

Module 15: Troubleshooting Windows 2000 Network Services

Contents

Overview	1
Troubleshooting Network Problems	2
Identifying the Symptoms and Causes of Network Problems	3
Resolving TCP/IP Problems	5
Resolving Name Resolution Problems	15
Lab A: Troubleshooting Routing (Simulation)	21
Troubleshooting Network Services	24
Monitoring the Network	28
Lab B: Troubleshooting Network Problems by Using Network Monitor	36
Review	40



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

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

© 2000 Microsoft Corporation. All rights reserved.

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

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

Simulations and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
75 Minutes

This module provides students with the knowledge and skills necessary to identify and resolve network connectivity problems by using Microsoft® Windows® 2000 troubleshooting tools and utilities.

Labs:
75 Minutes

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

- Troubleshoot network connectivity problems.
- Identify the symptoms and causes of network problems.
- Resolve Transmission Control Protocol/Internet Protocol (TCP/IP) problems.
- Resolve name resolution problems.
- Troubleshoot network services.
- Monitor the network data stream.

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 following materials:

- Microsoft PowerPoint® file 2153a_15.ppt.
- Lab exercise file 2153a_RoutTrb.exe and the supporting files and folders in the Lab Simulations folder.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Search for and read the topic “TCP/IP Troubleshooting” in the TCP/IP Core Networking Guide in the Windows 2000 Server Resource Kit.
- Search for and read the section “Network Monitor” in Windows 2000 Help.

Module Strategy

Use the following strategy to present this module:

- Troubleshooting Network Problems

This topic provides information about the three phases of the network troubleshooting process. Describe each phase, and explain the tasks that are involved in each of them.

- Identifying the Symptoms and Causes of Network Problems

This topic provides information about how to identify the symptoms and causes of network problems. Emphasize that students must check hardware components, such as cables and network adapters, before taking further action toward identifying the cause of network problems. Explain that Windows 2000 displays error messages when a network operation fails and provides suggestions about how to resolve the error. Identify the other methods that you can use to locate troubleshooting information and diagnose network problems.

- Resolving TCP/IP Problems

This topic provides information about how to determine whether a network problem has occurred as a result of the TCP/IP process. Describe the steps that the TCP/IP protocol performs in the TCP/IP process to provide the basis for understanding how to resolve TCP/IP problems. Describe the Ipconfig utility, which you can use to verify TCP/IP configuration information, and demonstrate how to it.

Explain that you can use the Ping utility to test TCP/IP connectivity to other host computers on a network. Demonstrate how to use the **ping** command to test TCP/IP configuration and connections, and then explain how to verify TCP/IP properties. Explain how to use the Ping utility to verify valid Internet Protocol Security (IPSec) connections.

Identify the components of the IP-to-media access control (MAC) resolution process by describing the Address Resolution Protocol (ARP) and the ARP cache, and explain how to use the Arp utility to detect invalid entries in the ARP cache. Finally, identify the utilities that you can use to troubleshoot IP routing, including Ping, Tracert, and Pathping.

- Resolving Name Resolution Problems

This topic describes how to troubleshoot name resolution problems by distinguishing host name resolution problems from network basic input/output system (NetBIOS) name resolution problems. Demonstrate the procedure for verifying host name resolution configuration, and explain how to check the Hosts file to verify that the name of the remote computer is correct. Describe the Nslookup utility, describe the error messages that may be returned by the **nslookup** command, and then explain why the error messages occur. Describe the NetDiag support tool and how it helps isolate networking and connectivity problems.

Explain how to resolve NetBIOS problems by describing the NetBIOS name resolution process and identifying the utilities that help to diagnose the NetBIOS name resolution process. Finally, describe common NetBIOS name resolution errors and how to resolve them.

- Troubleshooting Network Services

This topic provides information about how to use Services in Microsoft Management Console (MMC) to troubleshoot and resolve network services problems on local and remote computers. Describe the network services information that is displayed in the details pane of the Services window, and then describe the configuration options on each tab of the **Properties** dialog box for a service.

- Monitoring the Network

This topic provides information about how to use Network Monitor to capture and display network packets. Describe the purpose of network monitor and explain how you can use it for troubleshooting purposes. Describe the procedure for installing Network Monitor. Explain that the Capture window is the basic Network Monitor interface, and then describe the four major areas of the Capture window. Demonstrate the procedures for starting and stopping a data capture, and saving captured data to a file. Describe the purpose of capture filters and capture triggers. Finally, explain how to display data in Network Monitor by displaying a capture file and describing the fields in the Capture Summary windows.

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

The labs in this module require that you perform the procedure specified in the Classroom Setup Guide before performing the labs.

Lab Result

Performing the labs in this module introduces the following configuration change: Management and Monitoring Tools are installed.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn how to troubleshoot and resolve problems that may occur on your network.

- Troubleshooting Network Problems
- Identifying the Symptoms and Causes of Network Problems
- Resolving TCP/IP Problems
- Resolving Name Resolution Problems
- Troubleshooting Network Services
- Monitoring the Network

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

Microsoft® Windows® 2000 includes many protocols and services that you can use to build your network, and each of these technologies has specific requirements and dependencies. Therefore, it is important to understand how these network components function and how they interact to be able to effectively and efficiently troubleshoot network problems that may occur.

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

- Troubleshoot network connectivity problems.
- Identify the symptoms and causes of network problems.
- Resolve Transmission Control Protocol/Internet Protocol (TCP/IP) problems.
- Resolve name resolution problems.
- Troubleshoot network services.
- Monitor the network data stream.

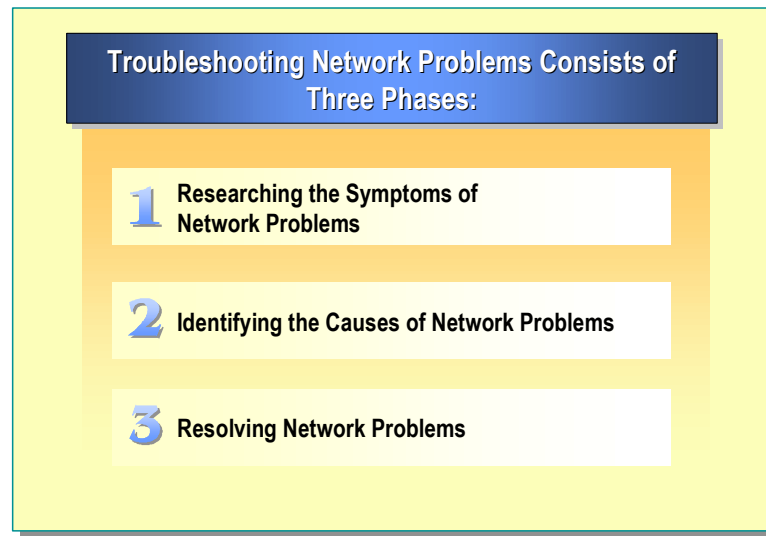
Troubleshooting Network Problems

Topic Objective

To list the phases for troubleshooting network problems.

Lead-in

Identify the symptoms and causes of a network problem before you attempt to resolve the problem.



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

The Windows 2000 network infrastructure consists of many different components and connections, and network problems can occur in any of them. This complicates the network troubleshooting process, because a problem can have more than one probable cause. For example, if a user cannot access a shared folder, the problem could be the result of a faulty network cable or incorrect user permissions. Therefore, you must be able to identify the symptoms and causes of network problems to isolate and correct the problem.

Effective network troubleshooting consists of three phases:

- *Researching the symptoms of network problems.* Gather specific information that is related to a network problem, such as the error message that a user received when the problem occurred.
- *Identifying the causes of network problems.* Identify all possible causes for the problem, based on the symptoms. This phase often requires additional research. After you have identified all possible causes, you must isolate the specific cause of the problem. This is the most challenging part of the network troubleshooting process.
- *Resolving network problems.* Apply your knowledge of Windows 2000 and its networking technologies to resolve the problem. This phase is often the easiest of the network troubleshooting process, because you have already identified the cause of the problem.

Delivery Tip

Describe the three phases of the troubleshooting process.

Identifying the Symptoms and Causes of Network Problems

Topic Objective

To list the methods that are available for identifying the symptoms and causes of network problems.

Lead-in

Check hardware components to ensure that they are functioning properly before taking further action to identify the cause of a network problem.

After You Have Verified That All Hardware Components Are Functioning Properly:



Identify Error Messages by Using Windows 2000 Help or the `net helpmsg` Command



Diagnose Network Problems by Using Troubleshooters



Diagnose Network Problems by Using Event Viewer

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

Verify that hardware components, such as cables and network adapters, are working properly before you begin to research the symptoms and causes of network problems. If a network problem is hardware related, checking these components first can reduce the amount of time spent researching software-related network problems. If the problem is not hardware-related, you must investigate further to identify its symptoms and causes.

Identifying Error Messages

Windows 2000 often displays error messages when a network operation fails. These error messages include a brief description of the problem that has occurred. Windows 2000 also provides troubleshooting information for common system errors, which can assist you in diagnosing the problem.

Click **Help** in an error message to receive a detailed description of the error, suggestions about how to resolve the error, and a list of related tools and Help topics that may help to prevent the error from occurring in the future.

You can also use the `net helpmsg` command to locate troubleshooting information for a specific error message. The `net helpmsg` command explains why an error occurred and how to resolve the problem. To view an explanation of an error message that a core component of Windows 2000 generated, at a command prompt, type `net helpmsg number` (where *number* is the number that is associated with the error message).

Key Points

Click **Help** in an error message to receive information about the error and how to resolve it.

Use the `net helpmsg` command to locate troubleshooting information for a specific error message.

Note For more information about error messages, see the “Error and Event Messages Help” section in the Windows 2000 Support Tools.

Diagnosing Network Problems by Using Troubleshooters

Windows 2000 Help includes troubleshooters, which you can use to quickly solve common network configuration or interoperability problems. Troubleshooters are wizards that ask a series of questions and provide detailed information about troubleshooting the problem. There are several different troubleshooters, each of which is designed to solve a different type of problem.

Delivery Tip

Identify the troubleshooters that are available for Windows 2000 networking components.

Use troubleshooters to diagnose and solve technical problems with the following networking components:

- Client Service for NetWare
- Dynamic Host Configuration Protocol (DHCP)
- Group Policy and the Active Directory™ directory service
- Domain Name System (DNS)
- Internet connections
- Networking (TCP/IP)
- Routing and Remote Access
- Remote Installation Services (RIS)
- Server Management
- Windows Internet Name Service (WINS)

Diagnosing Network Problems by Using Event Viewer

Key Point

By using Event Viewer, you can view and manage event logs, and gather system information.

Event Viewer is a monitoring and diagnostic Windows 2000 administrative tool that allows you to view logs about program, security, and system events on your computer. You can use Event Viewer to view and manage event logs, and to gather system information to identify when a particular service has been started, stopped, or failed to start because of an error. By using Event Viewer, you can monitor event logs to predict and identify the sources of system problems.

Note For information about using Event Viewer, see Windows 2000 Help, or course 2151, *Microsoft Windows 2000 Network and Operating System Essentials*.

◆ Resolving TCP/IP Problems

Topic Objective

To list the topics that are related to resolving TCP/IP problems.

Lead-in

You must understand the functions that the TCP/IP protocol performs to determine whether a network problem has occurred as a result of the TCP/IP process.

- Verifying TCP/IP Configuration
- Testing IP Configuration
- Testing IP-to-MAC Resolution
- Troubleshooting IP Routing

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

To determine whether a network problem occurred as a result of a TCP/IP failure, you must be able to verify TCP/IP configuration and connectivity, test IP configuration and IP-to-media access control (MAC) resolution, and check IP security configuration and the IP routing process.

Delivery Tip

Describe the steps that the TCP/IP protocol performs in the TCP/IP process.

The TCP/IP process that enables computers to communicate over a network can be divided into four distinct steps. Before it sends a packet from a sending host, the TCP/IP protocol:

1. Resolves the host name or network basic input/output system (NetBIOS) name to an IP address.
2. Determines the interface to use and the forwarding IP address by using the destination IP address and the IP routing table.
3. Uses the Address Resolution Protocol (ARP) to resolve the forwarding IP address to a MAC address. This occurs for unicast IP traffic on shared access technologies such as Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI).

For multicast IP traffic on Ethernet and FDDI, the destination multicast IP address is mapped to the appropriate multicast MAC address. Multicast IP traffic on Token Ring uses the functional address of 0xC0-00-00-04-00-00. For broadcast traffic on shared access technologies, the MAC address is mapped to 0xFF-FF-FF-FF-FF-FF.

4. Sends the packet to the MAC address that is resolved by using ARP or multicast mapping.

The TCP/IP stack follows this sequence when it determines how to send a packet from point-to-point. If the destination to be reached by an application is in the form of a NetBIOS name or host name, name resolution is required before IP can send the first packet.

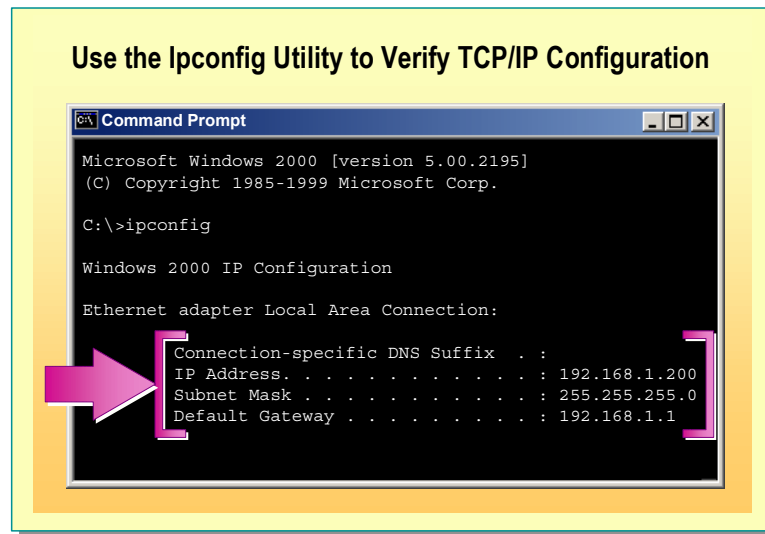
Verifying TCP/IP Configuration

Topic Objective

To illustrate the TCP/IP configuration values that are displayed when using the Ipconfig utility.

Lead-in

Windows 2000 includes the Ipconfig utility, which you can use to view TCP/IP configuration information.



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

When troubleshooting a TCP/IP networking problem, begin by checking the TCP/IP configuration on the computer on which the problem occurs. The Ipconfig utility is a command-line tool that displays current TCP/IP network configuration values, including the:

- IP address
- Subnet mask
- Default gateway

Key Point

Type **ipconfig** at a command prompt to view TCP/IP configuration information, including the IP address, the subnet mask, and the default gateway.

This information helps to determine whether the configuration is initialized, or whether a duplicate IP address exists on a network. To view TCP/IP configuration information, at a command prompt, type **ipconfig**

Note If the local address is returned as 169.254.x.x, the Automatic Private IP Addressing feature of Windows 2000 has assigned the IP address. This local address of 169.254.x.x. indicates that the local DHCP server is not configured properly or cannot be reached from your computer, and an IP address has been assigned automatically with a subnet mask of 255.255.0.0. Enable or correct the DHCP server, and restart the local computer.

Key Point

Type **ipconfig /all** at a command prompt to view TCP/IP configuration details.

Displaying TCP/IP Configuration Details

You can use the **/all** switch to produce a detailed configuration report for all interfaces, including any configured remote access adapters. At a command prompt, type **ipconfig /all** to verify configuration information.

The result of the **ipconfig /all** command is as follows:

- If a network connection was initialized, the Ipconfig utility displays the IP address and subnet mask. The default gateway also appears, if it has been assigned.
- If a duplicate IP address exists, the Ipconfig utility indicates that the IP address is configured; however, the subnet mask is 0.0.0.0.
- If the computer is unable to obtain an IP address from a DHCP server on the network, the Ipconfig utility displays the IP address provided by Automatic Private IP Addressing.
- If the computer obtained its address from a DHCP server, the Ipconfig utility displays the IP address of the DHCP server.

The output of the **ipconfig /all** command also includes additional configuration information, such as the addresses of DNS and WINS servers that you configured or that a DHCP server assigned.

Saving Ipconfig Output

Key Point

You can save Ipconfig output in an existing folder.

Ipconfig output may be redirected to a file and pasted into other documents. To save Ipconfig output, at a command prompt, type **ipconfig > folder name\file name** (where *folder name* is the name of a folder that already exists, and *file name* is the name that you want to assign to the file when it is created). A file that contains the Ipconfig output is created with the specified file name, in the specified folder.

You can review the Ipconfig output to identify problems in the computer network configuration. For example, if a computer has been configured with a duplicate IP address, the subnet mask appears as 0.0.0.0. If no problems appear in the TCP/IP configuration, the next step is to test TCP/IP connectivity to other host computers on the network.

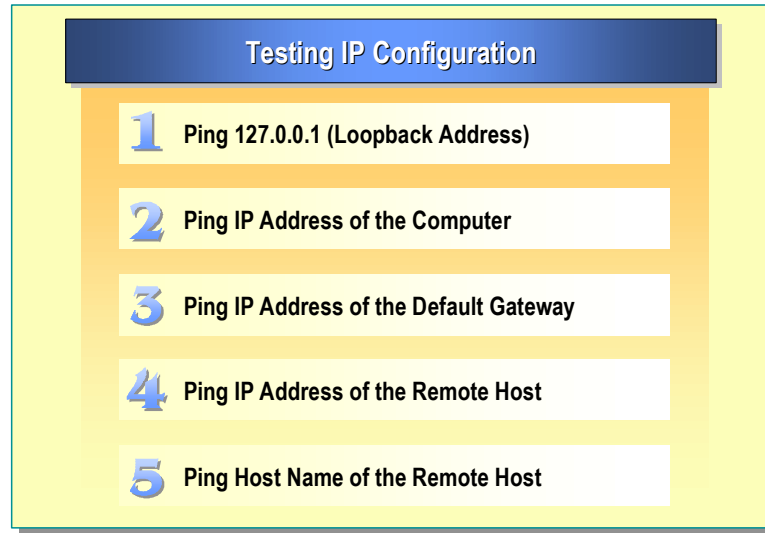
Testing IP Configuration

Topic Objective

To list the steps that are performed when testing IP configuration.

Lead-in

You can use the Ping utility to test TCP/IP connectivity to other host computers on the network.



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

The Ping utility is a diagnostic tool that you can use to test TCP/IP configuration and diagnose connection failures by sending an Internet Control Message Protocol (ICMP) Echo Request to a target host name or IP address. Use the Ping utility to determine whether a particular TCP/IP host is available and functional.

Testing Network Connections

To verify that a route exists between the local computer and a network host, at a command prompt, type **ping** *IP address* (where *IP address* is the IP address of the network host to which you want to connect). By default, the following message appears four times after a successful **ping** command:

Reply from *IP_address*

Delivery Tip

Demonstrate the result of successful and unsuccessful **ping** commands by typing the following commands: **ping 127.0.0.1** (which is successful) and **ping 192.168.0.108** (which is not successful).

Testing TCP/IP Configuration and Connections

Perform the following tasks to test TCP/IP configuration and connections:

1. Use the **ping** command with the loopback address (**ping 127.0.0.1**) to verify that TCP/IP is correctly installed and bound to your network adapter.

If this step fails, the IP stack is not responding. Possible causes for this include:

- The TCP drivers are damaged or missing.
- The network adapter is not working.
- Another service is interfering with IP.

2. Use the **ping** command with the IP address of the local computer to verify that the computer was added to the network correctly and does not have a duplicate IP address. If the routing table is correct, this simply forwards the packet to the loopback address of 127.0.0.1.

3. Use the **ping** command with the IP address of the default gateway to verify that the default gateway is operational and that your computer can communicate with a host on the local network.

4. Use the **ping** command with the IP address of a remote host to verify that the computer can communicate through a router.

If the **ping** command is successful after this step, steps 1 through 3 are successful by default. If the **ping** command is not successful, **ping** the IP address of another remote host because the current host might be turned off.

5. Use the **ping** command with the host name of a remote host to verify that the computer can resolve a remote host name.

Ping uses host name resolution to resolve a computer name to an IP address, so if pinging by IP address succeeds, but fails by host name, the problem is with host name resolution, not network connectivity.

Delivery Tip

Demonstrate how to verify TCP/IP properties by opening the **Internet Protocol (TCP/IP) Properties** dialog box and clicking the **IP Address** tab.

Verifying TCP/IP Properties

If you cannot use Ping successfully at any point, verify that the local computer's IP address is valid and appears correctly on the **IP Address** tab of the **Internet Protocol (TCP/IP) Properties** dialog box. You can also use the Ipconfig utility to verify the IP address of the local computer.

Verifying Valid IPSec Connections

You can use the Ping utility to determine whether Internet Protocol Security (IPSec) communication can occur when a predefined policy is assigned to a computer. Using the Ping utility will allow you to separate network problems from IPSec issues.

If using the **ping** command results in a "Destination Host Unreachable" error message, the other computer cannot be contacted at all. If the result is a "Request Timed Out" error message, the computer can be contacted, but it may have an IPSec policy applied to it that is blocking communication.

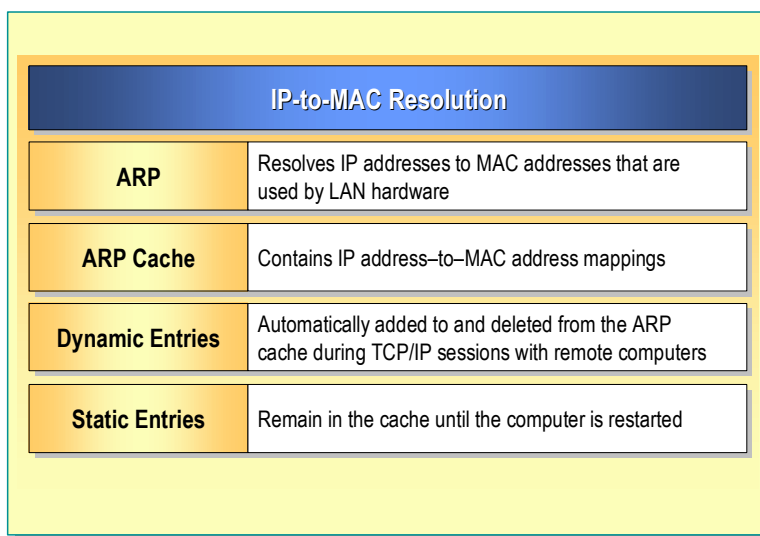
Testing IP-to-MAC Resolution

Topic Objective

To list the key components of the IP-to-MAC resolution process.

Lead-in

The Address Resolution Protocol identifies the MAC address of the network adapter on the destination computer.



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

Windows 2000 TCP/IP allows an application to communicate over a network with another computer by using an IP address, a host name, or a NetBIOS name. The destination must be resolved to a MAC address for shared access media, such as Ethernet and Token Ring, regardless of the naming convention that is used.

Key Point

ARP is a protocol in the TCP/IP suite that provides IP address-to-MAC address resolution for IP packets.

Address Resolution Protocol

The Address Resolution Protocol (ARP) is a protocol in the TCP/IP suite that provides IP address-to-MAC address resolution for IP packets. ARP resolves IP addresses to MAC addresses that are used by local area network (LAN) hardware. When given the node's IP address, ARP enables a host to find the MAC address of a node with an IP address on the same physical network.

ARP Cache

When an ARP request is answered, both the sender of the ARP reply and the original ARP requester record each other's IP address and MAC address in a local table called the ARP cache, which contains both dynamic and static entries. By using the Arp utility, you can view and modify the ARP cache. At a command prompt, type **arp -a** to view ARP cache entries on the local computer.

Delivery Tips

Describe the function of the ARP cache and the difference between dynamic and static entries.

Explain that you can use the Arp utility to view and modify ARP table entries on the local computer.

Note Each network adapter has a separate ARP cache on a computer running Windows 2000.

Dynamic Entries

Dynamic entries are automatically added to and deleted from the ARP cache during the normal use of TCP/IP sessions with remote computers. Dynamic entries age and expire from the cache if they are not reused within two minutes. If a dynamic entry is reused within two minutes, it may remain in the cache and age up to a maximum cache life of ten minutes before it is removed or requires cache renewal through the ARP broadcast process.

Key Points

Static entries can help minimize ARP broadcast traffic on your network. Use the **arp -s** command to add a static entry to the ARP cache.

Static Entries

Static entries remain in the cache until the computer is restarted, and can help minimize ARP broadcast traffic on your network. You can use the Arp utility to add static entries to the ARP cache. To add a static entry, at a command prompt, type **arp -s IP_address MAC_address** (where *IP address* is the IP address of a local TCP/IP node, and *MAC address* is the MAC address for a network adapter that is installed and used on the local TCP/IP node).

Detecting Invalid Entries in the ARP Cache

Invalid entries in the ARP cache can be the result of two computers that are using the same IP address on the network. The main source of these conflicts is most likely to be an incorrect static IP addresses, because DHCP-assigned addresses do not cause address conflicts.

Verifying Static Addresses

As a best practice, maintain a list of static addresses (and corresponding MAC addresses) as they are assigned. You can then compare the IP and MAC address pairs in the ARP cache with the recorded values to determine whether the static entries in the ARP cache were entered correctly.

If you do not have a record of all IP and MAC address pairs on your network, but you have a record of the network adapters that each computer uses, you can often deduce which adapter has a given MAC address by examining the manufacturer bytes of the MAC addresses of the network adapters. These three-byte numbers are called Organizationally Unique Identifiers (OUIs). You can compare the OUIs with the MAC addresses in the ARP cache to determine whether a static address was entered in error. You can obtain a list of OUIs from the Institute of Electrical and Electronic Engineers, Inc. (IEEE) at <http://standards.ieee.org/regauth/oui/index.html>.

Key Point

Use the **arp -d** command to delete invalid entries from the ARP cache.

Deleting Invalid Entries

Delete invalid static entries from the ARP cache by using the Arp utility. At a command prompt, type **arp -d IP_address** (where *IP address* is the IP address of the invalid entry). To add the correct address, use the **arp -s** command.

Troubleshooting IP Routing

Topic Objective

To illustrate the **ping**, **tracert**, and **pathping** commands.

Lead-in

To troubleshoot IP routing problems, verify the default gateway first. Next, use the Ping utility to verify communications between networks, and use the Tracert and PathPing utilities to troubleshoot IP routing problems.

```

C:\WINNT\SYSTEM32\cmd.exe

Ping
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Tracert
C:\>tracert 192.168.1.1

Tracing route to BONN [192.168.1.1]
Over a maximum of 30 hops:

  1  <10 ms    <10 ms <10 ms BONN [192.168.1.1]

Trace complete.

PathPing
C:\>pathping 192.168.1.1

Tracing route to BONN <192.168.1.1>
Over a maximum of 30 hops:
  0  london.nwtraders.msft [192.168.1.200]
  1  BONN [192.168.1.1]

Computing statistics for 25 seconds...
Source to Here   This Node/Link
Hop  RTT  Lost/Sent = Pct  Lost/Sent = Pct  Address
london.nwtraders.msft [192.168.1.200]
0]
  1   0ms   0/100 = 0%       0/100 = 0%       {
[192.168.1.1]
0/100 = 0%       0/100 = 0%       BONN
[192.168.1.1]

Trace complete.
  
```

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

The first step for troubleshooting IP routing is to verify that a default gateway is configured and that the link between the host and the default gateway is operational. Make sure that only one default gateway is configured. Although it is possible to configure more than one default gateway, additional gateways are only used if the IP stack determines that the original gateway is not functioning. To determine the status of the first configured gateway, delete all other gateways to simplify the troubleshooting process.

Key Point

Verify that the default gateway is on the same network as the local host, to enable messages from the host to be forwarded outside the local network.

Verifying the Default Gateway

If the gateway address is not on the same network as the local host, messages from the host computer cannot be forwarded to any location that is outside the local network. Therefore, you must verify that the default gateway address is correct. Next, check to see that the default gateway is configured as a router, and that it is enabled to forward IP datagrams.

Delivery Tip

Describe the error messages that the **ping** command may return if a routing problem exists.

Verifying Communications Between Networks

If the default gateway is configured correctly, use the **ping** command with the IP address of a remote host to ensure that network-to-network communications are functioning properly. The **ping** command may return the following error messages if a routing problem exists:

- *TTL Expired in Transit.* Indicates that the number of hops required to reach the destination exceeds the Time to Live (TTL) value that the sending host sets for forwarding packets. The default TTL value is 32, which may not be enough time for a packet to travel the required number of links to a destination. Use the **ping -i** command to increase the TTL value, up to a maximum of 255.

Note Some routers will drop packets with an expired TTL. This is known as a silent discard.

- *Destination Host Unreachable.* Indicates that the local system has no route to the desired destination, or a remote router reports that it has no route to the destination. If the “Destination Host Unreachable” message appears, no route from the local system exists, and the packets to be sent were never forwarded. If the “Reply From *IP address*: Destination Host Unreachable” message appears, the routing problem occurred at the remote router that is associated with the specified IP address.
- *Request Timed Out.* Indicates that no “Echo Reply” messages were received within the default time of one second. This message may be the result of network congestion, failure of the ARP request, packet filtering, a routing error, or a silent discard. Most often, it indicates that a route back to the sending host has failed, because the destination host, one of the intermediary routers, or the default gateway of the destination host does not recognize the route back to the sending host.

Check the routing table of the destination host to determine whether it has a route to the sending host before checking the routing tables of the individual routers. If the remote routing tables are correct and contain a valid route back to the sending host, use the **arp -a** command to determine whether the correct address is listed in the ARP cache. In addition, check the subnet mask to ensure that a remote address has not been interpreted as a local address.

- *Unknown Host.* Indicates that the requested host name cannot be resolved to its IP address. Verify that the name is entered correctly and that the DNS servers can resolve it.

Tracert Utility

Key Point

Use the **tracert** command to display a list of IP routers that are used to deliver packets to a destination.

The Tracert utility is a command-line tool that you can use to check the path to the destination IP address that you want to reach. The **tracert** command displays a list of IP routers that are used to deliver packets from your computer to the destination, and the amount of time that the packet remained at each hop. If the packets are unable to be delivered to the destination, you can use the **tracert** command to identify the last router that successfully forwarded the packets.

Note Some routers silently drop packets with expired TTLs. These routers do not appear in the Tracert display.

PathPing Utility

Key Point

Use the **pathping** command to determine whether a router is dropping packets.

The PathPing utility is a command-line tool that detects packet loss over multiple-hop trips. The **pathping** command sends packets to each router on the route to a final destination, and computes the results based on the packets that are returned from each hop. You can use the **pathping** command to identify the degree of packet loss at any given router or link and determine whether a particular router or link is causing network problems.

To verify that the routers on the route to the destination are operating correctly, at a command prompt, type **pathping** *IP address* (where *IP address* is the IP address of the remote host).

◆ Resolving Name Resolution Problems

Topic Objective

To list the topics that are related to resolving name resolution problems.

Lead-in

To troubleshoot name resolution problems, you must first determine whether the problem is with NetBIOS or host name resolution.

- Resolving Host Name Resolution Problems
- Resolving NetBIOS Name Resolution Problems

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

TCP/IP for Windows 2000 allows an application to communicate over a network with another computer by using an IP address, or either of the following types of destination designations:

- Host name
- NetBIOS name

If you are unable to access a system by host name or NetBIOS name, a problem with name resolution could exist on your network. You must determine whether it is a host or domain name or a NetBIOS name resolution problem. The first step in distinguishing host name resolution problems from NetBIOS name resolution problems is to determine whether the failing application uses NetBIOS or host names. If the application uses host names, the problem is the result of incorrect host name resolution.

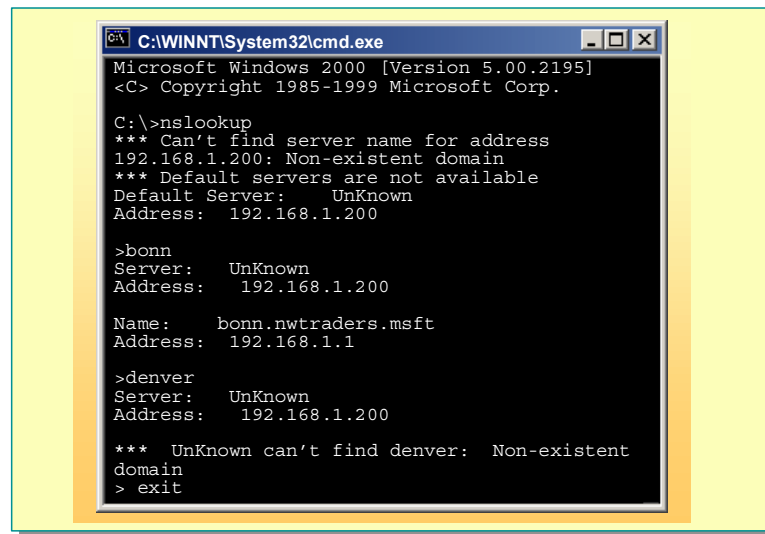
Resolving Host Name Resolution Problems

Topic Objective

To illustrate the results of the **nslookup** command.

Lead-in

To resolve host name resolution problems, ensure that the DNS service is configured properly, and that the Hosts file entries are correct. Use the Nslookup utility and the NetDiag support tool to troubleshoot host name resolution problems.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
<C> Copyright 1985-1999 Microsoft Corp.

C:\>nslookup
*** Can't find server name for address
192.168.1.200: Non-existent domain
*** Default servers are not available
Default Server: UnKnown
Address: 192.168.1.200

>bonn
Server: UnKnown
Address: 192.168.1.200

Name: bonn.nwtraders.msft
Address: 192.168.1.1

>denver
Server: UnKnown
Address: 192.168.1.200

*** UnKnown can't find denver: Non-existent
domain
> exit
```

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

Problems with host name resolution can be the result of an incorrectly configured Hosts file or DNS server, an incorrect Hosts file entry or IP address, or multiple entries for a single host in a Hosts file.

Verifying Host Name Resolution Configuration

To verify host name resolution configuration:

1. Open Network and Dial-up Connections, right-click **Local Area Connections**, and then click **Properties**.
2. In the **Local Area Connection Properties** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Advanced**.
4. On the **DNS** tab of the **Advanced TCP/IP Settings** dialog box, confirm that DNS is configured properly. If the DNS server IP address is missing, add it to the list of DNS server addresses.

Note This procedure does not take DHCP clients into account, because DNS servers are not listed for DHCP clients.

Delivery Tip

Demonstrate the procedure for verifying host name resolution configuration.

Key Point

Check the Hosts file to verify that the name of the remote computer is correct.

Checking the Hosts File

The Hosts file or a DNS server resolves host names to IP addresses whenever you use TCP/IP utilities such as the Ping utility. Verify that the name of the remote computer is spelled correctly in the Hosts file, and in the application that uses it for name resolution.

Note The Hosts file is located in the *systemroot\System32\Drivers\Etc* folder.

Nslookup Utility

Nslookup is a command-line utility that you can use to make DNS queries to test and troubleshoot your DNS installation. Name resolution errors can occur if DNS server or client entries are not configured correctly, the DNS server is not running, or there is a problem with network connectivity. At a command prompt, type **nslookup** to view the host name and IP address of the DNS server that is configured for the local system.

Delivery Tip

Describe the error messages that the **nslookup** command may return, and explain why they occur.

If the DNS server is offline, the DNS service is not enabled on the host computer, or if a hardware or routing problem exists, the following message appears:

```
C:\nslookup
*** Can't find server name for address <IP_Address>: No
response from server
*** Default servers are not available.
```

To look up a host's IP address by using DNS, type the host name and press ENTER. By default, Nslookup uses the DNS server configured for the computer on which it is running. If the DNS server cannot resolve the host name, the following message appears:

```
C:\nslookup <Destination_host>
Server: <fully_qualified_domain_name>
Address: <server_IP_address>
*** <fully_qualified_domain_name> can't find
<Destination_host>: Non-existent domain
```

If a query fails as a result of connectivity issues or network congestion, or if the DNS server is overloaded with requests, the following message appears:

```
C:\nslookup Valid_Host
Server: [IP_Address]
Address: w.x.y.z
DNS request timed out.
    timeout was 2 seconds.
```

NetDiag Support Tool

NetDiag is a command-line, diagnostic tool that helps isolate networking and connectivity problems by performing a series of tests to determine the state of the network client. NetDiag diagnoses network problems by checking all aspects of a host computer's network configuration and connections. In addition to troubleshooting TCP/IP issues, it examines a host computer's Internetwork Packet Exchange (IPX) and NetWare configurations. NetDiag is included in the Windows 2000 Support Tools.

Note For more information about NetDiag, see Windows 2000 Support Tools Help. For information about installing and using the Windows 2000 Support Tools and Support Tools Help, see the file Sreadme.doc in the \Support\Tools folder on the Windows 2000 Server compact disc.

Resolving NetBIOS Name Resolution Problems

Topic Objective

To illustrate the **nbtstat** and **net view** commands.

Lead-in

To resolve NetBIOS name resolution problems, you must understand the NetBIOS name resolution process. Use the **nbtstat** or **net view** command to diagnose NetBIOS name resolution problems.

The screenshot shows a Windows 2000 command prompt window with the title bar 'C:\WINNT\SYSTEM32\cmd.exe'. It displays the execution of two commands: **nbtstat -n** and **net view**.

nbtstat -n output:

```

C:\>nbtstat -n

Local Area Connection:
Node IpAddress: [192.168.1.200] Scope Id: []

NetBIOS Local Name Table

Name                Type               Status
-----
LONDON              <00>              UNIQUE             Registered
LONDON              <20>              UNIQUE             Registered
NWTRADERS           <00>              GROUP              Registered
NWTRADERS           <1C>              GROUP              Registered
NWTRADERS           <1B>              UNIQUE             Registered
NWTRADERS           <1E>              GROUP              Registered
LONDON              <03>              UNIQUE             Registered
NWTRADERS           <1D>              UNIQUE             Registered
**.... MS BROWSE....* <01>              GROUP              Registered
1 Net ~ Services    <1C>              GROUP              Registered
1S~ LONDON----- <00>              UNIQUE             Registered
  
```

net view output:

```

C:\net view

Server Name          Remark
-----
\\BONN
\\DENVER
\\LONDON
he command completed successfully.

C:\>
  
```

Below the first screenshot, the command **nbtstat -RR** is shown, with the output: 'The NetBIOS names registered by this computer have been refreshed.'

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

When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses by using several options for NetBIOS name resolution. These options include local cache lookup, WINS server query, broadcast, Lmhosts lookup, Hosts file query, and DNS server query.

NetBIOS Name Resolution Process

Windows 2000 first checks the host computer's internal NetBIOS name cache to resolve a NetBIOS name to an IP address. If this fails to provide an IP address, the NetBIOS name can be resolved to an IP address by using a broadcast, checking the Lmhosts file, or querying a WINS server. The order in which Windows 2000 uses these mechanisms depends on the node type of the client.

The default node type is hybrid or H-node, which queries a WINS server, and then attempts a local broadcast to resolve the name. If these mechanisms are unsuccessful, the client queries its Hosts file. If the Hosts file does not contain the IP address, the client queries its DNS server if it is configured to use one.

Note If the only problem is NetBIOS name resolution, the computer should still be able to reach the remote resource by IP address.

Delivery Tip

Describe the NetBIOS name resolution process.

Diagnosing NetBIOS Name Resolution Problems

You can use the **nbtstat** or **net view** command to diagnose NetBIOS name resolution problems.

Key Point

Use the **nbtstat** command to view protocol statistics for NetBT connections.

Nbtstat

You use the Nbtstat utility to view and register NetBIOS names on a computer running Windows 2000. Nbtstat displays protocol statistics and name information used by NetBT connections, which can help with troubleshooting NetBIOS name resolution problems. For example, to identify the NetBIOS names that a computer has registered by using NetBT, type **nbtstat -n** at a command prompt.

In Windows 2000, you can re-register NetBIOS names with the name server after a computer has already been started. Type **nbtstat -R** at a command prompt to re-register NetBIOS names.

Note For more information on the parameters that you can use with the Nbtstat utility, type **nbtstat** at a command prompt.

Key Point

Use the **net view** command to view a list of domains, a list of computers, or the resources that the specified computer shares.

Net View Command

You can use the **net view** command to display a list of domains, a list of computers, or the resources that the specified computer shares. At a command prompt, type **net view** to display a list of computers in your current domain.

The following table describes the parameters that you can use with the **net view** command to troubleshoot NetBIOS name resolution problems.

Parameter	Description
<i>\\computer name</i>	Specifies the computer whose shared resources you want to view.
<i>/domain:domain name</i>	Specifies the domain for which you want to view the available computers. If <i>domain name</i> is omitted, all domains in the network will be displayed.

Delivery Tip

Explain the most likely cause of a "Network Path Not Found" error message, and describe the method for determining the cause of the error.

Resolving Common NetBIOS Name Resolution Errors

The most common symptom of a problem in NetBIOS name resolution is when the Ping utility returns a Network Path Not Found (Error 53) error message. This message is generally returned when name resolution fails for a particular computer name. This type of error can also occur when there is a problem establishing a NetBIOS session.

Determining the Cause of the Error

To determine the cause of a Network Path Not Found error message, at a command prompt, type **net view \\hostname** (where *hostname* is an active network resource). If this command is successful, name resolution is probably not the source of the problem. Use the **ping** command with the host name to confirm that name resolution is working properly. If the **ping** command returns an Unknown Host error message, name resolution has failed and you must check the status of your NetBIOS session.

Checking the Status of a NetBIOS Session

To check the status of your NetBIOS session, at a command prompt, type **net view \\IP address** (where *IP address* is the IP address of the network resource that you specified when determining the cause of the error).

If the computer is on the local subnet, confirm that the name is spelled correctly and that the target computer is running TCP/IP. If the computer is not on the local subnet, be sure that its name and IP address mapping are available in the DNS database, the Hosts or Lmhosts file, or the WINS database. If all TCP/IP elements appear to be installed properly, use the **ping** command with the remote computer to ensure that the TCP/IP protocol is working.

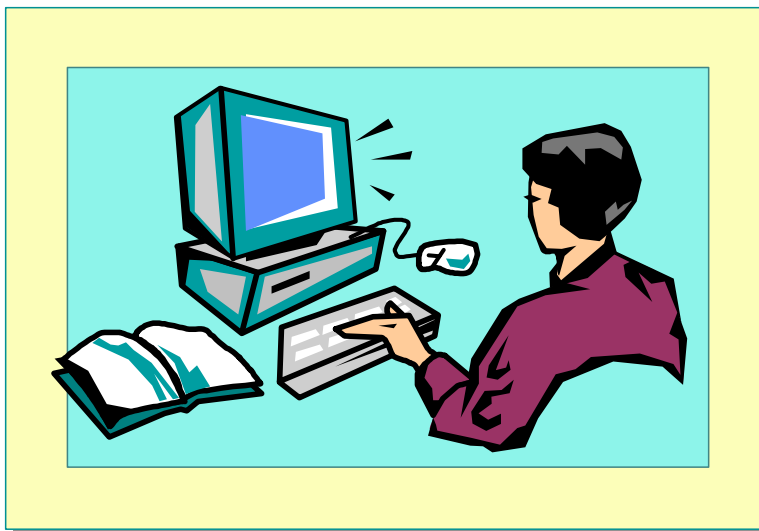
Lab A: Troubleshooting Routing (Simulation)

Topic Objective

To introduce the Troubleshooting Routing simulation.

Lead-in

In this lab, you will troubleshoot router connectivity problems and a demand-dial connection.



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

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Troubleshoot router connectivity problems.
- Troubleshoot a demand-dial connection.

Prerequisites

Before working on this lab, you must have:

- Knowledge about the differences between a workgroup and a domain.
- Experience logging on and off Windows 2000.
- The knowledge and skills to create user accounts by using User Manager for Domains.

Lab Setup

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

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

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.

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.

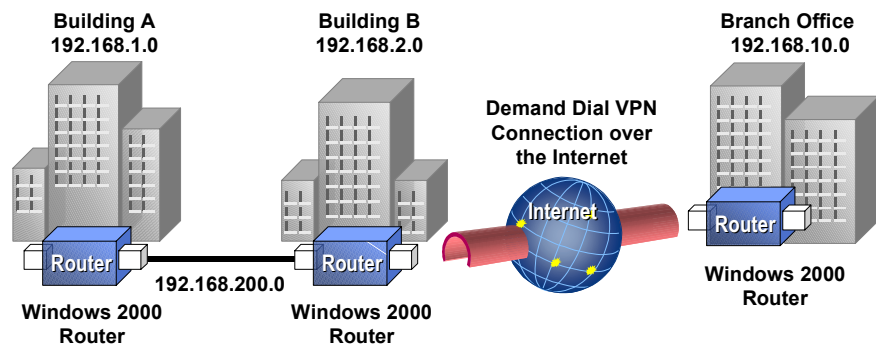
► To start the lab

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, expand Lab Simulations and then click **Troubleshooting Routing**.
4. Read the introduction, and then click the link to start the lab.

Scenario

You are responsible for configuring and maintaining the routers for your company, Contoso Ltd. Contoso has two buildings in its headquarters office, and a branch office that is connected by a demand-dial virtual private network (VPN) connection. The diagram below shows the routers and connections that are used in the Contoso Ltd. network. If a problem occurs with the routers at any time, you are responsible for determining the cause of the error and fixing it.

Contoso



Estimated time to complete this lab: 45 minutes

◆ Troubleshooting Network Services

Topic Objective

To list the topics that are related to troubleshooting network services.

Lead-in

Services enables you to troubleshoot and resolve network services problems on local and remote computers.

- Viewing Service Information
- Modifying Service Properties

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

To troubleshoot and resolve problems with network services, use Services, which you can access from the **Administrative Tools** menu or from Computer Management. For example, you can use Services to start, stop, pause, or resume services on remote and local computers, and configure startup and recovery options.

Some services are configured to start automatically in Windows 2000, depending on the computer configuration and the network services and protocols that are in use. You can use Services to determine which services are configured to start automatically and which services are not starting.

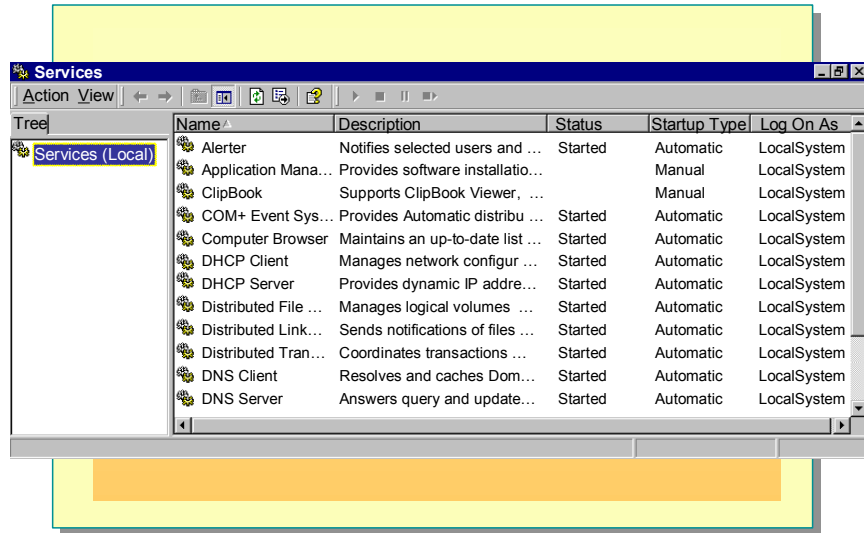
Viewing Service Information

Topic Objective

To illustrate the user interface of Services.

Lead-in

You can view information about network services in the details pane of Services.



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

Delivery Tip

Describe the information that the details pane of Services includes.

Open Services from the **Administrative Tools** menu, or from Computer Management. The details pane of Services contains network service information, such as the service name and description, whether the service has started, how it is configured to start, and the logon account that the service uses. The information in the details pane of the Services window is organized into the following columns:

- **Name.** Displays the names of the network services that are installed on the computer.
- **Description.** Provides a brief description of the services that are installed on the computer. The description is not available when connecting to a remote computer running earlier versions of Windows.
- **Status.** Shows the status of the services that are installed on the computer.
- **Startup Type.** Identifies the startup type for the services that are installed on the computer, as follows:
 - *Automatic.* Specifies that the service is designed to start automatically when the system starts.
 - *Manual.* Specifies that a user or a dependent service can start the service. Services with manual startup do not start automatically when the system starts.
 - *Disabled.* Prevents the service from being started by the system, a user, or any dependent service.
- **Log On As.** Specifies the logon account that is used by the services that are installed on the computer. Most services log on as the system account, but some services can be configured to log on as other user accounts. This enables the service to access resources, such as files and folders, by using the access permissions of the user account that you specify.

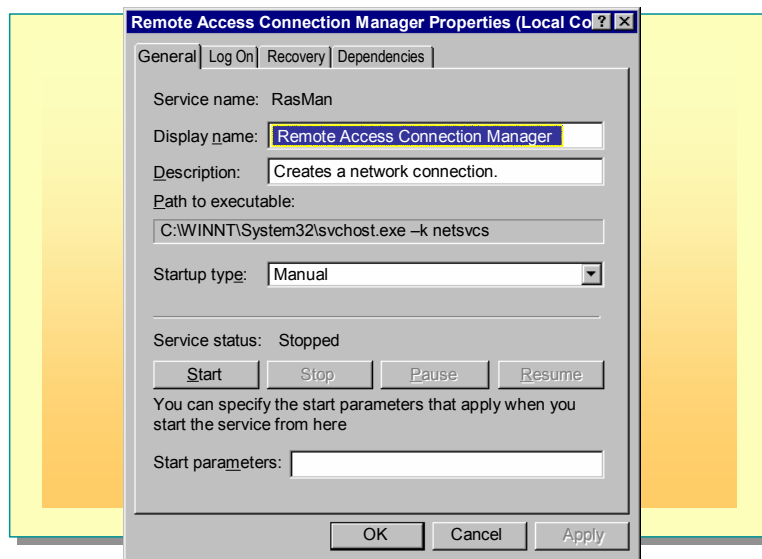
Modifying Service Properties

Topic Objective

To illustrate the **Properties** dialog box for a service.

Lead-in

Use the **Properties** dialog box to modify service information, set recovery actions, and view dependencies for a service.



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

To modify the properties of a service, open Services. In the details pane, right-click the name of the service that you want to modify, and then click **Properties**.

Delivery Tip

Describe the configuration options on the **General** tab of a service's **Properties** dialog box.

General Tab

To modify the information that appears in the details pane of the Services window, configure the options on the **General** tab of the **Properties** dialog box for a service. After you have modified the service properties, click **OK**. You can use the **General** tab to:

- Change the name of the service that appears in the **Name** column.
- Modify the description that appears in the **Description** column.
- Change the startup type that appears in the **Startup Type** column.

You can also view the service's status, and start, stop, pause, or resume the service by clicking the appropriate button under **Service status**. Before you start a service by clicking the **Start** button under **Service status**, you can specify the start parameters that apply when the service starts in the **Start parameters** box.

Note You can view the path and file name of the service on the **General** tab, under **Path to executable**. This information cannot be changed.

Delivery Tip

Describe the configuration options on the **Log On** tab of a service's **Properties** dialog box.

Log On Tab

To modify the information that appears in the **Log On As** column of the Services window, configure the options on the **Log On** tab of the **Properties** dialog box for a service. You can use the **Log On** tab to:

- Select one of the following options to specify the account that the service uses to log on.
 - *Local System account.* Specifies that the service will log on by using the system account, rather than a user account. Most services log on as the local system account.
 - *This account.* Assigns a logon account to the service. Although most services log on as the system account, some services can be configured to log on to special user accounts so that the service can access resources, such as files and folders, by using the access permissions of the user account that you specify.

Note Select the **Allow service to interact with desktop** check box to enable the service to provide a user interface on the desktop when the service is started. This option is available only if the service is running as the Local System account.

- Enable or disable the service for a specific hardware profile.

Delivery Tip

Describe the configuration options on the **Recovery** tab of the **Properties** dialog box for a service.

Recovery Tab

Use the **Recovery** tab to specify the recovery actions that you want to occur if a service fails, such as restarting the service automatically or restarting the computer. You can set a different recovery action for the first failure, the second failure, and for all subsequent failures of a service. Set recovery actions to configure Windows 2000 to take no action, restart the service, run a file, or restart the computer if a service fails.

If you select **Run a File**, specify the file name under **Run file**. Do not specify programs or scripts that require user input. If you select **Reboot the Computer**, click **Restart Computer Options** to specify the amount of time that Windows 2000 will wait before restarting the computer. You can also create a message to send to computers on the network before the computer restarts.

Delivery Tip

Describe the information that appears on the **Dependencies** tab of the **Properties** dialog box for a service.

Dependencies Tab

The **Dependencies** tab lists other services that depend on the service, or that the service depends on. When you open the **Properties** dialog box for a particular service, the **Dependencies** tab:

- Lists the other network services that the service requires to run properly.
- Lists the other network services that require the service to run properly.

This information is useful when troubleshooting network services, because a network service failure may be the result of a problem with a dependent service.

◆ Monitoring the Network

Topic Objective

To list the topics that are related to monitoring the network.

Lead-in

By using Microsoft Network Monitor, you can capture and display network packets.

- Installing Network Monitor
- The Network Monitor Interface
- Capturing Data by Using Network Monitor
- Displaying Data by Using Network Monitor

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

You can use a network packet analyzer to compile information about network functionality. A network packet analyzer is a tool that captures, filters, and analyzes network traffic. Network packet analyzers can be software based, or a combination of specialized hardware and software. By using network packet analyzers, you can:

- Monitor real-time network utilization or bandwidth.
- Troubleshoot network errors by diagnosing cable connections, bandwidth or protocol issues, or defective network cards.
- Use monitoring information to determine how you can optimize the network by dividing it into subnets.
- Use monitoring information to plan the purchase of additional devices for your network.

Delivery Tip

Describe the purpose of Network Monitor.

Microsoft Network Monitor

Microsoft Network Monitor is a software-based traffic analysis tool that enables you to capture and display network packets that a computer running Windows 2000 Server sends to and receives from a LAN. By using Network Monitor, you can:

- Capture packets directly from the network.
- Display and filter packets immediately after a capture, or save the captured data for later analysis.
- Edit captured packets and transmit them back onto the network.
- Capture packets from a remote computer.

Important To install or use Network Monitor, you must be a member of the Administrators group.

Delivery Tip

Explain how Network Monitor can be used for troubleshooting purposes.

Troubleshooting Network Problems

You can use Network Monitor to detect and troubleshoot networking problems on a local computer. For example, use Network Monitor to diagnose hardware and software problems when a server cannot communicate with other computers. In addition, you can save to a file the packets that Network Monitor captures, and then send the file to professional network analysts or support organizations for analysis.

Simple Version vs. Full Version

Network Monitor is included with Windows 2000 Server (simple version), and with Microsoft Systems Management Server (full version). The following table describes the differences between the simple and full versions of Network Monitor.

Function	Network Monitor (simple)	Network Monitor (full)
Local capturing	To and from the computer running Network Monitor only	All devices on the entire subnet
Remote capturing	Not available	Available
Determining the top user of network bandwidth	Not available	Available
Determining which protocol consumed the most bandwidth	Not available	Available
Determining which devices are routers	Not available	Available
Resolving a device name into a MAC address	Not available	Available
Editing and retransmitting network traffic	Not available	Available

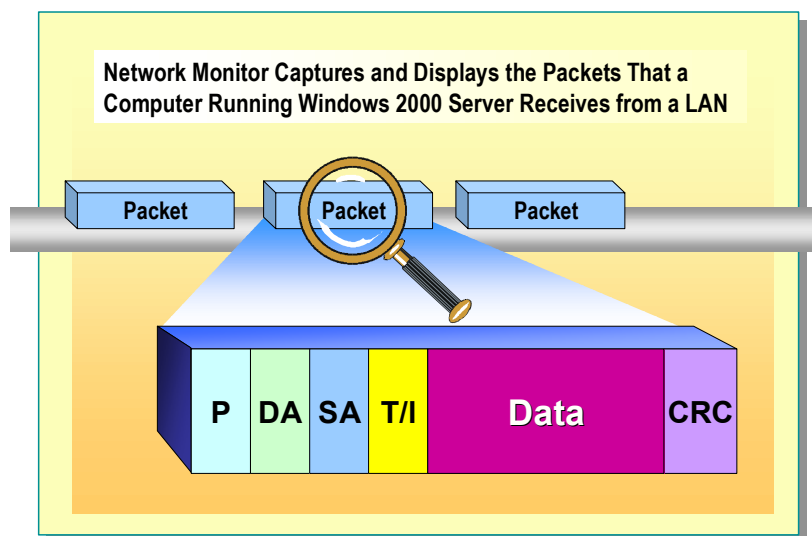
Installing Network Monitor

Topic Objective

To illustrate the contents of a packet.

Lead-in

You can use Network Monitor to detect and troubleshoot networking problems on a local computer.



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

Network Monitor captures and displays the packets that a computer running Windows 2000 Server receives from a LAN. Install Network Monitor on the computer from which data will be captured. When you install Network Monitor, the Network Monitor Driver is installed automatically on the same computer. The Network Monitor Driver appears as a network service in the **Properties** dialog box for local area connections.

Note Network Monitor can be installed only on computers running Windows 2000 Server.

Delivery Tip

Describe the procedure for installing Network Monitor.

To install Network Monitor:

1. Open Control Panel, and then double-click **Add/Remove Programs**.
2. In the **Add/Remove Programs** dialog box, click **Add/Remove Windows Components**.
3. In the Windows Components wizard, click **Management and Monitoring Tools**, and then click **Details**.
4. In the **Management and Monitoring Tools** dialog box, select the **Network Monitor Tools** check box, click **OK**, and then click **Next**.
5. If you are prompted for additional files, insert your Windows 2000 Server compact disc, or type a path to the location of the files on the network, and then click **OK**.
6. Click **Next**, and then click **Finish**.

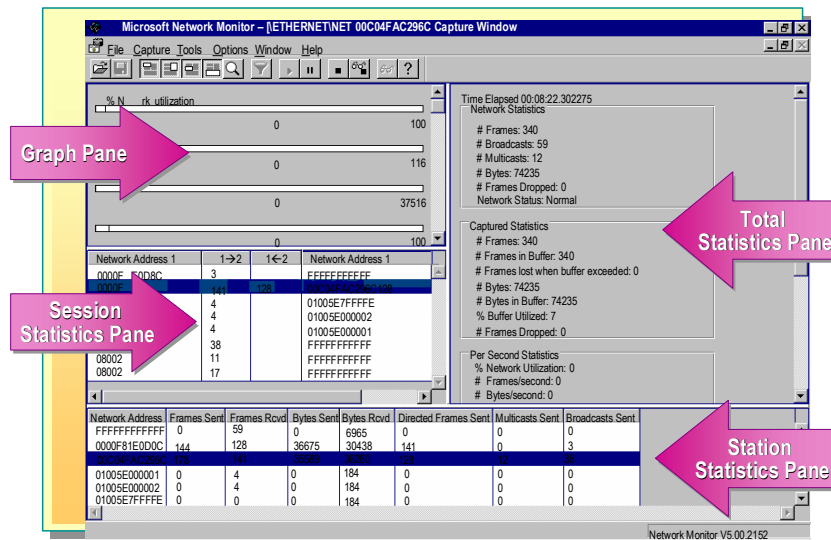
The Network Monitor Interface

Topic Objective

To illustrate the Network Monitor user interface.

Lead-in

Network Monitor provides statistical data in the Capture window, which you can use to analyze network performance.



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

Open Network Monitor from the **Administrative Tools** menu. The first window to appear in Network Monitor is the Capture window, which is the basic Network Monitor interface. The Capture window provides different types of statistical data that is useful in analyzing overall network performance.

Delivery Tip

Describe the contents of the Capture window.

The Capture window is divided into the four major areas, as described in the following table.

Pane	Description
Graph	Displays the current activity as a set of bar charts that indicate the percentage of network utilization, frames per second, bytes per second, broadcasts per second, and multicasts per second during the capture process.
Session Statistics	Provides a summary of the conversations between two hosts, and indicates which host is initiating broadcasts and multicasts.
Total Statistics	Displays statistics for the traffic that is detected on the network, statistics for the frames captured, per-second utilization statistics, and network adapter card statistics.
Station Statistics	Provides a summary of the total number of frames that a host initiates, the number of frames and bytes sent and received, and the number of initiated broadcast and multicast frames.

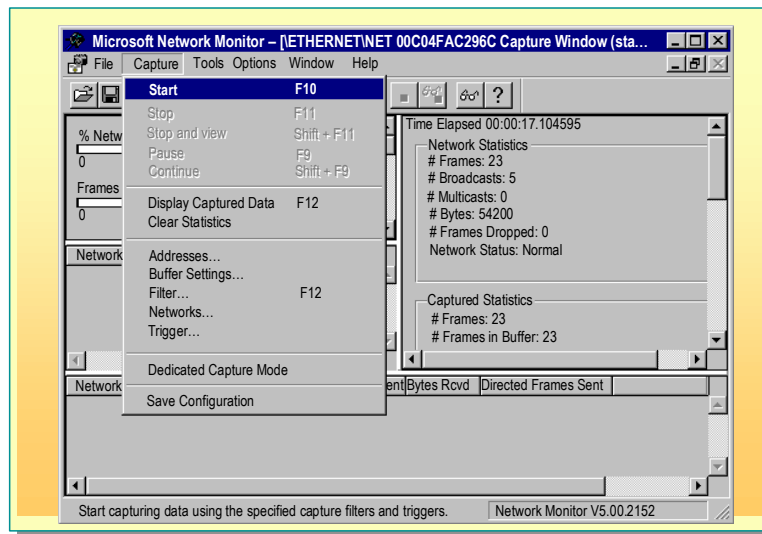
Capturing Data by Using Network Monitor

Topic Objective

To illustrate the user interface for initiating a data capture by using Network Monitor.

Lead-in

As Network Monitor captures data, information will appear in each of the four sections of the Capture window.



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

Network Monitor performs much of the data analysis for you by translating captured data into its logical frame structure. After data has been captured, it can be analyzed immediately or saved to a capture file (.cap) for later analysis.

Delivery Tips

Demonstrate the process for starting and stopping a data capture. Next, demonstrate the procedure for saving captured data to a file.

Capturing Network Traffic

To capture network traffic:

1. Open Network Monitor.
2. If you are prompted for a default network on which to capture frames, select the local network from which you want to capture data.
3. Click **Capture**, and then click **Start**.

As data is being captured, information will appear in each of the four sections of the Capture window. This includes current network statistics, in addition to statistics for the captured data.

4. To stop the capture, click **Capture**, and then click **Stop**.

Saving Captured Data

You can save captured data to a capture file (.cap) for later analysis. You can view these files in Network Monitor at a later time, or you can send the file to professional network analysts or support organizations for analysis. To save captured data to a file, on the **File** menu, click **Save As**. In the **Save As** dialog box, specify the folder in which you want to save the file.

Important You must use the .cap file extension if you want to be able to view the file in Network Monitor at a later time.

Capture Filters

A common method for controlling the amount of data that is captured is to set a capture filter. A capture filter describes the frames that are to be captured, buffered, displayed, and saved. Before any frame can be buffered, it must pass through the filter. Filters are commonly configured for specific types of traffic (protocols), such as IP and IPX, or on source or destination addresses. These addresses can be MAC addresses, or protocol addresses (IP or IPX).

Capture Triggers

You can also specify a set of conditions that trigger an event in a Network Monitor capture filter. By using triggers, Network Monitor can respond to events on your network. For example, you can start an executable file when Network Monitor detects a particular set of conditions on the network.

Note For more information about capture filters and triggers, open Network Monitor, and then click **Help**.

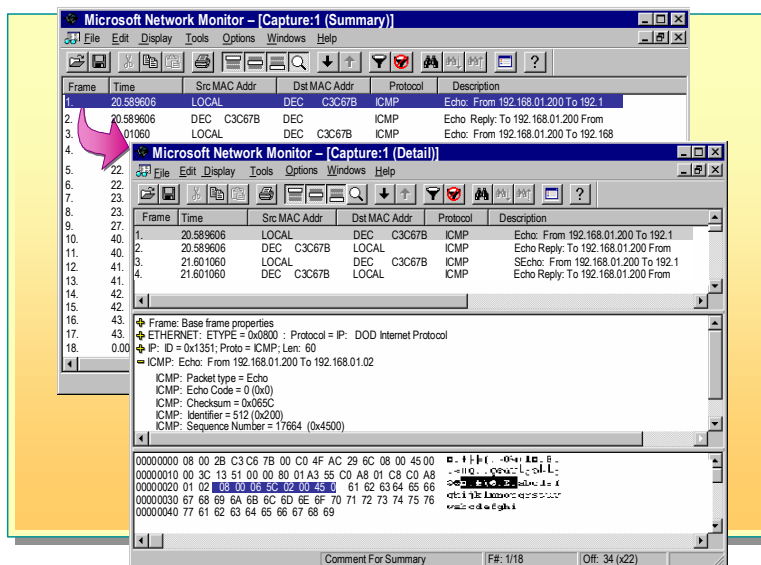
Displaying Data by Using Network Monitor

Topic Objective

To illustrate the user interface for displaying data by using Network Monitor.

Lead-in

To display data by using Network Monitor, click **Capture**, and then click **Stop and View** when you want to stop the capture.



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

Delivery Tips

Display a capture file. Choose a frame and lead students through the details. Show students the different fields in the Capture Summary window, and demonstrate how to open a frame and display frame details.

Delivery Tip

If students can only view one pane in the Capture Summary window, verify that **Zoom** is not selected on the **Window** menu.

Network Monitor simplifies data analysis by interpreting raw data collected during the capture and displaying it in the Capture Summary window. To view captured data, start a capture. When you want to stop the capture, click **Capture**, and then click **Stop and View**.

Displaying Frames

The Capture Summary window displays a summary of all captured frames, and includes three panes—the Summary pane, the Detail pane, and the Hexadecimal pane. If you want to focus on a particular pane, you can change the appearance of the Capture Summary window so that one pane fills the entire window.

To view only one pane in the Capture Summary window, click anywhere inside the pane that you want to view, click **Window**, and then click **Zoom**. To view all three panes, perform the same procedure and verify that **Zoom** is not selected on the **Window** menu.

Summary Pane (Top)

This pane lists all frames that are included in the current view of the captured data. When a frame is selected in the Summary pane, Network Monitor displays the frame's contents in the Detail and Hexadecimal panes. The columns in the Summary pane include the following.

Column	Description
Frame	Displays the frame number. All frames captured during one capture session are numbered in the order of capture time.
Time	Displays the frame's capture time relative to the beginning of the capture process. It can be configured to display the time of day when the frame was captured, or the time that has elapsed since the previous frame capture.

(continued)

Column	Description
Src MAC Addr (Source MAC Address)	Displays the hardware address of the computer that sent the frame.
Dst MAC Addr (Destination MAC Address)	Displays the hardware address of the target computer.
Protocol	Lists the protocol that was used to transmit the frame.
Description	Displays a summary of the frame's contents. The summary information can include the first protocol used in that frame, the last protocol used in that frame, or an automatic selection.
Src Other Addr (Source Other Address)	Provides an additional identifying address for the originator of the frame, other than the MAC address. This can be an IP or IPX address.
Dst Other Addr (Destination Other Address)	Provides an additional identifying address for the destination of the frame.
Type Other Addr (Type Other Address)	Specifies which type of address is displayed in the previous two columns.

Detail Pane (Middle)

The Detail pane displays protocol information for the frame that is selected in the Summary pane. When a frame contains several protocol layers, the Detail pane displays the outermost level first.

When you select a protocol in the Detail pane, the associated hexadecimal strings for the current frame are in the Hexadecimal pane. When you expand the protocol information, a line of data appears for each property associated with that frame.

Hexadecimal Pane (Bottom)

The Hexadecimal pane displays the content of the selected frame in hexadecimal format. When you select information in the Detail pane, the corresponding hexadecimal data is selected in the Hexadecimal pane. This information is often the focus of data analysis, especially when determining the appropriate application programming interface (API) call that is used in a transaction.

Filtering Data

You can set display filters to filter frames of interest, such as those from a particular host, or those using a particular protocol. You can configure display filters for a specific protocol or a specific MAC or protocol address, or for a unique property of a frame, such as a specific source or destination port.

Note For more information about display filters, see Network Monitor Help.

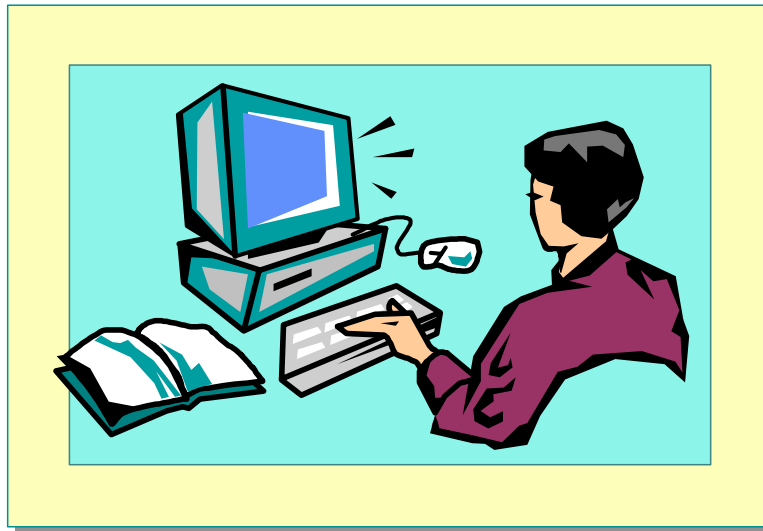
Lab B: Troubleshooting Network Problems by Using Network Monitor

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will use Network Monitor to troubleshoot network problems by capturing and displaying network traffic.



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

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Install Network Monitor.
- Use Network Monitor to capture and display network traffic.

Prerequisite

Before working on this lab, you must be familiar with Network Monitor concepts, utilities, and operations.

Lab Setup

To complete this lab, you need a computer running Windows 2000 Advanced Server.

Scenario

Your production department has 25 new employees. You have installed 25 new computers on your network. As the new employees begin using these computers, you notice problems on the subnet in which users are periodically losing their connections to the network. You want the ability to monitor the network so that you can prevent connectivity issues, keep track of performance, and prevent future problems.

Estimated time to complete this lab: 30 minutes

Exercise 1

Installing Network Monitor

Scenario

You are the administrator for Northwind Traders. You have connected new computers to the network for newly hired employees. After installing these new computers, you notice problems with network performance.

Goal

In this exercise, you will install Network Monitor.

Task	Detailed Steps
1. Install Network Monitor.	- 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, and then 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. (continued)	- In the Windows Components wizard on the Windows Components page, under Components, select Management and Monitoring Tools, and then click Details. - In the Management and Monitoring Tools window, select the Network Monitor Tools check box, click OK, and then click Next. - If the Insert Disk dialog box appears, click OK. 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.

Exercise 2

Capturing Data with Network Monitor

Scenario

You have installed Network Monitor. You want to discover why your network is having performance problems.

Goal

In this exercise, you will use Network Monitor to collect data about your network.

Tasks	Detailed Steps
1. Determine the media access control address of the network card associated with the Classroom connection.	a. At a command prompt, type ipconfig /all and then press ENTER.
 What is the physical address of the network card associated with the Classroom connection? The physical address will be in the following format: XX-XX-XX-XX-XX-XX. Answers will vary.	
1. (continued)	b. Minimize the command prompt window.
2. Set a Network Monitor trigger.	a. Open Network Monitor from the Administrative Tools menu. b. Click OK to close the Network Monitor – Select Default Network dialog box.
 Note: You must select a default network because the computer has more than one network card.	
2. (continued)	c. In the Select a network dialog box, expand Local Computer. d. Click the Ethernet adapter that is associated with the physical address of the Classroom network connection, and then click OK.  <i>The Network Monitor Capture window appears.</i> e. On the Capture menu, click Trigger.  <i>The Capture Trigger dialog box appears.</i> f. Under Trigger on, click Buffer space. g. Under Buffer space, click 50%. h. Under Trigger Action, click Stop Capture, and then click OK.

(continued)

Tasks	Detailed Steps
3. Capture network data and generate network traffic.	a. On the Capture menu, click Start. b. Click Start, and then click Run. c. In the Open dialog box, type \\London and then click OK.  <i>A list of resources on \\London appears.</i> d. In the London window, double-click Setup.
4. View network data statistics.	a. Restore Network Monitor. b. On the Capture menu, click Stop. c. On the Capture menu, click Display Captured Data. d. Scroll through the list of captured frames, and view the addresses that are listed in the Src MAC Addr and Dst MAC Addr columns. View the protocols that are listed in the Protocol column.  <i>Notice the London server name is in the Src and Dst MAC Addr columns. TCP, SMB and RIP are protocols that you will see in the Protocol column.</i> e. Close Network Monitor. f. Close all windows, and then log off.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

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

- Troubleshooting Network Problems
- Identifying the Symptoms and Causes of Network Problems
- Resolving TCP/IP Problems
- Resolving Name Resolution Problems
- Troubleshooting Network Services
- Monitoring the Network

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

1. What are the three phases of effective network troubleshooting?

Researching the symptoms of network problems, identifying the causes of network problems, and resolving network problems.

2. Which of the Windows 2000 administrative tools can you use to diagnose network problems, and what does it allow you to do?

Event Viewer, which you can use to monitor event logs to predict and identify the sources of system problems.

3. What are the four main areas in which TCP/IP problems can occur?

TCP/IP problems can result from problems with:

- TCP/IP configuration, such as an IP address, subnet mask, or gateway that is not configured correctly.
- IPSec configuration, such as invalid policy configuration.
- IP-to-MAC address resolution, such as an invalid static entry, or duplicate IP addresses on the network.
- IP routing, such as a gateway that is not configured correctly.

4. What is the easiest way to distinguish host name problems from NetBIOS name resolution problems?

Determine whether the failing application uses NetBIOS names or host names. If the application uses host names, the problem is the result of incorrect host name resolution.

5. You have added five TCP/IP clients to your network. You now notice that the subnet to which you added the clients periodically disconnects some of them from the network. What tool can you use to troubleshoot this problem?

You can use Network Monitor to diagnose hardware and software problems when a system cannot communicate with other computers. In addition, you can save to a file the packets that Network Monitor captures, and then send the file to professional network analysts or support organizations for analysis.

6. Your network uses TCP/IP and is connected to the Internet. You are unable to access a particular host on the Internet. You have verified that the gateway is functional, because you can access other sites on the Internet. Which TCP/IP utility can you use to troubleshoot this problem?

Use Ping to verify that TCP/IP is configured correctly and to determine whether the remote TCP/IP host is available.

