Microsoft®

Module 5: Isolating Common Connectivity Issues

Contents

Instructor Notes

Presentation:
60 minutes

Lab:
60 minutes

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

The tasks in this module are 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 array 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:

- Determine the causes of connectivity issues.
- Describe utilities and tools to resolve connectivity issues.
- Describe the client startup communication process.

Required materials

To teach this module, you need the following materials:

- Microsoft® Office PowerPoint® file 2276C_05.ppt
- Appendix B, "Problem Isolation Flowchart"

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, some features of the slides might not be displayed correctly.

Preparation tasks

To prepare for this module:

- Read all the materials for this module.
- Complete the lab exercises.
- Practice presenting the build slides.
- Become familiar with Appendix B, "Problem Isolation Flowchart."

How to Teach This Module

This section contains information that will help you to teach this module, which contains three lessons. The first lesson describes the eight communication steps in the client startup process and common errors during startup. The second lesson describes a five-step issue-isolation method. The third lesson describes some of the utilities that an SA can use for gathering the data and creating the tests required to isolate connectivity issues.

Lesson: Analyzing Client Startup Communication

This section describes the instructional methods for teaching this lesson.

This lesson describes the steps in the client startup communication process as well as common errors in the process. Understanding this process will help students to troubleshoot connectivity problems.

Client Startup Communication

This topic discusses eight communication steps that are performed as part of the client startup process. Explain each step to the students. Understanding these steps is essential to understanding the next topic.

Client Startup Communication Issues

Discuss the ramifications of each communication issue. Stress that the two most common errors during the startup process are the inability to obtain an IP address and an incorrect DNS server configuration.

Practice: Analyzing Client Startup Communication

For students who are not familiar with Network Monitor, this practice might take up to 20 minutes. Be sure that you are available to answer questions about the packets that they have captured. It is not essential that you describe each packet, but you should be able to identify the basic parts of the startup process.

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 focuses on 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 general problems that illustrate almost every type of issue that occurs on a network.

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 who would like more information about network performance should see Course 2275, *Maintaining a Microsoft Windows Server 2003 Environment*.

Actions to Take 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. The list, and the rest of this lesson, provide guidelines that the SA can follow as appropriate.

Actions to Take to Isolate the Issue

This is the most important topic in this lesson because it introduces the Problem Isolation Flowchart in Appendix B. Have students look at the chart briefly, and tell them that they will use the chart in the lab at the end of the module.

Actions to Take to Resolve the Issue

The recommendations in this topic are more applicable to large organizations than to 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, the tasks are good ideas to keep in mind when they might be needed.

The Process to Follow 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: Using Network Utilities and Tools 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 and might appear very similar to each other if they are described too quickly. Be sure of the uses for and differences between 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.

Address Resolution Utilities Included with TCP/IP

Demonstrate how to use the Nbtstat and Nslookup utilities. Many times, students are particularly interested in how Nslookup can be used to find mail servers. For the Address Resolution Protocol (ARP), stress that implementing static entries in the ARP cache is not recommended.

Other Utilities Included with TCP/IP

Demonstrate how to use Hostname, Ipconfig, and Netstat. Emphasize Netstat, because it has not yet been seen in this course and it is useful for troubleshooting. Students should already be familiar with Ipconfig from earlier sections of the course.

Actions to Test Connectivity by Using Ping

This topic describes the process for testing connectivity to a remote host by using Ping. Offer examples of how the scope of the problem is defined as each step is performed.

Ping Error Messages

For each error, discuss how the error can be resolved and whether it is within the scope of the student's organization to resolve. Many times, these errors are seen when accessing Internet resources, not just internal resources.

To demonstrate the various Ping error messages, use the following procedures. Use your host operating system to demonstrate these procedures so that the computer has Internet access.

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

Note To cause the Time to Live (TTL) to expire, you must be able to ping across routers.

1. Open a command prompt window.
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 window as **Administrator**, type **route delete 0.0.0.0**, and then press ENTER.
2. Type **ping 172.1.1.1**, and then press ENTER.

   Because the route of the default gateway has been deleted, the destination host is unreachable.
3. To restore the deleted route, type **ipconfig/renew**, and then 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 command prompt window.
2. Type **ping 172.1.1.1**, and then press ENTER.

   Because a local route exists (0.0.0.0) to attempt to reach 172.1.1.1, you receive a "Request 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 command prompt window.
2. Type **ping invalidhost**, and then 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.
```

Other Connectivity Testing Tools

Ensure that students understand the differences between Tracert and Pathping. Demonstrate both by using the host operating system on your computer so that the computer has Internet access.

Features of the Network Connections Repair Option

Ensure that the students understand that this command can be used as a quick fix for TCP/IP issues without harming TCP/IP configuration settings on the local computer. Demonstrate how to repair a network connection.

What Is the Network Diagnostics Feature?

Demonstrate to students where to find Network Diagnostics and how to use it. Review a Network Diagnostics report with the students.

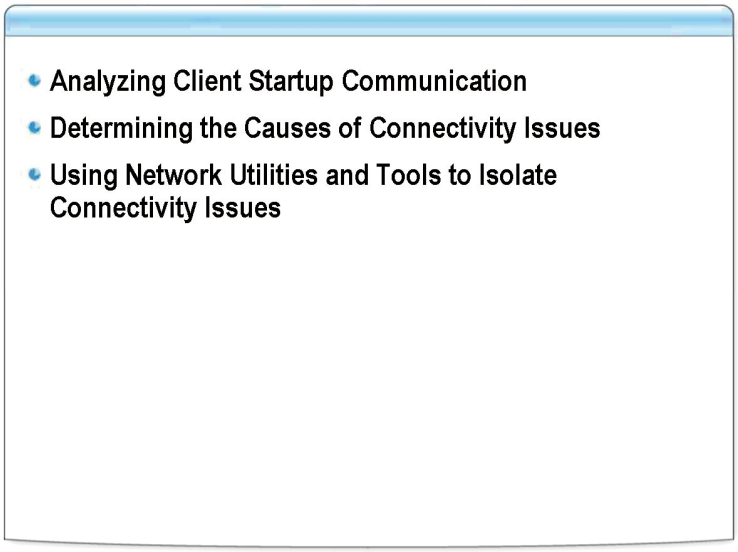
What Is Netsh?

Explain to students that Netsh can be used at a command prompt and in batch scripts. Discuss occasions when using Netsh in batch scripts might be useful. Demonstrate how to access the Interface IP context and Show IP configuration information.

Practice: Using Network Utilities and Tools to Isolate Connectivity Issues

This practice will take about 10 minutes to complete. Many students are unfamiliar with Netsh and might ask additional questions about it.

Overview



Introduction

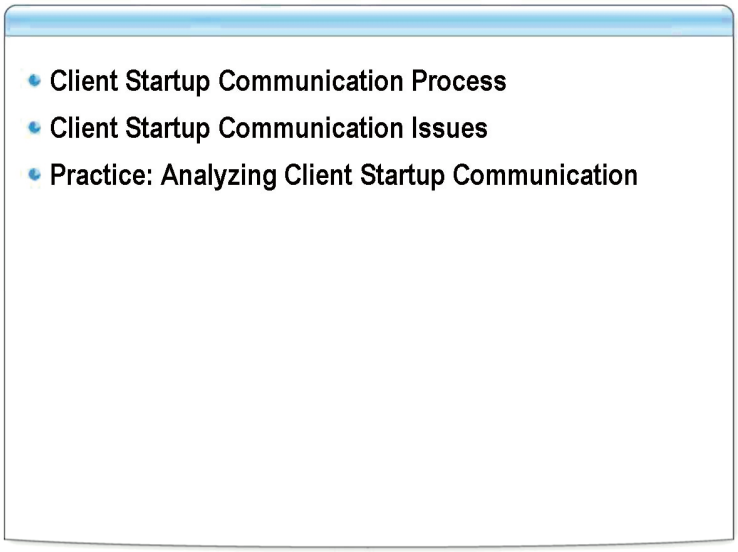
The information in this module introduces you to a process for isolating common connectivity issues and also describes how you can use network utilities and tools as part of this process. To maintain network connectivity, you must be able to isolate issues that interrupt it. When you isolate connectivity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

Objectives

After completing this module, you will be able to:

- Describe client startup communication.
- Determine the causes of connectivity issues.
- Describe the utilities and tools used to resolve connectivity issues.

Lesson: Analyzing Client Startup Communication



Introduction

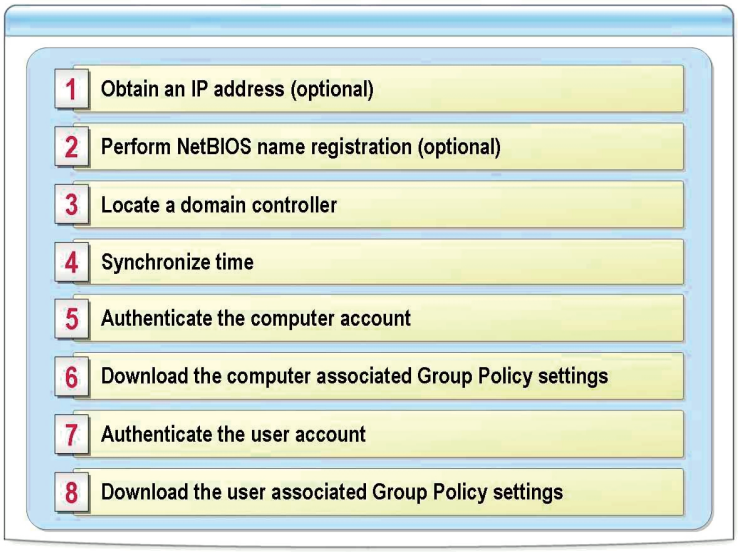
One of the most common times when users experience problems is during logon. Understanding the client startup communication process will help you understand how to fix logon problems.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the client startup communication process.
- Identify client startup communication issues.
- Analyze client startup communication.

Client Startup Communication Process



Introduction

Each time a client is started, a consistent communication process is performed. All the steps in the communication process must be properly completed for a client to access all network resources. If any step is unsuccessful, the client might not be able to log on.

Steps in client startup communication

The client startup communication steps are as follows:

1. Obtain an Internet Protocol (IP) address (optional).

   If a client is configured to obtain an IP address automatically, it will obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server or by using automatic configuration. This step is not performed for clients with a static IP address.

2. Perform network basic input/output system (NetBIOS) name registration (optional).

   If NetBIOS over Transmission Control Protocol/Internet Protocol (TCP/IP) is enabled on a client, it will register its computer name as a NetBIOS name and will register itself as a member of the domain. This step is not performed for clients with NetBIOS over TCP/IP disabled.

3. Locate a domain controller.

   Clients locate a domain controller by using Domain Name System (DNS). They query for the Lightweight Directory Access Protocol (LDAP) service records in the local site. The query returns the host name of a domain controller and the TCP port number.

4. Synchronize the time.

   Time synchronization is essential for authentication using the Kerberos version 5 authentication protocol. To ensure that the time is synchronized, clients will synchronize their clocks with the domain controller in their domain by using the Network Time Protocol (NTP).

5. Authenticate the computer account.

   The computer account is authenticated using the Kerberos protocol. This is necessary before a user can log on to the network.

6. Download the computer-associated Group Policy settings.

   After the computer account is authenticated, it is able to download the computer-associated Group Policy settings. These settings are downloaded only if they have been modified; otherwise, a cached version is used. However, version verification is done each time.

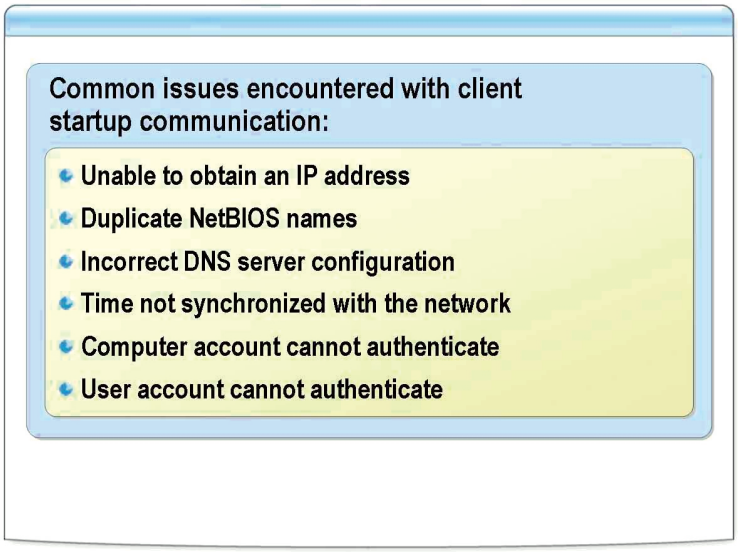
7. Authenticate the user account.

   All the preceding steps are completed before the logon window is displayed to the user. The user can then log on. Kerberos is used to perform the authentication.

8. Download the user-associated Group Policy settings.

   Similar to computer-associated Group Policy settings, user-associated Group Policy settings are downloaded after user authentication. These settings are downloaded only if they have been modified; otherwise, a cached version is used. However, version verification is performed each time.

Client Startup Communication Issues



Introduction

When any step in the client startup communication process fails, there will be issues. Most of these issues result in reduced performance or some resources being unavailable.

Issues and symptoms

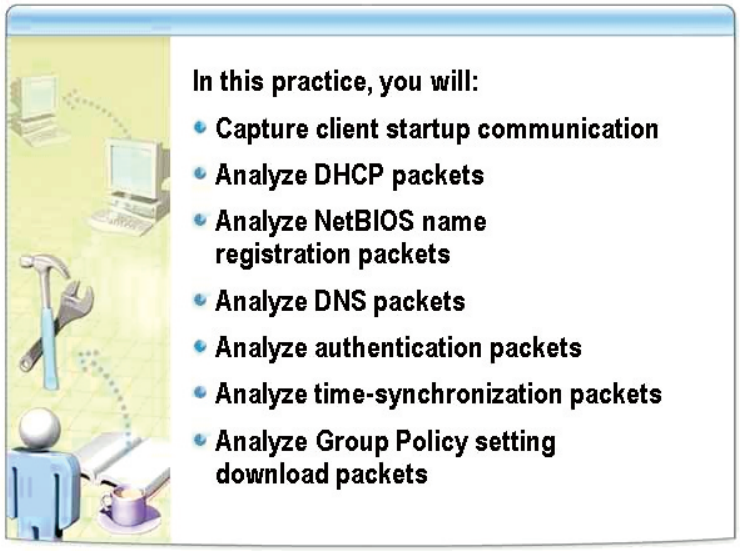
To fix client startup communication problems, you must understand their symptoms. The following table lists client startup communication problems and the symptoms that indicate that they are occurring.

Issue	Symptoms
Unable to obtain an IP address.	Clients without an IP address still allow domain users to log on using cached credentials. However, the clients will not be able to access any network resources.
Duplicate NetBIOS names.	Duplicate NetBIOS names prevent clients from registering a NetBIOS name. If there is a duplicate NetBIOS name, all NetBIOS services will be unavailable. In Microsoft® Windows® 2000, Windows XP, and Windows Server™ 2003, this has a minimal impact, because file sharing and printer sharing do not require NetBIOS. A warning message will appear, indicating that there is a name conflict.
Incorrect DNS server configuration.	The most common symptom of the DNS server being incorrectly configured on a client is a slow network logon—typically, two minutes or more. This is because the client attempts to find a domain controller by using DNS before failing over to locating a domain controller by using NetBIOS. If NetBIOS name resolution also cannot locate a domain controller, the client will not be authenticated to the network and will not have access to network resources.

(*continued*)

Issue	Symptoms
Time not synchronized with the network.	If there is more than a five-minute time difference between clients and the domain controller to which they are logging on, they will receive an error message indicating that they cannot be logged on due to a time difference between the client and server. Network resources will be inaccessible. This should occur only when a client has been reconfigured to obtain time from a source other than a local domain controller, or a local domain controller has the incorrect time.
Computer account cannot authenticate.	If a computer account cannot authenticate, its trust with the domain is broken, and it cannot log on domain users, except with cached credentials. Additionally, new Group Policy settings will not be downloaded. This can occur when a client is reimaged by using an image older than 30 days. Computer accounts change their passwords every 30 days, and an image older than 30 days will not have the current password. Events in the system log will indicate that the computer account could not be authenticated. To fix this, reset the computer account.
User account cannot authenticate.	When a user account cannot authenticate, the following message will appear: “The system could not log you on.” This is typically due to an incorrect password or user name. However, this also happens when the **Log On To** box is not configured with the correct name.

Practice: Analyzing Client Startup Communication



Objectives

In this practice, you will:

- Capture client startup communication.
- Analyze DHCP packets.
- Analyze NetBIOS name registration packets.
- Analyze DNS packets.
- Analyze authentication packets.
- Analyze time-synchronization packets.
- Analyze Group Policy settings download packets.

Instructions

Ensure that the DEN-DC1 virtual machine is running. The DEN-CL1 virtual machine should not be running.

Practice

► **Capture client startup communication**

1. On DEN-DC1, log on as **Administrator**, with a password or **Pa$$w0rd**.
2. Click **Start**, point to **Administrative Tools**, and then click **Network Monitor**.
3. Click **OK** to begin selecting the network on which you want to capture data.
4. Expand **Local Computer**, click **Local Area Connection**, and then click **OK**.
5. On the **Capture** menu, click **Start**.
6. Start the DEN-CL1 virtual machine.
7. On DEN-DC1, watch the number of frames being captured in Network Monitor. When the number of frames has stabilized (approximately 175 to 250 frames), take note of the Time Elapsed. This is the time for prelogon communication. Notice that most of the communication will take place after the **Welcome To Windows** dialog box appears.

8. On DEN-CL1, log on as **Paul**, with a password of **Pa$$word**.
9. On DEN-DC1, watch the number of frames being captured in Network Monitor. When the number of frames has stabilized (approximately 650 frames), on the **Capture** menu, click **Stop and View**.

► **Analyze NetBIOS name registration packets**

1. On the **Display** menu, click **Filter**.
2. Double-click **Protocol==Any**.
3. Click **Disable All**.
4. Under **Disabled Protocols**, double-click **NBT**, and then click **OK** twice. Read the first 10 NBT packets. The first few are broadcasts registering the NetBIOS name DEN-CL1 for the client. The next few register the client in the CONTOSO domain.

► **Analyze DNS packets**

1. On the **Display** menu, click **Filter**.
2. Double-click **Protocol==NBT**.
3. Click **Disable All**.
4. Under **Disabled Protocols**, double-click **DNS**, and then click **OK**.
5. Click **OK**. Notice that only 16 frames are now visible. These are the DNS packets.
6. Double-click the first DNS packet. In the middle pane, notice the name that the query is for. This is the client locating a logon server.
7. Click the second DNS packet, and in the middle pane, select **DNS**. Read the ASCII text in the bottom pane. The DNS server has responded with DEN-DC1.contoso.msft as the domain controller.
8. Click the fifth DNS packet. This packet is the client resolving DEN-DC1.contoso.msft to an IP address.

► **Analyze authentication packets**

1. On the **Display** menu, click **Filter**.
2. Add a filter for User Datagram Protocol (UDP) Port 88.
   a. Double-click **Protocol==DNS**.
   b. Click the **Property** tab, scroll down, and then expand **UDP**.
   c. Click **Destination Port**, click the **Decimal** button, type **88** in the **Value** box, and then click **OK**.
   d. With **UDP** selected, click the **OR** button, and then click the **Expression** button.
   e. Under **UDP**, click **Source Port**, and then click **OK**.
3. Click **OK**. The visible frames are the Kerberos authentication for both the computer account and the user account.

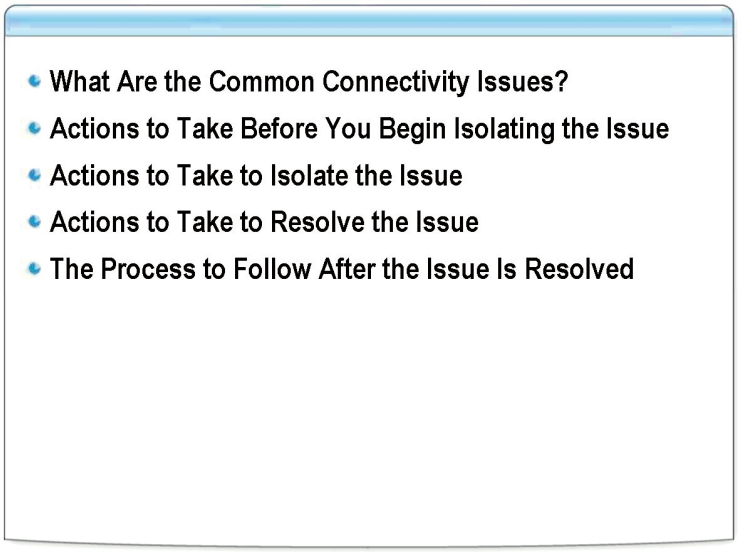
► **Analyze time synchronization packets**

1. On the **Display** menu, click **Filter**.
2. Double-click **UDP:Source Port**, type **123** in the **Value** box, and then click **OK**.
3. Double-click **UDP:Destination Port**, type **123** in the **Value** box, and then click **OK**.
4. Click **OK**. These are the packets for time synchronization.

► **Analyze Group Policy settings download packets**

1. On the **Display** menu, click **Filter**.
2. In the **Delete** category, click the **Branch** button.
3. Click **OK** to confirm.
4. In the **Add** category, click the **Expression** button.
5. On the **Property** tab, expand **SMB**, and then click **File name**.
6. Click the **ASCII** button, type **Policies** in the **Value** box, and then click **OK**. Please note that this value is case-sensitive.
7. Click **OK**. The visible packets are the computer-based and user-based Group Policy settings being downloaded to the client.
8. Close **Network Monitor**. Do not save the frame capture.

Lesson: Determining the Causes of Connectivity Issues



Introduction

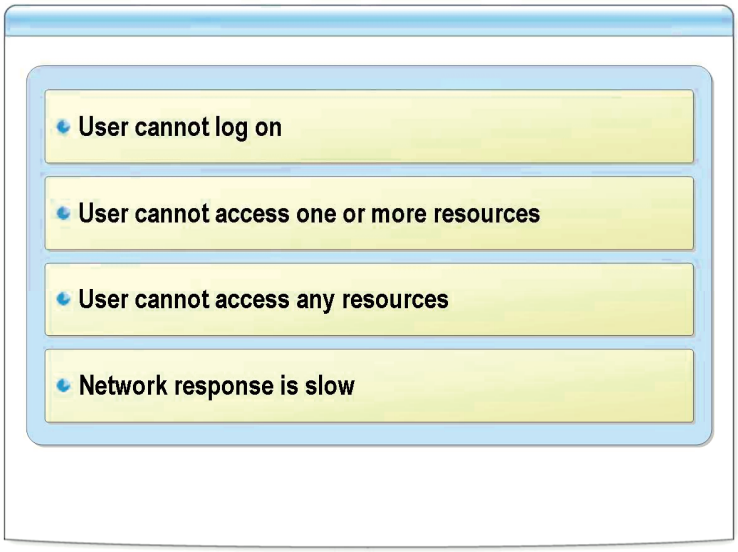
One of the key elements in isolating a network problem is using a consistent, effective strategy for determining the cause. Many of the trouble calls that you receive will be due to user errors that can be resolved through a little training for the user. When you are faced with a more complex complaint,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

Lesson objectives

After completing this lesson, you will be able to:

- List common connectivity issues.
- Identify actions to take before isolating the issue.
- Describe how to isolate the issue.
- Describe how to resolve the issue.
- Describe the process to follow after the problem is resolved.

What Are the Common Connectivity Issues?



Introduction

As a systems administrator, you will not be able to 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 a problem that you need to refer to other experts in your organization.

Common issues

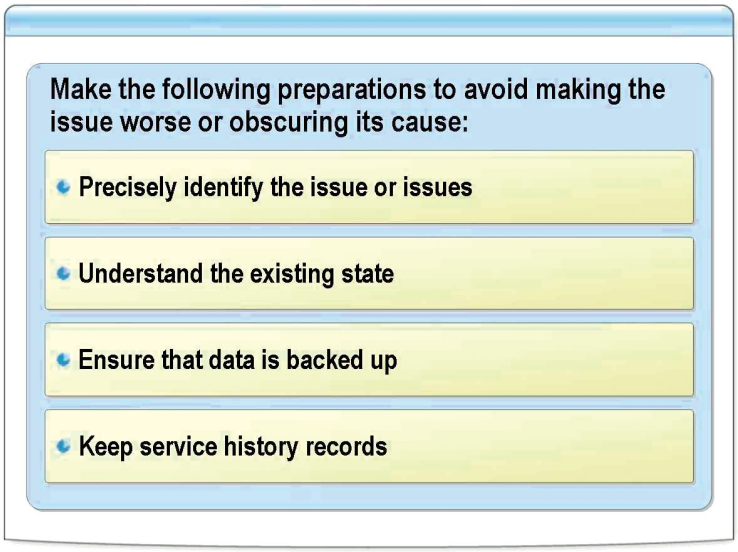
Most issues will be presented to you by users who find that they are unable to perform a specific action on their computers—either something that they were able to do or something that they believe they should be able to do.

There are only a few basic types of complaints:

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

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

Actions to Take Before You Begin Isolating the Issue



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. For this reason, the first action of the isolation is to obtain accurate information about what has occurred.

To understand the nature of an issue, you must know the following:

- What exactly was the user doing when the problem occurred?
- Is this the first time that the problem occurred?
- Which users are affected by the issue? One, a group, or all?
- Which resources are affected by the issue? One, a group, or all?
- Where are the affected resources? A single server or different servers?
- Have there been any recent changes? Network reconfiguration, new software, new hardware?

Understand the existing 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 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 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

Many companies have policies in place dictating that all data must be stored on servers rather than local workstations. However, in most cases, users save some files locally anyway. When troubleshooting a client where there is a risk of data loss, it is important to ensure that any local data is safely backed up. Backups can also be used to restore the system state if problems occur.

Your backup should include the following items:

- The user's personal folder, 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 included with Microsoft Windows XP. To start the wizard, in **Control Panel**, in **Performance and Maintenance**, 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.

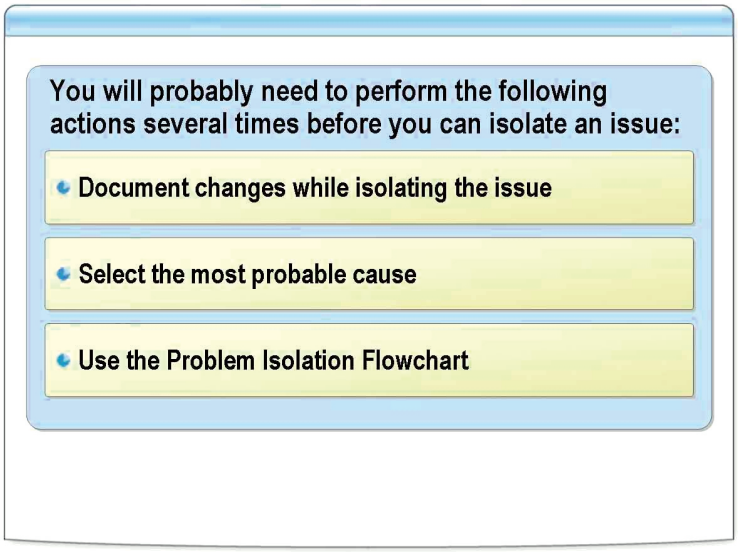
Regardless of the medium on which it is stored, each record should start with baseline performance information gathered when the host was added to the network. Update the baseline information after installing new hardware or software so that you can compare past and current behavior and performance levels.

Your service history records should include:

- 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.

Actions to Take to Isolate the Issue



Introduction

Locating the source of a problem might be a long and an arduous process, or it might take only a few minutes. In either case, the Problem Isolation Flowchart (in Appendix B) can help you to identify the shortest path to a solution.

Document changes while isolating the issue

Documenting all changes during troubleshooting is essential to ensure that issues are correctly isolated. Each change made during troubleshooting must be reversed if it does not resolve the problem.

Documenting changes ensures that:

- You do not create additional issues.
- You correctly understand the effects of your changes.

Documenting the steps you take while troubleshooting will also help you review your actions after you resolve the problem. This is useful for 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 recur.

Note Begin documenting your actions at the start of issue isolation, rather than waiting until 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 cannot communicate with a file server, do not begin by checking the routers between the two systems. Check the simple, basic details on the client first—such as whether the network cable is connected to the computer.

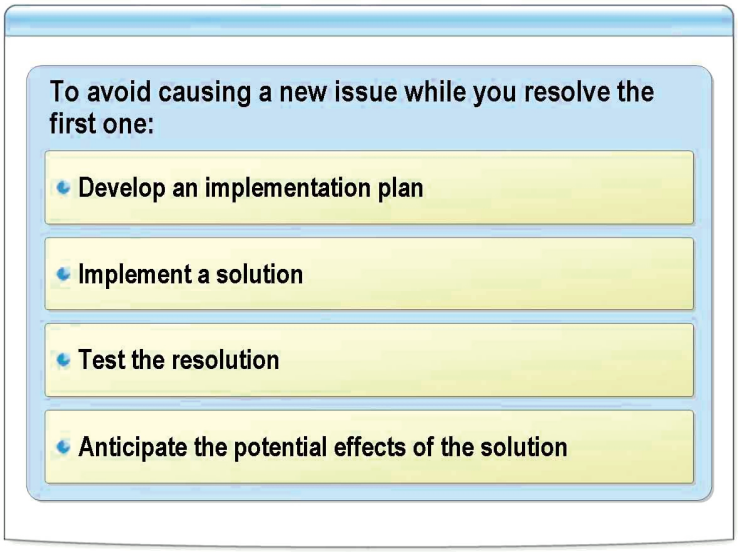
When isolating network connectivity issues, the fastest way to find the source of the problem is to divide the process into halves. For example, if a client cannot communicate with a server, verify whether the client can communicate with devices halfway between the server and the client. If this is successful, try communicating with a device halfway between the midpoint and the server. Continue this process until the problematic device is found.

Use the Problem Isolation Flowchart

The Problem Isolation Flowchart begins with simple logon problems and progresses in complexity through problems with client configuration, name resolution, routers, firewalls, and other servers. For example, you can use it to isolate an issue such as a single client not obtaining a 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. Because you know that this issue is applicable to only 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 refer to other experts in your organization.

Actions to Take to Resolve the Issue



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.
- Substitute hardware, if the failing equipment performs a vital 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

For most problems, you will have a number of potential solutions. When selecting a solution to implement, consider the likelihood that the solution will fix the problem, and how difficult the solution is to implement. It makes sense to try a few quick fixes that are easy to implement before trying an elaborate one, even if the elaborate one is more likely to fix the problem.

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 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.

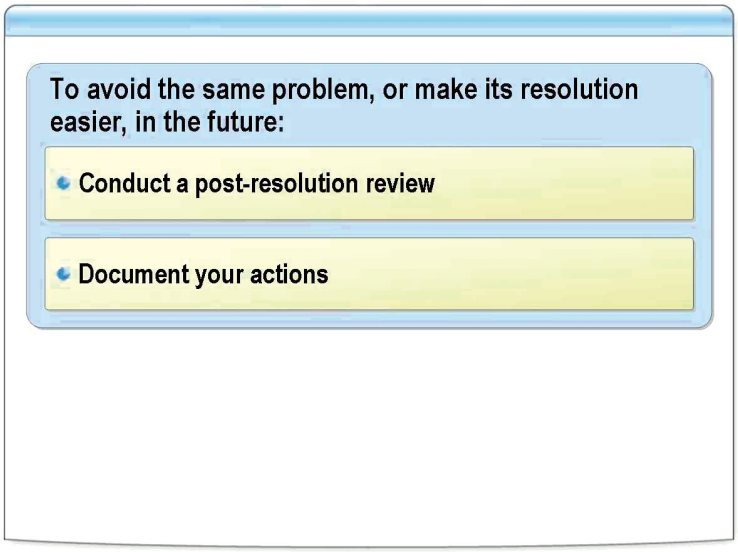
It is at this point that the time you spent documenting the isolation process shows its value. You should repeat exactly the procedures that you used to duplicate the problem, to ensure that the problem the user originally experienced has been eliminated and not just temporarily masked. If the problem was intermittent, it might take 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 recurring.

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.

The Process to Follow After the Issue Is Resolved



Introduction

When the network is functioning normally again, review and document just what has happened 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 his or her actions caused the problem, exacerbated it, or made it more difficult to resolve. Such conversations can make the resolution of future issues significantly easier.

Document your actions

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: Using Network Utilities and Tools to Isolate Connectivity Issues

- Address Resolution Utilities Included with TCP/IP
- Other Utilities Included with TCP/IP
- Actions to Test Connectivity by Using Ping
- Ping Error Messages
- Other Connectivity Testing Tools
- Features of the Network Connections Repair Option
- What Is Network Diagnostics?
- What Is Netsh?
- Practice: Using Network Utilities and Tools to Isolate Connectivity Issues

Introduction

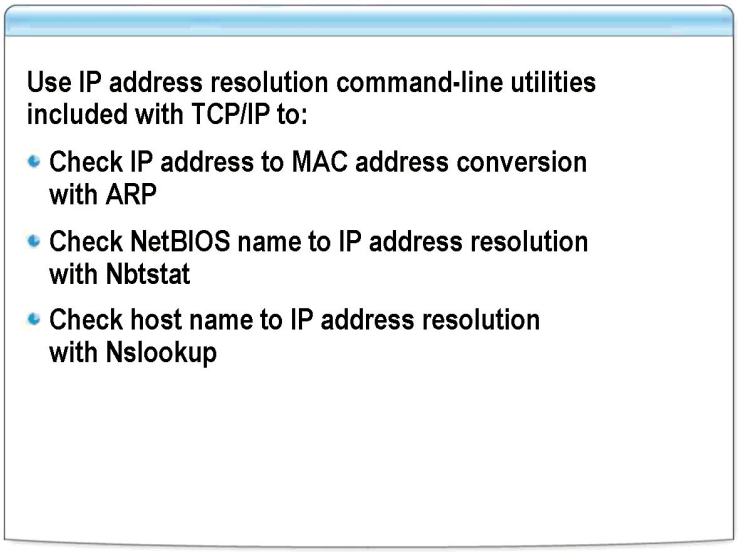
Windows automatically installs most of the utilities that you need for isolating network problems when you install the operating system. There are several additional utilities that you can install from the Windows compact disc when you need them.

Lesson objectives

After completing this lesson, you will be able to:

- Describe how ARP, Nbtstat, and Nslookup are used to isolate connectivity issues.
- Describe how Hostname, Ipconfig, and Netstat are used to isolate connectivity issues.
- Describe how to use the Ping utility to troubleshoot connectivity problems.
- Interpret the error messages created by Ping while troubleshooting connectivity problems.
- Describe how Tracert and Pathping are used to isolate connectivity issues.
- Describe the features of the Network Connections Repair option.
- Describe Network Diagnostics.
- Describe Netsh.
- Isolate connectivity issues by using TCP/IP utilities and tools.

Address Resolution Utilities Included with TCP/IP



Introduction

You can use three of the utilities included with TCP/IP to test whether address resolution is being performed properly. The three types of address resolution are:

- IP address to media access control (MAC) address
- NetBIOS name to IP Address
- Host name to IP Address

Use ARP to check IP address to MAC address conversion

ARP converts IP addresses to the MAC addresses that data-link-layer protocols require to transmit frames. To minimize the amount of network traffic that 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 (between 2 and 10 minutes) in case the computer has additional packets to send to the same address.

When the network card in a server is changed but retains the same IP address, the client ARP cache will contain outdated information because the new network card will have a different MAC address. Until the cache is updated, clients will be unable to communicate with the server. This problem will resolve itself within 10 minutes. However, it can also be resolved by manually clearing the ARP cache.

Note It is possible to place static entries in the ARP cache. However, this is not recommended, because it is likely to cause network communication problems during network changes and results in minimal network traffic reduction.

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 name 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 NetBIOS name 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: [10.10.0.50] Scope Id: []

                    NetBIOS Remote Cache Name Table

   Name               Type       Host Address     Life [sec]
------------------------------------------------------------
   DEN-DC1      <03>  UNIQUE     10.10.0.2        -1
   DEN-DC1      <00>  UNIQUE     10.10.0.2        -1
   DEN-DC1      <20>  UNIQUE     10.10.0.2        -1
```

Use Nslookup to check host 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. If a DNS server is not specified, the primary DNS server in the TCP/IP configuration will be used.

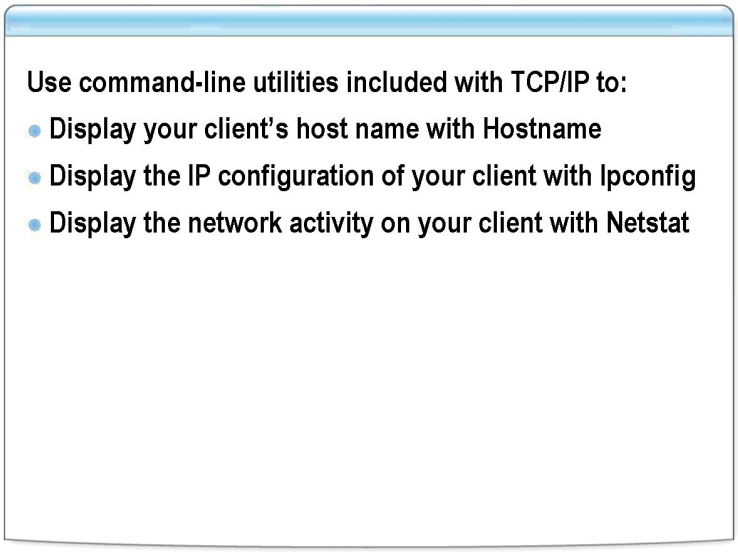
The output generated by the utility looks like the following sample:

```
C:\>nslookup microsoft.com
Server:  den-dc1.contoso.msft
Address:  10.10.0.2

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

The output sample shows that when queried, the den-dc1.contoso.msft DNS server returns 207.46.249.222 as the IP address associated with microsoft.com. The ability to specify a DNS server makes this utility useful when checking that records on multiple DNS servers are synchronized.

Other Utilities Included with TCP/IP



Introduction

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

Use Hostname to display your client's name

The Hostname utility displays the host name that is assigned to your client. 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 to display the current TCP/IP configuration 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.

Use Netstat to display the network activity on your client

Netstat displays information 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 whether a port is available or in use.

A common use of Netstat is to view whether unauthorized services, such as Spyware, are running on a client. All services listening on a TCP or UDP port can be listed by running **netstat –a**. Unknown listings can be tracked down. Be aware that client utilities will also be listed and typically use random course port numbers 1024 and above.

The network connection listing displayed by Netstat on a computer running Windows XP appears as follows:

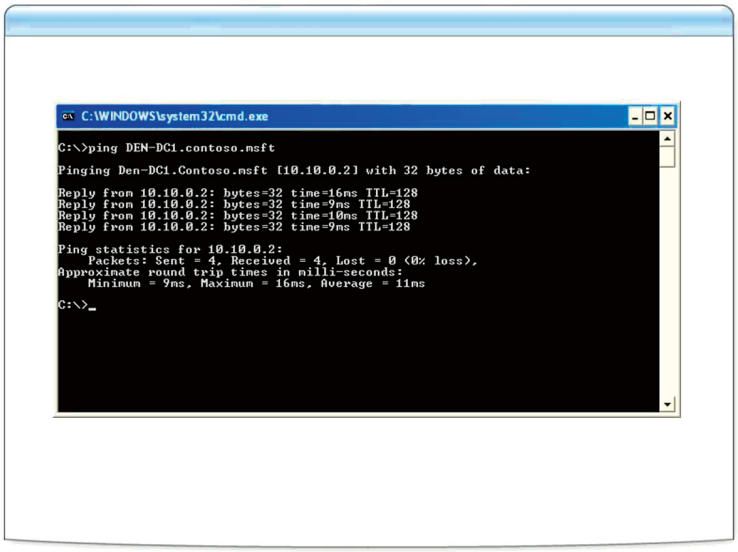
```
C:\>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State

TCP    Den-CL1:epmap          Den-CL1.Contoso.msft:0  LISTENING
TCP    Den-CL1:microsoft-ds   Den-CL1.Contoso.msft:0  LISTENING
TCP    Den-CL1:netbios-ssn    Den-CL1.Contoso.msft:0  LISTENING
TCP    Den-CL1:1043           10.10.0.2:microsoft-ds  TIME_WAIT
TCP    Den-CL1:1049           10.10.0.2:ldap          TIME_WAIT
TCP    Den-CL1:1056           10.10.0.2:domain        TIME_WAIT
TCP    Den-CL1:1028           Den-CL1.Contoso.msft:0  LISTENING
UDP    Den-CL1:microsoft-ds   *:*
UDP    Den-CL1:isakmp         *:*
UDP    Den-CL1:1037           *:*
UDP    Den-CL1:4500           *:*
UDP    Den-CL1:ntp            *:*
UDP    Den-CL1:netbios-ns     *:*
UDP    Den-CL1:netbios-dgm    *:*
UDP    Den-CL1:1900           *:*
UDP    Den-CL1:ntp            *:*
UDP    Den-CL1:1039           *:*
UDP    Den-CL1:1900           *:*
```

Actions to Test Connectivity by Using Ping



Introduction

The Ping utility is one of the most frequently used TCP/IP utilities. When it is used to isolate connectivity issues, Ping tests are done to find the scope of the connectivity issue and the location. When you ping a DNS name, it also tests name resolution.

Testing connectivity to a remote host

The following steps describe how to use the Ping utility to perform tests on your network connectivity. The process starts by testing communication to the remote host and works progressively closer to the local host. An alternative method is to follow these steps in reverse order, starting with step 6.

1. Ping the remote host.

   This confirms whether the connectivity problem still exists. If you can successfully ping a host, you know that the problem is not physical, as packets are able to be transmitted from the client to the remote host. If you can ping a host but cannot access a service on it, the problem is usually with the services.

   In most companies, ping packets are allowed between all subnets. However, some organizations block ping packets to server subnets as a security measure. If this is the case, there will be no response, even if the remote host is operational.

2. Ping another host on the same subnet.

   If this is successful, you know that the problem is limited to accessing the remote host and not a general network problem. After concluding this, you can visit the remote host and begin troubleshooting.

3. Ping a host on another subnet.

   If this is successful, the problem is likely limited to a accessing a single subnet. This might indicate a routing problem. Most routing problems are due to incorrect router configuration or router failure.

4. Ping the default gateway.

   If this is successful, you know that you can communicate on the local network, and the problem is likely a routing problem. Verify that the default gateway is correctly configured.

5. Ping the local client.

   Successfully pinging the IP address of the local client verifies that TCP/IP is correctly configured on the client.

6. Ping the loopback address (127.0.0.1).

   Successfully pinging the loopback address verifies that TCP/IP is both installed 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.

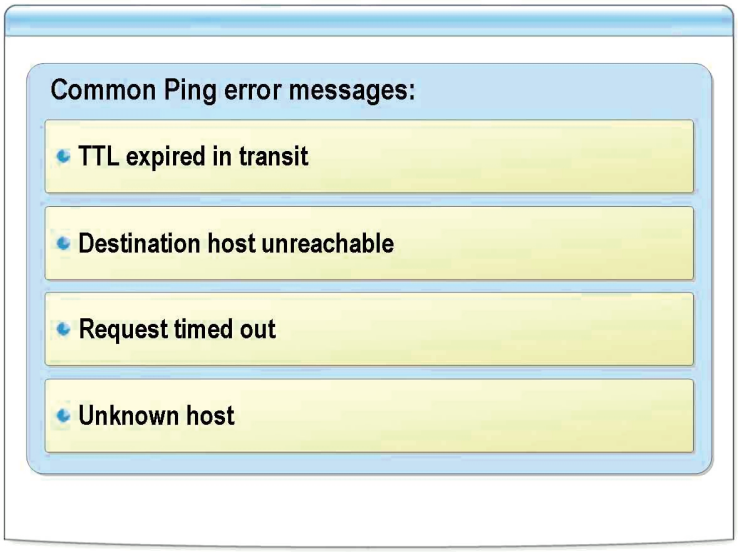
   Removing and reinstalling TCP/IP is a common solution to fix problems with pinging the loopback address or the local client. In Windows XP and Windows Server 2003, you cannot remove TCP/IP to reinstall it, but you can reset it by running the command **netsh in tip reset *logfile***, where *logfile* is a text file that results will be logged to.

   Note For more information about repairing a corrupted TCP/IP stack, see "How to Reset Internet Protocol (TCP/IP) in Windows XP" in the Microsoft Knowledge Base.

7. Temporarily turn off IP Security (IPSec), and then retry all the preceding **ping** commands.

   If none of the preceding **ping** commands are successful, check whether 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.

Ping Error Messages



Introduction

Each time you ping a host, the Ping utility will display a message box 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

"TTL expired in transit" indicates that the number of hops required to reach the destination exceeds the TTL 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 rare cases, this is not enough to travel the required number of hops to a destination. You can increase the TTL by using the **-i** switch, to a maximum of 255 hops.

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

"Destination host unreachable" 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," 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," the routing problem occurred at a remote router.

"Request timed out"

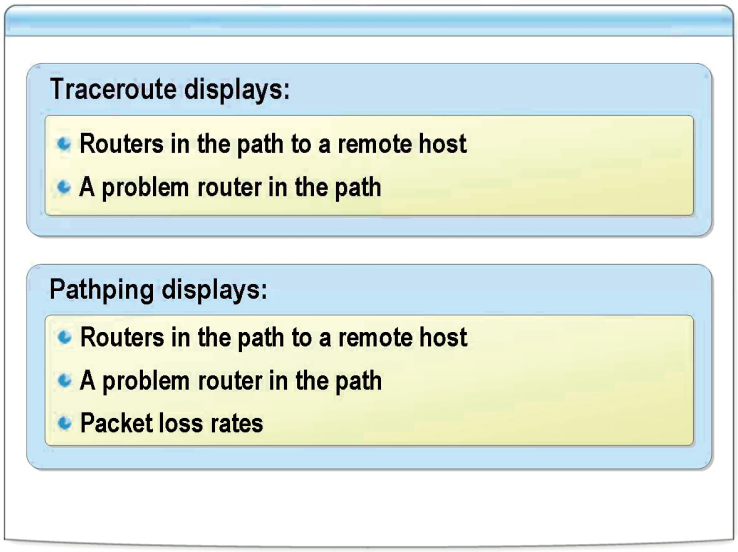
In most cases "Request timed out" indicates that the remote host is not responding. This usually indicates a problem on the remote host or a network problem preventing packets from reaching the remote host. However, it is not a router problem, as that would be indicated by the message "Destination host unreachable."

In most circumstances, the latency to communicate with a remote host is less than 1000 milliseconds, even when accessing hosts around the world on the Internet. Ping allows 4000 milliseconds for a response to be returned before displaying "Request timed out." In rare situations, such as satellite links, "Request timed out" might indicate excessive latency between the client and the host. You can test for excessive latency by increasing the wait time by using the **–w** switch.

Unknown host

This error message appears as "Ping request could not find host *host name*. Please check the name and try again." This 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.

Other Connectivity Testing Tools



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 encounter 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, as Ping does, but it changes 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 systems running Windows, 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 uses 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

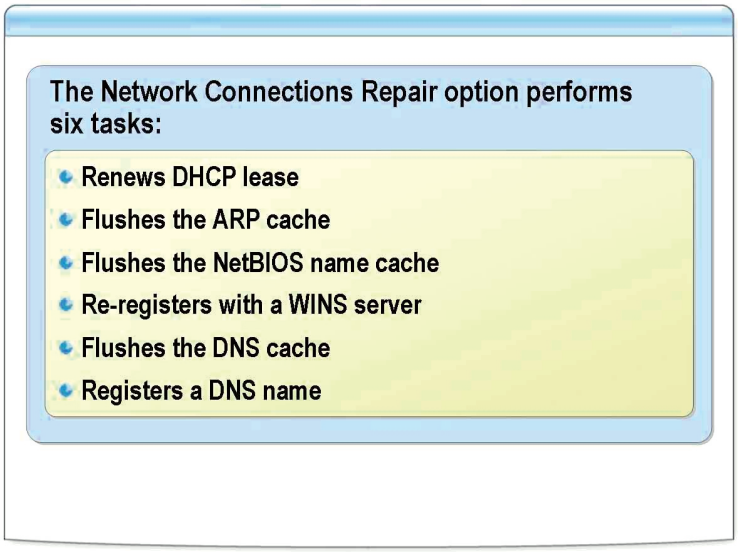
Like Traceroute, Pathping discovers the path to a destination. However, by default, Pathping sends 100 Echo Request messages to each router between a source and destination over a period of time and then computes results based on the packets returned from each router.

In addition to displaying the path to a destination, Pathping displays the degree of packet loss at any given router. A router with packet loss might indicate congestion or configuration problems.

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.

Features of the Network Connections Repair Option



Introduction

The Network Connections Repair option 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 renewal

This is the equivalent of a DHCP broadcast renewal at 87.5 percent of the lease time. This was chosen because it is 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 cannot 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. Repairing a network connection performs the equivalent of running the **nbtstat –R** command which clears the NetBIOS name cache and then reloads any NetBIOS name entries in the Lmhosts file with the #PRE flag.

Reregister the client's name with a WINS server

Repairing a network connection performs the equivalent of running the **nbtstat –RR** command which reregisters 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 confirm that the refresh was successful.

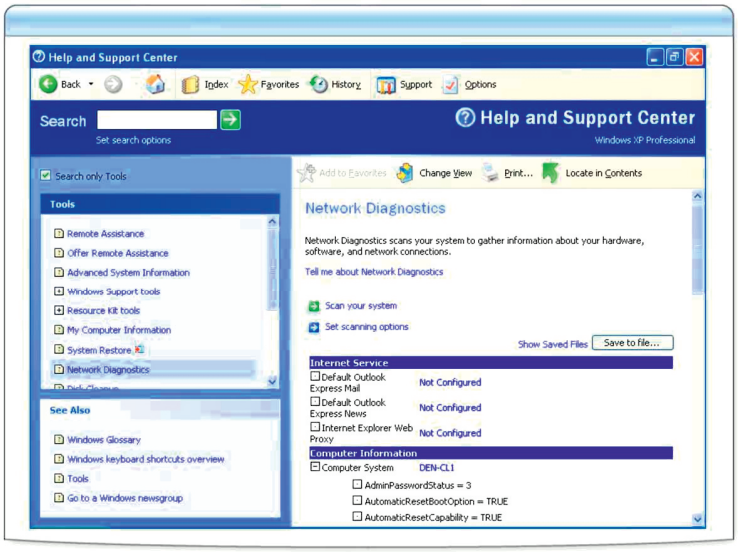
Flush the DNS cache

Repairing a network connection performs the equivalent of running the **ipconfig /flushdns** command which flushes the DNS resolver cache entries from memory. This can be useful in isolating problems with DNS name resolution.

Register a DNS name

Repairing a network connection reregisters the DNS name of the client with a DNS dynamic update server. This is similar to running the **ipconfig /registerdns** command.

What Is Network Diagnostics?



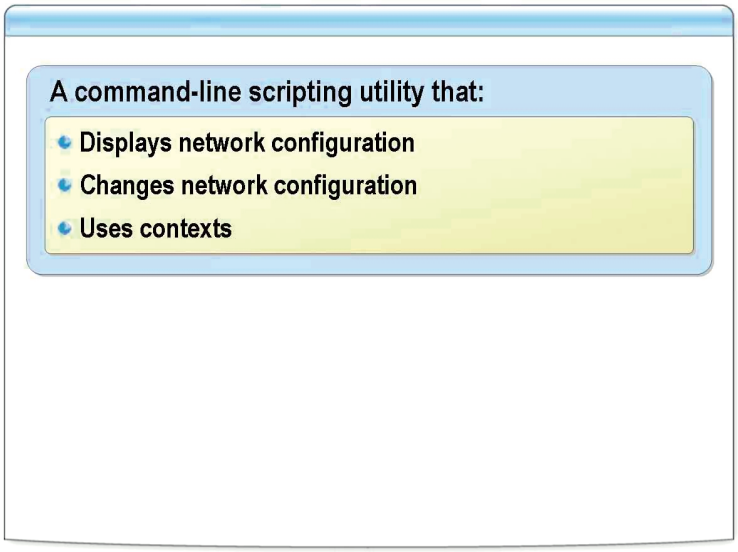
Introduction

The Network Diagnostics utility 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.

Using Network Diagnostics

Unlike most of the other network utilities, Network Diagnostics is a Windows-based utility rather than a command-line utility. It is accessed by clicking **Help and Support Center** on the **Tools** menu for both Windows XP and Windows Server 2003.

What Is Netsh?



Introduction

Netsh is a command-line scripting utility that allows you to, either locally or remotely, display or modify the network configuration of a computer that is currently running. Netsh also provides a scripting feature that allows you to run a group of commands in batch mode against a specified computer. Netsh can also save a configuration script in a text file for archival purposes or to help you configure other servers.

Netsh contexts

Netsh interacts with other operating system components using dynamic-link library (DLL) files. Each Netsh helper DLL provides an extensive set of features called a context, which is a group of commands specific to a networking component. These contexts extend the functionality of Netsh by providing configuration and monitoring support for one or more services, utilities, or protocols. For example, Dhcpmon.dll provides Netsh the context and set of commands necessary to configure and manage DHCP servers.

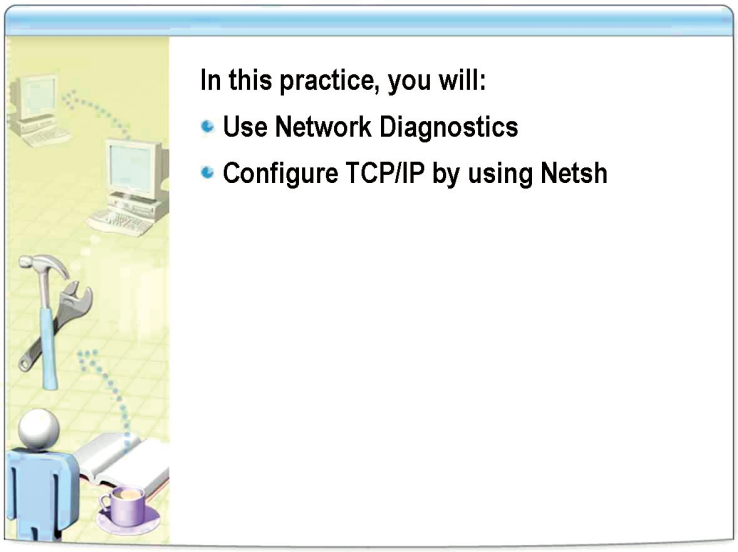
You must run the **netsh** command from a command prompt and change to the context that contains the command that you want to use. The contexts that are available to you depend on which networking components you have installed. For example, if you type **dhcp** at the Netsh command prompt, you change to the DHCP context, but if you do not have DHCP installed, the following message appears:

```
The following command was not found: dhcp.
```

The following table lists contexts available in Netsh.

Context	Description
aaaa	Shows and sets the configuration of the authentication, authorization, accounting, and auditing (AAAA) database used by the Internet Authentication Service (IAS) and the Routing and Remote Access Service (RRAS).
bridge	Enables or disables Layer-3 compatibility mode and shows configuration information for the Network Bridge adapters.
dhcp	Administers DHCP servers and provides an equivalent alternative to console-based management.
diag	Administers and troubleshoots operating system and network service parameters.
interface ip	Configures the TCP/IP protocol (including addresses, default gateways, DNS servers, and WINS servers) and displays configuration and statistical information.
interface ipv6	Queries and configures IP version 6 (IPv6) interfaces, addresses, caches, and routes.
interface portproxy	Administers servers that act as proxies between IPv4 and IPv6 networks and applications.
ipsec	Provides an equivalent alternative to the console-based management and diagnostic capabilities provided by the IP Security Policy Management and IP Security Monitor snap-ins available in the Microsoft Management Console (MMC). By using the Netsh commands for IPSec, you can configure and view static or dynamic IPSec main-mode settings, quick-mode settings, rules, and configuration parameters.
ras	Administers remote access servers.
routing	Administers routing servers.
rpc	Changes, resets, or displays selective system-binding settings.
wins	Administers WINS servers.

Practice: Using Network Utilities and Tools to Isolate Connectivity Issues



Objectives

In this practice, you will:

- Use Network Diagnostics.
- Configure TCP/IP by using Netsh.

Instructions

Ensure that the DEN-DC1 and DEN-CL1 virtual machines are running.

Practice

► **Use Network Diagnostics**

1. On DEN-CL1, log on as **Paul**, with a password of **Pa$$w0rd**.
2. Click **Start**, and then click **Help and Support**.
3. Under **Pick a task**, click **Use Tools to view your computer information and diagnose problems**.
4. In the **Tools** pane, click **Network Diagnostics**.
5. Click **Set scanning options**.
6. Scroll down, and select the **Domain Name System (DNS)** check box and the **Internet Protocol Address** check box. These check boxes are selected in addition to the default selections.
7. Scroll up, and click **Scan your system**.
8. When the report is complete, scroll down, and expand **DNS Servers**. Notice that the status of **DNS Servers** is **Passed**.
9. Expand **DNSServerSearchOrder = 10.10.0.2**. Notice that this displays the communication that Network Diagnostics performed with the DNS server.
10. Expand **Network Adapters**. Notice that a wide variety of network information is listed here.
11. Close **Help and Support Center**.

► Configure TCP/IP by using Netsh

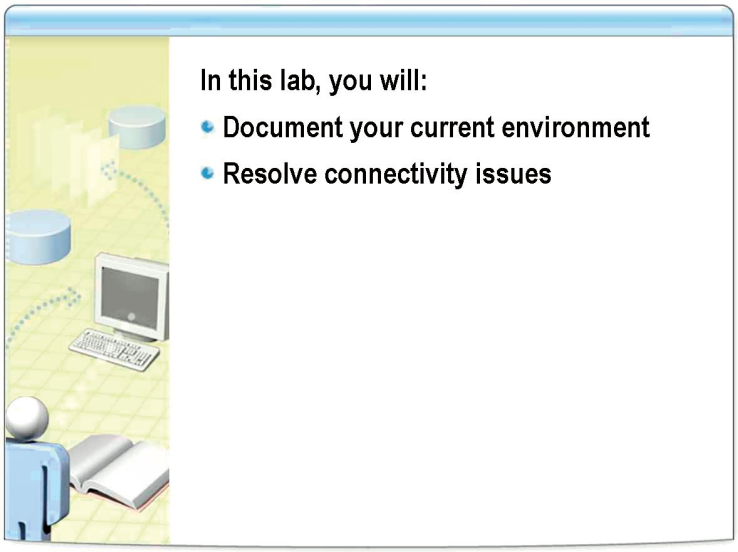
1. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **netsh**, and then press ENTER.
3. Type **interface ip**, and then press ENTER.
4. Type **show**, and then press ENTER.
5. Type **show config**, and then press ENTER. Notice that the address is **10.10.0.20**. We will change the address to **10.10.0.21**.
6. Type **help**, and then press ENTER.
7. Type **set**, and then press ENTER.
8. Type **set address**, and then press ENTER. Read the help message that is displayed.
9. Type **set address name= "Local Area Connection" source=static addr=10.10.0.21 mask=255.255.0.0**, and then press ENTER.
10. Type **show config**, and then press ENTER. Notice that the address is now **10.10.0.21**.
11. Type **reset C:\netshlog.txt**, and then press ENTER.
12. Type **quit**, and then press ENTER.
13. Type **notepad C:\netshlog.txt**, and then press ENTER to view the log file. Read the registry changes that were made.
14. Close Notepad.

► Prepare for the next lab

- Restart DEN-CL1.

Important Do not shut down the virtual machines.

Lab: Isolating Common Connectivity Issues



Objectives

After completing this lab, you will be able to:

- Document your current environment.
- Resolve connectivity issues.

Prerequisites

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

Instructions

Ensure that the DEN-DC1 and DEN-CL1 virtual machines are running.

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 Flowchart, see Appendix B.

Estimated time to complete this lab: 60 minutes

Exercise 1
Documenting Your Current Environment

As you run the scripts to introduce scenarios, you might be changing the configuration settings of your computer 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 the settings are correctly configured after you reset your computer.

On DEN-CL1, log on to the CONTOSO domain as **Paul**, with a password of **Pa$$w0rd**.

Item	Configuration
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	

Exercise 2
Resolving Connectivity Issues

This exercise consists of four scenarios. Each scenario outlines a connectivity issue that you will need to resolve. You will use the Problem Isolation Flowchart in Appendix B 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 help desk 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 pass it on to a systems engineer.

Tasks	Specific instructions
1. Introduce the problem.	**a.** If necessary, log on as **Paul**, with a password of **Pa$$w0rd**. **b.** Run **D:\2276\Labs\Mod05 \s1.bat**.
2. Isolate the issue.	**a.** Use the Ping utility to send an Echo Request to localhost. **b.** Ping DEN-DC1. **c.** Verify your own IP configuration.
? After you pinged localhost, did the TCP/IP stack function properly?	
? After you pinged DEN-DC1, 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.	▪ In **Control Panel**, navigate to **Network Connections**, and then click **Local Area Connection** and correct the problem.
4. Reset the computer configuration.	▪ Run **D:\2276\Labs\Mod05\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.	▪ Run **D:\2276\Labs\Mod05\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 **Local Area Connection**, correct the problem.
4. Reset the computer configuration.	▪ Run **D:\2276\Labs\Mod05\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 some shared folder files, but the DEN-DC1 computer is inaccessible to her. You are at the user's computer to isolate the connectivity issue and either fix it yourself or pass it on to a systems engineer. For this scenario, you are working to restore connectivity to the DEN-DC1 computer.

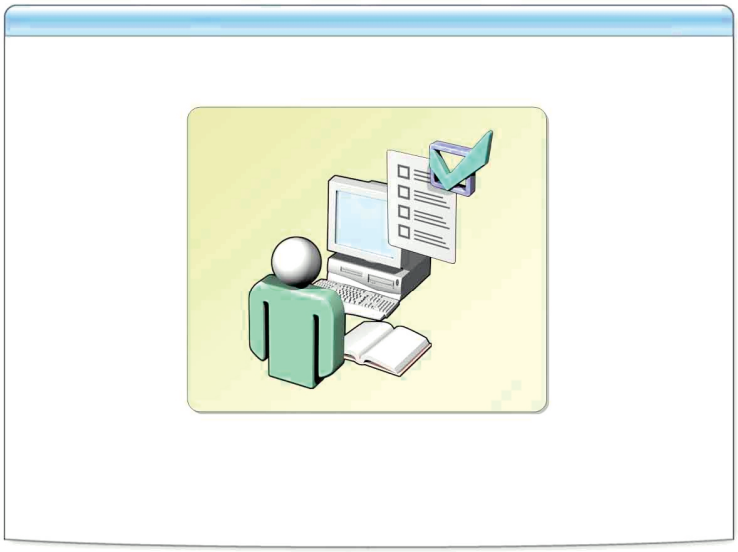
Tasks	Specific instructions
1. Introduce the problem.	▪ Run **D:\2276\Labs\Mod05\s3.bat**.
2. Isolate issues associated with this scenario.	**a.** Ping localhost. **b.** Ping DEN-DC1. **c.** Run Nslookup to query the DEN-DC1 computer.
Can you ping the localhost? Did you receive an answer?	
Can you ping DEN-DC1? What is the response? What is the displayed address for DEN-DC1?	
Was the Nslookup query on the DEN-DC1 computer successful?	
What is the most likely problem?	
3. Correct the problem.	
4. Reset the computer configuration.	▪ Run **D:\2276\Labs\Mod05\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 DEN-DC1 computer and cannot access any of the files located in shared folders on the DEN-DC1 computer. In this scenario, you are working to restore connectivity to the DEN-DC1 computer.

Tasks	Specific instructions
1. Introduce the problem.	▪ Run **D:\2276\Labs\Mod05\s4.bat**.
2. Isolate issues associated with this scenario.	**a.** Ping localhost. **b.** Ping DEN-DC1. **c.** Ping 10.10.0.2.
Can you ping localhost successfully? Is TCP/IP functioning properly?	
Can you ping DEN-DC1 successfully? What does the output of the ping indicate?	
Can you ping 10.10.0.2? What is the reply?	
What is the issue?	
3. Correct the problem.	
4. Reset the computer configuration.	▪ Run **D:\2276\Labs\Mod05\r4.bat**.
5. Complete the lab exercise.	▪ Close all programs and shut down all computers. Do not save changes.

Course Evaluation



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

To complete a course evaluation, go to the Metrics That Matter page of the Knowledge Advisors Web site at http://www.metricsthatmatter.com/MTMStudent/ClassListPage.aspx?&orig=6&VendorAlias=survey.

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