
Module 14: Managing a Windows 2000 Network

Contents

Overview	1
Windows 2000 Administrative Strategies	2
Performing Administrative Tasks Remotely by Using Terminal Services	3
SNMP Operation	11
Implementing the Windows 2000 SNMP Service	19
Lab A: Managing a Windows 2000 Network	27
Review	36
Course Evaluation	37



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

Lab:
60 Minutes

This module provides students with the knowledge and skills necessary to manage Microsoft® Windows® 2000–based computers and networks by using Terminal Services remote administration and the Simple Network Management Protocol (SNMP).

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

- Identify Windows 2000 administrative strategies.
- Perform administrative tasks remotely by using Terminal Services.
- Explain how the SNMP protocol works.
- Implement the Windows 2000 SNMP service.

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 Microsoft PowerPoint® file 2153a_14.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Read the white paper *Using Terminal Services for Remote Administration of the Windows 2000 Server Family*, under **Additional Reading** on the Web page on the Student Materials compact disc.
- Read RFC 1157 *A Simple Network Management Protocol (SNMP)* under **Additional Reading** on the Web page on the Student Materials compact disc.
- Read the entire “Simple Network Management Protocol” section in the Windows 2000 Server Resource Kit.
- Read the entire “Terminal Services” section in Windows 2000 Server Help.

Module Strategy

Use the following strategy to present this module:

- **Windows 2000 Administrative Strategies**

This section is designed to provide an overview of the administrative strategies that students can use to administer Windows 2000–based computers and networks. Explain the two options available to students: Terminal Services remote administration and SNMP. Briefly explain the benefits and uses of each.

- **Performing Administrative Tasks Remotely by Using Terminal Services**

This section is designed to explain how to administer a network remotely by using Terminal Services. Start by explaining how Terminal Services allows students to administer a network remotely. Explain the concept of Terminal Services and what it allows users to do. Next, explain the requirements for using Terminal Services for remote administration. Define the operating system requirements and the hardware requirements for the service.

Next, explain how to install Terminal Services for remote administration. Clarify the differences between installing Terminal Services for remote administration and installing Terminal Services for application sharing. Finally, explain how to configure Terminal Services for remote administration. Explain how to configure performance parameters to increase system performance, and security parameters to ensure secure connections while administering network computers.

- **SNMP Operation**

This topic is designed to provide an overview of SNMP and the benefits that it provides to network administration. Start by giving an overview of SNMP and what it is used for. Next, differentiate between management systems and agents. Point out that Windows 2000 can serve as an agent, but not a management system. Next, explain how students can make a Windows 2000–based computer serve as an agent by using the Windows 2000 SNMP service. Next, describe the management information base (MIB) and what it does. Point students to the Windows 2000 Server Resource Kit, which provides more information about the MIBs included with Windows 2000. Next, explain the hierarchical name tree, and reference the name tree assigned to Microsoft Corporation. Finally, define SNMP communities and explain how they support network administration.

- **Implementing the Windows 2000 SNMP Service**

This topic is designed to describe how to implement the Windows 2000 SNMP service. First, explain how to install the SNMP service on computers running Windows 2000. Next, explain how to configure SNMP service security. Next, explain how to configure the Windows 2000 SNMP agent properties. And finally, explain how students can use the SNMPUTIL utility to confirm the SNMP connection with the management agent computer.

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 how to use Terminal Services to perform remote administration, and you will learn about SNMP.

- **Windows 2000 Administrative Strategies**
- **Performing Administrative Tasks Remotely by Using Terminal Services**
- **SNMP Operation**
- **Implementing the Windows 2000 SNMP Service**

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

As a network professional, you may be required to perform administrative tasks even when you are not physically present at the server that needs attention. Microsoft® Windows® 2000 provides solutions for your remote administrative needs. Using Terminal Services, you can control the server remotely to perform your administrative tasks. You can also use the Simple Network Management Protocol (SNMP) to manage network elements from a central location.

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

- Identify Windows 2000 administrative strategies
- Perform administrative tasks remotely using Terminal Services
- Explain how the SNMP protocol works
- Implement the Windows 2000 SNMP Service

Windows 2000 Administrative Strategies

Topic Objective

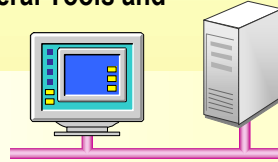
To introduce Windows 2000 tools for remote administration and network management.

Lead-in

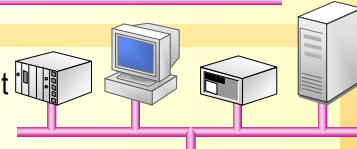
Windows 2000 provides tools and methods that facilitate remote administration, in addition to the ability to use third-party tools for data collection.

Windows 2000 Provides Several Tools and Methods for Administration

- Terminal Services



- Simple Network Management Protocol (SNMP)



- SNMP Service



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

Windows 2000 provides you with a great deal of flexibility when you administer your network. The tools and methods provided in Windows 2000 include:

- *Terminal Services*. From a client computer, you can run interactive sessions on a remote computer that is running Windows 2000 Server so that you can administer the server from the client computer as if you were using the server locally.
- *SNMP*. SNMP is a standard for retrieving information from a wide range of networking devices. It can also alert network administrators about events on these devices. You can manage computers running Windows 2000 by using an SNMP-based management application.
- *SNMP Service*. Windows 2000 supports SNMP with the SNMP service. The SNMP service provides Windows 2000 with the ability to use SNMP to query computers for data and communicate with the third-party management systems.

◆ Performing Administrative Tasks Remotely by Using Terminal Services

Topic Objective

To introduce using Terminal Services for remote administration.

Lead-in

You can use Terminal Services to administer computers remotely.

- Using Terminal Services for Remote Administration
- Requirements for Terminal Services Remote Administration
- Installing Terminal Services for Remote Administration
- Configuring Terminal Services for Remote Administration

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

You can use Terminal Services in Windows 2000 to remotely administer a network or a device on that network. Terminal Services allows you to open interactive sessions on a remote server and administer the server from a client computer as if you were using the server locally. The desktop of the server appears in a window on the desktop of your local computer. The Terminal Services client sends keystrokes and mouse movements to the Terminal server and receives screen updates from the server.

Using Terminal Services for Remote Administration

Topic Objective

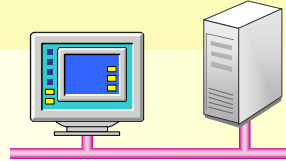
To present the benefits of using Terminal Services for remote administration.

Lead-in

By using Terminal Services, you can remotely administer a server as if you were using the server locally.

Benefits of Using Terminal Services For Remote Administration:

- Allows remote server administration
- Operates with Windows 2000 in addition to non-Windows 2000 operating systems
- Requires minimal client software
- Performs well over a slow network link



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

Key Points

You can use Terminal Services to perform all of the administrative tasks that you are permitted to perform locally on a server, including software installation.

Administrators can connect to a server with Terminal Services installed from client computers running operating systems other than Windows 2000.

Using Terminal Services for remote administration provides the following benefits:

- You can perform all administrative tasks on a server from a remote computer, including software installation.
- You can connect to a server running Terminal Services from client computers running Windows 2000, Microsoft Windows NT®, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 3.1, and Microsoft Windows CE.
- The Terminal Services client software requires minimal resources to run. The installation files for the client computer fit on two to four floppy disks.
- Terminal Services provides excellent performance, even over a slow network link. Because the Terminal Services client transmits only keystrokes and mouse movements, and Terminal Services only transmits screen updates, bandwidth requirements are low.

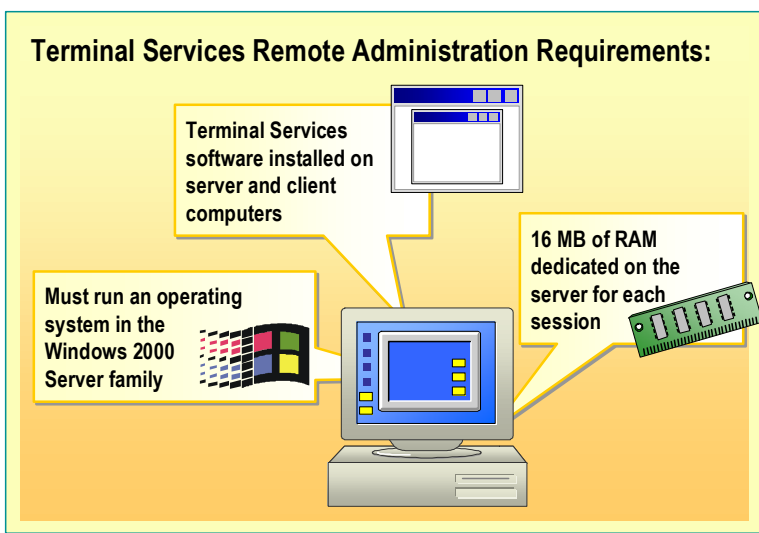
Requirements for Terminal Services Remote Administration

Topic Objective

To identify the system requirements for using Terminal Services for remote administration.

Lead-in

You must ensure that your hardware meets the requirements to support remote administration.



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

Key Point

Terminal Services dedicates approximately 16 MB of RAM on the server for each Terminal Services session.

The computer on which you install Terminal Services must meet the following requirements to use Terminal Services for remote administration:

- The computer must be running one of the operating systems in the Windows 2000 Server family.
- You must install Terminal Services on the server and Terminal Services Client on the client computer.
- Each active session on the server requires approximately 16 megabytes (MB) of random access memory (RAM), in addition to memory requirements for the application in the Terminal Services session and other memory that the server is using. This amount of RAM is therefore unavailable for other use.

Note For more information about Terminal Services, see module 15, "Installing and Configuring Terminal Services," in course 2152, *Implementing Microsoft Windows 2000 Professional and Server*.

Installing Terminal Services for Remote Administration

Topic Objective

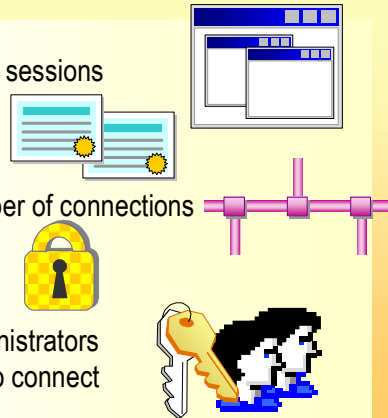
To demonstrate the installation of Terminal Services in remote administration mode.

Lead-in

Terminal Services can be installed in either application server mode or remote administration mode.

Features of Terminal Services Installation:

- Limited to two concurrent sessions
- Comes with two licenses
- Optimized for small number of connections
- Higher security settings
- By default, only the Administrators Group has permissions to connect



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

When you install Terminal Services on a computer running Windows 2000, you must decide whether to install it in application server mode or in remote administration mode. You must select the appropriate mode when you install Terminal Services. In order to use Terminal Services to administer your network, select remote administration mode when installing Terminal Services.

Characteristics of Remote Administration Mode

In remote administration mode:

- Terminal Services is limited to two concurrent connections.
- Two Terminal Services licenses are included. You do not need to purchase additional client licenses.
- Terminal Services performance is optimized for a small number of connections.
- Terminal Services security settings are configured to be higher than in application server mode.
- By default, only members of the Administrators group have permissions to connect to the remote computer by using Terminal Services.

Installing Terminal Services

To install Terminal Services:

1. Open Add/Remove Programs from Control Panel, and then click **Add/Remove Windows Components**.
2. In the Windows Components wizard, on the **Windows Components** page, select the **Terminal Services** check box, and then click **Next**.
3. On the **Terminal Services Setup** page, click **Remote administration mode**, click **Next** when prompted type the path to the setup files, and then click **Finish**.
4. When prompted, click **OK** to restart your computer.

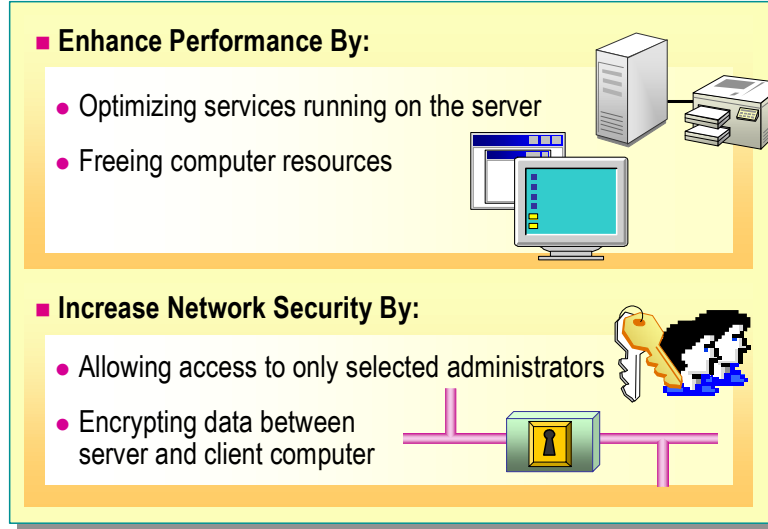
Configuring Terminal Services for Remote Administration

Topic Objective

To show how to configure Terminal Services to enhance performance and network security.

Lead-in

By default, Terminal Services is optimized for a small number of client connections. You can further improve performance and security by performing additional configuration steps.



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

When you install Terminal Services for remote administration, Windows 2000 automatically optimizes many settings for a small number of client connections.

Windows 2000 also configures some security settings for a higher level because administrators may access confidential data while accessing the Terminal server from an insecure client computer. For example, only administrators have permissions to log on to a terminal server. Also, when you install Terminal Services in remote administration mode, Windows 2000 ensures that no data from a session can remain on the client computer's Clipboard. You can improve performance and security further by performing additional configuration steps.

Configuring Performance Parameters

You can configure two performance parameters to enhance the performance of the Terminal Services session.

Optimizing Services Running On The Server

Because performance for multiple Terminal Services sessions is not the primary purpose of the server that you are configuring, you must optimize the performance of background services, such as file and printer sharing.

To configure background services:

1. In Control Panel, double-click **System**.
2. In the **System Properties** dialog box, on the **Advanced** tab, click **Performance Options**.
3. For the **Optimize performance for** option, click **Background services**.

Freeing Computer Resources

You can configure Terminal Services to close inactive and disconnected Terminal Services client sessions after a designated amount of time. This is useful if you limit the number of concurrent sessions and an administrator forgets to end a session. These settings also enhance security.

To maximize resource availability, you should set the idle session limit to ten minutes and the time limit to end a disconnected session to five minutes.

To set the idle session limit and the time to end disconnected session limit:

1. Open Terminal Services Configuration from the **Administrative Tools** menu.
2. In the **RDP-Tcp Properties** dialog box, on the **Sessions** tab, ensure that **Override user settings** is selected.
3. In the **Idle session limit** list, click **10 minutes**.
4. In the **End a disconnection session** list, click **5 minutes**.

Configuring Security Parameters

You can configure two settings to enhance Terminal Services security. You configure all settings by using Terminal Services Configuration.

Controlling Administrator Access

You can control administrator access to the Terminal server to control which administrators can use Terminal Services for remote administration. To maintain a high level of security, you should allow only those administrators who are authorized to administer a specific server to connect from a Terminal Services client.

To configure administrator access:

1. Open Terminal Services Configuration from the **Administrative Tools** menu.
2. In Terminal Services Configuration, select **Connections**, and in the right pane, right-click the **RDP-Tcp** connection and then select **Properties**.
3. On the **Permissions** tab, assign the **Full Control** permission only to groups for selected administrators.
4. Remove all other user accounts and groups in the **Name** box, except for the System account.

Encrypting Terminal Services Data

You can encrypt the data between the Terminal Services server and client computer to prevent access to unauthorized people. Encrypting this data can decrease performance on slow client computers, but high encryption is recommended due to the often confidential nature of administrative tasks.

To encrypt data between Terminal Services clients and servers:

1. Open Terminal Services Configuration from the **Administrative Tools** menu.
2. In Terminal Services Configuration, select **Connections**, and in the right pane, right-click the **RDP-Tcp** connection and then select **Properties**.
3. On the **General** tab, click **High** to set the encryption level to high.

Note To use high encryption, you must also install the Windows 2000 High Encryption Pack.

◆ SNMP Operation

Topic Objective

To provide an overview of the SNMP protocol.

Lead-in

SNMP is a standard Internet protocol that allows a third-party management system to collect data centrally from many network devices, including computers running Windows 2000.

- Overview of SNMP
- Management System and Agents
- The Windows 2000 SNMP Service
- The Management Information Base
- The Hierarchical Name Tree
- Defining SNMP Communities

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

SNMP is an industry-standard network management protocol that is used to manage network nodes (servers, workstations, routers, bridges, and hubs) from a centrally located host. SNMP is widely used with Transmission Control Protocol/Internet Protocol (TCP/IP) networks and, more recently, with Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) networks. Windows 2000 supports SNMP through the SNMP service.

Understanding how to use SNMP helps you effectively implement SNMP to manage your network.

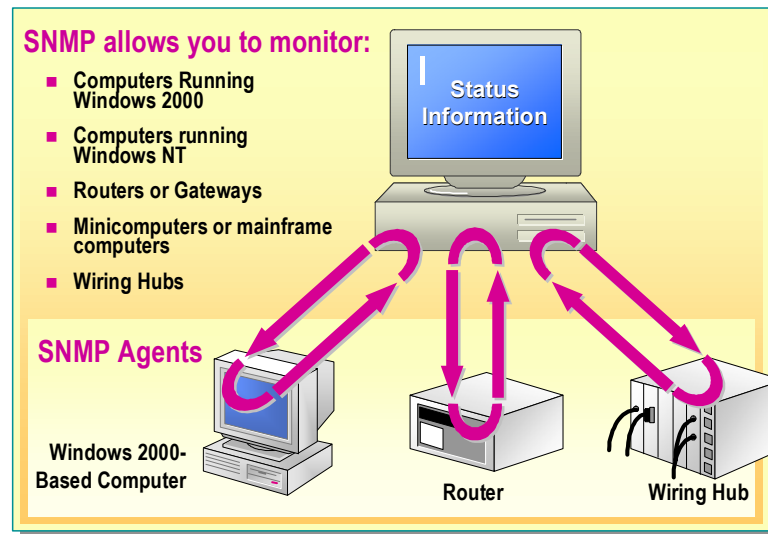
Overview of SNMP

Topic Objective

To define SNMP.

Lead-in

SNMP provides the ability to monitor networking devices and communicate status information between computers on a network.



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

SNMP, a part of the TCP/IP protocol suite, was developed in the Internet community to monitor and troubleshoot routers and bridges. SNMP provides the ability to monitor and communicate status information between many different networking devices, such as:

- Computers running Windows 2000
- Computers running Windows NT
- Routers or gateways
- Minicomputers or mainframe computers
- Wiring hubs

The SNMP service sends status information to one or more hosts when the host requests the information, or when a significant event occurs—for instance, when a host runs out of hard disk space.

Note For more information about SNMP, see RFC 1157 under **Additional Reading** on the Web page on the Student Materials compact disc. Many other RFCs update specific aspects of SNMP. For a more extensive listing of applicable RFCs, see the “Simple Network Management Protocol” section in the Windows 2000 Server Resource Kit.

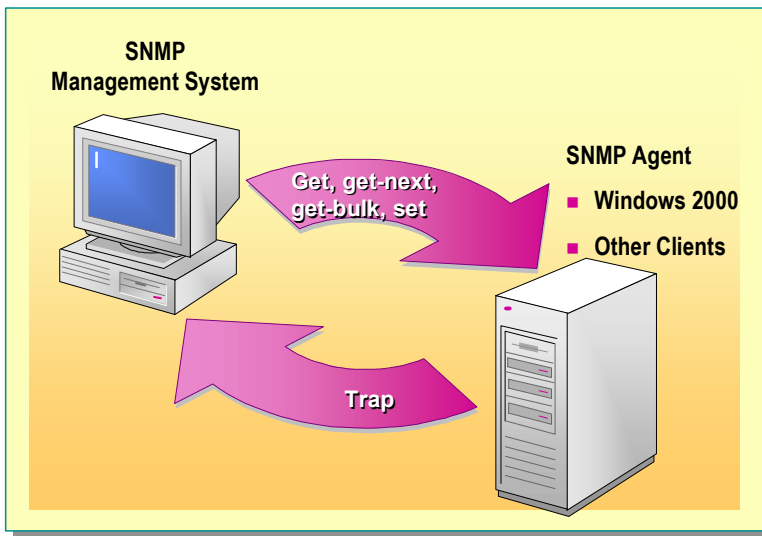
Management System and Agents

Topic Objective

To explain how SNMP management systems and SNMP agents communicate.

Lead-in

SNMP uses a distributed architecture that consists of management systems and agents.



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

SNMP uses a distributed architecture. This architecture consists of two components: management systems and agents.

- *Management system.* A management system is any computer running SNMP management software. The primary function of any management system is to request information from an agent.
- *Agents.* An agent is any device running SNMP agent software, such as a server or router. The primary function of an agent is to send information that the management system requests.

SNMP Management System Information Request

A management system can request information through the **get**, **get-next**, **get-bulk**, and **set** operations.

- The **get** operation is a request for a specific value, such as the amount of hard disk space available.
- The **get-next** operation is a request for the “next” value. You use this operation to request data that follows the current data.
- The **get-bulk** operation is a request for a large amount of management data. You use this request to minimize the number of protocol exchanges.
- The **set** operation changes a value. You rarely use this operation, because most values have read-only access and cannot be set.

SNMP Agent Trap Messages

The notify operation, also called a trap message, alerts management systems to an unusual event, such as a password violation. You configure an SNMP agent to specify under what conditions it sends a trap, and to what management systems it sends traps.

Note The only management operation that an agent can initiate is a trap.

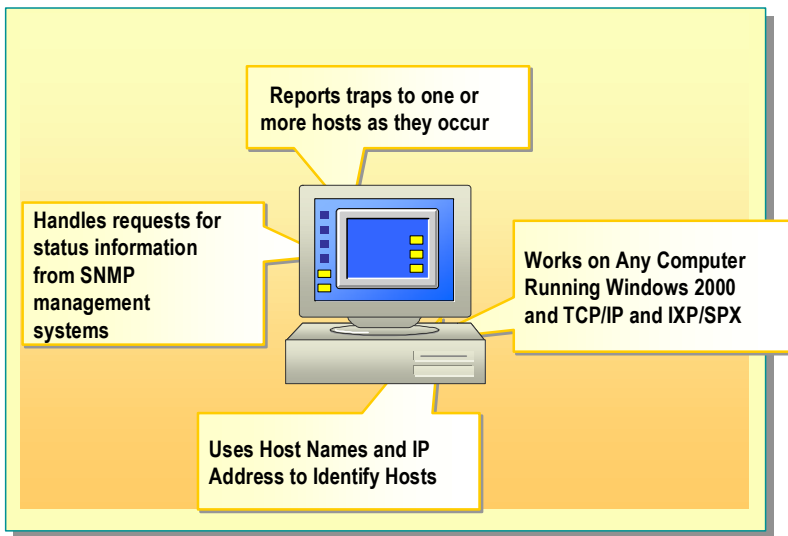
The Windows 2000 SNMP Service

Topic Objective

To provide an overview of the Windows 2000 SNMP service.

Lead-in

Computers running Windows 2000 can serve as SNMP agents by using the Windows 2000 SNMP service.



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

Computers running Windows 2000 can serve as SNMP agents by using the Windows 2000 SNMP service. Computers running Windows 2000 with the SNMP service installed can communicate with SNMP management systems.

The Windows 2000 SNMP service:

- Reports traps to one or more hosts as they occur.
- Handles requests for status information from SNMP management systems.
- Can be installed and used on any computer running Windows 2000 and TCP/IP or IPX/SPX.
- Uses host names and IP addresses to identify the hosts to which it reports information and from which it receives requests.

Note SNMPUTIL, an SNMP management tool in the Windows 2000 Resource Kit, provides SNMP management features. In addition, there are many third-party products available to provide SNMP management features on a Windows 2000 network.

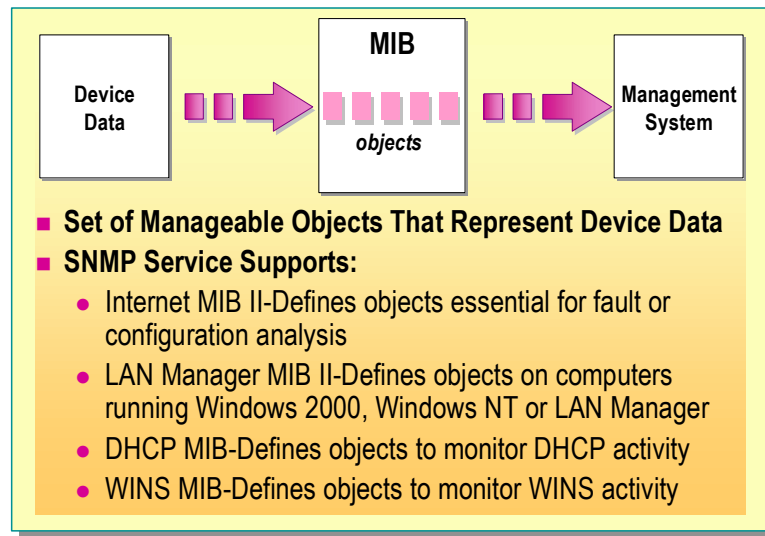
The Management Information Base

Topic Objective

To define a MIB and list the MIBs that the SNMP service supports.

Lead-in

A MIB defines the information that can be queried.



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

A management information base (MIB) defines what data a management system can request from an agent, how the management system must request the data, and how the agent formats the information that it returns. A MIB serves as a set of manageable objects that represent information about a network device, such as the number of active sessions or the version of network operating system software that runs on a host. SNMP management systems and agents must share a common understanding of MIB objects in order to operate.

A MIB combines similar objects. For example, the Internet MIB II defines 171 objects that are essential for either fault analysis or configuration analysis. The LAN Manager MIB defines objects to monitor computers running Windows 2000, Windows NT, or LAN Manager. Other MIBs cover components such as Dynamic Host Configuration Protocol (DHCP) or Windows Internet Name Service (WINS).

Typically, an SNMP management system removes the intricacies of understanding MIB definitions for manageable objects from an administrator. However, when selecting an SNMP management system, you must ensure that it supports all of the MIBs that Windows 2000 uses.

Note For more information about Internet MIB II, see RFC 1213 under **Additional Reading** on the Web page on the Student Materials compact disc. For a complete list of the MIBs that Windows 2000 includes, see the appendix “MIB Object Types” in the Windows 2000 Server Resource Kit.

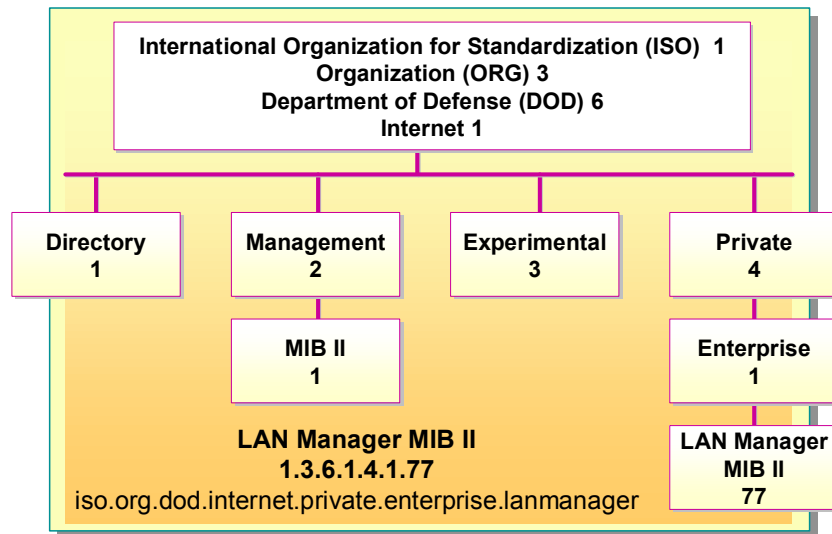
The Hierarchical Name Tree

Topic Objective

To describe the name tree that is used to map MIB objects.

Lead-in

The namespace for MIB objects is hierarchical.



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

The MIB object namespace is hierarchical. It is structured so that each manageable object can be assigned a globally unique name. The International Organization for Standardization (ISO) has authority for the root of the namespace and assigns authority for parts of the namespace to individual organizations. This allows organizations to assign names without consulting an Internet authority for each assignment.

Object Identifier Format

The object identifier in the hierarchy is written as a sequence of labels beginning at the root and ending at the object. Labels are separated with periods. For example: 1.3.6.1.4.1.77.

Microsoft Object Identifier Namespace

Microsoft Corporation has been assigned object identifier namespace 1.3.6.1.4.1.311. All new MIBs for Microsoft are created under that branch. Microsoft has the authority to assign names to objects anywhere below that namespace.

For example, the object identifier for MIB II is iso.org.dod.internet.management.mibii, with an object number of 1.3.6.1.2.1. The object identifier for LAN Manager MIB II is iso.org.dod.internet.private.enterprise.lanmanager, with an object number of 1.3.6.1.4.1.77.

Note The namespace used to map object identifiers is distinct and separate from the hierarchical Domain Name System (DNS) namespace.

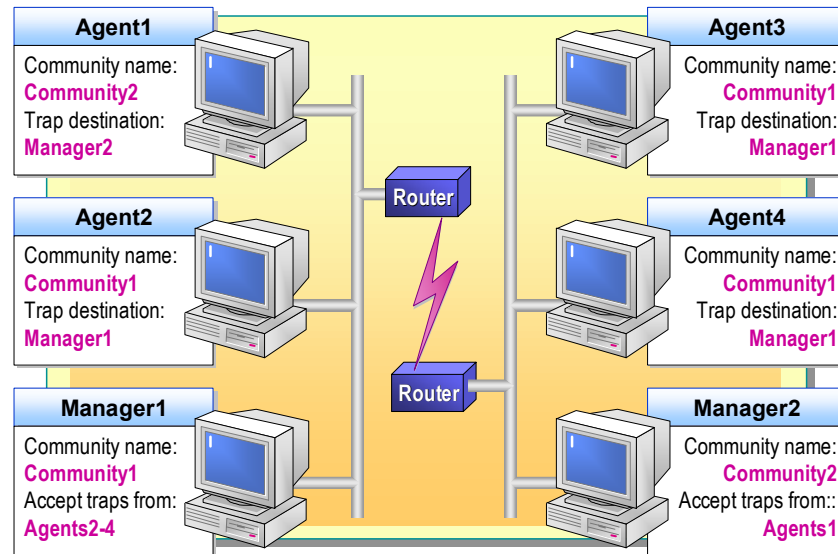
Defining SNMP Communities

Topic Objective

To explain how an SNMP community is used to group hosts.

Lead-in

After installing SNMP, you must define an SNMP community.



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

Delivery Tip

Use the graphic to explain how an SNMP community defines which hosts can communicate with each other.

SNMP agents and management systems belong to groups called *communities*. Communities are identified by a community name. The use of a community name provides primitive security and context checking for agents and for management systems.

Only agents and managers that are members of the same community can communicate with each other. An agent will not accept a request from a management system outside the agent's configured community.

Note The default community that most SNMP agents and management systems use is *public*. It is recommended that you change the default community name to a name other than public because public is the default, and keeping the default name can compromise security.

In the example in the previous slide, there are two defined communities: Community1 and Community2. An SNMP agent can be a member of multiple communities at the same time. This allows the SNMP agent to communicate with SNMP managers of the communities where the SNMP agent has membership.

- Agent1 can receive and send messages to Manager2 because they are both members of the Community2 community.
- Agent2, Agent3, and Agent4 can receive and send messages to Manager1 because they are all members of the Community1 community.

◆ Implementing the Windows 2000 SNMP Service

Topic Objective

To introduce the topics covered in this section.

Lead-in

Before a computer running Windows 2000 can function as an SNMP agent, you must first install and configure the Windows 2000 SNMP service.

- Installing the SNMP Service
- Configuring SNMP Service Security
- Configuring Windows 2000 SNMP Agent Properties
- Configuring SNMP Traps
- Using SNMPUTIL to Confirm the SNMP Configuration

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

Before a computer running Windows 2000 can function as an SNMP agent, you must install and configure the Windows 2000 SNMP service.

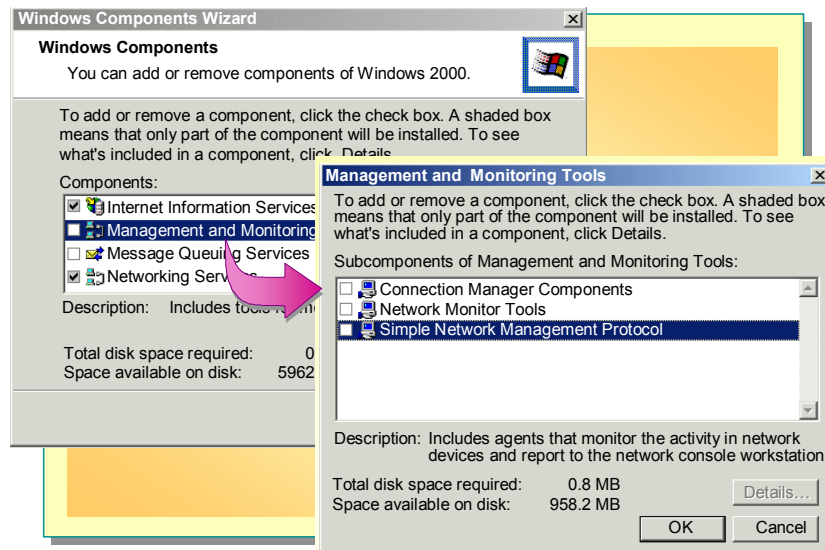
Installing the SNMP Service

Topic Objective

To explain the procedure for installing the SNMP service on a Windows 2000-based computer.

Lead-in

If you want to monitor a Windows 2000-based computer with a third-party SNMP manager, you must first install the SNMP service.



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

To install the SNMP service:

1. In Control Panel, double-click **Add/Remove Programs**.
2. In the **Add/Remove Programs** dialog box, click **Add/Remove Windows Components**.
3. In the Windows Components wizard, on the **Windows Components** page, click **Management and Monitoring Tools**, and then click **Details**.
4. In the **Management and Monitoring Tools** dialog box, select the **Simple Network Management Protocol** check box, and then click **OK**.
5. On the **Windows Components** page, click **Next**, and when Windows 2000 has configured all settings, click **Finish**.

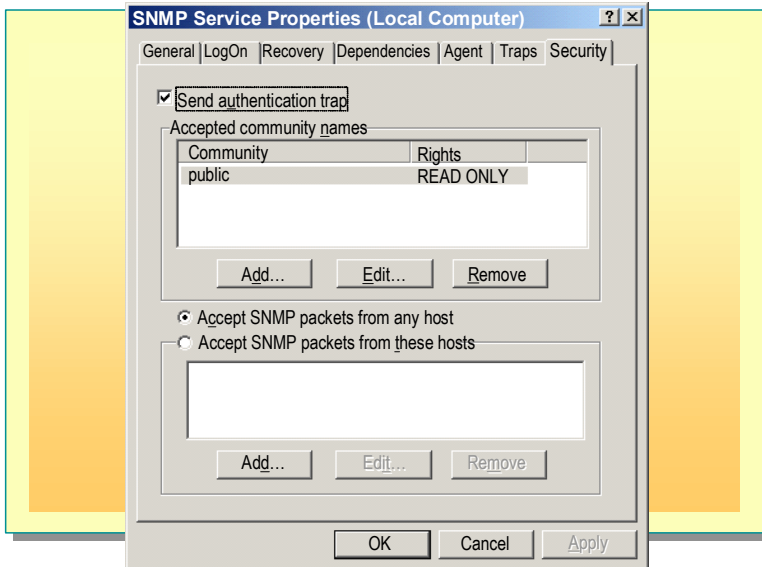
Configuring SNMP Service Security

Topic Objective

To explain the procedure for configuring SNMP service security.

Lead-in

An agent does not accept a request from a management system outside the agent's community.



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

Delivery Tips

Demonstrate the steps to configure SNMP security.

Mention that Windows 2000 sends an authentication trap by default.

The SNMP service provides primitive security and context checking for Windows 2000–based agents and for management systems.

To configure SNMP security on a Windows 2000–based agent:

1. Open Computer Management from the **Administrative Tools** menu.
2. In Computer Management, expand **Services and Applications**, and then in the console tree, click **Services**.
3. In the details pane, right-click **SNMP Service**, and then click **Properties**.
4. In the **SNMP Service Properties** dialog box, click the **Security** tab.
5. Configure the following parameters:
 - **Send authentication trap.** If someone attempts to manage the system from an unauthorized SNMP management system, or a query is sent to the wrong community, the send authentication trap allows the SNMP agent to send an SNMP trap to the configured SNMP management station.
 - **Accepted community names.** A host must belong to a community that appears on this list for the SNMP service to accept requests from that host. Typically, all hosts belong to public, which is the standard name for the common community of all hosts. Add or remove community names and select the rights for a management system. The default right is Read-Only.

- **Accept SNMP packets from any host.** If you click this option, the agent accepts all SNMP packets regardless of which host they originated from.
- **Only accept SNMP packets from these hosts.** If you click this option, the agent only accepts SNMP packets from the hosts listed.

Note The security recommendations are to enable the **Accept SNMP packets from these hosts** option and add the designated SNMP management stations. This ensures that agents accept only SNMP packets from authorized SNMP management stations. It is also recommended that you enable the **Send authentication trap** option, which enables authentication traps to log when an unauthorized host tries to access the system.

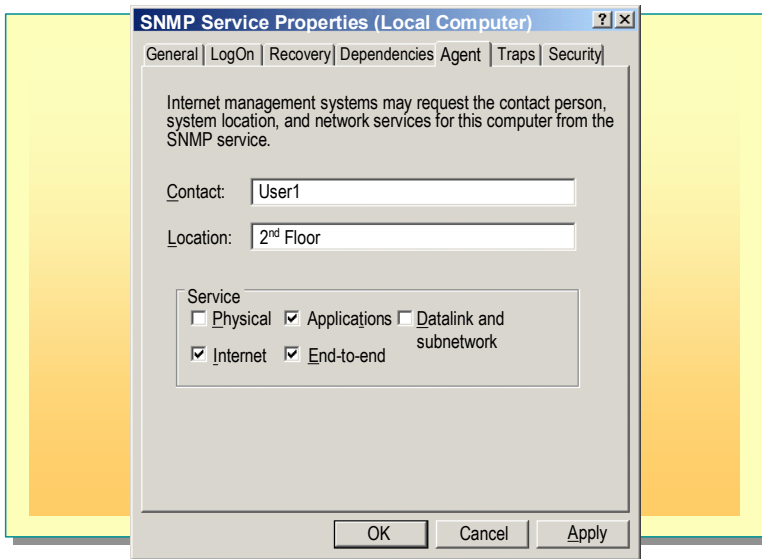
Configuring Windows 2000 SNMP Agent Properties

Topic Objective

To explain the procedure for configuring the SNMP agent properties.

Lead-in

The SNMP service enables a Windows 2000-based computer to provide a management system with information about activity that occurs at different layers of the TCP/IP protocol suite.



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

The SNMP service can provide an SNMP management system with information about itself. You enter information about a contact, a location, and the layer of the TCP/IP protocol suite at which the computer operates.

To configure SNMP agent properties:

1. In the **SNMP Service Properties** dialog box, click the **Agent** tab.
2. In the **Contact** box, type a contact name, such as an administrator, and in the **Location** box, type a description for the location of the computer.
3. Under **Service**, select the check boxes for the types of services that the computer on which SNMP is running provides.

Service	Select this option if
Physical	This host manages any physical devices, such as repeaters.
Applications	This host uses any applications that use TCP/IP. This option should always be selected.
Datalink and subnetwork	This host manages a bridge.
Internet	This host acts as an IP gateway (router).
End-to-end	This host is an IP host. This option should always be selected.

Note The Applications, Internet, and End-to-end services are enabled by default.

4. Click **OK**.

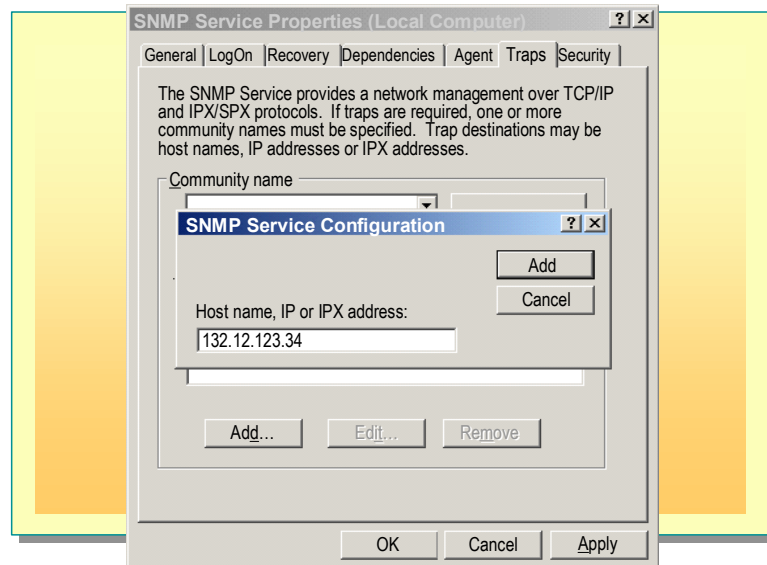
Configuring SNMP Traps

Topic Objective

To illustrate the configuration of SNMP traps.

Lead-in

You can configure the SNMP service to send notification messages to a management system that collects these notification messages for a particular community name.



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

You can configure the SNMP service to send notification messages to a management system that collects these notification messages for a particular community name.

You must select the **Send authentication trap** box on the **Security** tab before Windows 2000 can generate traps. With this option selected, Windows 2000 generates traps when:

- A management system makes an attempt to connect to an agent by using an invalid community name.
- A management system makes an attempt to connect to an agent from an unauthorized host.

To set destinations for traps:

1. On the **Traps** tab, in the **Community name** box, type a valid community name, and then click **Add to list**.
2. In the **Community name** box, click a community name, and then in the **Trap destinations** box, add one or more computer names or IP addresses of management systems that collect traps for that community.

Using SNMPUTIL to Confirm the SNMP Configuration

Topic Objective

To explain how to use the SNMPUTIL utility to test communications with a computer running the SNMP service.

Lead-in

SNMPUTIL is a utility provided by Microsoft to test SNMP installation.

SNMPUTIL:

Windows 2000 Server Resource Kit Utility

■ Command Syntax

```
snmputil command community object_identifier_(OID)
```

■ Valid Commands

- **get**
- **Get-next**
- **walk**

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

Microsoft provides a utility that you can use to test your SNMP installation. The Windows 2000 Server Resource Kit includes the SNMPUTIL utility, which you can use to send simple commands to an SNMP agent to verify whether the SNMP service has been correctly configured to communicate with SNMP management systems. SNMPUTIL sends the same SNMP commands as an SNMP management system.

SNMPUTIL Commands

There are three SNMPUTIL commands:

- **Get.** Gets the value of the requested object identifier.
- **Get-next.** Gets the value of the next object following the specified object identifier.
- **Walk.** Steps through the MIB branch specified by the object identifier. An SNMP management system uses this command to retrieve a large number of objects by using a single command.

Delivery Tips

Explain that the SNMP management tool, SNMPUTIL, in the Windows 2000 Resource Kit provides SNMP management features.

If you have the Windows 2000 Resource Kit available, demonstrate the SNMPUTIL tool.

Note The SNMP management tool, SNMPUTIL, in the Windows 2000 Resource Kit provides SNMP management features.

SNMPUTIL Syntax

The syntax of SNMPUTIL is as follows:

snmputil *command community object_identifier_(OID)*

For example, to determine the number of DHCP server addresses leased by a DHCP server named dhcp.nwtraders.msft in the Public community, you would issue the following command:

snmputil get-next dhcp.nwtraders.msft Public .1.3.6.1.4.1.311.1.3.2.1.1.1

An SNMP agent that is a DHCP server responds with the object identifier and counter value for the object identifier in question—in this case, the number of IP leases that are issued.

Note To use the SNMPUTIL utility, you must know the relevant MIB structure.

Lab A: Managing a Windows 2000 Network

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will manage a Windows 2000 network.



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

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Configure Terminal Services for remote administration.
- Use Terminal Services to remotely administer a computer.
- Install the SNMP service.
- Configure SNMP.
- View the configuration of a remote computer by using SNMP.

Prerequisites

Before working on this lab, you must have:

- Knowledge of how Terminal Services works.
- Knowledge of the role of SNMP in a Windows 2000 network.

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
- A partner with a similarly configured computer
- The files in the C:\Moc\Win2153\Labfiles\Module14\ folder

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

You need to administer a large number of servers that are located in several locations. Because of time and budget restrictions, you cannot travel to the remote locations when problems arise. To do your job, you must implement methods of remotely administering and monitoring all servers.

Estimated time to complete this lab: 60 minutes

Exercise 1

Using Terminal Services to Administer a Remote Computer

Scenario

You want to install software on remote computers without physically being at those computers. You have found that you cannot use a Microsoft Management Console (MMC) console running on another computer for this purpose. You decide to install Terminal Services on your servers so that you can accomplish all administrative tasks on these servers, including the installation of software.

Goal

In this exercise, you will install Terminal Services, optimize Terminal Services security for remote administration, optimize Terminal Services performance for remote administration, log on to a remote computer by using Terminal Services, and install the Windows 2000 Support Tools by using Terminal Services.

Tasks	Detailed Steps
1. Add Terminal Services in remote administration mode.	- 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. - On the Windows Components page, select the Terminal Services check box, and then click Next. - On the Terminal Services Setup page, verify that Remote administration mode is selected, and then click Next. - In the Files Needed dialog box, type \\London\Setup\Winsrc and then click OK. - When the configuration process is complete, click Finish. - In the System Settings Change dialog box, click Yes to restart your computer.
 Tip: When changing Terminal Services configuration settings, refer to the tables in this module for an explanation of each setting.	
2. Optimize Terminal Services for remote administration by optimizing performance for background services. Configure Terminal Services to end disconnected sessions after 5 minutes, and end idle sessions after 10 minutes.	- Log on as administrator@domain.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password. - Minimize Control Panel. - Right-click My Computer, and then click Properties. - In the System Properties dialog box, on the Advanced tab, click Performance Options. - In the Performance Options dialog box, under Optimize performance for, verify that Background services is selected, and then click OK. - Click OK to close the System Properties dialog box. - Open Terminal Services Configuration from the Administrative Tools menu.

Tasks	Detailed Steps
2. (continued)	h. In Terminal Services Configuration, in the details pane, right-click RDP-Tcp, and then click Properties.  <i>Changing the RDP-Tcp properties alters the configuration for all Terminal Services connections that use the Remote Desktop Protocol (RDP) over TCP/IP.</i> i. In the RDP-Tcp Properties dialog box, on the Sessions tab, select the first Override user settings check box. j. In the End a disconnected session box, click 5 minutes. k. In the Idle session limit box, click 10 minutes.
3. Increase Terminal Services security by removing permissions to use Terminal Services from all users except those from the Administrators group, and by setting the encryption level to high.	a. On the General tab, in the Encryption level box, click High. b. On the Permissions tab, remove the Administrators group, add the Administrator user account from your domain, and allow Full Control for the Administrator account. c. Click OK to close the RDP-Tcp Properties dialog box. d. Close Terminal Services Configuration.
4. Install the Terminal Services client software from the C:\winnt\system32\clients\ts client folder.	a. Click Start, and then click Run. b. In the Open box, type C:\winnt\system32\clients\tsclient\net\win32\Setup.exe and then click OK. c. In the Terminal Services Client Setup dialog box, click Continue. d. In the Name and Organization dialog box, type your name and organization, and then click OK. e. In the Confirm Name and Organization Information dialog box, confirm that the information is correct, and then click OK. f. In the License Agreement dialog box, review the license agreement, and then click I Agree. g. In the Terminal Services Client Setup dialog box, click the large button. h. In the Terminal Services Client Setup dialog box, click Yes to apply the same configuration to all users. i. After Terminal Services Client Setup copies all required files, click OK to close the Terminal Services Client Setup message box.
 Before starting the following procedure, verify that your partner has completed the preceding procedure.	

(continued)

Tasks	Detailed Steps
5. Log on to your partner's computer as Administrator by using Terminal Services.	- Click Start, point to Programs, point to Terminal Services Client, and then click Terminal Services Client. - In the Terminal Services Client dialog box, in the Server box, type the name of your partner's computer. - In the Screen area box, verify that 640x480 is selected. - Verify that the Enable data compression check box is selected, select the Cache bitmaps to disk check box, and then click Connect.
 Note: Configuring Terminal Services for low-speed connections by enabling data compression and caching bitmaps reduces network traffic and provides faster responses. These settings are particularly useful if you use Terminal Services over a dial-up connection.	
5. (continued)	- In the Log On to Windows dialog box, use the following information: User Name: administrator@domain.nwtraders.msft (where <i>domain</i> is your domain) Password: password - Click OK.
 Perform the following procedures entirely inside the Terminal Services window.	
6. Use Add/Remove Programs to install the Windows 2000 Support Tools on your partner's computer from the \Support\Tools folder on the Windows 2000 compact disc Installation Type: Typical	- In Control Panel, double-click Add/Remove Programs, click Add New Programs, and then click CD or Floppy. - In the Install Program From Floppy Disk or CD-ROM wizard, click Next. - On the Run Installation Program page, in the Open box, type \\london\support\setup.exe and then click Finish. - On the Welcome to the Windows 2000 Support Tools Setup Wizard page, click Next. - On the User Information page, in the Name box, type Studentx (where <i>x</i> is your student number) if necessary, and then click Next. - On the Select An Installation Type page, verify that Typical is selected, and then click Next. - On the Begin Installation page, click Next. - On the Completing the Windows 2000 Support Tools Setup Wizard page, click Finish. - Close Add/Remove Programs.
7. Verify that the Windows 2000 Support Tools are available.	- On the Programs menu, verify that Windows 2000 Support Tools is available, and then log off the Terminal session. - Close the Terminal Services Client window.

Exercise 2

Installing and Using SNMP

Scenario

Your organization has purchased an SNMP management system to monitor and control most devices in your network centrally. You need to configure the computers that are running Windows 2000 so that they can be monitored by using SNMP.

Goal

In this exercise, you will install the SNMP service and then confirm that it works by using the Snmputil.exe program.

Tasks	Detailed Steps
1. Install SNMP.	- 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 Management and Monitoring Tools rather than the check box to avoid selecting all options under Management and Monitoring Tools .	
1. <i>(continued)</i>	- On the Windows Components page, click Management and Monitoring Tools, and then click Details. - In the Management and Monitoring Tools dialog box, select the Simple Network Management Protocol check box, click OK, and then click Next. - On the Terminal Services Setup page, click Next. - In the Files Needed dialog box, type \\London\Setup\Winsrc and then click OK. - When the configuration process is complete, click Finish, and then close all open windows.
 Important: In the following three procedures, type community names in lowercase. SNMP community names are case sensitive.	
2. Configure SNMP with your contact information and a community name of private , and configure it to accept packets only from your computer.	- Open Computer Management from the Administrative Tools menu. - In the console tree, expand Services and Applications, and then click Services. - In the details pane, right-click SNMP Service, and then click Properties. - In the SNMP Service Properties (Local Computer) dialog box, on the Agent tab, in the Contact box, type your name. - In the Location box, type the location of your classroom. - On the Security tab, verify that the Send authentication trap check box is selected.

Tasks	Detailed Steps
2. (continued)	g. Under Accepted community names, click public, and then click Edit. h. In the SNMP Service Configuration dialog box, in the Community rights box, verify that READ ONLY is selected. i. In the Community Name box, type private and then click OK. j. Click Accept SNMP packets from these hosts, and then click Add. k. In the SNMP Service Configuration dialog box, type the IP address of your Classroom connection, and then click Add. l. Repeat the preceding step for your PartnerNet connection. m. Click OK to close the SNMP Service Properties (Local Computer) dialog box. n. Close Computer Management.
3. Use Snmputil.exe to retrieve the description of your computer.	a. At a command prompt, change to the C:\MOC\Win2153\Labfiles\Module14 directory. b. Type snmputil getnext ip_address public .1.3.6.1.2.1 (where <i>ip_address</i> is the IP address of your Classroom connection), and then press ENTER.  After approximately one minute, an error message appears.
 Why did Snmputil display an error message when you specified public as the community name? You configured the SNMP service to only recognize private as a valid community name. For security reasons, the SNMP service only responds to requests that specify a valid community name.	
3. (continued)	c. Type snmputil getnext ip_address private .1.3.6.1.2.1 (where <i>ip_address</i> is the IP address of your Classroom connection), and then press ENTER.  Snmputil displays the system description for your computer. d. Close the command prompt window.

Exercise 3

Restoring Your Configuration

Scenario

After you have tested remote administration and configuration features in Windows 2000, you must restore your original configuration.

Goal

In this exercise, you will restore the original computer configuration.

Tasks	Detailed Steps
 Before starting the following procedure, verify that your partner has completed the preceding procedure.	
1. Use Add/Remove Programs to remove Terminal Services Client and Windows 2000 Support Tools from your computer.	- In Control Panel, double-click Add/Remove Programs. - Verify that Terminal Services Client is selected, and then click Change/Remove. - In the Terminal Services Client Setup dialog box, click Remove All. - In the Setup Message dialog box, click Yes.  <i>Terminal Services Client is removed from your computer.</i> - In the Terminal Services Client – Restart Windows dialog box, click Exit Setup to postpone restarting Windows 2000. - In the Terminal Services Client – Restart Failed message box, click OK. - In the Terminal Services Client Setup message box, click OK. - In Add/Remove Programs, click Windows 2000 Support Tools, and then click Remove. - In the Add/Remove Programs dialog box, click Yes.  <i>Windows 2000 Support Tools is removed from your computer.</i>
2. Use the Windows Components wizard to remove Terminal Services and SNMP from your computer, and then restart your computer.	In Add/Remove Programs, click Add/Remove Windows Components.
 Note: In the next detailed step, click the text Management and Monitoring Tools rather than the check box to avoid selecting all options under Management and Monitoring Tools .	

Tasks	Detailed Steps
2. <i>(continued)</i>	b. On the Windows Components page, click Management and Monitoring Tools, and then click Details. c. In the Management and Monitoring Tools dialog box, clear the Simple Network Management Protocol check box, and then click OK. d. On the Windows Components page, clear the Terminal Services check box. e. Click Next. f. When the configuration process is complete, click Finish. g. In the System Settings Change dialog box, click No to postpone restarting your computer. h. Close all open windows, and then restart your computer.

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.

- **Windows 2000 Administrative Strategies**
- **Performing Administrative Tasks Remotely by Using Terminal Services**
- **SNMP Operation**
- **Implementing The Windows 2000 SNMP Service**

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

1. You need to administer a server remotely from several locations, including over a dial-up connection. Which is the best method to use?

Use Terminal Services. You do not need to install MMC snap-ins when using Terminal Services, and you have all of the control of using the server locally. Terminal Services also provides excellent performance over slow links, such as dial-up connections.

2. Which SNMP operations are initiated by a management system? Which SNMP operation does an agent initiate?

Management systems initiate get, get-next, and set operations.

Agents initiate trap operations.

3. What is the purpose of a community name?

To provide primitive security and context checking for agents that send traps and for management systems that receive traps.

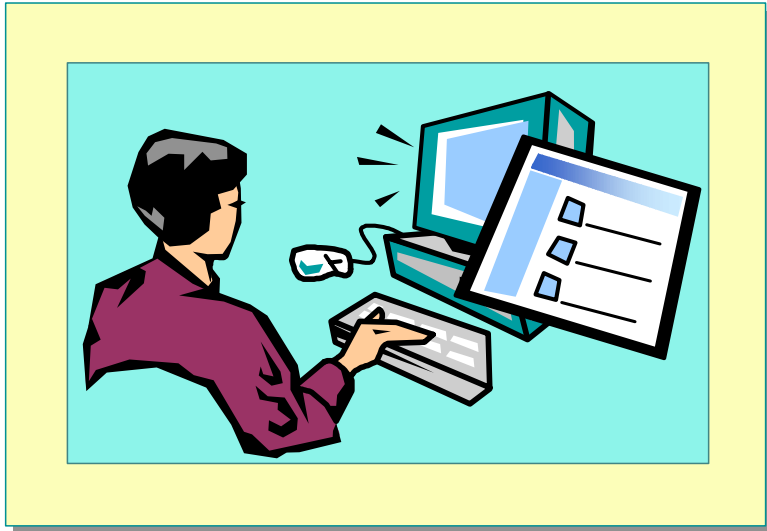
Course Evaluation

Topic Objective

To direct students to a Web site to complete a course evaluation.

Lead-in

Go to the Web site listed on this page to complete a course evaluation.



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

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

At a convenient time between now and the end of the course, please complete a course evaluation, which is available at <http://www.metricsthatmatter.com/survey>.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.

