
Module 9: Extending Remote Access Capabilities by Using IAS

Contents

Overview	1
Introduction to IAS	2
Installing and Configuring IAS	5
Lab A: Configuring Internet Authentication Service	13
Review	22



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, BackOffice, FrontPage, IntelliMirror, NetShow, Outlook, PowerPoint, Visual Studio, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Simulations and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
75 Minutes

This module provides students with the knowledge and skills necessary to install and configure Internet Authentication Service (IAS) in a Microsoft® Windows® 2000 network.

Lab:
30 Minutes

At the end of this module, students will be able to:

- Describe the use of IAS in a network.
- Install and configure IAS.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the Microsoft PowerPoint® file 2153a_09.ppt

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Read the entire “Internet Authentication Service” section in the Windows 2000 Server Resource Kit.
- Read the entire “Internet Authentication Service” section in Windows 2000 Help.
- Read the following RFCs under **Additional Reading** on the Web page on the Student Material compact disc.
 - RFC 2138 *Remote Authentication Dial In User Service (RADIUS)*
 - RFC 2139 *RADIUS Accounting*

Module Strategy

Use the following strategy to present this module:

- Introduction to IAS

Introduce the module by explaining that in Windows 2000, the combination of Routing and Remote Access and IAS provides support for Remote Authentication Dial-In User Service (RADIUS). Describe the RADIUS authentication process. Ensure that students understand the client/server terminology used for RADIUS, which can be confusing. Briefly explain some of the deployment strategies that use IAS.

- Installing and Configuring IAS

Describe the procedure for installing IAS, and then explain why IAS must be authorized in the Active Directory™ directory service before the service can authenticate users. Demonstrate the procedure for configuring a RADIUS client and explain the purpose of a shared secret. Describe the procedures for configuring a remote access server to use RADIUS authentication and accounting. Finally, describe the settings that you can configure for accounting logs, and emphasize that logs must be imported into a database program in order for you to analyze the data.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Lab Setup

There are no lab setup requirements that affect replication or customization.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about Internet Authentication Service and how it integrates with remote access servers.

- Introduction to IAS
- Installing and Configuring IAS

*****ILLEGAL FOR NON-TRAINER USE*****

Organizations that outsource dial-up remote access, or perform joint ventures with other organizations, require authentication of user accounts outside the private network. Also, organizations that provide the outsourcing services, such as Internet service providers (ISPs), require remote user connection accounting so that they can charge subscribers.

Remote Authentication Dial-In User Service (RADIUS) is an industry-standard protocol that provides the solution to these authentication and remote user accounting requirements. In Microsoft® Windows® 2000, the combination of Routing and Remote Access and the Internet Authentication Service (IAS) provides support for RADIUS.

At the end of this module, you will be able to:

- Describe the use of IAS in a network.
- Install and configure IAS.

◆ Introduction to IAS

Topic Objective

To introduce the topics related to IAS.

Lead-in

IAS enables organizations to centrally manage and control remote access to their networks, and track usage statistics of the network centrally.

- IAS and RADIUS in a Windows 2000 Network
- Purpose and Use of IAS

*****ILLEGAL FOR NON-TRAINER USE*****

Corporations and ISPs maintaining remote access service for employees and customers face the increasing challenge of managing all remote access from a single point of administration. IAS performs centralized authentication, authorization, auditing, and accounting of connections for dial-up, virtual private network (VPN), and demand-dial connections. IAS enables organizations to centrally manage and control remote access to their networks, and track usage statistics of the network centrally. IAS also enables network administrators to centrally manage remote access permissions and connection properties.

Note For more information about RADIUS, see RFC 2138 and RFC 2139 under **Additional Reading** on the Web page on the Student Materials compact disc.

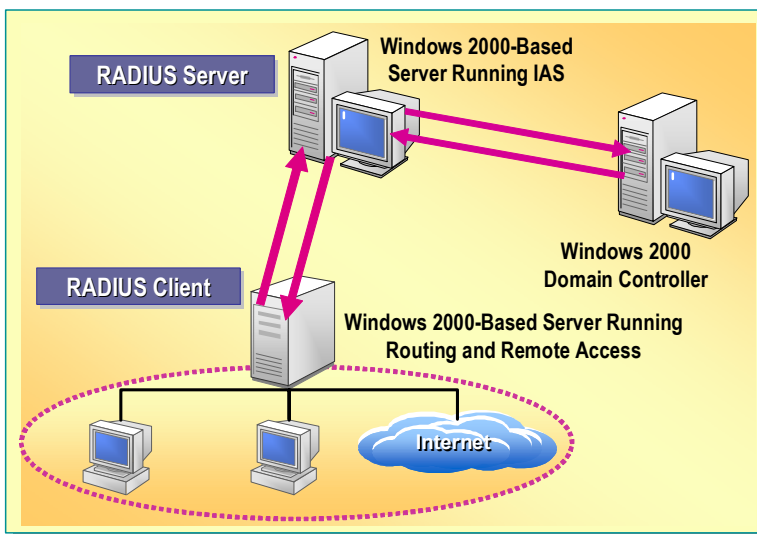
IAS and RADIUS in a Windows 2000 Network

Topic Objective

To illustrate the use of RADIUS and IAS in a Windows 2000 network.

Lead-in

RADIUS is a client/server protocol that enables remote access servers to submit authentication and accounting requests to a RADIUS server.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

A RADIUS client can be a network access server (NAS), or it can be a remote access server, such as a Windows 2000-based server running Routing and Remote Access.

RADIUS is a *client/server protocol* that enables RADIUS clients to submit authentication and accounting requests to a RADIUS server. A RADIUS client can be a network access server (NAS) that accepts Point-to-Point Protocol (PPP) connections and places clients on the network, or it can be a remote access server, such as a Windows 2000-based server running Routing and Remote Access. In a Windows 2000 network infrastructure, the RADIUS server is a Windows 2000-based server running IAS.

The RADIUS Authentication Process

The following steps describe the basic process that remote servers, a RADIUS server, and RADIUS clients use to perform authentication and authorization:

1. A user connects to a Windows 2000-based computer that is running Routing and Remote Access by using a dial-up connection or a VPN connection.
2. The Windows 2000-based computer that is running Routing and Remote Access forwards authentication requests to an IAS server. When doing this, the computer running Routing and Remote Access acts as a RADIUS client.
3. The IAS server accesses the user account information on a domain controller and checks the remote access authentication credentials. When doing this, the IAS server performs the functions of a RADIUS server.
4. If the user's credentials are authenticated and the connection attempt is authorized, the IAS server authorizes the user's access and logs the remote access connections as accounting events.

During the session, interim accounting packets are sent. When the user disconnects, an accounting-stop packet is sent to the IAS server, indicating the end of the user session. When logging accounting information, the computer running Routing and Remote Access acts as a RADIUS client, and the IAS server acts as a RADIUS server.

Purpose and Use of IAS

Topic Objective

To list examples of deployment scenarios that use IAS.

Lead-in

You can set up IAS to support several business scenarios.

- **Dial-up Corporate Access**
- **Extranet Access for Business Partners**
- **Internet Access**
- **Outsourced Corporate Access Through Service Providers**

*****ILLEGAL FOR NON-TRAINER USE*****

The main benefit of using RADIUS for authentication and accounting is that it is a standards-based protocol that allows for interoperability with other vendors' solutions.

You can set up IAS to support several business scenarios, including:

- *Dial-up corporate access.* You can set up IAS to support remote employees with authenticated dial-up connections. For example, the IAS server can give access to employees based on the group to which they belong.
- *Extranet access for business partners.* You can set up IAS to make network resources available to other companies with which an organization has partnership agreements. For example, the IAS server can limit a partner's access to corporate network resources.
- *Internet access.* You can set up IAS to support customer-authenticated dial-up connections to an ISP. For example, the IAS server can give access to customers based on the service plan for which they sign up.
- *Outsourced corporate access through service providers.* You can set up IAS to support a company that outsources remote access infrastructure to ISPs but retains control over user authentication, authorization, and accounting. For example, when an employee connects to the remote access server at the ISP, the authentication and usage records are forwarded to the organization's IAS server. The IAS server enables the company to control user authentication, track usage, and control which employees are allowed to gain access to the network.

Explain that an organization can use an ISP with RADIUS instead of setting up modem banks in different cities to support remote employees.

◆ Installing and Configuring IAS

Topic Objective

To introduce the topics related to installing and configuring IAS.

Lead-in

Before you can use IAS for authentication and accounting for remote access usage, you must configure remote access and IAS servers.

- Installing an IAS Server
- Configuring an IAS Server
- Configuring a Remote Access Server to Use RADIUS Authentication
- Configuring a Remote Access Server to Use RADIUS Accounting
- Configuring Logs for Accounting Information

*****ILLEGAL FOR NON-TRAINER USE*****

Before you can use IAS, you must install and configure IAS on a computer running Windows 2000 Server. You also must configure servers that have Routing and Remote Access installed to integrate with the IAS servers. You can configure the remote access server to use the IAS server to authenticate remote access users. Although the remote access servers can also authenticate users, each server has its own remote access policy to authorize user access to the network. Integration of these servers with IAS provides centralized authentication and authorization. You can also configure IAS to record the duration of the connection and the volume of data that a user has transferred.

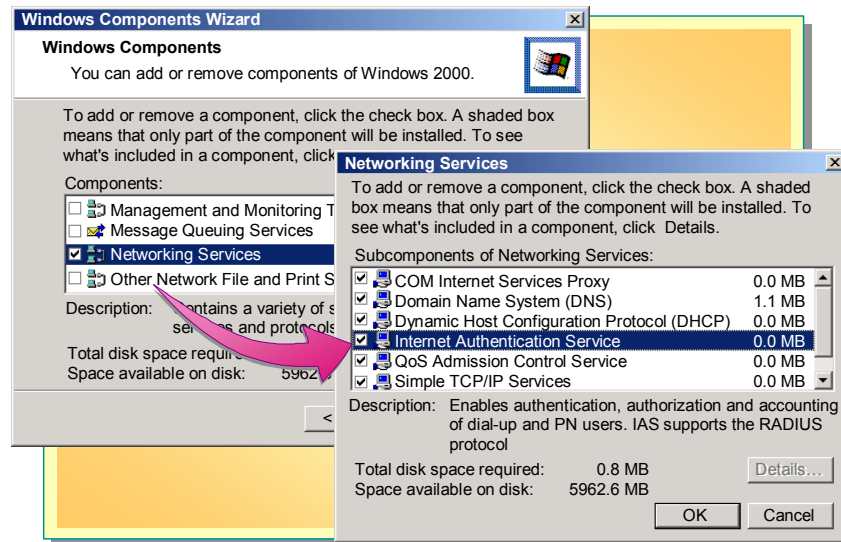
Installing an IAS Server

Topic Objective

To illustrate the interface for installing an IAS server.

Lead-in

Before a remote access server can access an IAS server, you must install the IAS network component.



*****ILLEGAL FOR NON-TRAINER USE*****

Before a RADIUS client can access an IAS server, you must first install IAS on the server.

To install IAS:

1. In Control Panel, double-click **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. On the **Windows Components** page, under **Components**, click **Networking Services** (but do not select or clear the check box), and then click **Details**.
4. Select the **Internet Authentication Service** check box, and then click **OK**.
5. Click **Next**, and then click **Finish**.

When you install the IAS network component, **Internet Authentication Service** is added to the **Administrative Tools** menu.

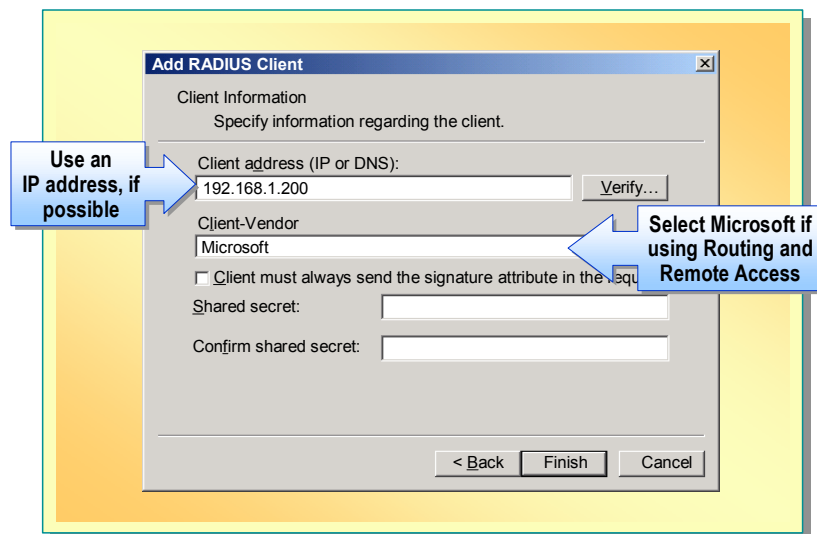
Configuring an IAS Server

Topic Objective

To identify the tasks for configuring an IAS server.

Lead-in

For the IAS server to authenticate users by using Active Directory, you must first authorize the IAS server in Active Directory.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Authorizing the server verifies that the IAS service has the correct permissions to access account information from Active Directory.

Before you configure the IAS server to authenticate users by using the Active Directory™ directory service, you must authorize the IAS server to ensure that the IAS service has the correct permissions to access account information from Active Directory.

You must also add the RADIUS clients to the IAS server. The RADIUS clients are the remote access servers that will use the IAS server for authentication and authorization. Finally, you can configure the size and location of the logs that store the accounting information collected by an IAS server.

Authorizing an IAS Server

If an IAS server must access Active Directory to authenticate users, you must authorize the IAS server in Internet Authentication Service in Microsoft Management Console (MMC). Only members of the Enterprise Admins group can authorize an IAS server.

To authorize an IAS server in Active Directory:

1. Open Internet Authentication Service from the **Administrative Tools** menu.
2. Right-click **Internet Authentication Service (Local)**, and then click **Register Service in Active Directory**.
3. In the **Register Internet Authentication Service in Active Directory** dialog box, click **OK**.

Note When you authenticate an IAS Server, Windows 2000 adds the server's computer account to the RAS and IAS Servers security group, which has the required Active Directory permissions to access user data in Active Directory.

Configuring RADIUS Clients

After you authorize the IAS server, you must configure the server for the RADIUS clients that will use this server.

To configure the IAS Server for RADIUS clients:

1. Open Internet Authentication Service from the **Administrative Tools** menu.
2. In the console tree, right-click **Clients**, and then click **New Client** to start the Add Client wizard.
3. On the **Add Client** page, in the **Friendly Name** box, type a name for the RADIUS client that you are configuring, and then click **Next**.
4. On the **Client Information** page, specify the following:
 - **Client address (IP or DNS)**. Type the Internet Protocol (IP) address or Domain Name System (DNS) name for the RADIUS client. Typically, it is more efficient to specify an IP address so that IAS does not have to resolve all host names at startup. If you only know a client's DNS name, click **Verify** to resolve the name to an IP address.
 - **Client-Vendor**. Select **Microsoft** if you are adding a Routing and Remote Access server. If you are adding a RADIUS client from a vendor that is not listed, select **RADIUS Standard**.

Note The Client-Vendor setting is only required if you are using remote access policies that are based on a client-vendor attribute.

- **Client must always send the signature attribute**. Select this check box if the RADIUS client must send a signature attribute in the Access-Request packet. You must specify a signature attribute if you use Extensible Authentication Protocol (EAP) for authentication.
- **Shared secret**. Type the secret, and then retype the secret in the **Confirm shared secret** box.

A *shared secret* is a text string that serves as a password between an IAS server and the remote access servers that forward requests to it. Shared secrets:

- Must be exactly the same on both servers.
 - Are case sensitive.
 - Can use any standard alphanumeric and special characters. Using combinations of uppercase and lowercase letters, numbers, and special characters will make the shared secret more secure.
 - Can be up to 255 characters long. Long shared secrets are more secure than shorter ones.
5. Click **Finish**.

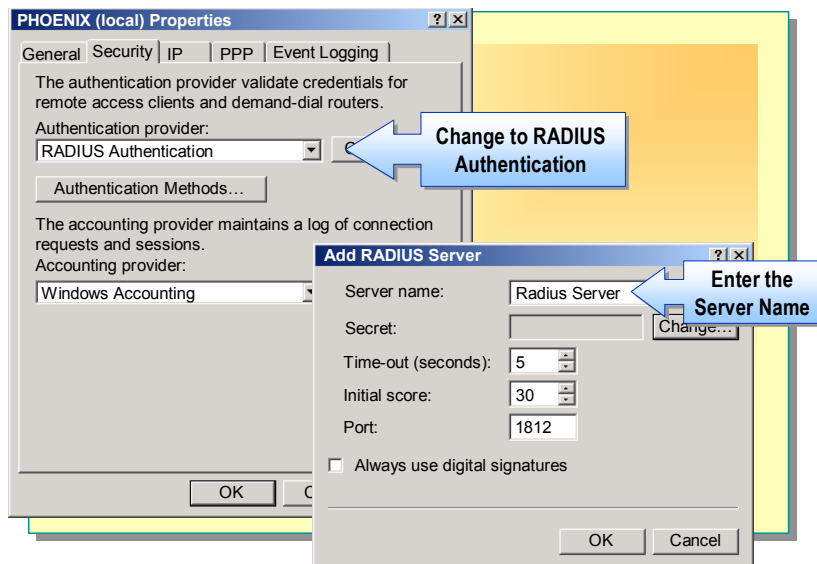
Configuring a Remote Access Server to Use RADIUS Authentication

Topic Objective

To identify the settings for configuring a remote access server to use RADIUS authentication.

Lead-in

For a remote access server to use RADIUS authentication, you must configure the server to forward authentication requests to an IAS server, making the remote access server a RADIUS client.



*****ILLEGAL FOR NON-TRAINER USE*****

To configure a remote access server as a RADIUS client, you must configure the server to forward authentication requests to an IAS server.

To configure RADIUS authentication:

1. Open Routing and Remote Access from the **Administrative Tools** menu.
2. In the console tree, right-click *server* (where *server* is the name of your computer), and then click **Properties**.
3. On the **Security** tab of the **Properties** dialog box for the server, in the **Authentication provider** box, click **RADIUS Authentication**, and then click **Configure**.
4. In the **RADIUS Authentication** dialog box, click **Add**.
5. In the **Add RADIUS Server** dialog box, in the **Server name** box, type the name of the IAS server that you are using for RADIUS authentication.
6. If you have a shared secret configured on the IAS server, click **Change** to set the shared secret on the remote access server.
7. If you are using digital signatures, select the **Always use digital signatures** check box.

You must specify this option if the RADIUS server is an IAS server and you selected the **Client must always send the signature attribute in the request** option when you added the client to the IAS server.

8. Click **OK** to close all dialog boxes, and then restart Routing and Remote Access.

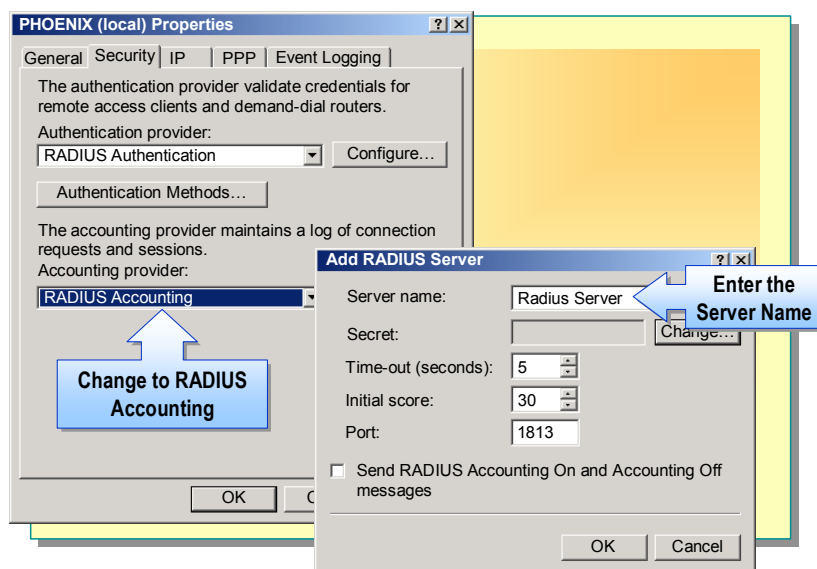
Configuring a Remote Access Server to Use RADIUS Accounting

Topic Objective

To identify the settings for configuring a remote access server to use RADIUS accounting.

Lead-in

To use RADIUS accounting, you must configure the remote access server to send accounting information to an IAS server.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

You can configure a remote access server to send accounting information to a RADIUS server such as an IAS server.

For a remote access server to use RADIUS accounting, you must configure the server to forward accounting requests to an IAS server.

To configure RADIUS accounting:

1. Open Routing and Remote Access from the **Administrative Tools** menu.
2. In the console tree, right-click *server* (where *server* is the name of your computer), and then click **Properties**.
3. On the **Security** tab of the **Properties** dialog box for the server, in the **Accounting provider** box, click **RADIUS Accounting**, and then click **Configure**.
4. In the **RADIUS Accounting** dialog box, click **Add**.
5. In the **Add RADIUS Server** dialog box, in the **Server name** dialog box, type the name of the IAS server that you have configured for RADIUS accounting.
6. If you have a shared secret configured on the IAS server, click **Change** to set the shared secret on the remote access server.
7. Select the **Send RADIUS Accounting On and Accounting Off messages** check box to send messages to the IAS server when you start or stop Routing and Remote Access.
8. Click **OK** to close all dialog boxes, and then restart Routing and Remote Access.

Configuring Logs for Accounting Information

Topic Objective

To list the settings that you can configure for accounting information.

Lead-in

There are a number of settings that you can configure for accounting logs.

Configure Settings for Accounting Logs:

■ Select Events to Log

- Log accounting requests
- Log authentication requests
- Log periodic status

■ Select Log File Format

- Database-compatible format
- IAS format

■ New Log Time Period

■ Log File Directory

*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

You can configure IAS to create accounting logs, but to analyze the data, you must import the logs into a database program.

You can configure settings for the accounting information logs, including events to log, file format, time period to log, and location of files. You can configure IAS to create accounting logs, but to analyze the data, you must import the logs into a database program.

Note For more information about importing IAS logs into a database, see “Importing IAS log files into a database” in Windows 2000 Help.

To configure settings for accounting logs:

1. Open Internet Authentication Service from the **Administrative Tools** menu.
2. In the console tree, click **Remote Access Logging**.
3. In the details pane, right-click **Local File**, and then click **Properties**.
4. On the **Settings** tab, select from the following events to log:
 - **Log accounting requests.** Specifies whether the account packets, such as accounting start or stop, are logged in the IAS log file.
 - **Log authentication requests.** Specifies whether the authentication requests, such as access-accept or access-reject, are logged in the IAS log file.
 - **Log periodic status.** Specifies whether interim accounting packets are logged in the IAS log file. This option is not generally recommended because it can fill hard drive space quickly.

5. On the **Local File** tab, specify the following:
 - **Log file format.** Click **Database-compatible format** to store information in a comma-delimited format, which you can import into most database programs. Click **IAS Format** to log data in a format that is compatible with IAS servers running Microsoft Windows NT® version 4.0. Click this option only if required for migration or compatibility reasons.
 - **New log time period.** Specify when IAS creates a new log file: daily, weekly, monthly, or when the file reaches a certain size.
 - **Log file directory.** Select the location for your logs.
6. Click **OK**.

Lab A: Configuring Internet Authentication Service

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will configure the Internet Authentication Service.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Install IAS.
- Configure Windows 2000 as a RADIUS client.
- Configure RADIUS authentication and accounting.

Prerequisites

Before working on this lab, you must have:

- The ability to install and configure Routing and Remote Access.
- An understanding of how user accounts are authenticated.

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server that is configured as a domain controller in native mode.
- A lab partner with a similarly configured computer.

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Scenario

Your company is increasing the number of remote access servers that it uses, and now you want to centrally control access to these servers through RADIUS. Also, you want centralized logging of remote access accounting information, and centralized authentication.

To achieve this, you are going to configure a server running the IAS, and then configure your remote access servers to use this IAS server for authentication, accounting, and remote access policies.

Estimated time to complete this lab: 30 minutes

Exercise 1

Installing and Configuring Internet Authentication Service

Scenario

You have been asked to centralize the administration and access for your remote access users in your organization. To do this, you have decided to use IAS for authentication of users connecting remotely, and also to use IAS for accounting to track the use of remote access throughout the organization.

Goal

In this exercise, you will install IAS, configure a RADIUS client for this service, and then configure shared secrets for this server.

Tasks	Detailed Steps
1. Install IAS.	- Log on as administrator@domain.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password. - In Control Panel, double-click Add/Remove Programs. - In Add/Remove Programs, click Add/Remove Windows Components.
Note: In the next detailed step, click the text Networking Services rather than the check box to avoid selecting all options under Networking Services .	
1. (continued)	- In the Windows Components wizard, on the Windows Components page, click Networking Services, and then click Details. - In the Networking Services dialog box, select the Internet Authentication Service check box, and then click OK. - On the Windows Components page, click Next. - If the Files Needed dialog box appears, type \\London\Setup\Winsrc and then click OK. - When the configuration is complete, click Finish, and then close all open windows.

(continued)

Tasks	Detailed Steps
2. Register IAS in Active Directory, and then specify your server as a new RADIUS client. Use password as your shared secret.	a. Open Internet Authentication Service from the Administrative Tools menu. b. In the console tree, right-click Internet Authentication Service (Local), and then click Register Service in Active Directory. c. Click OK to close the Register Internet Authentication Service in Active Directory dialog box. d. Click OK to close the Service registered message box. e. In the console tree, under Internet Authentication Service (Local), click Clients. f. Right-click Clients, and then click New Client. g. On the Name and Protocol page, in the Friendly name box, type <i>server</i> (where <i>server</i> is the name of your computer), and then click Next. h. On the Client Information page, in the Client address (IP or DNS) box, type the IP address of your computer's Classroom network adapter. i. In the Client-Vendor box, click Microsoft. j. In the Shared secret and Confirm shared secret boxes, type password and then click Finish.
3. Configure IAS to log all accounting requests.	a. In the console tree, click Remote Access Logging, and then in the details pane, click Local File. b. Right-click Local File, and then click Properties. c. On the Settings tab, select all of the check boxes. d. On the Local File tab, under Log file directory, type c:\moc\win2153 and then click OK. e. Close Internet Authentication Service.

Exercise 2

Configuring a Windows 2000 RADIUS Client

Scenario

You have installed IAS on a computer running Windows 2000, and you must configure your remote access servers to be RADIUS clients to this server.

Goal

In this exercise, you will configure your computer to be a RADIUS client.

Tasks	Detailed Steps
1. Enable Routing and Remote Access. Use the Configuration wizard to configure the remote access server with the following values: IP address: 10.x.0.10 (where <i>x</i> is your student number) Address Range: Five addresses	- Open Routing and Remote Access from the Administrative Tools menu. - In the console tree, right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Configure and Enable Routing and Remote Access. - In the Routing and Remote Access Server Setup wizard, click Next. - On the Common Configurations page, click Remote access server, and then click Next. - On the Remote Client Protocols page, click Next. - On the Network Selection page, under Name, verify that Classroom is selected, and then click Next. - On the IP Address Assignment page, click From a specified range of addresses, and then click Next. - On the Address Range Assignment page, click New. - In the Start IP address box, type 10.x.0.10 (where <i>x</i> is your student number), and then in the Number of addresses box, type 5. - Click OK, and then click Next. - On the Managing Multiple Remote Access Servers page, verify that No, I don't want to set up this server to use RADIUS now is selected, click Next, and then click Finish. - Click OK to close the Routing and Remote Access message box.

(continued)

Tasks	Detailed Steps
2. Configure your remote access server to use RADIUS authentication. Specify your server as your own RADIUS server, and use a secret of password .	- In Routing and Remote Access, right-click <i>server</i>, and then click Properties. - In the Properties dialog box for your server, on the Security tab, in the Authentication provider box, click RADIUS Authentication, and then click Configure. - In the RADIUS Authentication dialog box, click Add. - In the Add RADIUS Server dialog box, in the Server name box, type <i>server</i>. - To the right of the Secret box, click Change. - In the Change Secret dialog box, in the New secret and Confirm new secret boxes, type password and then click OK.
 Note: The secret is configured on the RADIUS server for a client, and on the RADIUS client itself. The secret is used in the setup of a secure, authenticated channel between RADIUS client and server.	
2. <i>(continued)</i>	- Click OK to close the Add RADIUS Server dialog box, and then click OK to close the RADIUS Authentication box. - Click OK to close the Routing and Remote Access dialog box.
 Important: Do not restart the Routing and Remote Access service at this time.	
3. Configure your remote access server to use RADIUS accounting. Specify your server as your own RADIUS server, and use a secret of password .	- In the Properties dialog box, on the Security tab, in the Accounting provider box, click RADIUS Accounting, and then click Configure. - In the RADIUS Accounting dialog box, click Add. - In the Add RADIUS Server dialog box, in the Server name box, type <i>server</i>. - To the right of the Secret box, click Change. - In the Change Secret dialog box, in the New secret and Confirm new secret boxes, type password and then click OK. - In the Add RADIUS Server dialog box, select the Send RADIUS Accounting On and Accounting Off messages check box, and then click OK. - Click OK to close the RADIUS Accounting dialog box. - Click OK to close the Routing and Remote Access message box, and then click OK to close the <i>server (local)</i> Properties dialog box. - Click OK to close the Routing and Remote Access dialog box. - Click OK to close the Routing and Remote Access dialog box.
4. Stop and then restart Routing and Remote Access.	- In the console tree, right-click <i>server</i>, point to All Tasks, and then click Restart. - Minimize Routing and Remote Access.

Exercise 3

Monitoring Remote Access by Using RADIUS

Scenario

You need to check usage statistics for your remote access server.

Goal

In this exercise, you will connect to your remote access server and then verify the usage statistics by viewing the RADIUS Accounting log file.

Tasks	Detailed Steps
1. Create a VPN connection called RADIUS Test to your server.	- Right-click My Network Places, and then click Properties. - In Network and Dial-up Connections, double-click Make New Connection. - Click Next. - On the Network Connection Type page, click Connect to a private network through the Internet, and then click Next. - On the Public Network page, verify that Do not dial the initial connection is selected, and then click Next. - On the Destination Address page, type the IP address of your computer's Classroom network adapter, and then click Next. - On the Connection Availability page, verify that For all users is selected, and then click Next. - On the Internet Connection Sharing page, click Next. - On the Completing the Network Connection Wizard page, type RADIUS Test in the text box, and then click Finish.
2. Using the VPN connection that you created in the previous task, connect to your computer, and then disconnect.	- In the Connect RADIUS Test dialog box, verify that Administrator appears in the Username box. - In the Password box, type password and then click Connect.
 Note: Wait for the VPN connection to be established. This connection will generate a RADIUS accounting log that you will examine in the next step.	
2. <i>(continued)</i>	- Click OK to close the Connection Complete message box, and then disconnect the connection. - Close Network and Dial-up Connections.
3. Open the RADIUS accounting log file at <code>c:\moc\win2153\iaslog.log</code> .	- Click Start, then click Run. - In the Open box, type <code>c:\moc\win2153\iaslog.log</code> and then click OK.

(continued)

Tasks	Detailed Steps
? What can you use the information in the RADIUS accounting log for? (Select all that apply.) A. Tracking the amount of time that users spend connected to a remote access server. B. Monitoring problems with recursive DNS queries. C. Calculating remote access usage times for a user. D. Performance monitoring of remote access. E. Detecting errors with a remote access server. A and C. RADIUS accounting logs record information about user connections and usage statistics. _____ _____ _____ _____	
3. <i>(continued)</i>	c. Close Notepad.

Exercise 4

Removing the Internet Authentication Service

Scenario

You now want to use this server for another purpose, so you need to remove IAS and Routing and Remote Access.

Goal

In this exercise, you will remove IAS and Routing and Remote Access.

Tasks	Detailed Steps
1. Remove IAS.	- In Control Panel, double-click Add/Remove Programs. - In Add/Remove Programs, click Add/Remove Windows Components.
 Note: In the next detailed step, click the text Networking Services rather than the check box to avoid selecting all options under Networking Services .	
1. <i>(continued)</i>	- In the Windows Components wizard, on the Windows Components page, click Networking Services, and then click Details. - In the Networking Services dialog box, clear the Internet Authentication Service check box, and then click OK. - On the Windows Components page, click Next. - When the configuration process is complete, click Finish, and then close all windows.
2. Disable Routing and Remote Access on your computer, close all windows, and then log off.	- Restore Routing and Remote Access. - Right-click <i>server</i> (where <i>server</i> is the name of your computer), and then click Disable Routing and Remote Access. - In the Routing And Remote Access dialog box, click Yes. - Close Routing and Remote Access, and then log off.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to IAS
- Installing and Configuring IAS

*****ILLEGAL FOR NON-TRAINER USE*****

1. You must configure a remote access server to use RADIUS authentication. What steps must you take to do this?

You must add the RADIUS client to the IAS server, configuring it with a shared secret. You must then configure the remote access server properties so that the server uses RADIUS authentication instead of Windows Authentication. Next, you must configure the remote access server to be a RADIUS client, and configure it to use the same shared secret that you defined on the IAS server.

2. Your company has a worldwide remote access infrastructure in place, and you want to be able to track usage statistics for users connecting to all servers worldwide. You also want to be able to control connection properties for users at a central location, instead of at each remote access server. How can you do this?

Install IAS and then configure the remote access servers to be RADIUS clients of the IAS server. Configure the remote access servers to use the IAS server as the RADIUS accounting server, and configure remote access profiles to control connection properties for users.

3. You must create reports on remote access usage in your organization. You have configured all remote access servers as RADIUS clients of an IAS server. What else must you do to create the reports?

You must configure the IAS server to log accounting information. You must then import the log files into a database program to create the reports.