Microsoft®
Training &
Certification

Microsoft® Official Curriculum

Module 5: Isolating Common Connectivity Issues

Contents

Microsoft®

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, place or event 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.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, MSDN, PowerPoint, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Instructor Notes

Presentation:
60 minutes

Lab:
60 minutes

This module introduces students to a process for isolating common connectivity issues, and also describes how to use network utilities as part of that process. To maintain network connectivity, students must be able to isolate issues that affect a network and determine the best ways to resolve them.

The tasks in this module are purposely referred to as isolating connectivity issues rather than troubleshooting because the systems administrator (SA) job for which your students are preparing can have a wide range of responsibilities. These can range from resetting passwords to resolving hardware and software problems, but at some point a problem will originate in an area beyond the SA's control. The goal of this module is for students to be able to find a problem and decide whether they can solve it themselves, or whether they will need assistance from people responsible for other areas of the network.

Objectives

After completing this module, students will be able to:

- Employ a method to systematically resolve connectivity issues.
- Use utilities and a job aid to isolate common connectivity issues.

Required materials

To teach this module, you need the following materials:

- Microsoft® PowerPoint® file 2276B_05.ppt
- Appendix C: Problem Isolation Flow Chart

Important It is recommended that you use PowerPoint 2002 or later to display the slides for this course. If you use PowerPoint Viewer or an earlier version of PowerPoint, all the features of the slides may not be displayed correctly.

Preparation tasks

To prepare for this module:

- Read all of the materials for this module.
- Complete the lab exercises.
- Practice presenting the build slides.
- Become familiar with the Problem Isolation Flow Chart in Appendix C.

How to Teach This Module

This section contains information that will help you to teach this module. There are two lessons in this module. The first lesson describes a four-step issue isolation method. The second lesson describes the utilities that an SA can use for gathering the data and making the tests required to isolate connectivity issues.

Lesson: Determining the Causes of Connectivity Issues

This section describes the instructional methods for teaching this lesson.

This lesson describes a five-step process for isolating issues on a network. Because the responsibilities of SAs can vary greatly between organizations, this lesson refers to determining the causes of issues rather than troubleshooting problems. The emphasis is on finding the cause of an issue, the action to be taken by SAs, to resolve an issue or to escalate it, will depend on their responsibilities.

What Are the Common Connectivity Issues?

This topic sets the foundation for the lesson. It presents four very general problems that cover almost every type of issue that occurs on a network. The introductory sentence on the slide, "Various issues can have similar effects", refers to the fact that each of the issues could have many different causes.

The first three issues are actual problems that usually require corrective action to resolve. The rest of this module deals with resolving those types of issues. The fourth issue, slow network response, is a common complaint but it is not necessarily caused by a particular failure. Poor performance is more often a maintenance or optimization issue and as such it is not dealt with beyond this topic. Students interested in more information about network performance should take Course 2275, *Maintaining a Microsoft Windows Server 2003 Environment.*

Before You Begin Isolating the Issue

This is a short list of steps to take before making any changes to the client or the network. Assure the students that this is not an absolute list of formal actions that they must perform before every task. It, and the rest of this lesson, is a list of guidelines that the SA can follow as appropriate.

Isolating the Issue

This is the most important topic in this lesson because it introduces the Problem Isolation Flow Chart in Appendix C. Have students look at it briefly and tell them that they will get to use it in the lab at the end of the module.

Resolving the Issue

The recommendations in this topic are more applicable to large organizations than small ones. Make sure that your students realize that you are not saying that they must perform all the tasks described in this topic. Rather, that the tasks are good ideas to keep in mind when they might be needed.

After the Issue Is Resolved

The suggestions in this topic can be applied to issues and organizations of any size. It is important to know how to avoid small issues in addition to large problems.

Lesson: Network Utilities That You Can Use to Isolate Connectivity Issues

This section describes the instructional methods for teaching this lesson.

This lesson contains descriptions of various utilities, which are mostly command-line programs that will appear very similar to each other if they are described too quickly. Be sure of the uses and differences of each utility before teaching this lesson. Demonstrate the utilities whenever possible. Some of them are much easier to show than to describe, most notably Netsh.

How to demonstrate Ping errors in the classroom

To demonstrate the various Ping error messages, use the following procedures:

► **To display the TTL expired in transit error message (optional)**

Note To expire the TTL, you must be able to ping across routers.

1. Open a comment prompt.
2. Type **ping –i 1** <*remote IP address or remote host name*>

```
C:\>ping -i 1 www.microsoft.com

Pinging www.microsoft.akadns.net [207.46.249.27] with 32
bytes of data:

Reply from 192.168.0.1: TTL expired in transit.
Reply from 192.168.0.1: TTL expired in transit.
Reply from 192.168.0.1: TTL expired in transit.
Reply from 192.168.0.1: TTL expired in transit.

Ping statistics for 207.46.249.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

► To display the Destination Host Unreachable message

1. Using the Run As command, open the command prompt as Administrator and type **route delete 0.0.0.0** and press ENTER.
2. Type **ping 172.1.1.1** and press ENTER.

   Because the route the default gateway has been deleted, the destination host is unreachable.
3. To restore the deleted route, type **ipconfig/renew** and press ENTER.

```
C:\>route delete 0.0.0.0

C:\>ping 172.1.1.1

Pinging 172.1.1.1 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 172.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

► To display the Request timed out error message (optional)

1. Open a comment prompt.
2. Type **ping 172.1.1.1** and press ENTER.

   Since a local route exists (0.0.0.0) to attempt to reach 172.1.1.1, you receive a timed out message rather than a destination host unreachable message.

```
C:\>ping 172.1.1.1

Pinging 172.1.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

► To display unknown host error message (optional)

1. Open a comment prompt.
2. Type **ping invalidhost** and press ENTER.

   The host name invalidhost cannot be resolved and the error message is displayed.

   C:\>ping invalidhost

   Ping request could not find host invalidhost. Please check the name and try again.

Lab: Isolating Common Connectivity Issues

In Task 1 of Exercise 0, the students are instructed to use a network number as a variable value. You must tell the students their network numbers, which will be the same as their classroom number.

An answer key for each lab exercise is located on the Student Materials compact disc, in case the students need step-by-step instructions to complete the lab. They can also refer to the How To pages in the module.

Lab Setup

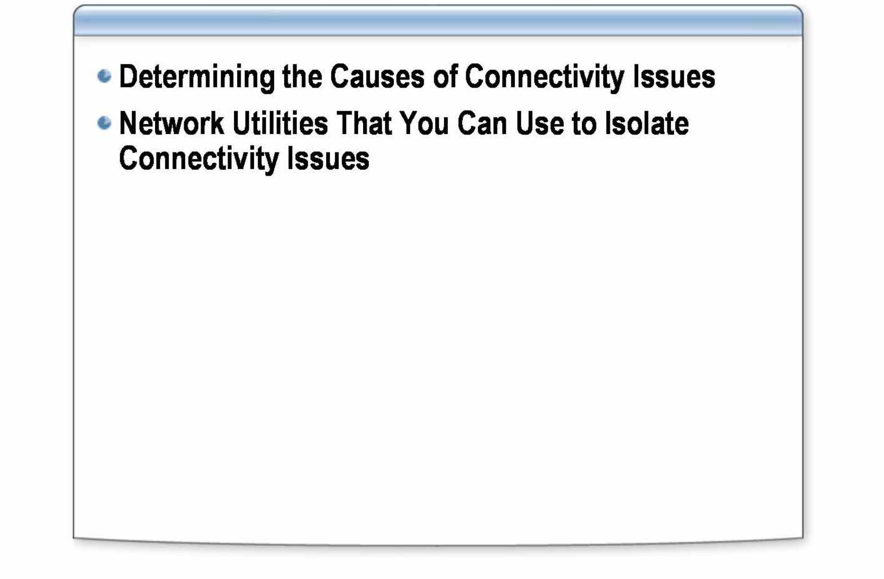
There are no lab setup requirements that affect replication or customization.

Lab Results

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

Important Each scenario in the lab has a batch file to reverse the changes introduced during the scenario. Students are instructed to run it as the last task in each scenario.

Overview



- Determining the Causes of Connectivity Issues
- Network Utilities That You Can Use to Isolate Connectivity Issues

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

Introduction

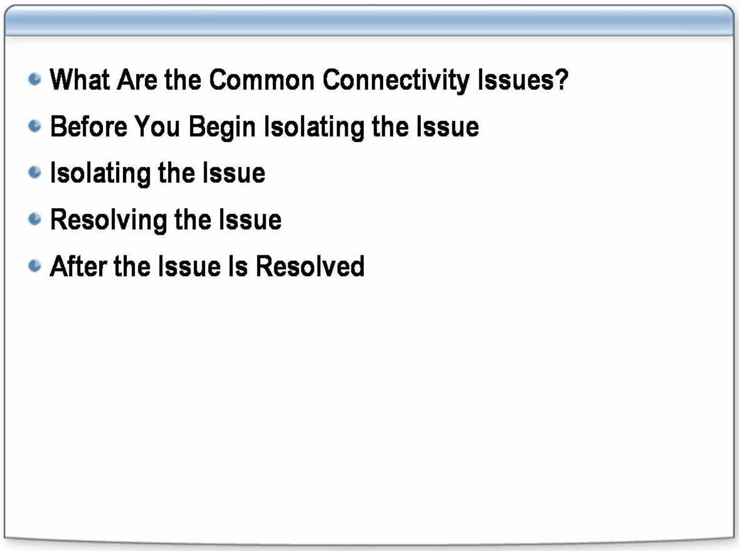
The information in this module introduces you to a process for isolating common connectivity issues, and also describes how you can use network utilities and tools as part of this process. To maintain network connectivity, you must be able to isolate issues that interrupt it. When you isolate connectivity issues, you are assisting systems engineers in resolving these issues as rapidly as possible.

Objectives

After completing this module, you will be able to:

- Employ a method to systematically resolve connectivity issues.
- Use utilities and a job aid to isolate common connectivity issues.

Lesson: Determining the Causes of Connectivity Issues



- What Are the Common Connectivity Issues?
- Before You Begin Isolating the Issue
- Isolating the Issue
- Resolving the Issue
- After the Issue Is Resolved

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

Introduction

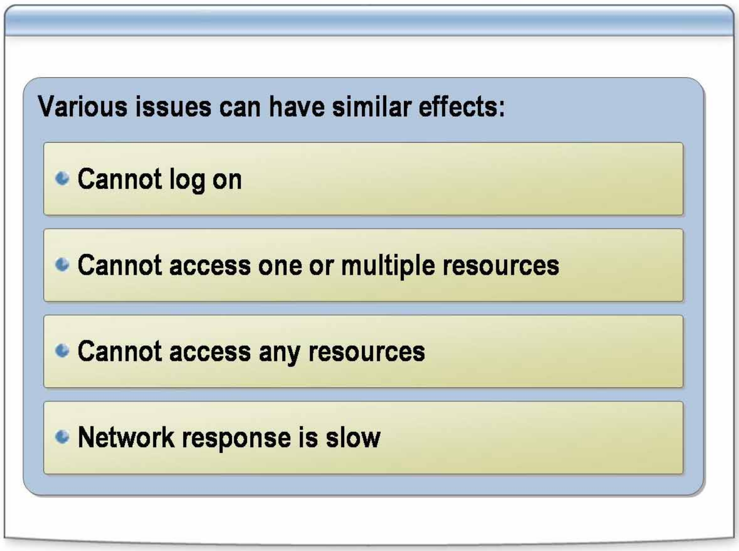
One of the key elements in isolating a network problem is using a consistent, effective strategy for determining the cause. Many of the trouble calls that you receive will be due to user errors that can be resolved through a little training for the user. When you are faced with a more complex complaint, however, you should follow a set procedure for isolating and resolving the issue.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the common connectivity issues.
- Make time-saving preparations before starting to isolate a problem.
- Follow the issue isolation procedure to the source of a problem.
- Make a plan for implementing a solution.
- Hold a post-resolution meeting and document the actions that led to the solution.

What Are the Common Connectivity Issues?



Various issues can have similar effects:

- Cannot log on
- Cannot access one or multiple resources
- Cannot access any resources
- Network response is slow

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

Introduction

As a systems administrator, you will not be able to personally resolve every issue that occurs on your network. However, you should be able to isolate the source of an issue, and to determine whether it is one that you can fix or something that you need to escalate to an expert.

Common issues

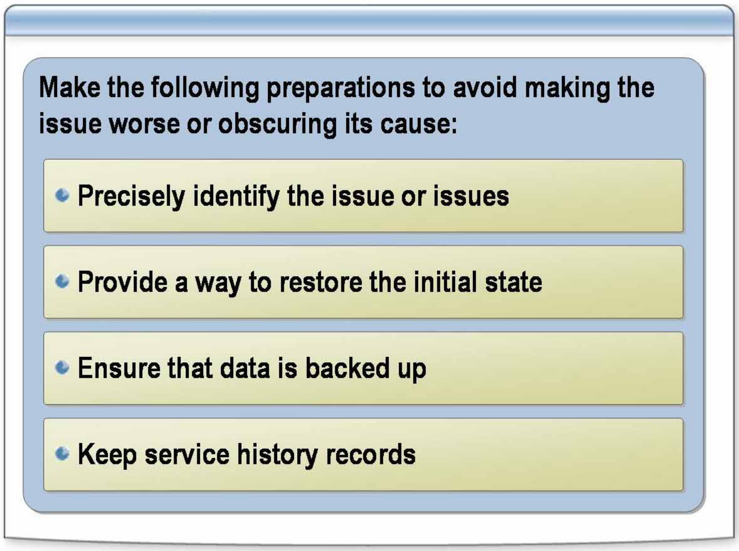
Most issues will be presented to you by users who find that they are unable to perform a specific action at their computers—either something that they were able to do previously or something that they think they should be able to do presently.

There are only a few basic types of complaints:

- User cannot log on.
- User cannot access either one resource or multiple resources.
- User cannot access *any* resources.
- Network response is slow.

A single basic problem may have a wide variety of causes. For example, a user who cannot log on may simply be entering the wrong password; or all the domain controllers may be offline; or the cause could lie in any of a large number of locations in between. Isolating the problem may be a long and complex process—or it may only take a minute—depending on the cause. The challenge for you is to isolate the single cause from the many possibilities.

Before You Begin Isolating the Issue



Make the following preparations to avoid making the issue worse or obscuring its cause:

- Precisely identify the issue or issues
- Provide a way to restore the initial state
- Ensure that data is backed up
- Keep service history records

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

Introduction

If you think that an issue will require a large effort to resolve, you can save yourself time by making preparations that will help you to both proceed as efficiently as possible and avoid making the problem worse.

Precisely identify the issue or issues

It can be difficult to determine the exact nature of an issue from the description given by a user. That is why the first action of the isolation is to obtain accurate information about what has occurred.

To help identify the issue or issues, ask the following questions:

- What exactly were you doing when the problem occurred?
- Was the computer operating normally just before the problem occurred?
- Has the problem occurred before?
- Have you had any other problems?
- Has any hardware or software been installed, removed, or reconfigured recently?
- Did you or anyone else make any changes while trying to resolve the problem?

Provide a way to restore the initial state

Before changing the configuration of a computer or other device, note its original settings. This can include:

- Noting the client's network configuration, which includes the Internet Protocol (IP) address, the default gateway’s IP address, and the subnet mask.
- Noting what services are set to automatic, but are not running.
- Reviewing the event log for errors that are already occurring before you change the configuration.
- Using the Ping utility to determine the level of connectivity to the gateway and remote computers before you start.

If disabling a feature or changing a setting does not produce the results that you want, use your notes to restore the feature or setting before trying another solution. Not restoring settings can cause new problems and can also make it difficult to determine which of your actions caused a particular effect.

Ensure that data is backed up

Backups are important for computers of all sizes, from clients to high-availability servers. If you suspect that your efforts to isolate a problem might worsen the situation, or that the situation presents any risk to important data, then perform a backup before you make any changes. This enables you to restore the system if you lose data, cause Stop errors, or create startup problems.

Your backup should include the following items:

- The user's personal folder that is located in the Documents and Settings folder. This includes the My Documents folder and folders that contain personalization information such as the user's Favorites list and Desktop settings.
- The system state, which includes the registry and other vital system files.

Note A quick way to back up important client data is by using the Backup or Restore Wizard that is included with Microsoft® Windows® XP. To start the wizard, in **Performance and Maintenance**, in Control Panel, click **Back up your data**.

After you make the backup, consider performing the following steps to check that the data is written correctly to the backup media:

- Use the verification option provided by your backup software.
- Restore a few files from the backup media.

Keep service history records

To detect trends and patterns in your network's performance, you should record each service action that is performed. If you have a small network, you could simply keep the records in a notebook but larger networks require a more versatile solution.

A useful way to store large numbers of records is to use a database management system to create a service history database with a record for each device on your network. Using a database enables you to search across all your records for similar types of problems or occurrences during a specific time period.

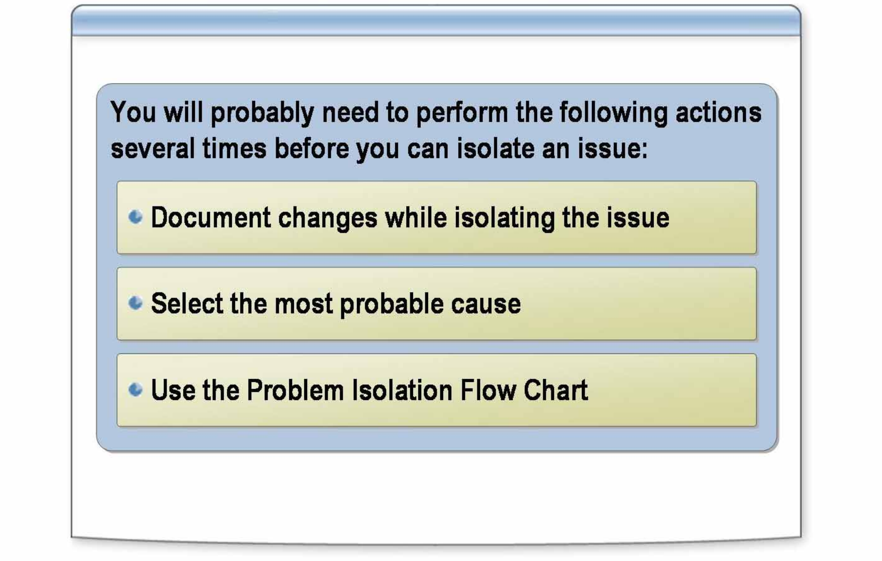
Regardless of the medium on which it is stored, each record should start with baseline performance information gathered when the host was added to the network. Update the baseline information after installing new hardware or software so you can compare past and current behavior and performance levels.

Your service history records should include the:

- Baseline performance data.
- Dates and times of problems and resolutions.
- Changes that you made.
- Reasons for the changes.
- Name of the person who made the changes.
- Positive and negative affects the changes had on the stability and performance of the client and network.
- Information provided by technical support.

Note For more information about creating a configuration management database, see the Information Technology Infrastructure Library (ITIL) and Microsoft Operations Framework (MOF) Web links provided on the Student Materials compact disc.

Isolating the Issue



You will probably need to perform the following actions several times before you can isolate an issue:

- Document changes while isolating the issue
- Select the most probable cause
- Use the Problem Isolation Flow Chart

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

Introduction

Locating the source of a problem may be a long and an arduous process, or it may take only a few minutes. In either case, the Problem Isolation Flow Chart can help you to identify the shortest path to a solution.

Document changes while isolating the issue

Documenting the steps you take while troubleshooting will help you review your actions after you resolve the problem. This is useful for very complex problems that require lengthy procedures to resolve. Documenting your steps:

- Helps you to verify that you are neither duplicating nor skipping steps.
- Allows others to assist you with the problem.
- Enables you to evaluate the effectiveness of your efforts.
- Makes it possible for you to identify the exact steps to take, if the problem should ever recur.

Begin documenting your actions at the start of issue isolation, rather than waiting until after you have finished and then attempting to remember all the steps that you took.

Select the most probable cause

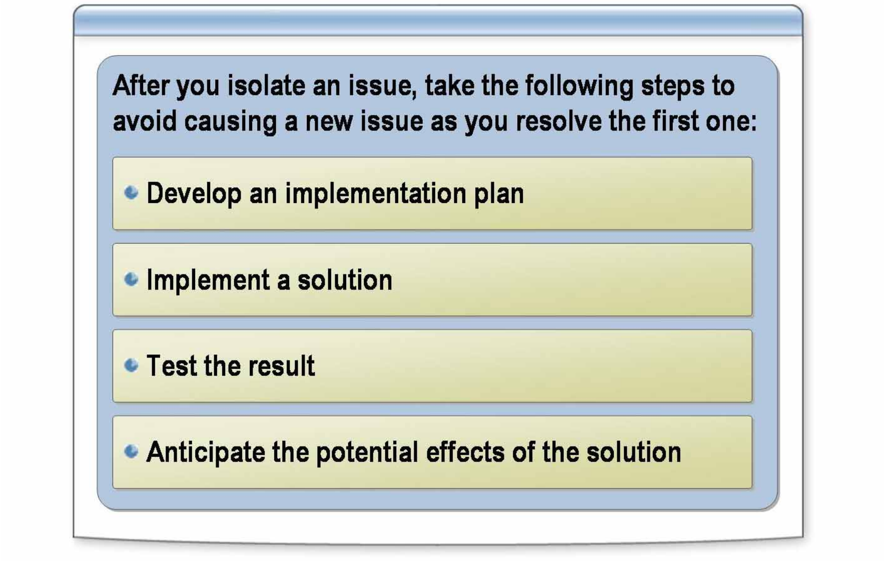
When you look for the causes of a problem, begin with the most obvious possibilities. For example, if a client is unable to communicate with a file server, do not begin by checking the routers between the two systems. Check the simple things on the client first—such as whether the network cable is connected to the computer.

Use the Problem Isolation Flow Chart

The Problem Isolation Flow Chart is located in Appendix C. It begins with simple logon problems and progresses in complexity through problems with client configuration, names resolution, routers, firewalls, and other servers. For example, you can use it to isolate an issue such as a single client not obtaining a Dynamic Host Configuration Protocol (DHCP) address. Following the decision tree, you avoid spending time troubleshooting specific applications or devices such as routers and bridges that apply to more than one computer. Since you know this issue is only applicable to a single computer, the flowchart directs you away from isolation tasks that involve more than one computer.

The flowchart helps you to take the most effective steps in the most logical order to isolate an issue. Using it will help you to determine whether the problem is a local issue that you can fix by yourself, or a broader problem that you will need to escalate.

Resolving the Issue



After you isolate an issue, take the following steps to avoid causing a new issue as you resolve the first one:

- Develop an implementation plan
- Implement a solution
- Test the result
- Anticipate the potential effects of the solution

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

Introduction

After you have isolated the source of an issue, you must decide how to resolve it. You can probably fix a simple problem on a client immediately. A larger issue, such as a problem that involves multiple servers that serve hundreds of clients, could require help and cooperation from several groups in your organization.

Develop an implementation plan

After you identify the problem and find a solution that has been tested on one or more computers, you might need an implementation plan if the solution will be deployed across your organization, possibly involving hundreds or thousands of computers. Coordinate your plan with managers and staff members in the affected areas to verify that the schedule does not conflict with important activities.

Your plan can include:

- Estimates of the time and resources that will be needed.
- Provisions for troubleshooting during off-peak work hours.
- A schedule to divide the work into stages over the necessary period.
- Substitute hardware, if the failing equipment performs a vival role, to be used until the equipment can be fixed.

As the number of users grows; the potential loss of productivity due to disruption increases. Your plan must account for dependencies, allow for last-minute changes, and include contingency plans for unforeseen circumstances.

Implement a solution

After you have isolated the problem to a particular piece of equipment, you can try to determine whether it is being caused by hardware or software. If it is a hardware problem, you might try replacing the unit that is at fault. For example: communication problems might force you to try replacing network cables until you find one that is faulty. If the problem is in a server, you might need to replace components (such as hard drives) until you find the failing piece. If you determine that the problem is caused by software, you can try storing data or running an application on a different computer, or try reinstalling the software on the client that has the problem.

Test the resolution

When the issue has been resolved, you should return to the beginning of the process and repeat the task that originally revealed the problem. If the problem no longer occurs, test all of the other functions that are related to the changes that you made, this ensures that in fixing one problem you did not create a new one.

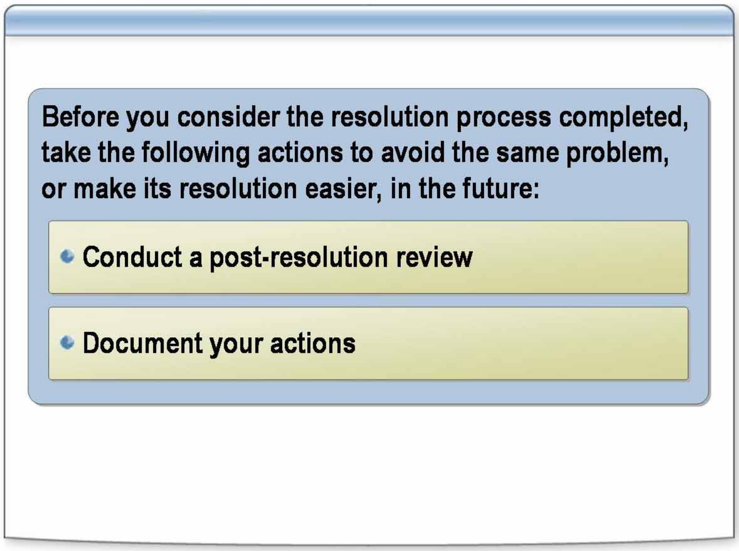
It is at this point that the time you spent documenting the isolation process shows its value. You should repeat exactly the procedures that you used to duplicate the problem, to ensure that the problem the user originally experienced has been completely eliminated and not just temporarily masked. If the problem was intermittent to begin with, it may take some time to ascertain whether your solution has been effective. You might need to check with the user several times to make sure that the problem is not reoccurring.

Anticipate the potential effects of the solution

It is important, throughout the troubleshooting process, to keep an eye on the big network picture, and not to let yourself become too involved in the problems experienced by only one user. It is sometimes possible, while implementing a solution to one problem, to create another problem that is more severe or that affects more users.

For example, if users on one subnet are experiencing high traffic levels that reduce their client performance, you might be able to remedy the problem by connecting some of their computers to a different subnet. However, although this solution might help the users with the original problem, you might overload another subnet in the process, causing a new problem that is more severe than the first one. You could consider a more far-reaching solution instead, such as creating a new subnet and then moving some of the affected users to that new subnet.

After the Issue Is Resolved



Before you consider the resolution process completed, take the following actions to avoid the same problem, or make its resolution easier, in the future:

- Conduct a post-resolution review
- Document your actions

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

Introduction

When the network is functioning normally again, it is a good investment of time to review and document just what has happened, in order to avoid (or at least to minimize the impact of) similar problems in the future.

Conduct a post-resolution review

Starting with your compiled documentation, conduct a post-troubleshooting review with the concerned parties, during which they can help you to pinpoint troubleshooting areas that need improvement. Some questions that you might ask during this self-evaluation period include:

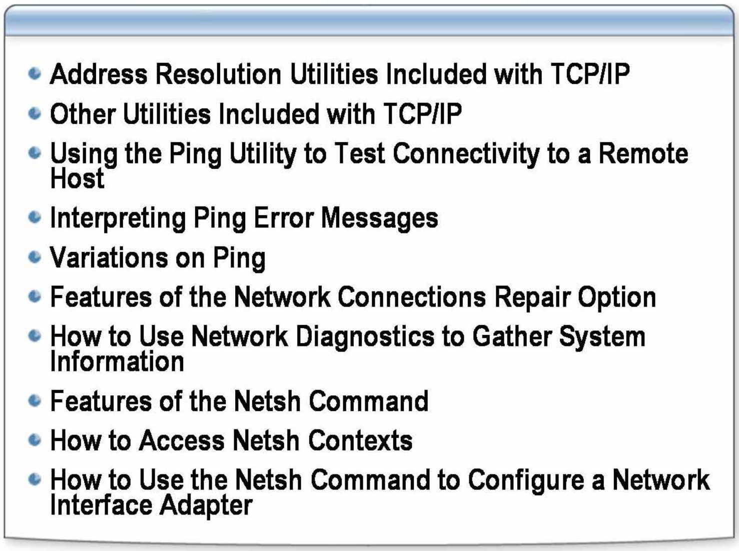
- What changes resulted in improvements?
- What changes made the problem worse?
- Was system performance restored to expected levels?
- What work was redundant or unnecessary?
- How effectively were technical support resources used?
- What utility or information was not used that might have helped?
- What unresolved issues require further root-cause analysis?

When it is practical, you should also explain to the user both *what* happened, and *why* it happened. The most important aspect of this conversation is letting the user know whether their actions caused the problem, exacerbated it, or made it more difficult to resolve. Such conversations can make the resolution of future issues significantly easier.

Compile your notes

The final phase of resolving the issue is to condense your notes and documentation into a concise description of both the problem and its resolution for inclusion in your service history database.

Lesson: Network Utilities That You Can Use to Isolate Connectivity Issues



- Address Resolution Utilities Included with TCP/IP
- Other Utilities Included with TCP/IP
- Using the Ping Utility to Test Connectivity to a Remote Host
- Interpreting Ping Error Messages
- Variations on Ping
- Features of the Network Connections Repair Option
- How to Use Network Diagnostics to Gather System Information
- Features of the Netsh Command
- How to Access Netsh Contexts
- How to Use the Netsh Command to Configure a Network Interface Adapter

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

Introduction

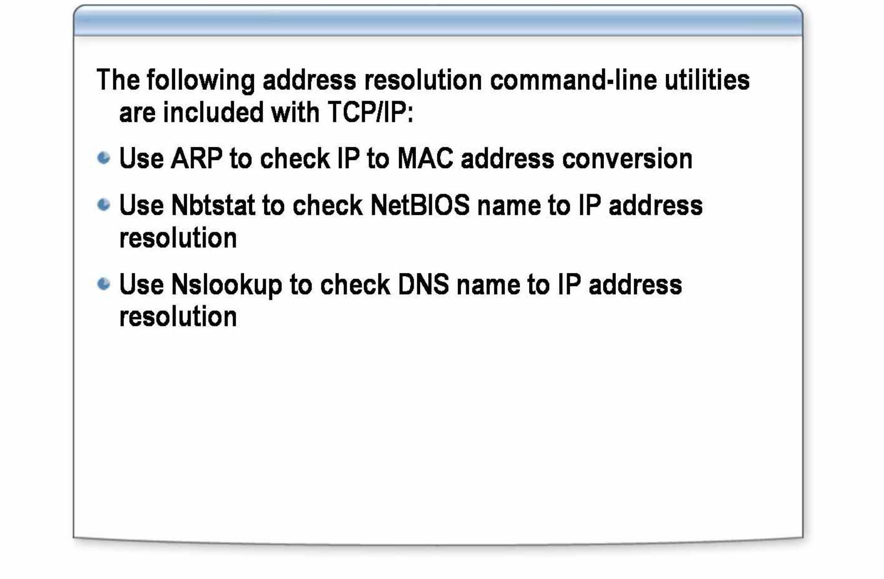
Windows Server 2003 automatically installs most of the utilities that you need for isolating network problems when you install the operating system. There are several additional utilities that you can install from the Windows Server 2003 compact disc (CD) when you need them.

Lesson objectives

After completing this lesson, you will be able to:

- Use the network utilities that you need for isolating connectivity issues.
- Analyze the output from the utilities to help you isolate connectivity issues.

Address Resolution Utilities Included with TCP/IP



The following address resolution command-line utilities are included with TCP/IP:

- Use ARP to check IP to MAC address conversion
- Use Nbtstat to check NetBIOS name to IP address resolution
- Use Nslookup to check DNS name to IP address resolution

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

Introduction

You can use three of the utilities included with the Transmission Control Protocol / Internet Protocol (TCP/IP) to test whether IP addresses are being converted to MAC addresses, Network Basic Input/Output System (NetBIOS) names are being converted to IP addresses, and Domain name System (DNS) names are being converted to IP addresses.

Use Arp to check IP to MAC address conversion

The Address Resolution Protocol (ARP) converts IP addresses to the MAC addresses that data-link layer protocols require in order to transmit frames. To minimize the amount of network traffic ARP generates, the client stores the resolved hardware addresses in a cache in system memory. The information remains in the cache for a short period of time (usually between 2 and 10 minutes), in case the computer has additional packets to send to the same address.

The Arp utility is used to manipulate the contents of the ARP cache. For example, you can use Arp.exe to add to the cache the hardware addresses of hosts that you contact frequently, thus saving both time and network traffic during the connection process. Addresses that you add to the cache manually are static, meaning that they are not deleted after the usual expiration period. The cache is stored in memory only, however, so it is erased each time that you restart your client.

If you want to preload the cache whenever you start your client, you can create a batch file containing Arp.exe commands, and execute the batch file from the Windows Startup group.

Arp.exe uses the following syntax:

```
ARP [-a {ipaddress}] [-n ipaddress] [-s ipaddress hwaddress
{interface}] [-d ipaddress {interface}]
```

- **-a *{ipaddress}*** This parameter displays the contents of the ARP cache. The optional *ipaddress* variable specifies the address of a particular cache entry to be displayed.
- **-n *ipaddress*** This parameter displays the contents of the ARP cache, where *ipaddress* identifies the network interface for which you want to display the cache.
- **-s *ipaddress hwaddress* {*interface*}** This parameter adds a new entry to the ARP cache, where the *ipaddress* variable contains the IP address of the client, the *hwaddress* variable contains the hardware address of the same client, and the *interface* variable contains the IP address of the network interface in the local system for which you want to modify the cache.
- **-d *ipaddress* {*interface*}** This parameter deletes the entry in the ARP cache that is associated with the host represented by the *ipaddress* variable. The optional *interface* variable specifies the cache from which the entry should be deleted.

An ARP table as displayed by Arp.exe, appears as follows:

```
Interface: 192.168.2.6 on Interface 0x1000003
  Internet Address    Physical Address      Type
  192.168.2.10        00-50-8b-e8-39-7a     dynamic
  192.168.2.99        08-00-4e-a5-70-0f     dynamic
```

Use Nbtstat to check NetBIOS to IP address resolution

You can use the Nbtstat command-line utility to isolate NetBIOS name resolution problems. For example, use **nbtstat –n** to determine whether a specific NetBIOS name is registered.

When a network is functioning correctly, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses. NetBT uses several options for NetBIOS name resolution, including local cache lookup, Windows Internet Naming Service (WINS) server query, broadcast, LMHOSTS lookup, HOSTS lookup, and DNS server query.

You can use Nbtstat to display a variety of information, including:

- NetBT protocol statistics.
- NetBIOS name tables both for the local client and for remote hosts.
  The NetBIOS name table is the list of NetBIOS names that corresponds to NetBIOS applications running on the client.
- The contents of the NetBIOS name cache. The NetBIOS name cache is the table that contains NetBIOS name–to–IP address mappings.

You can also use Nbtstat to refresh both the NetBIOS name cache and the names registered with WINS. The following output is an example of output created by using Nbtstat:

```
C:\Documents and Settings\Administrator>nbtstat -c

Local Area Connection:
Node IpAddress: [192.168.0.5] Scope Id: []

                  NetBIOS Remote Cache Name Table

   Name               Type       Host Address     Life [sec]
------------------------------------------------------------
   MYLONDON     <03>  UNIQUE     192.168.0.200    -1
   MYLONDON     <00>  UNIQUE     192.168.0.200    -1
   MYLONDON     <20>  UNIQUE     192.168.0.200    -1
```

Use Nslookup to check DNS name to IP address resolution

Nslookup enables you to generate DNS request messages and also to transmit them to specific DNS servers on the network. Use Nslookup to determine what IP address a particular DNS server has associated with a host name. The basic syntax of nslookup is as follows:

NSLOOKUP *DNSname DNSserver*

- ***DNSname*** Specifies the DNS name that you want to resolve.
- ***DNSserver*** Specifies the DNS name or IP address of the DNS server that you want to query for the name specified in the *DNSname* variable.

The output generated by the utility looks like the following sample.

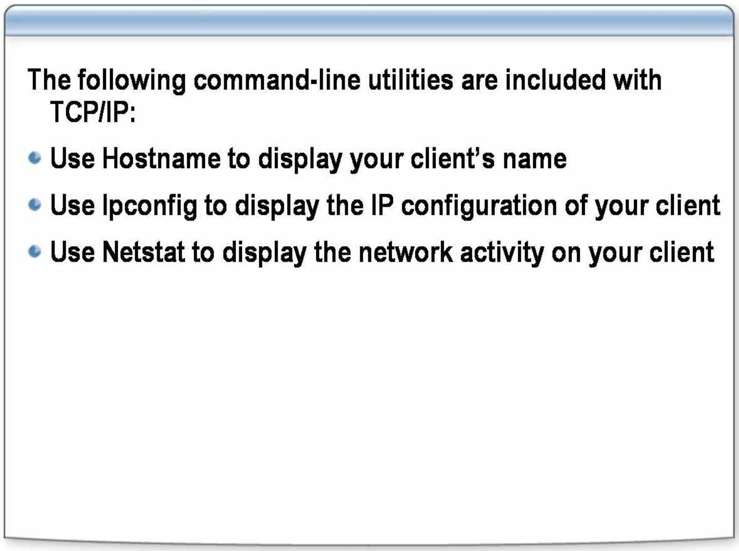
```
C:\>nslookup microsoft.com
Server:  dns1.rcsntx.sbcglobal
Address:  151.164.1.8

Non-authoritative answer:
Name:    microsoft.com
Address:  207.46.249.222
```

The output sample shows that when queried, the dns1.rcsntx.sbcglobal.net DNS server returns 207.46.249.222 as the IP address associated with microsoft.com.

The advantage of Nslookup is that you can test the functionality and the quality of the information on a specific DNS server by specifying it on the command line.

Other Utilities Included with TCP/IP



The following command-line utilities are included with TCP/IP:

- Use Hostname to display your client's name
- Use Ipconfig to display the IP configuration of your client
- Use Netstat to display the network activity on your client

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

Introduction

When Windows Server 2003 is installed, it automatically includes the TCP/IP protocol, as well as numerous utilities that you can use to monitor TCP/IP and to check how well it is functioning.

The most commonly used utilities are described in the following paragraphs.

Use Hostname to display your client's name

The Hostname utility displays the host name that is assigned to your client. By default, the host name is the computer name of your client.

Use Ipconfig to display the IP configuration of your client

You can use the Ipconfig command-line utility both to display the current configuration of the installed IP stack on a networked computer and to refresh DHCP and DNS settings. Ipconfig will:

- Display current TCP/IP network configuration values.
- Update or release DHCP allocated leases.
- Display, register, or flush DNS names.

Ipconfig is most useful for managing computers that obtain an IP address automatically, such as by using DHCP or Automatic Private IP Addressing (APIPA).

Use Netstat to display the network activity on your client

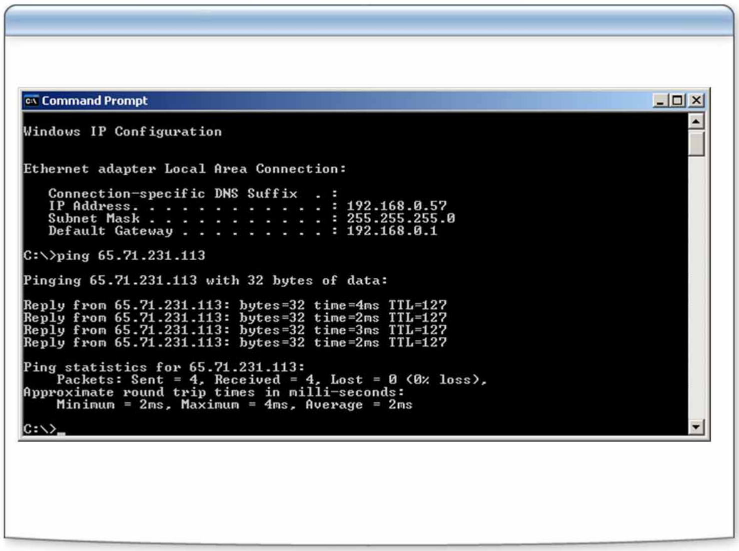
Netstat displays information both about the current network connections of a client running TCP/IP and about the traffic generated by the various TCP/IP protocols. Use Netstat when you want to determine if a port is available or in use. The network connection listing displayed by netstat on a Windows Server 2003 computer appears as follows:

```
C:\>netstat

Active Connections

  Proto  Local Address        Foreign Address      State
  TCP    bottxp:990           localhost:3124       ESTABLISHED
  TCP    bottxp:999           localhost:3127       ESTABLISHED
  TCP    bottxp:1024          localhost:3040       ESTABLISHED
  TCP    bottxp:3040          localhost:1024       ESTABLISHED
  TCP    bottxp:3119          localhost:7438       ESTABLISHED
  TCP    bottxp:3120          localhost:5679       ESTABLISHED
  TCP    bottxp:3124          localhost:990        ESTABLISHED
  TCP    bottxp:3125          localhost:5678       ESTABLISHED
  TCP    bottxp:3126          localhost:5678       ESTABLISHED
  TCP    bottxp:3127          localhost:999        ESTABLISHED
  TCP    bottxp:5678          localhost:3125       ESTABLISHED
  TCP    bottxp:5678          localhost:3126       ESTABLISHED
  TCP    bottxp:5679          localhost:3120       ESTABLISHED
  TCP    bottxp:7438          localhost:3119       ESTABLISHED
  TCP    bottxp:3098          etcdaldc1:4092       ESTABLISHED
```

Using the Ping Utility to Test Connectivity to a Remote Host



```
Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.0.57
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\>ping 65.71.231.113

Pinging 65.71.231.113 with 32 bytes of data:

Reply from 65.71.231.113: bytes=32 time=4ms TTL=127
Reply from 65.71.231.113: bytes=32 time=2ms TTL=127
Reply from 65.71.231.113: bytes=32 time=3ms TTL=127
Reply from 65.71.231.113: bytes=32 time=2ms TTL=127

Ping statistics for 65.71.231.113:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\>_
```

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

Introduction

The Ping utility and its variations are some of the most frequently used TCP/IP utilities. You can use Ping as your primary utility for isolating IP-level connectivity between two hosts. When it is used to isolate connectivity issues, Ping tests are done on successively more distant hosts until a failure is discovered. Use the following series of Ping commands to test connectivity between the local computer and a remote host.

Testing connectivity to a remote host

The following steps describe how to use the Ping utility to perform progressively more distant tests on your network connectivity.

1. Ping the loopback address—type **ping 127.0.0.1**

   Successfully pinging the loopback address verifies that TCP/IP is both installed on and correctly configured on the local client. If the loopback test fails, the IP stack is not responding. Lack of response can occur if the TCP drivers are corrupted, if the network adapter is not working, or if another service is interfering with IP. Open Event Viewer, and look for problems reported by Setup or by the TCP/IP service.

2. Ping the local client—type **ping <*IP address of local client*>**

   Successfully pinging the IP address of the local client verifies that the client was correctly added to the network. If you cannot successfully ping the local IP address after successfully pinging the loopback address, check that the local client's IP address is a valid IP address, check the routing table, and check the network adapter driver.

3. Ping the default gateway on the local computer—type **ping <*IP address of the default gateway*>**

   Successfully pinging the default gateway of the local client verifies both that the default gateway is functioning and that you can communicate with a local host on the local subnet. If you cannot successfully ping the default gateway after successfully pinging the local client, check the default gateway.

4. Ping the IP address of another computer or network device located on a remote network—type **ping** ***<IP address of remote host>***

   Successfully pinging the IP address of the remote host verifies that the local client can communicate with the remote host through a router. If the remote host is located across a high-delay link (such as a satellite link), try using the **-w** (wait) parameter to specify a longer time-out period than the default time-out of four seconds.

   If you cannot successfully ping the remote host IP address after successfully pinging the default gateway, this can indicate that the remote host is not responding, or that there is a problem in the network hardware between the source host and the destination host. To rule out the possibility of a problem in the network hardware, ping a different remote host on the same subnet where the first remote host is located.

5. Ping the host name of another host on a remote network—type **ping** ***<host name of remote host>***

   Successfully pinging the name of a remote host verifies that ping can resolve the remote host name to an IP address. If you cannot successfully ping the remote host name after successfully pinging the IP address of the remote host, the problem is host name resolution, not network connectivity. When pinging the host name of the target host, ping attempts to resolve the name to an address (first through a DNS server, and next through a WINS server, if one is configured), and then attempts a local broadcast. Check TCP/IP properties to see whether the client has DNS server and WINS server addresses configured, either typed manually or assigned automatically. If DNS server and WINS server addresses are configured in TCP/IP properties, and if they appear when you type **ipconfig /all**, then try pinging the server addresses to ascertain whether they are accessible.

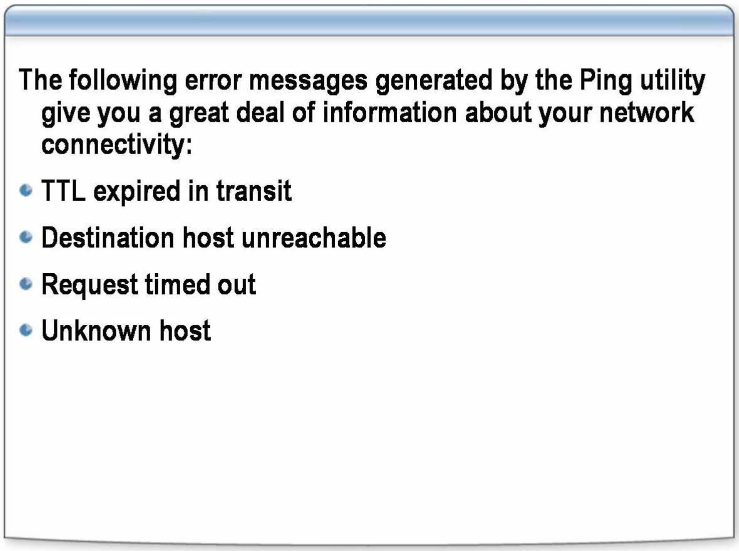
   On a network that uses DNS for name resolution, if the name entered is not a fully qualified domain name (FQDN), the DNS name resolver appends the computer's domain name or names to generate the FQDN. Name resolution might fail if you do not use an FQDN for a remote name. These requests fail because the DNS name resolver appends the local domain suffix to a name that resides elsewhere in the domain hierarchy.

6. Temporarily turn off IPSec—retry all of the preceding ping commands.

   If none of the preceding ping commands are successful, check whether IP Security (IPSec) is enabled. If IPSec is enabled locally, temporarily stop the IPSec Services service in the Services snap-in, and then try pinging again. If network connectivity between hosts works after you stop IPSec, ask the security administrator to troubleshoot the IPSec policy.

Note For more information about IPSec, see Module 8, "Securing Network Traffic by Using IPSec and Certificates," in Course 2277*, Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure: Network Services.*

Interpreting Ping Error Messages



The following error messages generated by the Ping utility give you a great deal of information about your network connectivity:

- TTL expired in transit
- Destination host unreachable
- Request timed out
- Unknown host

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

Introduction

Each time you ping a host, ping will display a message showing the result, either a successful response or an error message. The type of error is a good clue as to the source of a connectivity problem.

TTL expired in transit

This message indicates that the number of hops required to reach the destination exceeds the TTL (time to live) set by the sending host to forward the packets. The default TTL value for Internet Control Message Protocol (ICMP) Echo Requests sent by Ping is 128. In some cases, this is not enough to travel the required number of links to a destination. You can increase the TTL by using the -i switch, up to a maximum of 255 links.

If increasing the TTL value fails to resolve the problem, the packets are being forwarded in a routing loop, a circular path among routers.

Use Tracert to track down the location of the routing loop, which appears as a repeated series of the same IP addresses in the Tracert report. Next, make an appropriate change to the routing tables, or inform the administrator of a remote router of the problem.

Destination host unreachable

This message indicates one of two problems: either the local client has no route to the desired destination, or a remote router reports that *it* has no route to the destination. The form of the message can distinguish the two problems. If the message is simply Destination Host Unreachable, then there is no route from the local client, and the packets to be sent were never put on the network. Use the Route utility to check the local routing table for either a direct route to the destination or a default gateway.

If the message is “Reply From <*IP address*>: Destination Host Unreachable,” then the routing problem occurred at a remote router.

Request timed out

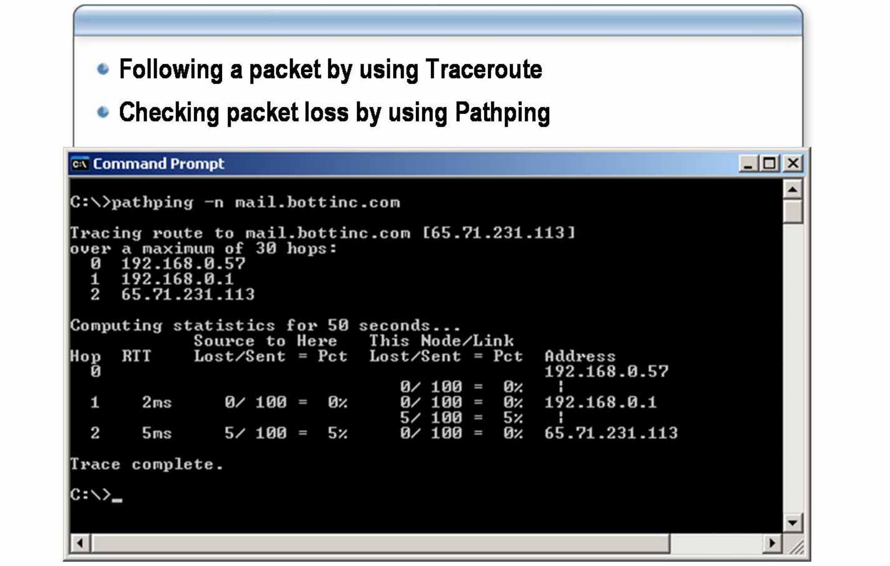
This message indicates that the Echo Reply messages were not received within the designated time-out period. By default, the Ping utility waits four seconds for each response to be returned before timing out. If the remote system pinged is across a high-delay link (such as a satellite link), responses might take longer to be returned. Use the **-w** (wait) switch to specify a longer time-out period.

To check for network congestion, simply increase the allowed latency by setting a higher wait time (such as 5000 milliseconds) by using the **-w** switch. Try to ping the destination again. If the request still times out, congestion is not the problem; an address resolution problem or a routing error is more likely the issue.

Unknown host

This error message appears as "Ping request could not find host <*host name*>. Please check the name and try again." It indicates that the requested host name cannot be resolved to its IP address; check that the name is entered correctly, and that the DNS servers can resolve it.

Variations on Ping



- Following a packet by using Traceroute
- Checking packet loss by using Pathping

```
C:\>pathping -n mail.bottinc.com

Tracing route to mail.bottinc.com [65.71.231.113]
over a maximum of 30 hops:
  0  192.168.0.57
  1  192.168.0.1
  2  65.71.231.113

Computing statistics for 50 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           192.168.0.57
                                0/ 100 =  0%   |
  1    2ms     0/ 100 =  0%     0/ 100 =  0%  192.168.0.1
                                5/ 100 =  5%   |
  2    5ms     5/ 100 =  5%     0/ 100 =  0%  65.71.231.113

Trace complete.

C:\>_
```

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

Introduction

Traceroute (tracert) is a variant of the Ping utility that displays the route that packets take to a destination, in addition to the usual Ping messages. Traceroute can show how far your packets are going before they run into a problem. Pathping combines features of both Ping and Traceroute to obtain additional information about router performance and link reliability that is not available to either of those tools.

Following a packet by using Traceroute

Because of the nature of IP routing, paths through an internetwork can change from minute to minute. Traceroute displays a list of the routers that are currently forwarding packets to a specified destination.

Traceroute uses ICMP Echo and Echo Reply messages in the same way as Ping does, but it modifies the messages by changing the value of the TTL field in the IP header. The TTL field is designed to prevent packets from getting caught in router loops that keep them circulating endlessly around the network. The computer generating the packet normally sets a relatively high value for the TTL field; on Windows systems, the default value is 128. Each router that processes the packet reduces the TTL value by one. If the TTL value reaches zero, the last router discards the packet and transmits an ICMP error message back to the original sender.

When you start Traceroute by using the tracert command with the name or IP address of a target computer, the utility generates its first set of Echo Request messages with TTL values of 1. When the messages arrive at the first router on their path, the router decrements their TTL values to 0, discards the packets, and reports the errors to the sender. The error messages contain the router's address, which Traceroute displays as the first hop in the path to the destination. Traceroute's second set of Echo Request messages use a TTL value of 2, causing the second router on the path to discard the packets and generate error messages. The Echo Request messages in the third set have a TTL value of 3, and so on. Each set of packets travels one hop farther than the previous set before causing a router to return error messages to the source. The list of routers displayed by Traceroute as the path to the destination is the result of these error messages.

Checking packet loss by using Pathping

Like Traceroute, Pathping discovers the path to a destination. Pathping sends multiple Echo Request messages to each router between a source and destination over a period of time and then computes results based on the packets returned from each router. Because Pathping displays the degree of packet loss at any given router or link, you can determine which routers or subnets might be having network problems. Pathping performs the equivalent of Traceroute by identifying which routers are on the path. It then pings all of the routers over a specified time period and computes statistics based on the value returned from each router.

The path data reported by Pathping includes:

- Information on the intermediate routers visited on the path.
- The round-trip time (RTT) value.
- Link loss information.

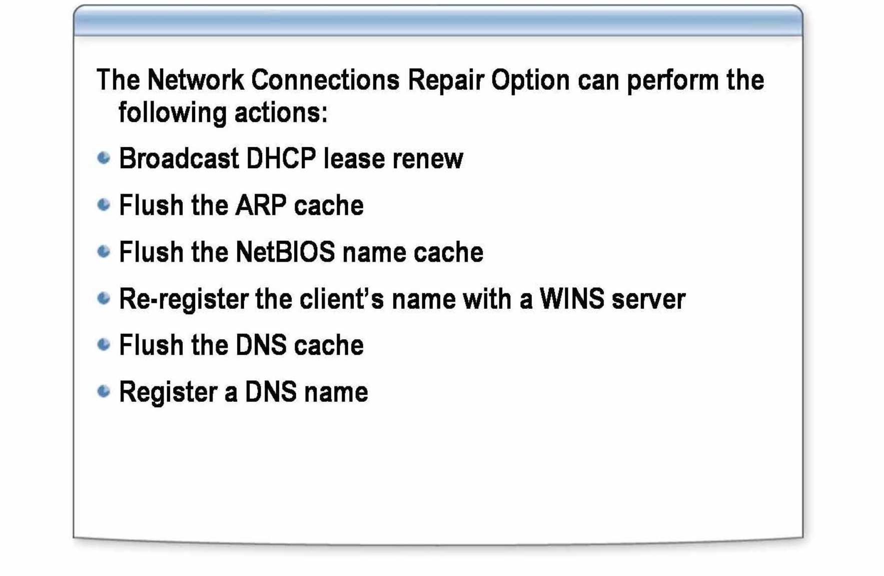
```
C:\Documents and Settings\Administrator>pathping microsoft.com

Tracing route to microsoft.com [207.46.249.27]
over a maximum of 30 hops:
  0  londonsbs [192.168.0.57]
  1  192.168.0.1
  2  adsl-65-71-231-118.dsl.rcsntx.swbell.net [65.71.231.118]
  3     *     dist1-vlan130.rcsntx.swbell.net
[151.164.162.130]
  4  bb1-g1-0.rcsntx.swbell.net [151.164.1.174]
  5     *     core1-6-0.crdltx.sbcglobal.net [151.164.240.66]
  6  core1-p11-0.crhnva.sbcglobal.net [151.164.243.218]
  7     *     bb1-p10-0.hrndva.sbcglobal.net [151.164.242.70]
  8  bb1-p6-0.pxvnva.sbcglobal.net [151.164.241.26]
  9     *     asn8075-microsoft.pxvnva.sbcglobal.net
[151.164.89.194]
 10     *     gig0-0.core1.was1.us.msn.net [207.46.33.101]
 11  gig4-2.edge2.ash1.us.msn.net [207.46.34.22]
 12  207.46.34.25
 13  207.46.33.61
 14  207.46.36.214
 15  207.46.155.13
 16     *        *        *
```

```
Computing statistics for 400 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           londonsbs
[192.168.0.57]
                                0/ 100 =  0%   |
  1    2ms     0/ 100 =  0%     0/ 100 =  0%  192.168.0.1
                                0/ 100 =  0%   |
  2   14ms     1/ 100 =  1%     1/ 100 =  1%  adsl-65-71-231-
118.dsl.rcsntx.swbell.net [65.71.231.118]
                                0/ 100 =  0%   |
  3   15ms     1/ 100 =  1%     1/ 100 =  1%  dist1-
vlan130.rcsntx.swbell.net [151.164.162.130]
                                0/ 100 =  0%   |
  4   14ms     0/ 100 =  0%     0/ 100 =  0%  bb1-g1-
0.rcsntx.swbell.net [151.164.1.174]
                                0/ 100 =  0%   |
  5   15ms     0/ 100 =  0%     0/ 100 =  0%  core1-6-
0.crdltx.sbcglobal.net [151.164.240.66]
                                0/ 100 =  0%   |
  6   31ms     0/ 100 =  0%     0/ 100 =  0%  core1-p11-
0.crhnva.sbcglobal.net [151.164.243.218]
                                0/ 100 =  0%   |
  7   30ms     0/ 100 =  0%     0/ 100 =  0%  bb1-p10-
0.hrndva.sbcglobal.net [151.164.242.70]
                                0/ 100 =  0%   |
  8   31ms     0/ 100 =  0%     0/ 100 =  0%  bb1-p6-
0.pxvnva.sbcglobal.net [151.164.241.26]
                                0/ 100 =  0%   |
  9   35ms     0/ 100 =  0%     0/ 100 =  0%  asn8075-
microsoft.pxvnva.sbcglobal.net [151.164.89.194]
                                1/ 100 =  1%   |
 10  ---     100/ 100 =100%    99/ 100 = 99%  gig0-
0.core1.was1.us.msn.net [207.46.33.101]
                                0/ 100 =  0%   |
 11  ---     100/ 100 =100%    99/ 100 = 99%  gig4-
2.edge2.ash1.us.msn.net [207.46.34.22]
                                0/ 100 =  0%   |
 12  ---     100/ 100 =100%    99/ 100 = 99%  207.46.34.25
                                0/ 100 =  0%   |
 13  ---     100/ 100 =100%    99/ 100 = 99%  207.46.33.61
                                0/ 100 =  0%   |
 14  ---     100/ 100 =100%    99/ 100 = 99%  207.46.36.214
                                0/ 100 =  0%   |
 15   62ms     1/ 100 =  1%     0/ 100 =  0%  207.46.155.13
                               99/ 100 = 99%   |
 16  ---     100/ 100 =100%     0/ 100 =  0%  londonsbs
[0.0.0.0]
```

Trace complete.

Features of the Network Connections Repair Option



The Network Connections Repair Option can perform the following actions:

- Broadcast DHCP lease renew
- Flush the ARP cache
- Flush the NetBIOS name cache
- Re-register the client's name with a WINS server
- Flush the DNS cache
- Register a DNS name

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

Introduction

Network Connections Repair Link combines six of the most commonly used TCP/IP troubleshooting commands in one Windows utility.

Running Network Connections Repair Link

Network Connections Repair Link can be accessed in any of three ways:

- Right-click a network connection icon in the Network Connections folder, and then click **Repair**.
- Right-click the information balloon that appears in the system tray when your IP configuration becomes invalid, and then click **Repair**.
- In the **Status** dialog box, click the **Support** tab, and then click **Repair**.

When selecting a network connection, look in the left-hand column (if shown) for the **Repair this connection** link.

The following tasks are performed in the order listed:

Broadcast DHCP lease renew

This is the equivalent of a DHCP broadcast renewal at 87.5% of the lease time. This was chosen because it is far safer than actually doing first a DHCP release and then a DHCP renew. If a DHCP server is unavailable to renew the address, the client keeps its current address. If a new DHCP server comes online, the DHCP server can not acknowledge (NACK) the client and restart the lease process, potentially fixing a client's IP address problem.

Flush the ARP cache

Sometimes an ARP cache entry becomes outdated, and then communication cannot occur again until the bad ARP cache entry expires. It is also possible for a bad static ARP cache entry that never expires to have been placed on the client. The ARP cache is naturally flushed at 2 minute and 10 minute intervals, so this operation is considered safe.

Note If your network relies on static ARP cache entries, make sure that there is a way to reenter the ARP cache addresses after this tool is run.

Flush the NetBIOS name cache

Often the NetBIOS cache can have outdated entries, and then communication cannot occur. The **nbtstat –r** command clears the NetBIOS name cache and then reloads any NetBIOS name entries in the Lmhosts file with the #PRE flag.

Re-register the client's name with a WINS server

The **nbtstat –rr** command is the equivalent of re-registering the client's name with a WINS server. This can be very useful in isolating problems with NetBIOS name resolution.

Note This task simply schedules the name refresh with the operating system; it does not check to determine whether the refresh was successful.

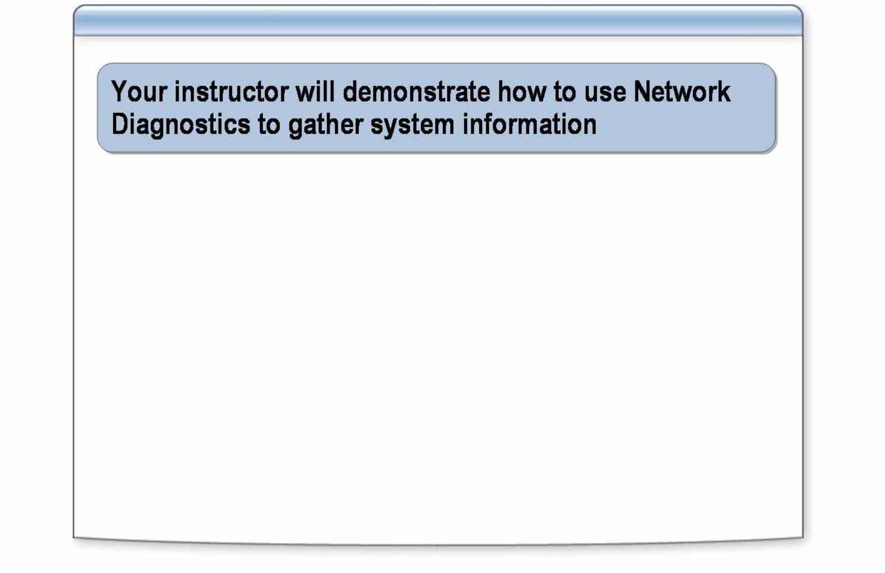
Flush the DNS cache

This task flushes any old or bad DNS cache entries from memory. This can be very useful in isolating problems with DNS name resolution.

Register a DNS name

This task re-registers the client's DNS name with a DNS dynamic update server.

How to Use Network Diagnostics to Gather System Information



Your instructor will demonstrate how to use Network Diagnostics to gather system information

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

Introduction

Network Diagnostics performs a series of tests to gather important information that can help you isolate the causes of network-related issues. Depending on the options you select, it checks your system for network connectivity and whether your network-related programs and services are running. It also gathers basic information about your computer.

Note Most of the utilities that you need to help you isolate network problems are automatically installed when you install Windows Server 2003. You can install Network Diagnostics and many additional Windows Server 2003 support tools from the operating system CD when you need them. After you install the support tools, Netdiag.exe appears in the C:\Program Files\Support Tools folder.

Using Network Diagnostics

Unlike most of the other network utilities, Network Diagnostics is a Windows-based utility rather than a command-line utility.

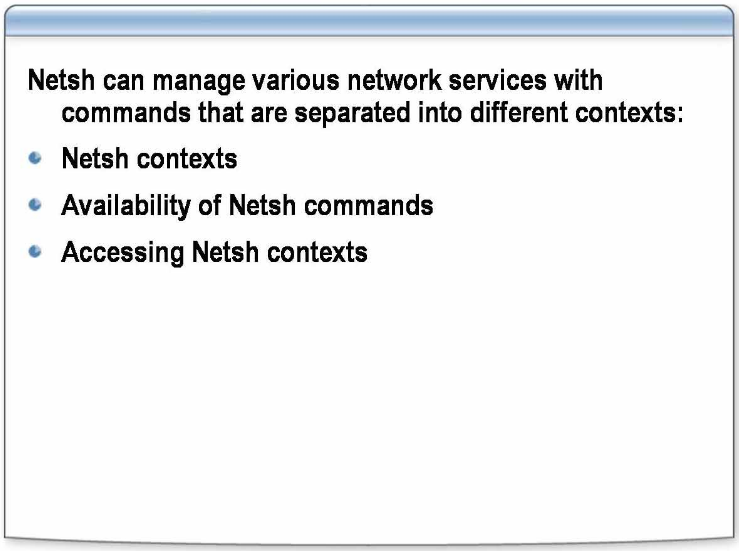
► **To scan your computer using Network Diagnostics**

1. Click **Start**, and then click **Help and Support**.
2. Click **Tools**.
3. Click **Help and Support Center Tools**.
4. Click **Network Diagnostics**.
5. Click **Set scanning options**.

   The list of scanning options appears.
6. Select all available options.
7. Click **Scan your system**.

   Network Diagnostics scans your system to gather information about your hardware, software, and network connections and presents the information as a report in the window.

Features of the Netsh Command



Netsh can manage various network services with commands that are separated into different contexts:

- Netsh contexts
- Availability of Netsh commands
- Accessing Netsh contexts

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

Introduction

Netsh is a command-line scripting interface that runs from a Command Prompt that contains a variety of contexts from which you can type commands. The context is indicated by the netsh prompt, which by default is **netsh>**. The Netsh commands are specifically for managing and monitoring network services such as DHCP, WINS, TCP/IP, and IPSec.

Netsh contexts

Each Netsh context contains the features for managing a specific related set of networking functions. A *Netsh context* is a state in which Netsh accepts commands related to a specific set of functions.

Availability of Netsh commands

Some commands are available only within a specific context. Some commands are available not only in the context shown in the command lists, but also in all subcontexts (if any exist) below that context.

Global commands work in all contexts. Some of these, like the help command, produce different results in different contexts. Others, such as add helper (used to load a new Helper dynamic link library [DLL] into Netsh) always produce the same result in Netsh, no matter which context you are working in.

Accessing Netsh contexts

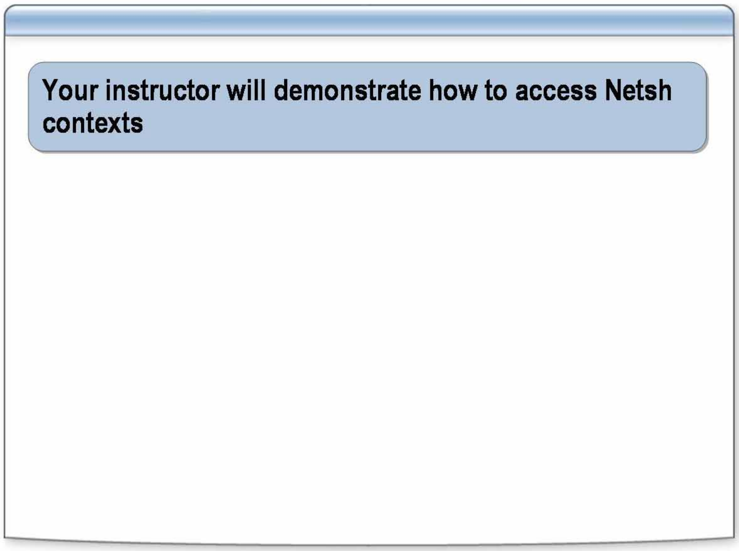
Contexts are arranged in a hierarchy. At the top of the context hierarchy is the Netsh root context. The following table lists the contexts and subcontexts in hierarchical order, in addition to the Helper DLL that provides each context. The **show helper** command in Netsh displays this information.

Context	Subcontext	Subcontext
aaaa		
diag		
dhcp		
	server	
		mscope
		scope
interface		
	ip	
ras		
	aaaa	
	appletalk	
	ip	
routing		
	ip	
		autodhcp
		dnsproxy
		igmp
		nat
		ospf
		relay
		rip
		routerdiscovery
wins		
	server	

You can change to another context by typing the name of the context (for example, **interface**) at the **netsh>** prompt. Your command prompt changes to match the context entered. If you are already in a context, you can go to a subcontext by typing the name of the subcontext (for example, **ip**).

Contexts are provided by Helper DLLs. If you cannot access a specific context, follow the instructions in Helper DLLs to make sure that the files for that context are loaded.

How to Access Netsh Contexts



Your instructor will demonstrate how to access Netsh contexts

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

Introduction

Related Netsh commands are grouped into contexts. In order to run a Netsh command, you must first invoke Netsh and then change to the context that contains the desired command.

Using Netsh command contexts

To access the Netsh command contexts:

1. Open a command prompt window, and enter **netsh** at the command prompt as shown:

   ```
   C:\>netsh
   ```

   Netsh becomes the active command line interpreter, or *shell*, and the command prompt changes to:

   ```
   netsh>
   ```

   At this point, you are in the root context of Netsh, and you can use a limited number of Netsh global commands.

2. To change to one of the Netsh contexts, such as the IP context under the Routing context, enter the context path at the Netsh prompt as shown:

   ```
   netsh>routing ip
   ```

   Netsh routing ip becomes the active context, and the command prompt changes to:

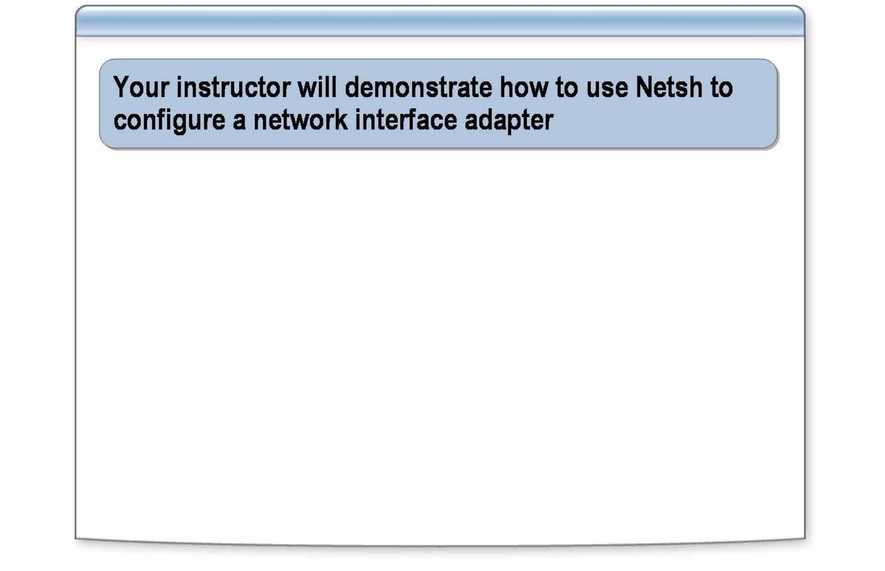
   ```
   netsh routing ip>
   ```

3. Enter a command that is available in the current context (such as the **set interface** command, which sets the specified IP interface mode):

   ```
   netsh routing ip>set interface name="Beta Network"
   state=enable
   ```

4. To move up the context hierarchy, type **..** (two periods), and then press ENTER.

How to Use the Netsh Command to Configure a Network Interface Adapter



Your instructor will demonstrate how to use Netsh to configure a network interface adapter

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

Introduction

The Netsh command provides you with the ability to change between static and dynamic IP addresses on a network interface adapter.

Using Netsh to configure a network interface adapter for static IP

To use the Netsh command to configure a network interface adapter to use a static IP address:

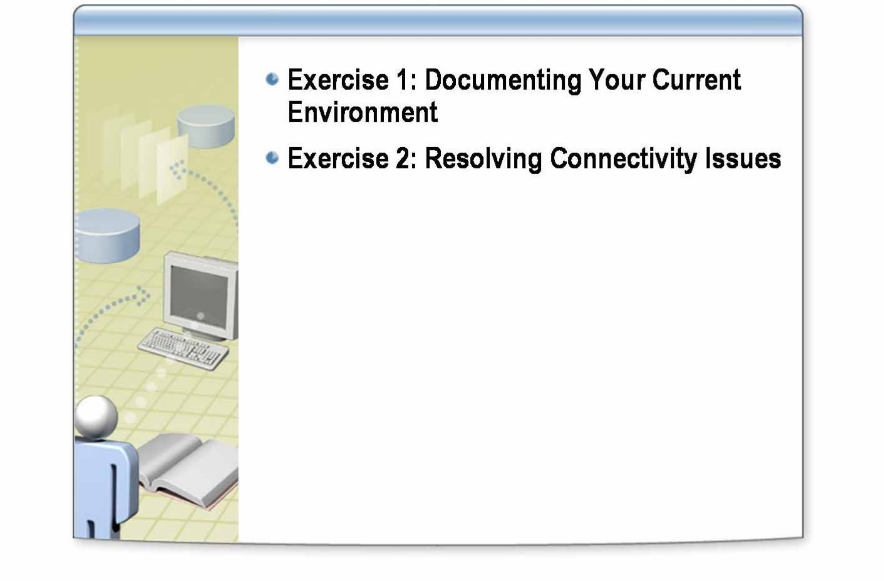
1. Open a command prompt.
2. To verify that you are currently using DHCP on your computer, type **ipconfig /all** and then press ENTER. The DHCP enabled=Yes message is displayed.
3. At the command prompt, type **netsh interface ip set address name="***interface_name***" source=static addr=192.168.***x***.***y* **mask=255.255.255.0** (where *interface_name* is the name of your local area connection, *x* is the network number, and *y* is the student number provided by your instructor), and then press ENTER.

Using Netsh to configure a network interface adapter for dynamic IP

To use the Netsh command to configure a network interface adapter to use a dynamic IP address:

1. Open a command prompt.
2. Verify that you are now using a static IP address on your computer by typing **ipconfig /all** and then pressing ENTER. The DHCP enabled=No message is displayed.
3. At the command prompt, type **netsh interface ip set address name="***interface_name***" source=dhcp** and then press ENTER.
4. Verify that your network interface is configured to obtain an IP address automatically by typing **ipconfig /all** and pressing ENTER. The DHCP enabled=Yes message is displayed.

Lab A: Isolating Common Connectivity Issues



- Exercise 1: Documenting Your Current Environment
- Exercise 2: Resolving Connectivity Issues

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

Objectives

After completing this lab, you will be able to isolate common connectivity issues using a troubleshooting flow chart.

Prerequisites

Before working on this lab, you must have knowledge of TCP/IP configuration settings on a client computer running a Windows operating system.

Scenario

This lab consists of four scenarios. Each scenario outlines a connectivity issue that you will need to resolve. You will use the Network Connectivity Job Aid to isolate client connectivity issues. In each scenario, you will execute a batch file that will introduce an issue into the system. You will then work through a series of steps to isolate and fix the issue.

Note To view the Problem Isolation Flow Chart, see Appendix C.

Lab answers

The detailed steps for this lab—along with the answers to the questions—are found at the end of this lab.

Estimated time to complete this lab: 60 minutes

Exercise 0 Lab Setup

In order to successfully complete this lab, you must add two environment variables to your computer and rename the network adapter icon in network connections. The environment variables are used in the batch files to create and undo the scenarios. For example, to reset your IP address, a batch file is run that has your IP address as part of a command. The environment variables supply the part of the network ID and the host ID for the batch file.

Tasks	Detailed steps
1. Set environment variables.	**a.** Log on as administrator with a password of **P@ssw0rd**. **b.** Click **Start**, point to **Control Panel**, and then click **System**. **c.** Click the **Advanced** tab, and then click **Environment Variables**. **d.** In the **System Variables** box, click **New**. **e.** In the **Variable name** box, type **mochost** and then, in the **Variable value** box, type the number of your host address according to the following table. **f.** Click **OK**. **g.** Repeat steps c through e, using **mocnet** as the variable name and the network number *x* (where *x* is the number of the classroom) as the variable value.
Note: The environment variables are single integers, not IP addresses. The mochost environment variable is an integer from 11 to 34 according to the table below. The mocnet variable is also a single integer that corresponds to the classroom number, for example 5.	
1. (*continued*)	**h.** To close the **Environment Variables** dialog box, click **OK**. **i.** To close the **System Properties** dialog box, click **OK**.
2. Name your LAN connection moclan.	**a.** Click **Start**, point to **Control Panel**, right-click **Network Connections**, and then click **Open**. **b.** Right-click your primary network connection, and then click **Rename**. **c.** Type **moclan** and then press ENTER.
3. Enable DHCP.	**a.** Click **Start**, point to **Control Panel**, point to **Network Connections**, and then click **MOCLAN**. The **MOCLAN Status** dialog box appears. **b.** Click **Properties**. The MOCLAN Properties dialog box appears. **c.** Click **Internet Protocol (TCP/IP)**, and then click **Properties**. The Internet Protocol (TCP/IP) Properties dialog box appears. **d.** Click **Obtain an IP address automatically**. **e.** Click **Obtain DNS server address automatically**, and then click **OK**. **f.** To close the **MOCLAN Properties** dialog box, click **Close**. **g.** To close the **MOCLAN Status** dialog box, click **Close**.

4. Close all windows.	▪ Close all windows and log off.
5. Log on as *Computer*User	▪ Log on as NWTRADERS\ComputerUser (where *Computer* is the name of your computer).

Computer Name	MOCHOST Value
Vancouver	11
Denver	12
Perth	13
Brisbane	14
Lisbon	15
Bonn	16
Lima	17
Santiago	18
Bangalore	19
Singapore	20
Casablanca	21
Tunis	22
Acapulco	23
Miami	24
Auckland	25
Suva	26
Stockholm	27
Moscow	28
Caracas	29
Montevideo	30
Manila	31
Tokyo	32
Khartoum	33
Nairobi	34

Exercise 1
Documenting Your Current Environment

As you run the scripts to introduce scenarios, you may be changing the configuration settings of your computer in order to solve the issue. At the end of each scenario, you will reset your computer. Document your configuration settings by completing the following table, and refer to this table to verify that settings are correctly configured after resetting your computer.

Item	Configuration
Your network number	
Your computer's IP address	
Your default gateway	
Your primary DNS Server	
Your secondary DNS Server	
Your WINS Server	
Your computer's NetBT node type	
Remote address (an address outside your local network)	

Exercise 2
Resolving Connectivity Issues

This lab consists of four scenarios. Each scenario outlines a connectivity issue that you will need to resolve. You will use the Problem Isolation Flow Chart in Appendix C to isolate client connectivity issues. In each scenario, you will execute a batch file that will introduce an issue into the system. You will then work through a series of steps to isolate and fix the issue.

Scenario 1: Resolving a Request Timed Out Connectivity Issue

A customer has logged a helpdesk request stating that he cannot access any network resources. He is receiving a Request timed out error. You are working at the user's computer to isolate the connectivity issue and either resolve it yourself or escalate it to a system engineer.

Tasks	Specific Instructions
1. Introduce the problem.	▪ Using administrator credentials, run **c:\moc\2276\labfiles\s1.bat**.
2. Isolate the issue.	**a.** Use the Ping utility to send an echo request to localhost. **b.** Ping London. **c.** Verify your own IP configuration.
❓ After you pinged localhost, did the TCP/IP stack function properly? ____________________	
❓ After you pinged London, did you receive a successful reply? ____________________	
❓ When you verified your own IP configuration, was it correct? If not, what was the issue? ____________________ ____________________	
3. Correct the problem.	▪ Navigate to **Network Connections** in Control Panel, use moclan and correct the problem.
4. Reset the computer configuration.	▪ Using administrator credentials, run **c:\moc\2276\labfiles\r1.bat**.

Scenario 2: User Cannot Access Any Network Resources

A user complains that he cannot access any network resource. He mentioned seeing a dialog box, stating something about a duplicate IP address on the network.

Tasks	Specific Instructions
1. Introduce the problem.	▪ Using administrator credentials, run **c:\moc\2276\labfiles\s2.bat**.
2. Isolate issues associated with this scenario.	**a.** Review the IP configuration information by using **ipconfig /all**. **b.** Determine whether DHCP is enabled. **c.** Verify that the ARP cache lists a network interface adapter. **d.** Isolate the issue.
❓ Is the adapter configured for DHCP? ____	
❓ What is the value of the IP address and the subnet mask? ____ ____	
❓ When you verify the ARP, what is the response? ____ ____	
❓ What is the issue? ____ ____	
3. Correct the problem.	▪ Using moclan, correct the problem.
4. Reset the computer configuration.	▪ Using administrator credentials, run **c:\moc\2276\labfiles\r2.bat**.

Scenario 3: Partial Access to Network Resources

A user at a remote office has only partial access to the network. She can access a coworker's shared folder files the London computer is inaccessible to her. You are at the user's computer to isolate the connectivity issue and either fix it yourself, or escalate it to a systems engineer. For this scenario, you are working to restore connectivity to the London computer.

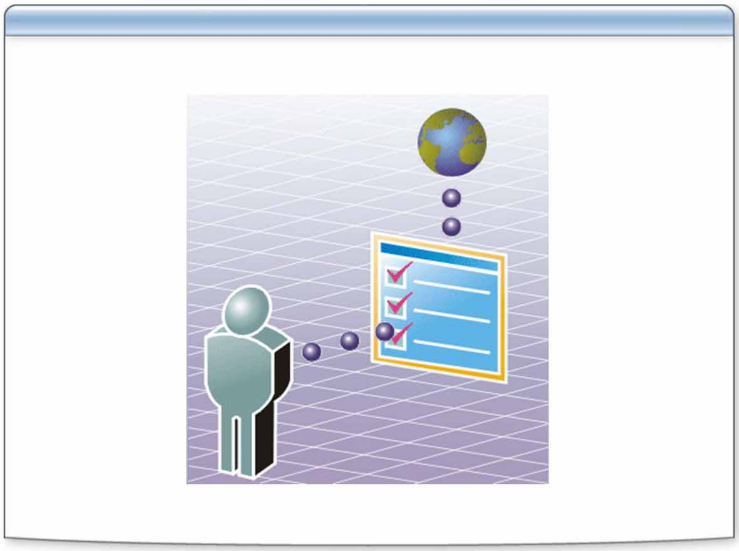
Tasks	Specific Instructions
1. Introduce the problem.	■ Using administrator credentials, run **c:\moc\2276\labfiles\s3.bat**.
2. Isolate issues associated with this scenario.	**a.** Ping localhost. **b.** Ping London. **c.** Run Nslookup to query the London computer.
❓ Can you ping the localhost? Did you receive an answer? ____________________	
❓ Can you ping London? What is the response? What is the displayed address for London? ____________________ ____________________	
❓ Was the nslookup query on the London computer successful? ____________________ ____________________	
❓ What is the most likely problem? ____________________ ____________________	
3. Correct the problem.	
4. Reset the computer configuration.	■ Using administrator credentials, run **c:\moc\2276\labfiles\r3.bat**.

Scenario 4: Unable to Access Host by IP Address

A user in the local office is having difficulty accessing the London computer. The user is unable to print to the print device connected to the London computer and cannot access any of the files located in shared folders on the London computer. In this scenario, you are working to restore connectivity to the London computer.

Tasks	Specific Instructions
1. Introduce the problem.	▪ Using administrator credentials, run **c:\moc\2276\labfiles\s4.bat**.
2. Isolate issues associated with this scenario.	**a.** Ping localhost. **b.** Ping London. **c.** Ping 192.168.*x*.200.
❓	Can you ping the localhost successfully? Is TCP/IP functioning properly?
❓	Can you ping London successfully? What does the output of the ping indicate?
❓	Can you ping 192.168.*x*.200? What is the reply?
❓	What is the issue?
3. Correct the problem.	
4. Reset the computer configuration.	▪ Using administrator credentials, run **c:\moc\2276\labfiles\r4.bat**.

Course Evaluation



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

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

To complete a course evaluation, go to http://www.CourseSurvey.com.

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