

Module 8: Supporting Remote Access to a Network

Contents

Overview	1
Examining Remote Access Policies	2
Examining Remote Access Policy Evaluation	4
Creating a Remote Access Policy	8
Lab A: Creating a Remote Access Policy and Profile	12
Troubleshooting Remote Access	19
Lab B: Troubleshooting Remote Access (Simulation)	29
Review	31



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:
60 Minutes

This module provides students with the knowledge and skills necessary to support remote access to a Microsoft® Windows® 2000 network through the use of remote access policies and profiles, and to troubleshoot common remote access problems.

Labs:
60 Minutes

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

- Explain remote access policy and profile concepts.
- Describe the process of remote access policy evaluation.
- Create a remote access policy and configure a remote access profile.
- Maintain and troubleshoot remote access.

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_08.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.

Module Strategy

Use the following strategy to present this module:

- **Examining Remote Access Policies**

Explain the purpose of remote access policies. Solicit examples of when remote access policies could benefit a company. Describe the components of a remote access policy.

- **Examining Remote Access Policy Evaluation**

Students must understand the evaluation process to effectively plan remote access policies in a network. Describe the evaluation process that occurs when a user attempts to access a network remotely. Next, discuss how the default remote access policy differs depending on the mode of the domain. Last, explain the impact of multiple remote access policies.

- **Creating a Remote Access Policy**

Explain how to configure dial-in settings, policy conditions, and policy settings, while emphasizing that all settings must match. Demonstrate each of the procedures.

- **Troubleshooting Remote Access**

Discuss the type of information that can be obtained by monitoring the remote access server. Explain how to trace remote access connections, but warn students about the effect of tracing on system resources. Next, demonstrate methods for checking communication hardware to locate the source of a remote access problem. Explain methods for checking the communication lines, and then discuss the different configuration settings that could be the source of a remote access problem.

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 labs in this module are 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 remote access policies, creating remote access policies, and troubleshooting remote access.

- Examining Remote Access Policies
- Examining Remote Access Policy Evaluation
- Creating a Remote Access Policy
- Troubleshooting Remote Access

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

In Microsoft® Windows® 2000, you can define and create remote access policies to control the level of remote access that a user or group of users has to the network. Remote access policies are a set of conditions and connection settings that give network administrators more flexibility in granting remote access permissions and usage. The Windows 2000 Routing and Remote Access service and Windows 2000 Internet Authentication Service (IAS) both use remote access policies to determine whether to accept or reject connection attempts. As the administrator, you are also required to troubleshoot and maintain the remote access server for optimum performance.

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

- Explain remote access policy and profile concepts.
- Describe the process of remote access policy evaluation.
- Create a remote access policy and configure a remote access profile.
- Maintain and troubleshoot remote access.

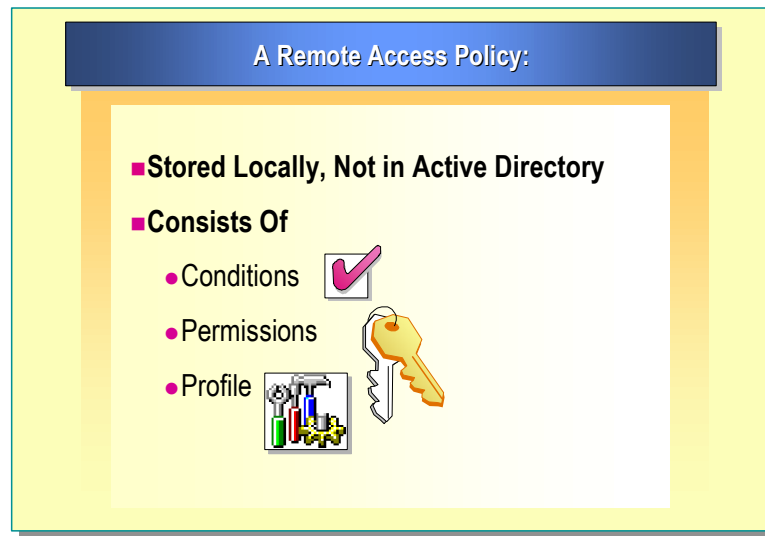
Examining Remote Access Policies

Topic Objective

To identify the concepts essential to an understanding of remote access policies.

Lead-in

To create effective remote access policies, you must understand the concepts behind policies, their associated profiles, and how they are evaluated and applied.



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

You can use remote access policies to assign settings to a connection, based on the user that is connecting and the properties of the connection. Understanding how policies are applied will help you provide customized access to the various users and groups in your organization. It is likely that the default policy settings are adequate for your remote access needs. However, it is important that you become familiar with remote access policies because using them effectively provides you with flexibility in granting remote access permissions and usage.

Key Points

Remote access policies are stored on the remote access server, not in Active Directory. This allows policies to vary according to the capabilities of the server.

Policies are Stored Locally

Windows 2000 stores remote access policies on the remote access server, not in the Active Directory™ directory service, so that policies can vary according to remote access server capabilities.

Note You can centralize remote access policies through the use of IAS. For more information about IAS, see module 9, “Extending Remote Access Capabilities by Using IAS,” in course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Components of a Policy

A remote access policy consists of three components that cooperate with Active Directory to provide secure access to remote access servers. The three components of a remote access policy are its conditions, permissions, and profile.

Conditions

The conditions of remote access policies are a list of parameters, such as the time of day, user groups, caller IDs, or Internet Protocol (IP) addresses, that are matched to the parameters of the client that is connecting to the server. The first set of policy conditions that match the parameters of the incoming connection request is processed for access permission and configuration.

Permissions

Remote access connections are permitted based on a combination of the dial-in properties of a user account and remote access policies. The permission setting on the remote access policy works with the user's dial-in permissions in Active Directory.

For example, a policy can grant access to all users in Group A from 8:00 A.M. through 5:00 P.M. However, the permissions for User X in Group A can be set to deny access in Active Directory, whereas the permissions for User Y in Group A can be set to allow access at all times. As a result, most users in Group A are controlled by the policy setting and can gain access only from 8:00 A.M. through 5:00 P.M. However, User X is denied access completely, and User Y is granted 24-hour access.

Profile

Each policy includes a profile of settings, such as authentication and encryption protocols, that are applied to the connection. The settings in the profile are applied to the connection immediately, and may cause the connection to be denied. For example, if the profile settings for a connection specify that the user can only connect for 30 minutes at a time, the user will be disconnected from the remote access server after 30 minutes.

◆ Examining Remote Access Policy Evaluation

Topic Objective

To identify topics related to remote access policy evaluation.

Lead-in

It is important to understand the logic of remote access policy evaluation, the function of the default policy, and the interaction of multiple policies.

- Following Policy Evaluation Logic
- Examining Default and Multiple Policies

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

It is important to understand how remote access policies are evaluated, so that you can determine the settings that will apply to incoming connections and plan your policies appropriately. Remote access policies are evaluated according to a logical flow that depends on whether the Windows 2000 domain is in mixed or native mode. (A mixed mode domain allows domain controllers to run Windows 2000 or Microsoft Windows NT® version 4.0. A native mode domain requires that all domain controllers run Windows 2000.) Familiarity with the logic of remote access policy evaluation, the features of the default policy, and the interaction of multiple policies will help you design effective remote access policies.

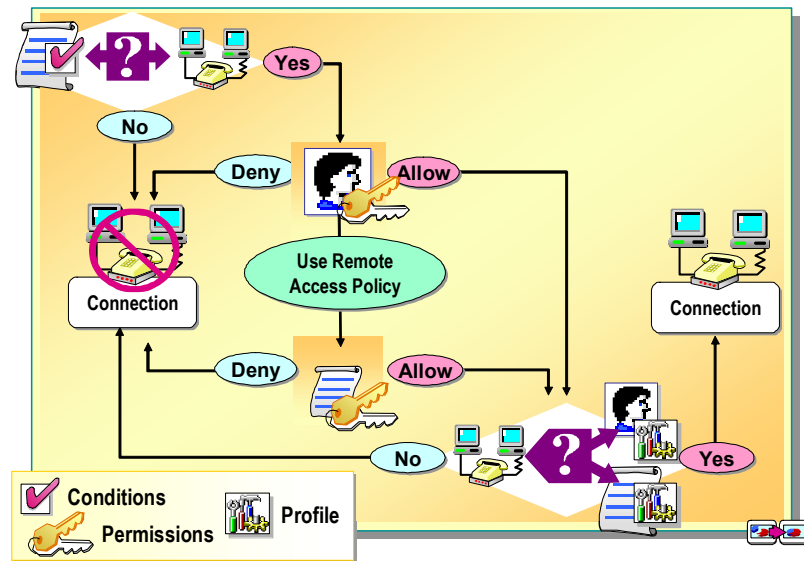
Following Policy Evaluation Logic

Topic Objective

To illustrate the logic that is used to evaluate remote access permissions, policies, and profiles.

Lead-in

Remote access policies work together with user properties to create a robust model for granting remote access to users and groups.



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

Delivery Tip

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

The numbers in the slide animation correspond to the numbers in this list. (The numbered text boxes are only visible in the animation.)

Use this text to explain the flowchart in the slide. Explain that the flow consists of essentially three parts: checking conditions, then permissions, and then the profile.

Windows 2000 evaluates a connection attempt based on logic that incorporates policy conditions, user and remote access permissions, and profile settings.

Remote access policies are evaluated as follows:

1. Routing and Remote Access matches the conditions of the remote access policy to the conditions of the attempted connection:
 - If there is no policy defined, all access is denied.
 - If there is no policy that matches, the access is denied.
 - If there is a match, the policy is used to determine access.
2. Routing and Remote Access checks the user account's dial-in permissions:
 - If the permission is set to **Deny access**, the user is denied access.
 - If the permission is set to **Allow access**, the user is granted access and the profile for the policy is applied.
 - If the permission is set to **Control access through Remote Access Policy**, the policy's permission setting determines user access.
3. Routing and Remote Access applies the settings in the policy's profile to the incoming connection.
 - The connection may not be allowed if a critical setting in the profile does not match a setting on the remote access server. For example, the profile for an incoming connection may specify that a group can only connect at night. If a user in that group tries to connect during the day, the connection attempt will be denied.
 - The connection may be disconnected at a later stage due to a setting in the profile, such as a time restriction on connecting.

Examining Default and Multiple Policies

Topic Objective

To identify additional topics that are relevant to remote access policy evaluation.

Lead-in

The default remote access policy provides a policy that will take effect on all users if no other policies exist.

■ Default Remote Access Policy

- Native mode (default policy denies all attempts unless User's account is set to **Allow Access**)
- Mixed mode (default policy overridden)

■ Multiple Policies

- Policies are checked in order until a policy matches the connection attempt
- Profile and user account settings are checked for the first matching remote access policy only

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

The default remote access policy will have no effect on incoming connections when the domain is in mixed mode, and the remote access policy has no profile settings associated with it. The default policy will be applied to all connection attempts that do not match any other policies. You should be aware of the settings of this policy and the implications of using the default policy in native mode and mixed mode domains. You should also understand how multiple policies interact.

Default Remote Access Policy

The default policy, called **Allow access if dial-in permission is enabled**, is created when Routing and Remote Access is installed. This policy controls access through the user's dial-in permission. The following table describes the settings of the default policy.

Setting	Value
Conditions	Current date/time = any day, any time
Permissions	Deny access
Profile	None

Native Mode and Standalone Servers

When your domain is running in native mode, or if your remote access server is a standalone server, setting the dial-in permission on every user account to **Control access through Remote Access Policy** will result in the rejection of all connection attempts if you do not change the default remote access policy. However, if you set one user's dial-in permission to **Allow access**, that user's connection attempts will be accepted. If you change the permission setting on the default policy to **Grant remote access permission**, all connection attempts are accepted.

Mixed Mode

The default policy is always overridden in a mixed mode domain because the user's dial-in permission, **Control access through Remote Access Policy**, is not available in mixed mode. However, the remote access server still applies remote access policies to users in a mixed mode domain. If the user's dial-in permission is set to **Allow access**, the user still must meet the conditions of a policy to gain access.

Important When converting from mixed mode to native mode, the permissions for all users with a dial-in setting of **Deny access** will be changed to **Control access through Remote Access Policy**. Permissions for all users with a dial-in setting of **Allow access** will remain set to **Allow access**. As a result, if the default remote access policy remains unaltered and no other policies exist, the conversion to native mode will have no effect on users' remote access permissions.

Multiple Policies

Key Point

If no remote access policy exists (if the default policy is deleted, for example), users will not be able to gain access to the network, regardless of their individual dial-in permissions.

Many organizations will have different remote access requirements for different groups in the organization. These organizations will require multiple remote access policies. You should create these policies carefully. If a connection attempt does not match any of the remote access policies, the connection attempt is rejected, even when a user's dial-in permission is set to **Allow access**.

When a user attempts to connect, the first policy in the ordered list of remote access policies is checked. If all of the conditions of the policy do not match the connection attempt, the next policy in the ordered list is checked, until a policy matches the connection attempt.

The connection attempt is then evaluated against the profile and user account settings of that profile. If the connection attempt does not match the profile or user account settings of the first remote access policy that matches the connection attempt, the connection attempt is rejected. No other policies are checked.

You can modify the order of remote access policies. For example, you might want the remote access policy that applies to the majority of your users to be checked first, so that fewer connection attempts must be evaluated against more than one policy.

To modify the order of remote access policies:

1. In Routing and Remote Access, in the console tree, click **Remote Access Policies**.
2. In the details pane, right-click the policy that you want to move, and then click either **Move Up** to move the policy up one level, or **Move Down** to move the policy down one level.

Important Because Routing and Remote Access requires that the conditions of at least one policy be matched, if the default policy is removed and there are no other policies, all connection attempts will be rejected. In most situations, you should leave the default policy unaltered to provide access for users who are explicitly granted access through their user permissions.

◆ Creating a Remote Access Policy

Topic Objective

To identify the topics that are relevant to the creation of a remote access policy.

Lead-in

Creating a remote access policy involves configuring the user's dial-in settings, creating the policy, and then defining the profile.

- **Configuring Remote Access Policy Conditions**
- **Configuring Remote Access Profile Settings**

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

You can create detailed rules for remote access that are as simple or as complex as your organization needs. A remote access policy consists of user dial-in settings, remote access policy conditions, and remote access policy settings. Although they do not need to be completed in any particular order, it is important to include all three components in your planning.

Note For more information about user dial-in settings, see module 7, “Configuring Remote Access,” in course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Configuring Remote Access Policy Conditions

Topic Objective

To illustrate the role of policy conditions.

Lead-in

Several conditions can be added to a single policy, so that you can create highly customized access for your organization.

Examples of Connection Attempt Conditions

- Is Between 8 A.M. and 5 P.M., Monday–Friday
- AND
- Is from Any IP Address That Matches 192.168.*.*
- AND
- Is from Any User in the Sales Group

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

Key Point

Explain that IAS uses several of these conditions for RADIUS support.

Remote access policy *conditions* are attributes that are compared to the settings of a connection attempt. If there are multiple conditions in a policy, all of the conditions must match the settings of the connection attempt, or the next policy is evaluated.

The following table lists the conditions that you can set for a remote access policy.

Note Some of these conditions apply to Remote Authentication Dial-In User Service (RADIUS). For more information about RADIUS, see module 9, “Extending Remote Access Capabilities by Using IAS,” in course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.

Condition name	Description	Wildcard okay (*)	Used by IAS
NAS IP Address	A character string that identifies the IP address of the network access server (NAS).	Yes	Yes
Service Type	The type of RADIUS service that is requested. Examples include framed (such as Point-to-Point Protocol [PPP] connections) and logon (such as Telnet connections). For more information about RADIUS service types, see RFC 2138 under Additional Reading on the Web page on the Student Materials compact disc.	No	Yes
Framed Protocol	The type of framing for incoming packets. Examples include PPP, AppleTalk, Serial Line Internet Protocol (SLIP), Frame Relay, and X.25.	No	Yes
Called Station ID	A character string that identifies the telephone number of the NAS.	Yes	No

(continued)

Condition name	Description	Wildcard okay (*)	Used by IAS
Calling Station ID	A character string that identifies the telephone number that the caller uses. The telephone line, hardware, and hardware driver must support reception of caller ID data.	Yes	No
NAS Identifier	A character string that identifies the NAS from which the request originated.	Yes	No
NAS Port Type	The type of media that the caller uses. Examples include analog telephone lines (or Async), Integrated Services Digital Network (ISDN), and virtual private networks (VPNs).	No	No
Day and Time Restrictions	The day of the week and the time of day of the connection attempt.	No	No
Client IP Address	A character string that identifies the IP address of the RADIUS client.	Yes	Yes
Client Vendor	The manufacturer of the NAS that is requesting authentication.	No	Yes
Client Friendly Name	A character string that identifies the name of the RADIUS client that is requesting authentication.	Yes	Yes
Windows Groups	The names of the Windows 2000 groups to which the user who is attempting the connection belongs. For a remote access server in a domain in native mode or an IAS server, use universal groups. There is no condition for a specific user name.	No	No
Tunnel Type	Tunneling protocols for incoming packets, such as Layer Two Tunneling Protocol (L2TP).	No	No

You can create a remote access policy and an associated profile under **Remote Access Policies** in the console tree of Routing and Remote Access.

Delivery Tip

Demonstrate how to create a remote access policy.

To add a remote access policy:

1. Open Routing and Remote Access from the **Administrative Tools** menu.
2. Right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
3. In the Add Remote Access Policy wizard, type the name of the profile in the **Policy friendly name** box, and then click **Next**.
4. To configure a new condition, click **Add**.
5. In the **Select Attribute** dialog box, click the attribute to add, and then click **Add**.
6. In the *attribute* dialog box (the name of this dialog box will vary according to the attribute selected), enter the information that the attribute requires, and then click **OK**.
7. Click **Add** to add another condition, or click **Next** to continue with the wizard.
8. To grant access to callers matching these conditions, click **Grant remote access permission**, or to deny access, click **Deny remote access permission**, and then click **Next**.
9. You can then create a profile, or click **Finish** to create a policy without a profile. You can add a profile after the policy is created.

Configuring Remote Access Profile Settings

Topic Objective

To illustrate the role of profile settings.

Lead-in

After permission has been granted to a connection attempt, the settings of the profile are applied to the connection. Once again, if there is no match, the connection is denied.

Examples of Profile Settings

- 90-Minute Connect Time
- AND
- Four Multilink Lines (line drops if 50% use for 10 minutes)
- AND
- Require IPSec Encryption

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

The remote access profile specifies what kind of access the user will be given if the conditions match. Access will be granted only if the connection attempt does not conflict with the settings of the user account or the profile. You can configure a profile in the **Edit Dial-in Profile** dialog box by clicking **Edit Profile** in the **Properties** dialog box for a policy. You can configure the following settings in the dialog box:

- **Dial-in Constraints.** You can use these settings to determine the amount of idle time before disconnection; the maximum session time; and the days, times, telephone numbers, and media types (ISDN, VPN, and so on) that are allowed.
- **IP.** You can configure client IP address assignment and Transmission Control Protocol/Internet Protocol (TCP/IP) packet filtering on this tab. You can define separate filters for inbound or outbound packets.
- **Multilink.** You can configure Multilink and Bandwidth Allocation Protocol (BAP) on this tab. Use these settings to disconnect a line if bandwidth falls below a certain level for a given length of time. Multilink can also be set to require the use of BAP.
- **Authentication.** You can use these settings to define the authentication protocols that are allowed for connections that use this policy. Make sure that any protocols that you select here are also enabled in the **Properties** dialog box for the server.
- **Encryption.** You can use this tab to specify the types of encryption that are prohibited, allowed, or required.
- **Advanced.** You can use this tab to configure additional network parameters that can be sent from RADIUS servers running non-Microsoft operating systems.

Lab A: Creating a Remote Access Policy and Profile

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will create a remote access policy and profile.



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

Objectives

After completing this lab, you will be able to:

- Create a remote access policy.
- Create a remote access profile.
- Test a policy and a profile.

Prerequisite

Before working on this lab, you must have a familiarity with remote access policy and profile concepts.

Lab Setup

To complete this lab, you need the following:

- Successful completion of Lab A, “Configuring a VPN Connection,” in module 7, “Configuring Remote Access” of course 2153, *Implementing a Microsoft Windows 2000 Network Infrastructure*.
- 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.
- You will also need the following information. If you are unsure about any of these values, please ask your instructor.

Number	Record value here
Your student number	x=
Your partner’s student number	y=

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 needs to have more control over which employees have access to its network remotely, and it also needs more control over how those employees connect to the network. To accomplish this, you are going to configure remote access policies to control access to your network.

In this lab, you will work with a partner to configure remote access policies. You will create a user account, and configure its dial-in properties and group membership. You will then create a remote access policy for this group, and configure access by using that policy. Your partner will then use the user account that you created to dial in to your computer by a VPN connection, to test the use of the policy.

Estimated time to complete this lab: 45 minutes

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.

Exercise 1

Configuring and Testing Remote Access Policies

Scenario

Northwind Traders has implemented remote access servers for the sales force, to allow for secure access to the company network from the Internet. As the administrator for the remote access servers on your network, you need to implement a remote access policy that grants access to the sales groups and denies access to everyone else. Before you set up the actual remote access policy, you will create a test user and a test group.

Goal

In this exercise, you will create a test user in a test group, verify that the default policy denies access to the test user, and then create and test a remote access policy that grants access to members of the test group.

Tasks	Detailed Steps
 Perform the following procedures on both computers.	
1. Create a user called RemoteUserx (where <i>x</i> is your student number), with a password of password. Configure the user properties to allow dial-in access.	a. Log on as administrator@domain.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password . b. Open Active Directory Users and Computers from the Administrative Tools menu. c. In the console tree, under <i>domain</i> , right-click Users , point to New , and then click User . d. In the New Object – User dialog box, in the First name box, type RemoteUserx (where <i>x</i> is your student number). e. In the User logon name box, type RemoteUserx . f. Click <i>domain.nwtraders.msft</i> , and then click Next . g. Set the password for the new user account to password , click Next , and then click Finish . h. In the details pane, right-click RemoteUserx , and then click Properties . i. On the Dial-in tab, click Allow access , and then click OK .

(continued)

Tasks	Detailed Steps
2. Create a new global group called RemoteGroupx. Add the user that you just created to the group.	- In the console tree, right-click Users, point to New, and then click Group. - In the New Object – Group dialog box, in the Group name box, type RemoteGroupx (where <i>x</i> is your student number). - Under Group scope, verify that Global is selected, and under Group type, verify that Security is selected, and then click OK. - Open the Properties dialog box for RemoteGroupx. - On the Members tab, click Add. - In the Select Users, Contacts, Computers, or Groups dialog box, in the Look in box, verify that your domain is displayed. - In the list of objects, click RemoteUserx, click Add, and then click OK. - Click OK to close the RemoteGroupx Properties dialog box. - Minimize Active Directory Users and Computers.
 Important: Wait until your partner has completed the previous procedures before starting the following procedure.	
3. Test your dial-in configuration by dialing in to your partner's computer by using the account that your partner created, and then close the connection.	- Right-click My Network Places, and then click Properties. - In Network and Dial-up Connections, double-click Virtual Private Connection. - Connect as RemoteUser_y (where <i>y</i> is your partner's student number) with a password of password. - Click OK to close the Connection Complete message, and then disconnect the VPN connection.
 Important: You must perform tasks 4 and 5 at the same time as your partner.	
4. Configure the dial-in permissions for RemoteUserx to have access controlled through the remote access policy.	- Restore Active Directory Users and Computers, and then open the Properties dialog box for RemoteUserx. - On the Dial-in tab, click Control access through Remote Access Policy, and then click OK.
 Note: The domain controllers must be running in native mode for the Control access through Remote Access Policy option to be available on the Dial-in tab.	
4. <i>(continued)</i>	Minimize Active Directory Users and Computers.

(continued)

Tasks	Detailed Steps
5. Test your dial-in configuration by dialing in to your partner's computer as RemoteUser_y.	a. In Network and Dial-up Connections, double-click Virtual Private Connection, and then connect as RemoteUser_y (where <i>y</i> is your partner's student number) with a password of password.  <i>The connection attempt was denied because the default remote access policy denies access to all users. In native mode, if you select Control access through Remote Access Policy, you must configure a policy that allows access for your users.</i> b. In the Error Connecting to Virtual Private Connection dialog box, click Cancel. c. Minimize Network and Dial-up Connections.
6. Use Routing and Remote Access to add a new policy called Allow RemoteGroup_x access, which allows access to users in the RemoteGroup_x group. Make sure that this policy is evaluated before the default policy.	a. Open Routing and Remote Access from the Administrative Tools menu. b. In the console tree, expand <i>server</i> (where <i>server</i> is the name of your computer), right-click Remote Access Policies, and then click New Remote Access Policy. c. On the Policy Name page, type Allow RemoteGroup_x access (where <i>x</i> your student number), and then click Next. d. On the Conditions page, click Add, and in the Select Attribute dialog box, click Windows-Groups, and then click Add. e. In the Groups dialog box, click Add. f. In the Select Groups dialog box, in the Look in list, click your domain. g. In the Select Groups dialog box, under Name, click RemoteGroup_x, click Add, and then click OK. h. In the Groups dialog box, click OK. i. On the Conditions page, click Next. j. On the Permissions page, click Grant remote access permission, and then click Next. k. On the User Profile page, click Finish. l. In Routing and Remote Access, in the console tree, click Remote Access Policies, and in the details pane, right-click Allow RemoteGroup_x access, and then click Move Up. m. Minimize Routing and Remote Access.
	Important: Wait until your partner has completed the previous procedure before starting the following procedure.

(continued)

Tasks	Detailed Steps
7. Test your dial-in configuration by dialing in to your partner's computer.	- Restore Network and Dial-Up Connections, double-click Virtual Private Network, and then connect as RemoteUserx with a password of password. - Click OK to close the Connection Complete message, and then disconnect the VPN connection.
8. Configure the order of the remote access policies so that the default policy is evaluated first.	- Restore Routing and Remote Access. - In the console tree, click Remote Access Policies, and in the details pane, right-click RemoteGroupx, and then click Move Down. - Minimize Routing and Remote Access.
9. Test your dial-in configuration by dialing in to your partner's computer.	- In Network and Dial-Up Connections, double-click Virtual Private Network, and then connect as RemoteUserx with a password of password.  <i>Notice that this connection attempt fails because the policy denies dial-in permission.</i> - In the "Error Connecting to Virtual Private Connection" message, click Cancel.
 Important: You must perform tasks 10 and 11 at the same time as your partner.	
10. Configure the user dial-in properties of RemoteUserx to allow access.	- Restore Active Directory Users and Computers. - Open the Properties dialog box for RemoteUserx. - On the Dial-in tab, click Allow access, and then click OK. - Close Active Directory Users and Computers.
11. Test your dial-in configuration by dialing in to your partner's computer.	- In Network and Dial-Up Connections, double-click Virtual Private Network, and then connect as RemoteUserx with a password of password. - Click OK to close the Connection Complete message, and then disconnect the VPN connection.

Exercise 2

Disabling Routing and Remote Access

Scenario

One of your remote access servers is going to be replaced. You need to disable Routing and Remote Access for the server before taking the server offline.

Goal

In this exercise, you will disable Routing and Remote Access on your server and then log off.

Tasks	Detailed Steps
1. Remove the remote access policy that you added in the previous exercise.	- Restore Routing and Remote Access. - In the console tree, click Remote Access Policies. - In the details pane, right-click Allow RemoteGroupx access, and then click Delete. - In the Delete Policy box, click Yes.
2. Use Routing and Remote Access to disable the service on your computer, close all open windows, and then log off.	- 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 all open windows, and then log off.

◆ Troubleshooting Remote Access

Topic Objective

To introduce the topics related to troubleshooting the Remote Access Server.

Lead-in

To ensure the smooth functioning of the Remote Access Server, it is important to monitor and troubleshoot the server regularly.

- **Monitoring Remote Access**
- **Tracing Remote Access Connections**
- **Troubleshooting Communication Hardware**
- **Troubleshooting Communication Lines**
- **Troubleshooting Configuration Settings**

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

Remote access to your organization requires the successful operation of many components, including computers, communication hardware, communication lines, and in some cases, the Internet. Because the successful operation of remote access relies on such a large number of components to function correctly, operational problems arise occasionally. The ability to diagnose and then fix problems is critical to keeping your local and remote users connected to your network.

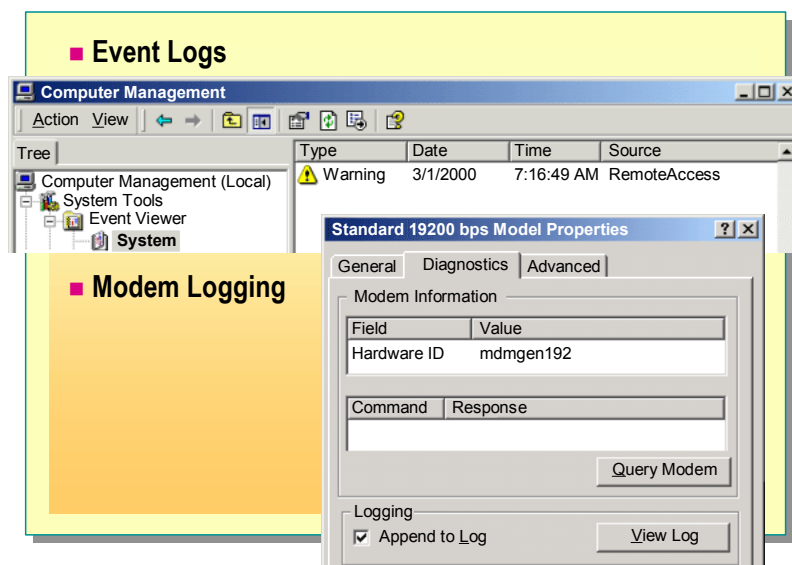
Monitoring Remote Access

Topic Objective

To explain the process of monitoring the remote access server.

Lead-in

It is important to monitor the remote access server to identify the source of a problem.



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

Monitoring the remote access server is the best method you can use to determine the source of problems on a remote access server. There are several tools and logs that can be used to monitor and troubleshoot remote access.

Event Logs

The Windows 2000 event log contains information about system components in Windows 2000 and is one of the first places to check for information about a problem. To access the event log, right-click **My Computer**, and then click **Manage**. Under **Computer Management**, expand **Event Viewer**, and then click **System**. The entries that have RemoteAccess listed in the source column are the event logs related to remote access.

Modem Logging

Windows 2000 Professional automatically records a log of communication made from the computer to a modem during a connection. This log is normally overwritten each time a new connection is made, but can be configured to append the log file. In Windows 2000 Server and Advanced Server, you must manually enable the log file.

To enable modem logging on Windows 2000 Server:

1. In Control Panel, double-click **Phone and Modem Options**.
2. In the **Phone and Modem Options** dialog box, on the **Modems** tab, click the modem that you are configuring, and then click **Properties**.
3. In the **Properties** dialog box for the modem, on the **Diagnostics** tab, click select the **Record a Log** check box, and then click **OK**. (In Windows 2000 Professional, this option appears as **Append to Log**. This means that each connection will not overwrite the existing log file.)

To view the log file, click **View log** on the **Diagnostics** tab.

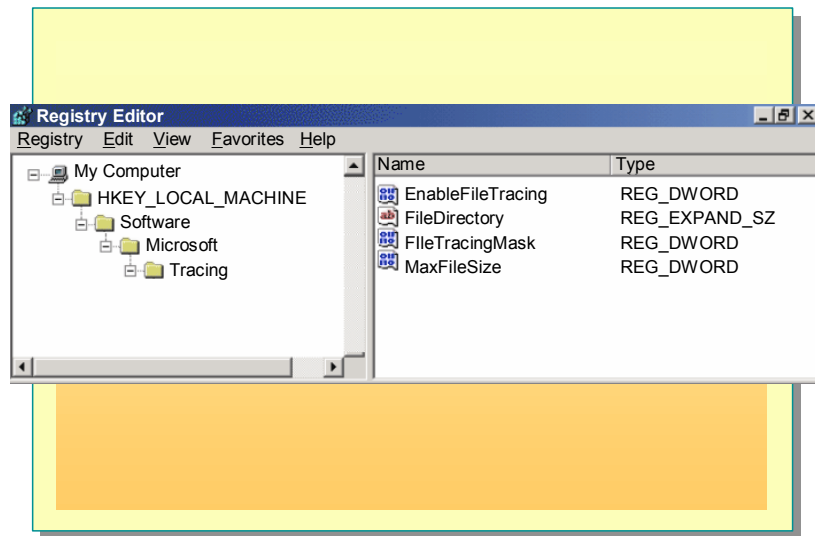
Tracing Remote Access Connections

Topic Objective

To explain the process of tracing remote access connections.

Lead-in

It is important to monitor the remote access server to identify the source of a problem.



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

Windows 2000 has an extensive tracing capability that you can use to troubleshoot complex network problems. You can enable the components in Windows 2000 Server to log tracing information to files. You must enable the tracing function by changing settings in the Windows 2000 registry under:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing

Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up all critical data on the computer.

You enable tracing for each remote access component by setting the registry values described in the following table

Value	Data type	Description
EnableFileTracing	REG_DWORD	You can enable logging tracing information to a file by setting the value of EnableFileTracing to 1. The default value is 0.
FileDirectory	REG_EXPAND_SZ	You can change the default location of the tracing files by setting FileDirectory to the path that you want. The file name of the log file is the name of the component for which tracing is enabled. By default, log files are placed in the <i>systemroot</i> \Tracing folder.

(continued)

Value	Data type	Description
FileTracingMask	REG_DWORD	FileTracingMask determines how much tracing information is logged to the file. The default value is FFFF0000, which is the maximum level of tracing.
MaxFileSize	REG_DWORD	You can change the size of the log file by setting different values for MaxFileSize . The default value is 65536 bytes (64 kilobytes).

Tracing consumes system resources, so you should use it only when necessary to help identify network problems. After the trace is captured or the problem is identified, you should immediately disable tracing. Do not leave tracing enabled on multiprocessor computers.

The tracing information can be complex and very detailed. Most of the time, this information is useful only to Microsoft Product Support Services engineers or to network administrators who are highly experienced with the Windows 2000–based router.

Troubleshooting Communication Hardware

Topic Objective

To identify the general areas that could be the source of problems in remote access.

Lead-in

When the user is unable to connect to the remote access server, the problem may be the hardware on the user's computer or the hardware on the remote access server.

■ User's Communication Hardware

- Refer to manufacturer's guidelines for hardware testing
- Query modem on **Diagnostics** tab
- View modem session log

■ Remote Access Server Communication Hardware

- Check hardware as you would on user's computer
- View system event logs

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

The first step in resolving a problem is to identify its source. After you identify the source of a problem, the solution is usually self-evident. When problems with remote access connections occur, the source may be the hardware on the user's computer or the hardware on the remote access server.

User's Communication Hardware

One of the first remote access components to check is the communication hardware that the user is using to connect remotely. This hardware may be a modem, network card, or some other device. Because most hardware has unique self-test procedures, refer to the hardware manufacturer's guidelines for information about how to check hardware.

If the connection is by a modem, make sure that the modem is configured correctly in Windows 2000, and that the modem's self-test functions correctly.

To check the modem:

1. In Control Panel, double-click **Phone and Modem Options**.
2. On the **Modems** tab, click your modem, and then click **Properties**.
3. Click the **Diagnostics** tab, and then click **Query Modem**.

If the modem is working correctly, a series of diagnostics responses should be returned. If the modem is faulty, try reinstalling the modem, or consult the modem manufacturer for more information.

To get more information about what the modem is doing during a connection attempt, you can view the modem session log information to determine the source of the error.

Remote Access Server Communication Hardware

Another possible source of problems with remote access connections is the communication hardware of the remote access server itself. To determine whether the communication hardware is functioning, check the system event logs for error messages, and use hardware testing methods provided by your hardware manufacturer.

If you suspect a problem with a modem, follow the same troubleshooting steps as for the client computer. Another way of determining a problem with remote access server modems is to call the modem with a normal telephone and hear whether the modem picks up the line and attempts to connect. If the remote access server modem does not try to connect, this is an indication that there is something wrong with the remote access server's modem.

Caution The noise generated during a connection attempt may be very loud when emitted from a normal telephone receiver. To avoid injury, hold the headset away from your ear.

Troubleshooting Communication Lines

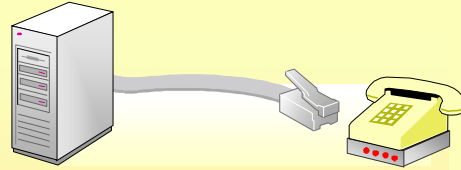
Topic Objective

To list how to troubleshoot problems with communication lines.

Lead-in

If the hardware is functioning properly, you should next check the communication lines.

■ Communication Line Failure



■ Intermittent Connection Failure

- Check system logs
- Check ports

■ VPN Connection Failure

- Check DNS
- Check firewall ports

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

If the communication hardware is functioning correctly, the next step is to verify that the communication lines are functioning.

Communication Line Failure

If the communication line is not working for some reason, or is not connected correctly, remote access connection attempts will fail. This can be the result of an incorrectly connected cable or disconnected telephone service.

In larger installations, it is common for many telephone lines to be used for remote access connections. Before connecting a telephone line to a modem, always check to make sure that the line is working correctly by using a normal telephone receiver.

Intermittent Connection Failure

Often, in large remote access installations, a single telephone number is used for dial-in and is then split into a number of separate telephone lines by a piece of hardware called a rotary splitter. Modems are then connected to each line. In this situation, it is possible for one modem to be faulty or incorrectly configured. This will give the end-user the appearance that the connection to the remote access server gives intermittent failures, because the connection attempt only fails when the rotary tries to connect the user by using the line connected to the faulty modem.

To identify the intermittent connection problem, use the system event logs; but if the problem is in the remote access hardware itself, check which ports are being used in Routing and Remote Access. The faulty modem port should appear as unused even during busy times.

VPN Connection Failure

When troubleshooting a VPN connection, the communication line is replaced by the Internet, which will result in different errors. If there is a problem connecting to a VPN server, check that the Domain Name System (DNS) name of the server is correct, and check that DNS name resolution is functioning correctly. Also, if you are connecting through a firewall, ensure that you have the correct ports open at the firewall to allow the VPN connection through the firewall. Another reason for VPN connection failure can be the use of network address translation (NAT). If you use NAT to protect internal IP addressing, you cannot use L2TP and IPSec to connect to a remote VPN server. IPSec cannot pass through a NAT.

Troubleshooting Configuration Settings

Topic Objective

To list how to troubleshoot problems with configuration settings.

Lead-in

After you check the hardware and communication lines, check the settings for the server and client computer.

■ Network Configuration

- Check TCP/IP configuration, and DNS and WINS IP addresses
- PING user

■ Remote Access Server Settings

- Check system event log
- Enable tracing

■ User's Computer Settings

- Check configuration
- Create new setting

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

After you determine that the source of the problem is not the hardware or communication lines, check the configuration settings.

Network Configuration

Network configuration error occurs when the user successfully connects, and appears to have a valid connection, but is still unable to access resources on the network. Network configuration error is usually due to a problem with the underlying network. It might occur if name resolution is not working correctly, or if some other critical network function, such as routing, is not configured correctly.

When network configuration error occurs, confirm that you can access resources when you are connected directly to the network, and check TCP/IP configuration properties by using the **ipconfig /all** command on the client. Make sure that the DNS and/or Windows Internet Name Service (WINS) server IP addresses are configured and working. Also, attempt to diagnose the problem as if the user's computer were connected directly to the local area network (LAN). Use the **ping** command on the user's computer to determine where the network connectivity problem resides.

Remote Access Server Settings

The settings that you configure on your remote access server can prevent users with incorrect settings from completing a connection. To determine whether a setting on the remote access server is causing a connection to fail, the user must successfully connect to the server and then become disconnected due to one of the configured settings.

To help determine which setting could be at fault, check the system event log on the remote access server and on the computer on which the user dials in. In some cases it may be necessary to enable tracing on the remote access server to determine the cause of the problem.

User Computer Settings

There are a number of settings that can be made to the computer and to the connection properties that will cause a remote access connection to fail. For example, if the computer on which the user dials in only uses the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol (NWLink) and the remote access server only uses TCP/IP, the connection will not be successful.

In the event of a connection failure, if the remote access server and communication lines are tested and found to be working correctly, the cause of the failure is probably in the user's computer settings. Examine the error messages that appear; if they do not show the cause, check the system event log and the modem log, if this is a modem connection.

A common problem with user computer settings occurs when a user has modified the connection properties in such a way that it causes the connection attempt to fail. A quick way to determine whether this is the problem is to re-create the outbound connection by using the Make New Connection wizard. Either create a new connection or instruct the user to create a new connection, and attempt to connect to the remote access server again. If this new connection succeeds, the configuration of the original connection was the problem.

Lab B: Troubleshooting Remote Access (Simulation)

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will troubleshoot remote access connections.



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

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Read event logs to determine the cause of an error
- Troubleshoot remote access problems

Prerequisites

Before working on this lab, you must have:

- The ability to configure a remote access connection
- An understanding of how VPN connections work

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Windows 2000, Windows NT 4.0, Microsoft Windows 98, or Microsoft Windows 95
- A minimum display resolution of 800 x 600 with 256 colors

► **To start the lab**

1. Insert the Student Materials compact disc into your CD-ROM drive.
2. At the root of the compact disc, double-click **Default.htm**.
3. On the Student Materials Web page, click **Lab Simulations**, and then click **Troubleshooting Remote Access**.
4. Read the introductory information, and then click the link to start the lab.

Estimated time to complete this lab: 15 minutes

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.

- **Examining Remote Access Policies**
- **Examining Remote Access Policy Evaluation**
- **Creating a Remote Access Policy**
- **Troubleshooting Remote Access**

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

1. You have been receiving many help-desk calls lately about users not being able to connect to your remote access servers because all available lines are busy. You monitor the incoming lines, and notice that many people connect and remain connected for many hours, even though they do not transmit or receive any data. How can you reduce the time that users stay connected while idle?

Create a remote access policy and specify in the conditions the busy times of the day for remote access. Next, configure the profile associated with that policy so that users are disconnected after 30 minutes of idle time.

2. You want to allow different time use and Multilink settings for different groups of users connecting to your remote access server. What steps do you need to perform to achieve this?

Create a remote access policy for each group of people that you want to have different settings. For each policy, configure the remote access profile so that users have specific connection limitations and Multilink settings.

3. You want to control dial-up access to your remote access server completely through policies, but when you attempt to configure this by using Active Directory Users and Computers, the option to **Control access through remote access policy** is not available. Why?

The ability to control remote access permissions through policies is only available to stand-alone servers and to servers in a domain that is in native mode.

4. Users are attempting to connect to your remote access server, but are receiving a message that they do not have dial-in permissions. You look up their accounts in Active Directory Users and Computers, and they do have dial-in permissions. What could be causing the problem?

There are no remote access policies created, or all of the policies have been deleted. You must have at least one remote access policy to enable users to connect.

5. A user is calling the help desk to say that he cannot connect to the organization's remote access servers. You look up the event logs on the remote access server for all remote access entries, but find no entries. What components of the remote access connection could be causing this error?

User's computer settings, user's communication hardware, server communication hardware, and the communication lines themselves.