
                <script language="VBScript">
                <![CDATA[
                        Initialize True, True
                        ConfigureCA
                        CloseDown
                ]]>
                </script>
```

In this excerpt, the job definition specifies that the .vbs files namely, constants.vbs, pkiparams.vbs, helper.vbs, and ca_setup.vbs contain functions, subroutines, or data required by this job; therefore, they need to be loaded. The final section specifies the top–level functions to be executed to start the job; in this case, these functions include Initialize (which sets up logging), ConfigureCA (which performs the main job of configuring the CA), and CloseDown (which closes the log).

In each of the .wsf files, the first job is defined to list the names (IDs) and descriptions of all of the jobs contained in the file. Thus, if the .wsf file is run without requesting a specific job, this default job runs and displays a short help screen with the names and descriptions of all available jobs in the file. The following table lists the jobs available in each of the .wsf files supplied with the solution.

Table D.2: List of Jobs in MSSSetup.wsf

Job Name	Description
ListJobs	Lists all jobs in the WSF file.
ConfigureCA	Configures the CA registry parameters.
ConfigureTemplates	Configures CA certificate templates.
CheckCAEnvironment	Checks environment prior to CA installation.
InstallCA	Installs Certificate services.
CreateShortcut	Creates shortcut to **MSS WLAN Tools** on desktop.
ImportSecurityGPO	Imports GPO with server security settings into domain.
ImportAutoEnrollGPO	Imports GPO with certificate autoenrollment settings into domain.
ImportWLANClientGPO*	Imports WLAN settings GPO
CheckDomainNativeMode	Checks to see if domain is in native mode.
VerifyCAInstall	Verifies that the CA installation was successful.
VerifyCAConfig	Verifies that the CA configuration was successful
CheckIASEnvironment	Checks the environment prior to installing IAS.
InstallIAS	Installs the Internet Authentication Services on server.
CreateWLANGroups	Creates security groups in Active Directory®.
AddWLANGroupMembers	Populates security groups with correct memberships.

21.

Note: The jobs marked with an asterisk (*) are not used in this solution.

Table D.3: List of Jobs in MSSTools.wsf

Job Name	Description
ListJobs	Lists all jobs in the WSF file.
AddRADIUSClient	Interactive procedure to add a RADIUS client to IAS (parameters: [/path:*OutputFileName*]).
AddSecRADIUSClients	Interactive procedure to add a RADIUS client to IAS (parameters: [/path:*InputFileName*]).
GenRADIUSPwd	Generates RADIUS client entry and secret (parameters: /client:*ClientName* /ip:*ClientIPAddress* [/path:*OutputFile*]).
ExportIASSettings	Exports IAS Server configuration to files (parameters: [/path:*FolderToSaveSettingsFiles*]).
ImportIASSettings	Imports IAS Server configuration from files (parameters: [/path:*FolderWithFilesToImport*]).
ExportIASClients	Exports IAS RADIUS clients to file (parameters: [/path:*FolderToSaveClientsFile*]).
ImportIASClients	Imports IAS RADIUS clients from file (parameters: [/path:*FolderWithClientsFileToImport*]).
BackupIAS	Back up all IAS settings to file (parameters: [/path:*FolderToSaveBackupFile*]).
RestoreIAS	Restore all IAS settings from file (parameters: [/path:*FolderFileToRestore*]).
CheckIAS	Check that the IAS server is responding (parameters: [/verbose]).
CheckCA	Check that the CA service is responding and certificate revocation list (CRL) is valid (parameters: [/verbose]).
EnableIASLockout*	Enable account lockout for IAS (parameters: [/maxdenials:*10*] [/lockouttime:*2880* (secs)]).
DisableIASLockout*	Disable account lockout for IAS.
ShowLockedOutAccounts*	Show locked out accounts (and accounts with failed authorizations).
ResetLockedOutAccount*	Reset a locked out account (parameters: /account:*DomainName:AccountName*).

22.

Note: The jobs marked with an asterisk (*) are not used in this solution.

Job Output

Most of the scripts log progress information to a console window and, in many cases, also to a log file. This information may include error information if the script encountered problems during execution. The monitoring scripts are the exception to this because they are designed to run as non–interactive scheduled jobs and not to send output to a console window.

The scripts use a simple scrollable window to display their output. At the completion of each script, you are prompted to choose whether you want to keep the window open (for reference) or close it.

For most of the setup procedures, the output is also logged to a file called %SystemRoot%\debug\MSSWLAN-Setup.log. Most regular operational tasks are not logged; however, the tasks that might have a significant security or operational impact, such as the import of IAS configuration, are logged. Tasks that could result in sensitive information being written to the log, such as adding RADIUS clients and generating RADIUS client secrets, are also not logged.

Executing the Jobs

Although the scripts can be executed directly, there are two command shell batch (.cmd) files that help simplify the syntax.

The syntax for executing the .wsf files directly is as follows:

```
Cscript //job:JobName MssSetup.wsf
```

Instead, you can use the .cmd files with the following simpler syntax:

```
MssSetup JobName
```

Running the .cmd file without specifying a job causes the first job (ListJobs) in the .wsf file to run; this job lists the IDs and descriptions of each job in the .wsf file.

Certain jobs also take additional parameters. The syntax for running these jobs and the information on additional parameters are covered in the relevant chapters of this solution. The general syntax for specifying additional parameters is: