

Module 4: Configuring a Client for Name Resolution

Contents

Overview	1
Lesson: Resolving Client Names	2
Lesson: Managing the ARP Cache	4
Lesson: Overview of NetBIOS	13
Lesson: Using Static Name Resolution	25
Lesson: Using Dynamic Name Resolution	35
Lesson: Summarizing the Name Resolution Process	44



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, Microsoft Press, 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:
100 minutes

Lab:
00 minutes

As part of the Microsoft® Windows® Server 2003 installation process, system administrators specify a name by which the computer is known to the network. The Windows Setup program refers to this as a computer name and it is used to generate other names, such as a Network Basic Input/Output System (NetBIOS) name and a Domain Name System (DNS) host name. To use NetBIOS names on a Transmission Control Protocol/Internet Protocol (TCP/IP) network, there must be mechanisms that resolve the names into Internet Protocol (IP) addresses and then to media access control (MAC) addresses needed for TCP/IP communication. This module describes the various types of name resolution mechanisms provided by the Windows operating systems and how students use them for clients on the network.

After completing this module, students will be able to:

- Describe how client names are resolved.
- Describe how Address Resolution Protocol (ARP) resolves client MAC addresses.
- Describe the function of NetBIOS.
- Configure a client to use a static IP address.
- Configure a client to use a dynamic IP address.
- Configure a client to use name resolution servers.

Required materials

To teach this module, you need the Microsoft PowerPoint® file 2276B_04ppt.

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 practices.
- Review the referenced Request for Comments (RFCs).

How to Teach This Module

This section contains information that will help you to teach this module.

Lesson: Resolving Client Names

This section describes the instructional methods for teaching this lesson.

Multimedia: The Name Resolution Process

This presentation describes the methods a DNS client can use to resolve an IP address from a fully qualified domain name (FQDN). Discuss the presentation with students. Emphasize that a comprehensive understanding of DNS is beyond the scope of this course.

Lesson: Managing the ARP Cache

This section describes the instructional methods for teaching this lesson.

Static and Dynamic ARP Cache Entries

Emphasize that each network adapter has its own MAC address which never changes. Demonstrate the dynamic entries in the ARP cache.

How ARP Resolves IP Addresses to MAC Addresses

Describe the steps of the ARP process by using the animated slide. Tell students that when they use Network Monitor, this is the traffic they are viewing.

Using the ARP Tool to Manage the ARP Cache

Use your computer to demonstrate the output from the **arp -a** command.

Practice: Identifying a MAC Address

Review the practice scenario, and make sure students know the value of *x*, the network number for the classroom.

Practice: Viewing and Modifying the ARP Cache

Review the practice scenario, and discuss the need for clearing the cache.

Lesson: Overview of NetBIOS

This section describes the instructional methods for teaching this lesson.

The Types of Names Computers Use

Review the different types of names, and emphasize that the NetBIOS name can represent a single computer or a group of computers.

What Is NetBIOS?

Use the graphic to explain how NetBIOS applications relate to both the TCP/IP and Open Systems Interconnection (OSI) models.

What Is a NetBIOS Name?

Review the table of suffixes, and tell students to use the **nbtstat** command to view the NetBIOS name on their computers.

What Is NetBT?

Emphasize that the types of NetBIOS over TCP/IP (NetBT) nodes determine how NetBIOS naming functions are performed.

Practice: Determining and Setting the NetBT Node Type of a Client

Review the practice scenario and ask students what other reasons might there be for changing the client node type.

What Is Nbtstat?

Use your computer to demonstrate **nbtstat** specifying the **-n** switch and explain the statistics that are displayed.

Lesson: Using Static Name Resolution

This section describes the instructional methods for teaching this lesson.

Using an Lmhosts File

Review how the Lmhosts file is used to resolve names, and use your computer to show the Lmhosts file for the London computer.

Practice: Adding an Entry to the Lmhosts File.

Review the practice scenario and tell students that **nbtstat** switches are case-sensitive. Use the example, **nbtstat -r** lists names resolved and **-R** purges and reloads the cache.

Using a Hosts File

Emphasize that students would only use a Hosts file for a small network, or when there is no DNS server. Contrast using a Hosts file with using an Lmhosts file.

Adding an Entry to the Hosts File

Review the practice scenario and ask students what they think is causing the problem.

Lesson: Using Dynamic Name Resolution

This section describes the instructional methods for teaching this lesson.

What Is WINS?

Emphasize that Microsoft Windows Internet Name Service (WINS) is used to resolve NetBIOS names. Tell students that WINS is more commonly used with earlier versions of Windows operating systems.

What Is DNS?

Use the graphic to review the hierarchy of the DNS namespace, and make sure students understand that they must include a period after com in an FQDN. Remind students that they do not need a comprehensive understanding of DNS.

The DNS Suffix

Tell students to look at the DNS suffix for their computers in **System Properties**.

Practice: Using Ipconfig to Manage the DNS Client Resolver Cache

Review the practice scenario and discuss the changes that occur when they flush the cache.

Practice: Configuring a Client to Use a Name Server

Review the practice scenario and discuss the reasons for using WINS.

Lesson: Summarizing the Name Resolution Process

This section describes the instructional methods for teaching this lesson.

How Client Names Are Resolved

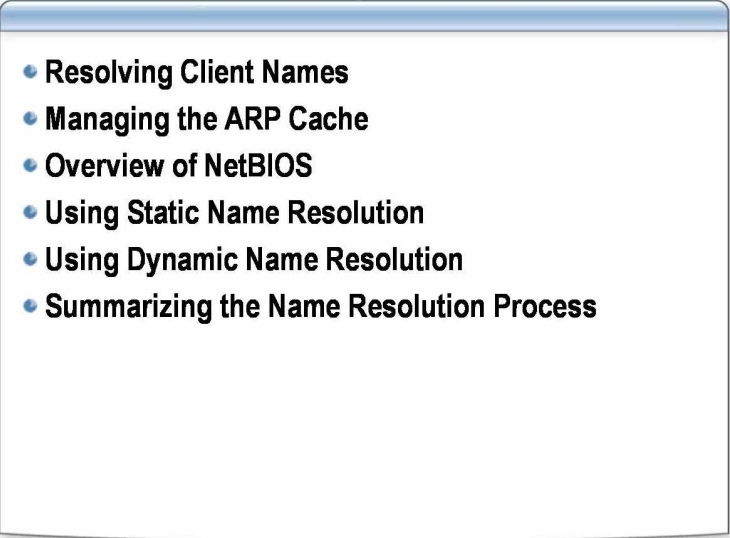
Use the animated graphic to review the name resolution process. Remind students that the resolution process varies according to node types.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

There are no labs in this module, and as a result, there are no lab setup requirements or configuration changes that affect replication or customization.

Overview

- 
- Resolving Client Names
 - Managing the ARP Cache
 - Overview of NetBIOS
 - Using Static Name Resolution
 - Using Dynamic Name Resolution
 - Summarizing the Name Resolution Process

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

Introduction

As part of the Microsoft® Windows® Server 2003 installation process, you specify a name by which the computer is known to the network. The Windows Setup program refers to this as a computer name, and it is used to generate other names such as a Network Basic Input/Output System (NetBIOS) name and Domain Name System (DNS) host name. To use NetBIOS names on a Transmission Control Protocol/Internet Protocol (TCP/IP) network, there must be mechanisms that resolve the names into Internet Protocol (IP) addresses and then to media access control (MAC) addresses needed for TCP/IP communication. This module describes the various types of name resolution mechanisms provided by the Windows operating systems and how to use them for clients on your network.

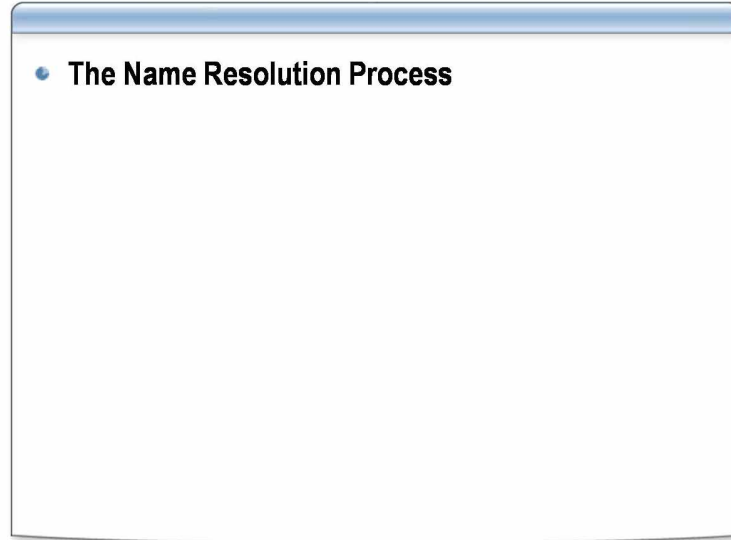
Note In this module, the term *client* refers to a computer running a Windows operating system on a network running TCP/IP. The term *host* includes clients and refers to any device on the network that has an IP address.

Objectives

After completing this module, you will be able to:

- Describe how client names are resolved.
- Describe how Address Resolution Protocol (ARP) resolves client MAC addresses.
- Describe the function of NetBIOS.
- Configure a client to use a static IP address.
- Configure a client to use a dynamic IP address.
- Configure a client to use name resolution servers.

Lesson: Resolving Client Names



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

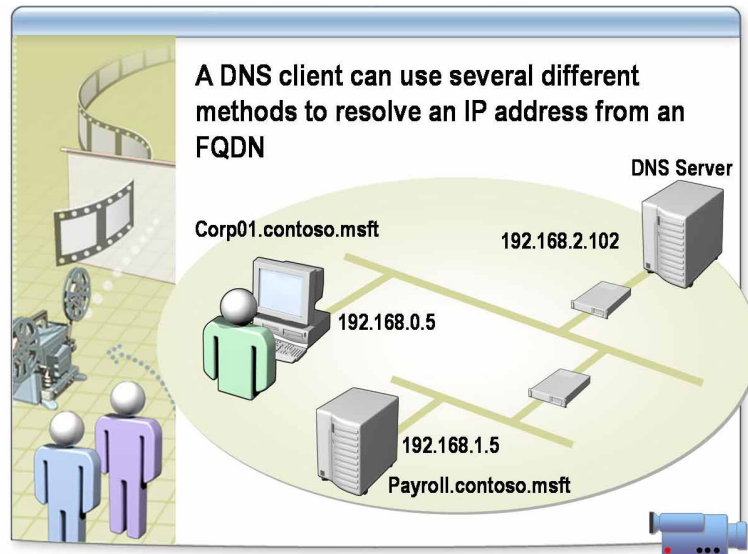
Introduction

You must configure the client computers on your network so that their computer names can be resolved into IP addresses. When you configure clients for name resolution, you are ensuring that they can communicate with other computers using computer names. For two hosts to communicate on a network, the MAC address of each host must be identified. An IP address is associated with a MAC address, and a computer name is associated with an IP address. Name resolution is the process of obtaining the IP address associated with the computer name. Knowing the various methods for resolving computer names assists you in performing these administrative tasks successfully.

Lesson objective

After completing this lesson, you will be able to describe how client names are resolved to IP addresses.

Multimedia: The Name Resolution Process



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

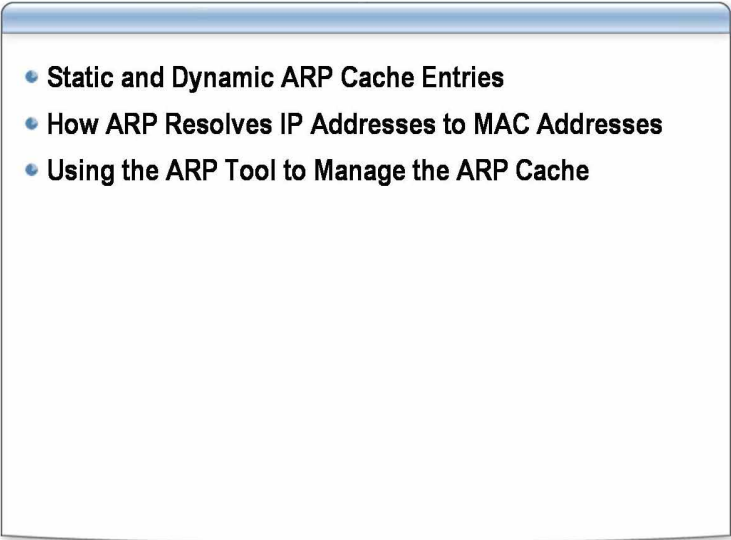
File location

To view the multimedia presentation, *The Name Resolution Process*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objective

Upon completion of this presentation, you will be able to describe the methods a DNS client can use to resolve an IP address from a fully qualified domain name (FQDN).

Lesson: Managing the ARP Cache

- 
- Static and Dynamic ARP Cache Entries
 - How ARP Resolves IP Addresses to MAC Addresses
 - Using the ARP Tool to Manage the ARP Cache

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

Introduction

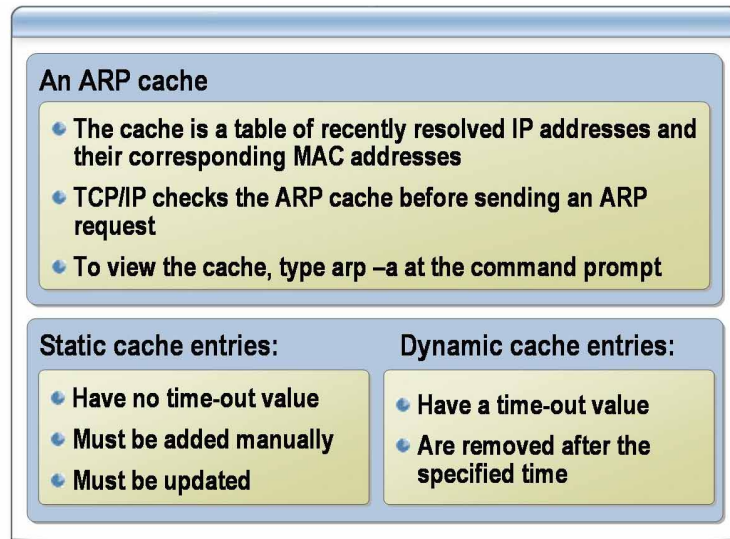
Each network adapter has a unique and permanent MAC address, also known as a physical address, which corresponds to one or more IP addresses associated with the adapter. The MAC address is used as a final destination address, and it must be resolved from the IP address so that the computer can receive data. You use ARP, which is a TCP/IP protocol, to resolve MAC addresses. To ensure that ARP is functioning correctly, you must know how ARP works and how to manage ARP entries.

Lesson objectives

After completing this lesson, you will be able to:

- Recognize static and dynamic ARP cache entries.
- Describe how ARP resolves IP addresses to MAC addresses.
- Use the ARP tool to manage the ARP cache.
- Modify the ARP cache.

Static and Dynamic ARP Cache Entries



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

Introduction

ARP performs IP address-to-MAC address resolution for outgoing packets of data. The packet includes the source and destination IP address. Each outgoing packet is encapsulated in a frame, at which time source and destination MAC addresses must be added. ARP determines the destination MAC address for each frame.

The ARP cache

To minimize the amount of broadcast network traffic that ARP generates, the computer stores recently resolved IP addresses and their corresponding MAC addresses in a cache. 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. TCP/IP checks the cache before sending out a broadcast request to obtain a MAC address.

Static cache entries

Windows Server 2003 includes a command-line utility called `Arp.exe` that you can use to view and manipulate the contents of the ARP cache. For example, you can use `Arp.exe` to add the MAC addresses of computers you contact frequently to the cache, thus saving time and network traffic during the connection process. Addresses that you add manually are static, meaning that they are not deleted after the usual expiration period. The cache is stored in memory, however, so it is erased when you restart the computer. It is rarely necessary to add static routes to the ARP cache. However, you might temporarily add a route to troubleshoot a network connectivity issue.

Adding routes incorrectly is likely to disrupt network communication to the host identified in the entry.

Note If you want to preload the cache when you start your system, you can create a batch file containing `Arp.exe` commands and execute it from the Windows Startup group. However, you must update these cache entries when computers are added to, or removed from, your network.

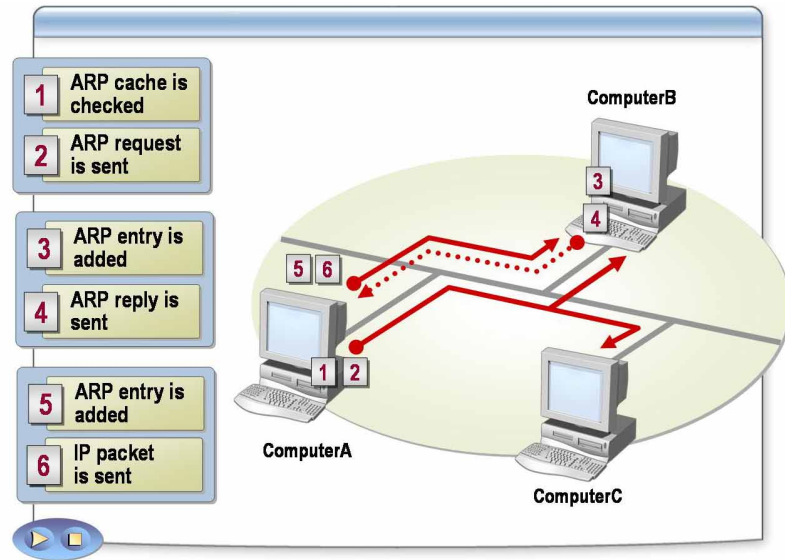
Dynamic cache entries

Dynamic entries are added to the cache during the ARP resolution process. Dynamic entries have a time-out value associated with them to remove them from the cache after a specific amount of time. Dynamic ARP cache entries for Windows Server 2003 are given a maximum time-out value of ten minutes.

How to view the ARP cache

To view the ARP cache on a Windows Server 2003–based computer, type **arp -a** at the command prompt.

How ARP Resolves IP Addresses to MAC Addresses



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

Introduction

Before transmitting an IP packet, TCP/IP clients must resolve the forwarding or next-hop IP address to its corresponding MAC address. If the MAC address for the next-hop is not in the ARP cache, the client will broadcast an ARP request frame to obtain the MAC address. The computer using that IP address responds with an ARP reply message containing its MAC address. With the information in the reply message, the computer can encapsulate the IP packet in the appropriate frame and transmit it to the next-hop.

The ARP process

In the proceeding illustration, ComputerA is broadcasting an ARP request to ComputerB and ComputerC. The following steps describe the process:

1. On ComputerA, ARP consults its own ARP cache for an entry for the destination IP address. If an entry is found, ARP proceeds to step 6.
2. If an entry is not found, ARP on ComputerA builds an ARP Request frame containing its own MAC address and IP address and the destination IP address. ARP then broadcasts the ARP Request.
3. ComputerB and ComputerC receive the broadcasted frame and the ARP Request is processed. If the receiving computer's IP address matches the requested IP address (the destination IP address), its ARP cache is updated with the address of the sender of the ARP Request, ComputerA.

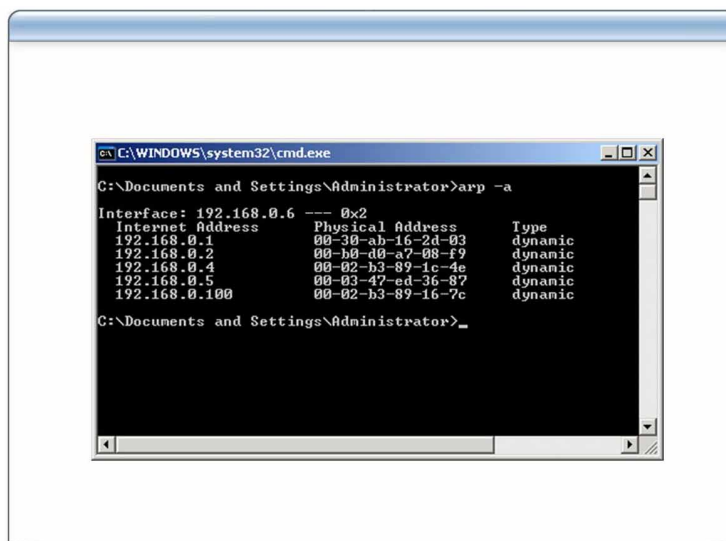
If the receiving host's IP address does not match the requested IP address, as in the case of ComputerC, the ARP Request is discarded.

4. ComputerB formulates an ARP Reply containing its own MAC address and sends it directly to ComputerA.
5. When ComputerA receives the ARP Reply from ComputerB it updates its ARP cache with the IP address and MAC address.

ComputerA and ComputerB now have each other's IP to MAC address mappings in their ARP caches.

6. ComputerA sends the IP packet to ComputerB.

Using the ARP Tool to Manage the ARP Cache



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

Introduction

You can use the ARP tool to view and modify entries in the local ARP cache. The ARP cache, which is a memory-resident list, contains one or more tables that store IP addresses and the corresponding MAC addresses that have been resolved from other computers on the same subnet. A separate table exists for each network adapter installed on the computer.

How to use ARP to isolate connection issues

You can use the ARP tool to isolate connections issues. For example, if two computers on the same subnet cannot communicate with each other, you can use ARP to determine if the correct MAC addresses are listed. To verify the MAC addresses are correctly listed in the ARP cache, you run the **arp -a** command on each computer. This displays the IP and MAC addresses listed in the ARP cache for each computer. You verify the MAC address listed in the ARP cache is the same as the actual MAC address for the destination computer by using Ipconfig.exe.

Example of output from the arp -a command

The following example shows the output for the **arp -a** command, which displays the ARP cache tables for all network interfaces.

```

C:\>arp -a
Interface: 172.16.0.142 on Interface 0x2
Internet address      Physical address      Type
172.16.0.1            00-e0-34-c0-a1-40     dynamic
172.16.1.231          00-00-f8-03-6d-65     Dynamic
172.16.3.34           08-00-09-dc-82-4a     Dynamic
172.16.4.53           00-c0-4f-79-49-2b     Dynamic
172.16.5.102          00-00-f8-03-6c-30     Dynamic

```

How to use the arp -a command

To display the ARP cache table specifically for the interface that is assigned the IP address 172.16.1.231, type **arp -a -N 172.16.1.231**

The **arp -a** command is also useful for determining whether the IP protocol is properly associated, or bound, to the network adapter. If it is not, the command shows an empty ARP cache. To determine bindings for the network adapter you are currently using, use the **ipconfig /all** command.

ARP syntax and parameters

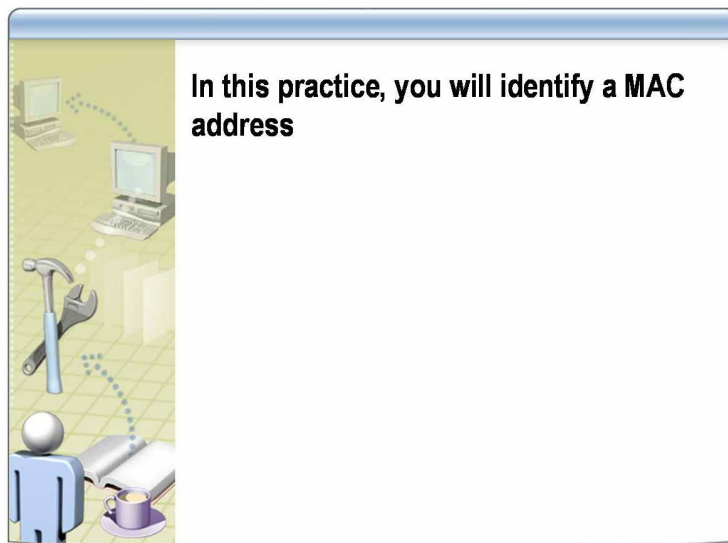
ARP uses the following syntax:

arp [-a [*InetAddr*] [-N *IfaceAddr*]] [-g [*InetAddr*] [-N *IfaceAddr*]] [-d *InetAddr* [*IfaceAddr*]] [-s *InetAddr EtherAddr* [*IfaceAddr*]]

The following table describes the function of the ARP parameters.

Parameter	Function
-a	Displays current ARP cache entries for all interfaces. To display the ARP cache entry for a specific IP address, type arp -a <i>InetAddr</i> , where <i>InetAddr</i> is an IP address.
-N	Lists ARP entries for the interface specified by -N <i>IfaceAddr</i> , where <i>IfaceAddr</i> is the IP address assigned to the interface. The -N parameter is case sensitive.
-g	Displays the current ARP entries for all interfaces if no <i>InetAddr</i> is specified. To display the ARP cache entry to a specific IP address, type arp -g <i>InetAddr</i> .
-d	Removes an entry specified by its IP address (<i>InetAddr</i>) from the ARP cache. To remove an entry for a specific interface, type arp -d <i>IfaceAddr</i> , where <i>IfaceAddr</i> is the IP address assigned to that interface. To delete all entries, use the asterisk (*) wildcard in place of <i>InetAddr</i> .
-s	Adds a static entry to the ARP cache that resolves the specified IP address (<i>InetAddr</i>) to the MAC address (<i>EtherAddr</i>). To add a static ARP cache entry to the table for a specific interface, type arp -s <i>IfaceAddr</i> , where <i>IfaceAddr</i> is the IP address assigned to that interface.
/?	Displays ARP parameters.

Practice: Identifying a MAC Address



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

Introduction

In this practice, you will identify the MAC address of your computer and the MAC address of the instructor computer.

Scenario

You are isolating connectivity issues and want to determine the MAC addresses of two computers.

Practice

► Identify the MAC address of the local computer

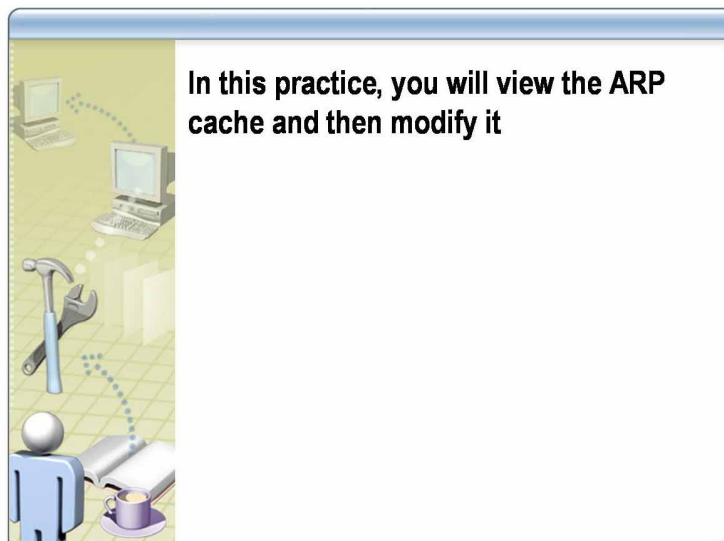
1. Log on to your computer with your *ComputerUser* account (where *Computer* is the name of your computer), and with a password of **P@ssw0rd**
2. Open a command prompt, type **ipconfig /all** and press ENTER.
3. Locate the Physical Address attribute.

The physical address value is your MAC address.

► Identify the MAC address of a remote computer on your network

1. At the command prompt type **ping 192.168.x.200** where *x* is the network number for the classroom, and press ENTER.
2. After receiving a successful reply, type **arp -a** and press ENTER.
3. Locate the physical address for 192.168.x.200. This is the MAC address for 192.168.x.200.
4. Close the command prompt.

Practice: Viewing and Modifying the ARP Cache



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

Introduction

In this practice, you will clear the ARP cache, use the Ping utility (Ping) on a client computer, and add an invalid ARP cache entry to determine the impact of an incorrect MAC address.

Scenario

You use Ping to test, or *ping* a remote computer and do not receive a reply. You decide to determine whether the ARP cache has the correct MAC address associated with the router's IP address. You determine that the MAC address for the router is incorrect and decide to add a static ARP cache entry.

Practice

► Clear the ARP cache and add a dynamic entry

1. Using Run as, open a command prompt as *Computer*\Administrator (where *Computer* is the name of your computer), type **arp -d *** and press ENTER.

The specified entry was not found reply will be displayed if the ARP cache is already cleared.

2. To view the contents of the ARP cache, type **arp -a** and press ENTER.
3. What items are listed?

Answer: The No ARP Entries found reply is displayed. No items exist in the ARP cache.

4. Type **ping 192.168.x.200** and press ENTER.
5. Did you receive a reply?

Answer: Yes.

6. Type **arp -a** and press ENTER.
7. What items are listed in the ARP cache?

Answer: 192.168.x.200, its MAC address and type (Dynamic) are listed in the ARP cache. After the successful ping to 192.168.x.200, ARP stores the MAC address as a dynamic entry.

► **Add an invalid static entry to the ARP cache and then remove it**

1. At the command prompt, type **arp -s 192.168.x.200 11-11-11-11-11-11** and press ENTER.
2. At the command prompt, type **ping 192.168.x.200** and press ENTER.
3. Did you receive a reply?

Answer: No, because the MAC entry is invalid. The packet was sent to a non-existent MAC address.

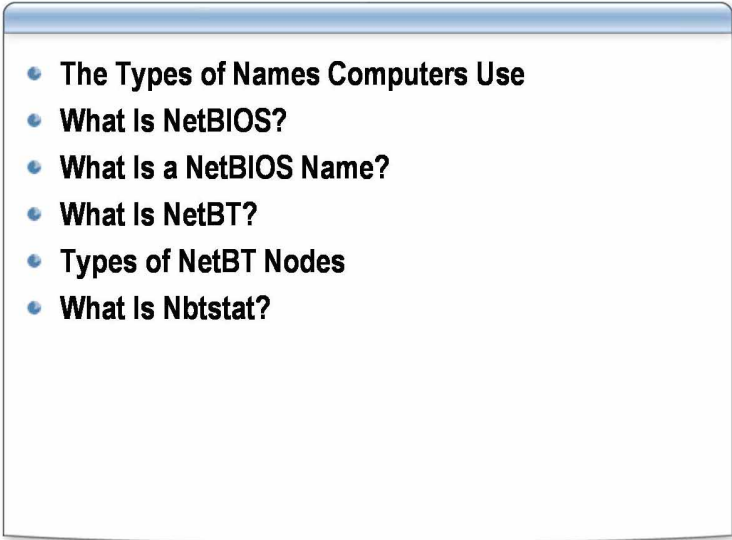
4. At the command prompt, type **arp -d *** and press ENTER.
5. At the command prompt, type **ping 192.168.x.200** and press ENTER.
6. Did you receive a reply?

Answer: Yes. When the ARP cache was cleared the invalid entry was deleted. When the ping command was issued, a new, valid entry was added to the ARP cache.

7. At the command prompt, type **arp -a** and press ENTER.
8. Is there an entry for 192.168.x.200?

Answer: Yes.

Lesson: Overview of NetBIOS

- 
- The Types of Names Computers Use
 - What Is NetBIOS?
 - What Is a NetBIOS Name?
 - What Is NetBT?
 - Types of NetBT Nodes
 - What Is Nbtstat?

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

Introduction

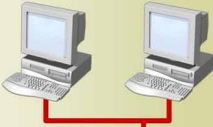

NetBIOS acts to connect applications together in the session and transport layers of TCP/IP, providing messaging and resource allocation. NetBIOS establishes logical names on the network, establishes sessions between two logical names on the network, and supports reliable data transfer between computer that have established a session. Understanding how NetBIOS functions in a network will assist you in understanding network communications.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the types of names computers use.
- Describe the function of NetBIOS.
- Determine the NetBT node type.
- Use Nbtstat.

The Types of Names Computers Use

Name	Description
 NetBIOS Names	<ul style="list-style-type: none"> • 16-byte address • Can represent a single computer or group of computers • 15 characters used for the name • 16th character is used by the services that a computer offers to the network
 Host Names	<ul style="list-style-type: none"> • Assigned to a computer's IP address • 255 characters in length • Can contain alphabetic and numeric characters, hyphens, and periods. • Can take various forms <ul style="list-style-type: none"> • Alias • Domain name

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

Introduction

TCP/IP identifies source and destination computers by their IP addresses. However, computer users are much better at remembering and using names than numbers, so common, or user-friendly names are assigned to the computers IP address. These names are either NetBIOS names or host names.

Note Microsoft Windows 2000 and Windows Server 2003 do not require NetBIOS names; however, previous versions of Windows require NetBIOS to support networking capabilities.

NetBIOS name

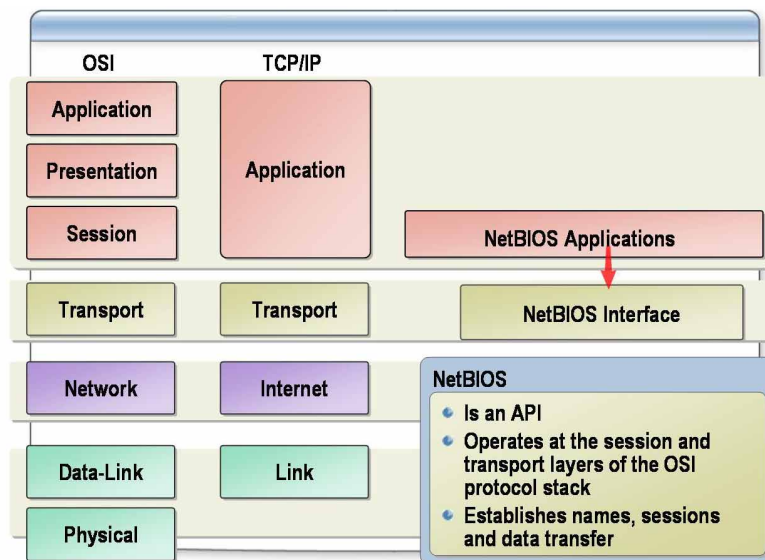
A NetBIOS name is a 16-character name that is used to identify a NetBIOS resource on the network. A NetBIOS name can represent a single computer or a group of computers. The first 15 characters may be used for the name. The final character is used to identify the resource or service that is being referred to on the computer.

An example of a NetBIOS resource is the File and Printer Sharing for Microsoft Networks component on a computer running Windows Server 2003. When your computer starts, this component registers a unique NetBIOS name, based on the name of your computer and character identifier that represents the component.

Host name

A host name is a user-friendly name that is assigned to a computer's IP address to identify it as a TCP/IP host. The host name can be up to 255 characters in length and can contain alphabetic and numeric characters, hyphens, and periods. Host names can take various forms. The two most common forms are alias and domain name. An alias is a single name associated with an IP address, such as *payroll*. A domain name is structured for use on the Internet and includes periods as separators. An example of a domain name is *payroll.contoso.com*.

What Is NetBIOS?



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

Introduction

NetBIOS is a specification created by IBM and Microsoft that allows distributed applications to access each other's network services independent of the transport protocol being used. It integrates with TCP/IP, running at the session and transport levels.

NetBIOS establishes names on the network, establishes sessions between two named services on the network, and supports reliable data transfer between computers that have established a session.

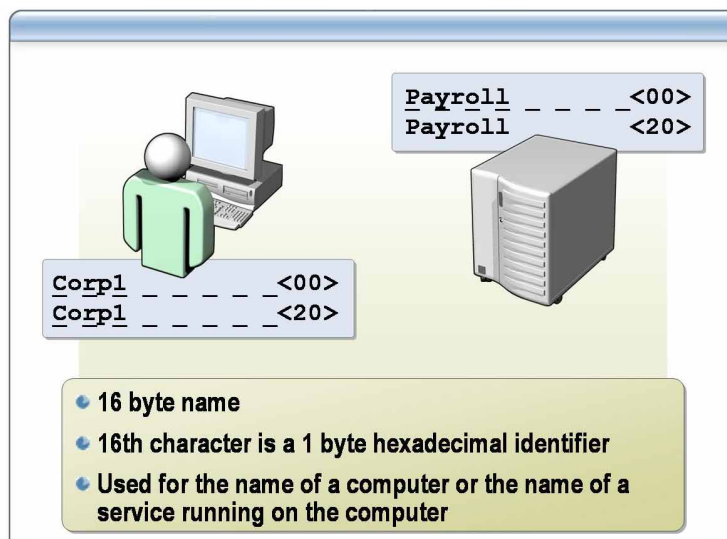
Definition of NetBIOS

NetBIOS provides network input/output services to support client/server applications on a network. From an architectural viewpoint, the NetBIOS specification defines:

- An interprocess communication (IPC) mechanism and application programming interface (API) that allows applications that are NetBIOS-enabled to communicate remotely over a network and request services from lower levels of the TCP/IP protocol stack. This is the primary and original definition of NetBIOS.
- A protocol operating at the session and transport layers of the Open Systems Interconnection (OSI) reference model that enables functions such as session establishment and termination as well as name registration, name renewal, and name resolution.

Note For more information about the TCP/IP and OSI models, see Module 1, "Reviewing the Suite of TCP/IP Protocols," in Course 2276A, *Implementing a Microsoft Windows Server 2003 Network Infrastructure: Network Hosts*.

What Is a NetBIOS Name?



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

Introduction

Each service that is NetBIOS-enabled requires a NetBIOS name to identify it on the network. This NetBIOS name consists of a name assigned to the computer during installation that can be up to fifteen characters, along with a sixteenth character that identifies the type of service or function that is being referred to on the computer.

NetBIOS names are registered dynamically when computers and services start and when users log on. The NetBIOS name space is flat, meaning that names can be used only once within a network.

How NetBIOS names are constructed

The fifteen-character name can include the computer name, the domain name, or the name of the user who is logged on. You must add spaces if needed to total fifteen characters. The sixteenth character is a 1-byte hexadecimal identifier.

For example, the sixteenth character identifying the Windows Server 2003 Messenger service has the 1-byte hexadecimal identifier 03h. On a computer running Windows Server 2003 named SERVER12 (Note the extra spaces make the name fifteen characters long), the Messenger service would be uniquely identified on the network with the NetBIOS name SERVER12 [03h]. NetBIOS names are also distinguished by whether they are:

- A unique name, which applies to a single IP address.
- A group name, which applies to multiple IP addresses.
- A multihomed name, which applies to a group of IP addresses assigned to a single host.

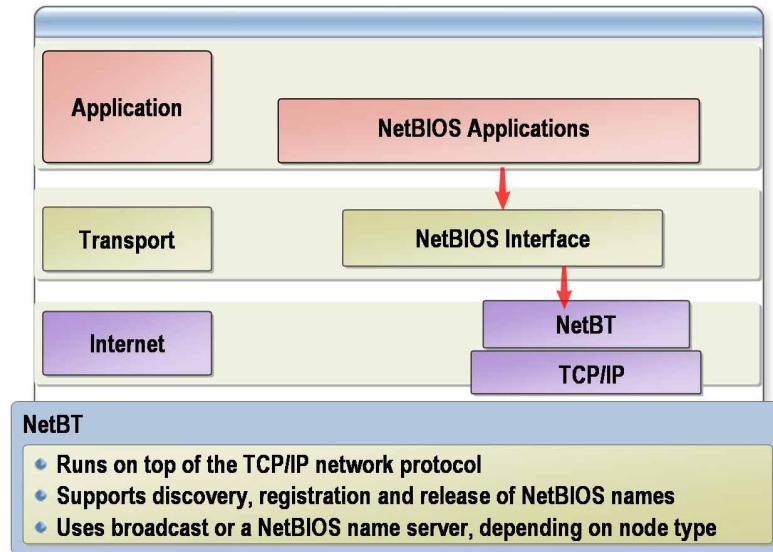
Common Suffixes for NetBIOS Names

The following table shows some of the more common suffixes that constitute the hidden sixteenth character of a NetBIOS name and the networking service with which they are associated.

Suffix (Hex)	First 15 Characters	Networking Service
00	Computer name	Workstation service
00	Domain name	Domain name
03	Computer name	Messenger service
03	User name	Messenger service
20	Computer name	File Server service
1B	Domain name	Domain master browser
1C	Domain name	Domain controllers
1D	Domain name	Master browser
1E	Domain name	Browser service election

Tip To view the NetBIOS names registered for your computer, use the **nbtstat -n** command.

What Is NetBT?



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

Introduction

By default, NetBIOS names do not function over a TCP/IP network. Windows Server 2003 enables NetBIOS clients to communicate over TCP/IP by providing the NetBIOS over TCP/IP (NetBT) protocol. By using this protocol, you are ensuring that NetBIOS-based applications can use TCP/IP to provide NetBIOS network services to NetBIOS applications. To effectively provide network communication between NetBIOS applications and hosts, you must understand NetBIOS naming functions.

What NetBT does

NetBT is the NetBIOS session-layer protocol and APIs running on top of TCP/IP. NetBT supports NetBIOS sessions, NetBIOS datagrams and naming functions such as the discovery, resolution, and release of NetBIOS names on a TCP/IP network.

How NetBIOS determines the method for naming functions

There are several ways that NetBT can perform naming functions. For example, NetBT can use a broadcast, or use a NetBIOS Name Server (NBNS) such as a Microsoft Windows Internet Name Service (WINS) server, or use both. The node type of the network device determines how NetBIOS naming functions are performed. Node refers to any uniquely addressable device on a network. The node type also determines the order in which the functions are performed.

The following list describes the NetBIOS naming functions:

- NetBIOS name resolution:
NetBT hosts that want to communicate with similar hosts must issue a NetBIOS name query request to resolve the NetBIOS name to its IP address.
- NetBIOS name registration:
NetBT hosts must register their unique NetBIOS names when they are initialized on a network to ensure that there are no duplicate names on the network. NetBIOS name registration can be done either by broadcasts or by unicast messages sent to a WINS server. Either or both methods can be used, and in either order, depending on the NetBT node type of the host.
- NetBIOS name release:
NetBT hosts must release their NetBIOS names when they are shut down or when a particular NetBIOS-enabled service is stopped on the server. This enables the released name to be used by another host. NetBIOS name release can be done by broadcasts or by unicast messages sent to a WINS server. Either or both methods can be used in either order, depending on the NetBT node type of the host.

Types of NetBT Nodes

NetBt Node Types	
B-node (broadcast)	Uses NetBIOS broadcast name queries
P-node (peer-to-peer)	Uses NBNS
M-node (mixed)	A combination of B-node and P-node. Uses broadcast by default
H-node (hybrid)	A combination of B-node and P-node. Uses NBNS by default
Microsoft enhanced B-node	Uses the Lmhosts file

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

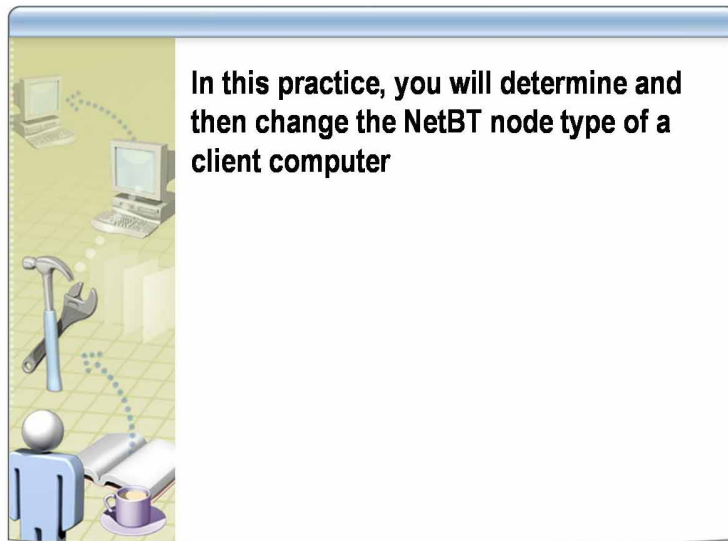
Introduction The method that NetBT applies to perform naming functions depends on the node type of the client.

NetBT Node Types The NetBT node types are listed in the following table.

Node Type	Method (in the Order Applied)	Comments
B-node (broadcast)	Broadcast only	Uses broadcast NetBIOS name queries for name registration and name resolution. Typically not forwarded by routers, so limited to local subnet. Can create excessive broadcast traffic for large subnets.
P-node (peer-to-peer)	NBNS only	Uses NBNS
M-node (mixed)	Broadcast, NBNS	A combination of B-node and P-node. Uses broadcast by default. If unable to resolve, uses NBNS.
H-node (hybrid)	NBNS, Broadcast	A combination of P-node and B-node. Uses NBNS by default. Default node type for Microsoft clients if an NBNS is configured on the network.
Microsoft enhanced B-node	NetBIOS name cache, Broadcast, Lmhosts file	An enhanced broadcast that utilizes the Lmhosts file. Default node type for Microsoft clients if no NBNS is configured on the network.

Tip You can configure the NetBIOS node type on a client running Microsoft Windows Server 2003 by using the registry, but the preferred way is to configure Dynamic Host Configuration Protocol (DHCP) to specify the node type to the client.

Practice: Determining and Setting the NetBT Node Type of a Client



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

Introduction In this practice, you will determine and set the NetBT node type of the client.

Scenario You are isolating NetBIOS name resolution issues. You have been asked to change the node type to b-node for a computer on a network segment that is unable to reach a name server.

Practice

► Determine the NetBT node type of your computer

1. At the command prompt, type **ipconfig /all** and press ENTER.
2. Locate the Node Type label. What is the NetBT node type?

Answer: Hybrid. Hybrid is the default node type for Windows Server 2003.

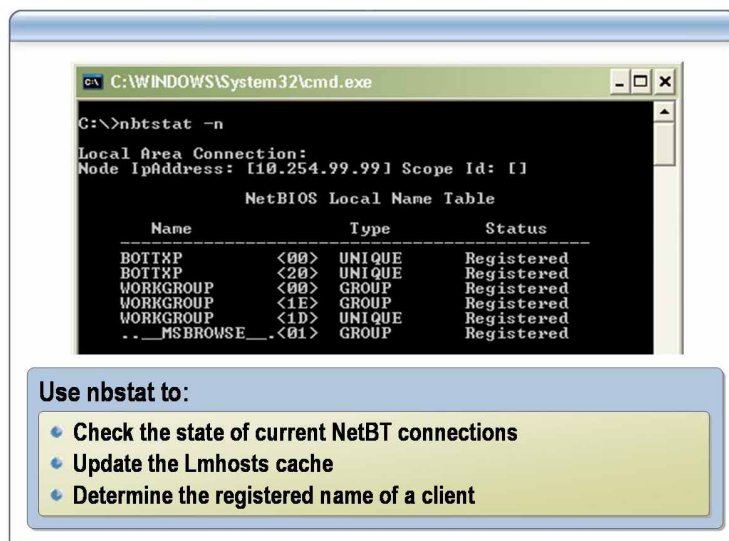
► Set the node type using a batch file

1. At the command prompt, type **cd c:\moc\2276\labfiles** and press ENTER.
2. Type **node p** and press ENTER.
3. Type **ipconfig /release** and press ENTER.
4. Type **ipconfig /renew** and press ENTER.
5. Type **ipconfig /all** and press ENTER.
6. Locate the Node Type label. What is the NetBT node type?

Answer: Peer-to-Peer. The batch file used Regini and p-node.ini to set the NodeType registry value to 2, which is Peer-to-Peer.

7. To return the node type to Hybrid, type **node h** and press ENTER.
8. Type **ipconfig /release** and press ENTER.
9. Type **ipconfig /renew** and press ENTER.
10. Type **ipconfig /all** and press ENTER.
11. Verify that Node Type is Hybrid.

What Is Nbtstat?



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

Introduction

Nbtstat is a TCP/IP utility that displays information about the NetBT connections that Windows uses when communicating with other Windows computers on the TCP/IP network. Nbtstat is installed on a computer running Microsoft Windows Server 2003 by default.

What nbtstat displays

Nbtstat displays NetBT protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. The NetBIOS name table is the list of NetBIOS names that corresponds to NetBIOS applications running on that computer. You can use Nbtstat to refresh the NetBIOS name cache and the names registered with WINS.

How to use nbtstat

You can use nbtstat to:

- View NetBT statistics on the computer.
- Determine the status of the computer's current network connections.
- Preload entries in an Lmhosts file into the NetBIOS name cache.
- View the NetBIOS name of a computer.
- Isolate NetBIOS name resolution issues.

To use nbtstat, run **nbtstat** from the command prompt.

Examples of nbtstat displays

nbtstat -n displays the NetBIOS names of the host that have been registered on the system;

nbtstat -c displays the current contents of the NetBIOS name cache, which contains NetBIOS name to IP address mappings for other hosts on the network.

Tip You can run nbtstat -a < ComputerName > to obtain the local NetBIOS name table on <ComputerName> and its MAC address.

Lesson: Using Static Name Resolution

- Using an Lmhosts File
- Guidelines for Configuring a Client to Use Lmhosts
- Using a Hosts File

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

Introduction

When users on your network specify a user-friendly name to communicate with a destination computer, TCP/IP requires an IP address for transmission to occur, so the computer name is resolved, or mapped to an IP address. This mapping is then stored in either a static or dynamic table, or in both tables. In a static table, mappings for NetBIOS names are stored in the Lmhosts file, and mappings for host names are stored in the Hosts file, or in both files.

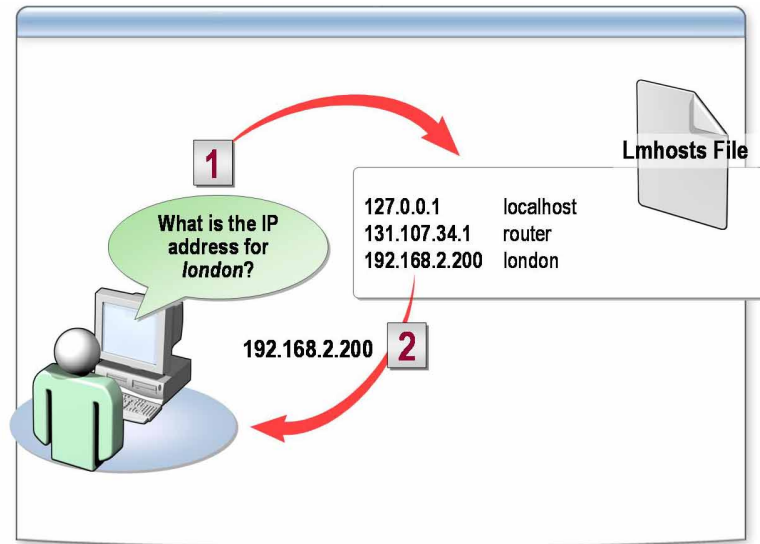
The advantage of using a static table is that, because it is a text file located on each computer, it is easy for you to customize. You can create any number of required entries, including easy-to-remember aliases or nicknames for frequently accessed resources. However, it is difficult to maintain and update static tables if the tables contain a large number of IP address mappings, or if the IP addresses change often.

Lesson objectives

After completing this lesson, you will be able to:

- Add an entry to an Lmhosts file.
- Add an entry to a Host file.

Using an Lmhosts File



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

Introduction

Windows Server 2003 enables you to map NetBIOS names manually to IP addresses by using the Lmhosts file. By using the Lmhosts file, you can reduce the number of IP broadcasts. Selected mappings from the Lmhosts file are maintained in a limited cache of mappings. This memory cache is local to the client computer and is initialized when the computer is started.

How the Lmhosts file resolves names

The name resolution process is as follows:

1. When the computer needs to resolve a name, the cache is examined first.
2. If there is no match in the cache, Windows Server 2003 uses broadcast NetBIOS Name Query request messages to try to find the NetBIOS computer.
3. If the IP broadcast name queries fail, the computer parses the complete Lmhosts file in addition to the cache to find the NetBIOS name and the corresponding IP address. In this way, the Lmhosts file can contain many mappings without requiring a large amount of static memory to maintain an infrequently used cache.
4. If the computer cannot resolve the name by using the Lmhosts file, the computer uses DNS for name resolution.

How to use the Lmhosts file

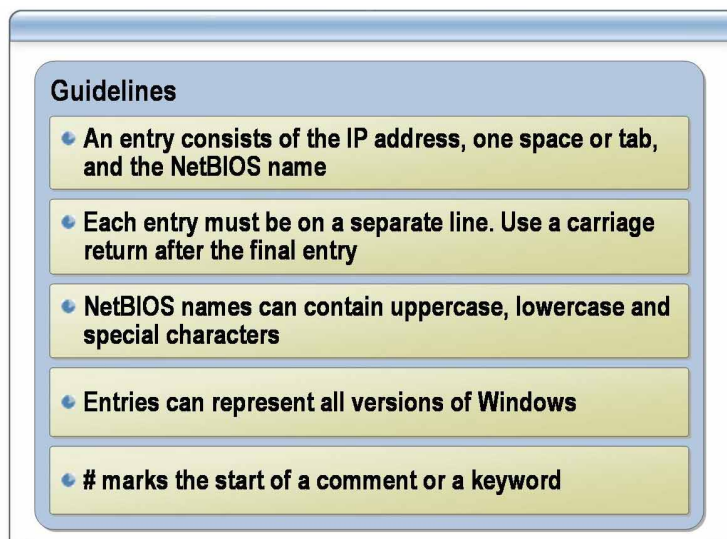
You can use the Lmhosts file to map computer names and IP addresses for computers outside of the local subnet; for example, you can use the Lmhosts file to find remote computers for network file, print, and remote procedure services. You can also use the Lmhosts file to locate domain controllers performing domain services such as logging on, browsing, and replication.

Before configuring a computer to use the Lmhosts file, you must create the primary Lmhosts file local to each computer, name the file Lmhosts, and save the file in the *systemroot*\System32\Drivers\Etc folder.

Because the Lmhosts file is a simple text file, you can create and change the Lmhosts file by using a text editor, such as Microsoft Notepad.

Caution An example Lmhosts file named Lmhosts.sam is provided in the Windows Server 2003 *systemroot*\System32\Drivers\Etc folder. This is only an example file. Do not use this file as the primary Lmhosts file.

Guidelines for Configuring a Client to Use Lmhosts



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

Introduction

There are no exact rules for configuring a client to use Lmhosts, however, there are guidelines you should follow to make sure that you configure the client correctly.

Guidelines for configuring a client to use Lmhosts

Use the following guidelines to create and edit entries in the Lmhosts file:

- To create an entry, use the IP address of the computer, followed by at least one space or tab and the NetBIOS name of the computer.

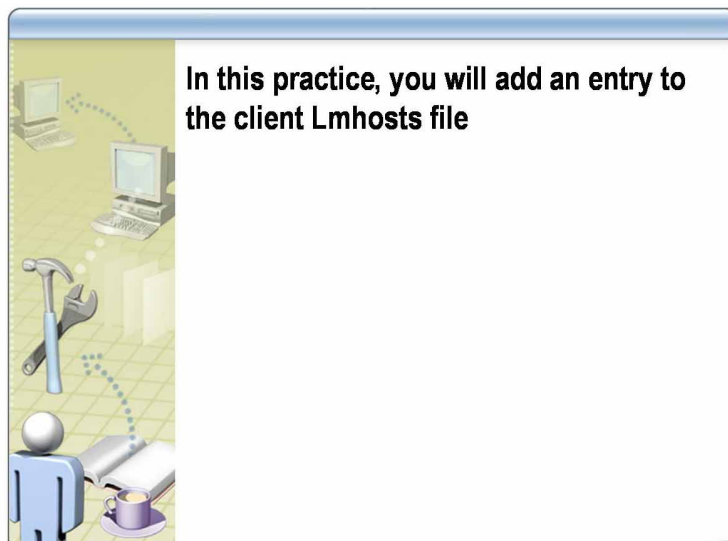
Caution You should not add an Lmhosts entry for a computer that is a DHCP client because the IP addresses of DHCP clients change dynamically. To avoid problems, make sure that the computers for which names are entered in the Lmhosts files are configured with static IP addresses.

- You must place each entry on a separate line. Add a carriage return after the final entry in the file.
- You can use uppercase and lowercase characters and special characters in NetBIOS names. If a name is placed between double quotation marks, it is used exactly as entered. For example, *AccountingPDC* is a mixed-case name, and *HumanRscSr* \0x03 specifies a name with a special character.
- Entries in the Lmhosts file can represent computers that are running Windows Server 2003 and earlier, as well as Microsoft LAN Manager and Microsoft Windows for Workgroups version 3.11 with Microsoft TCP/IP. There is no need to distinguish between different platforms in the Lmhosts file.

-
- Use the pound sign (#) to mark the start of a comment. You can also use # to designate special keywords. For example, #PRE which will cause the entry to be preloaded into the NetBIOS name cache.

Note For information about the keywords that you can use in the Lmhosts file, see “Creating Entries in the LMHOSTS File” in Appendix H of the *Microsoft Windows Server 2003 Resource Kit*.

Practice: Adding an Entry to the Lmhosts File



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

Introduction

In this practice, you will add an entry to an Lmhosts file, purge and reload the NBT Remote cache table, and verify that your entry has been loaded.

Scenario

You are isolating connectivity issues on a client computer and want to force NetBIOS name resolution using an Lmhosts file to preload a name into the NetBIOS name cache.

Practice

► Purge and view the contents of the NBT Remote cache

1. At the command prompt, type **nbtstat -R** and press ENTER.
A message is displayed stating the purge and preload of the NBT Remote Cache Name Table was successful.
2. Type **nbtstat -c** and press ENTER.
3. Record the entries, if any, below:

Answer: Answers will vary, however, most often the result will be **No names in cache**.

► Create review the sample Lmhosts file and add an entry to it

1. Click **Start**, point to **All Programs**, point to **Accessories**, right-click **Notepad** and then click **Run as**.
2. Click **Run as** and then click **The following user**.
3. In the **User name** box, verify that *Computer\Administrator* appears.
4. In the **Password** box, type **P@ssw0rd** and click **OK**.
5. On the **File** menu, click **Open**.

6. In the **Files of type** box, select **All Files**.
7. In the **File name** box, type **%windir%\system32\drivers\etc** and press ENTER.
8. Right-click **lmhosts.sam** and click **Rename**.
9. Delete “.sam” from the end of the file name, press ENTER, and then press F5.
10. Click **lmhosts** and then click **Open**.
11. Review the contents of the file.
The Lmhosts sample file contains information about how to create an lmhosts file.
12. On the **Edit** menu, click **Select all** and press the DELETE key.
13. At the first line of the file, type **192.168.x.200 MyLondon #PRE**
14. Save and close the Lmhosts file.

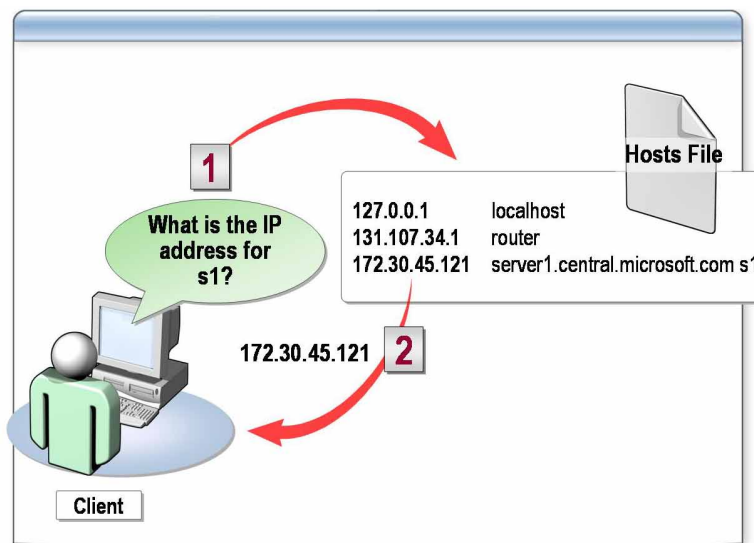
► **Purge and re-load the Lmhosts file into the NBT Remote cache**

1. At the command prompt, type **nbtstat -R** and press ENTER.
2. Type **nbtstat -c**, press ENTER, and then record the entries below:

Answer:

MYLONDON	<03> UNIQUE	192.168.x.200	-1
MYLONDON	<00> UNIQUE	192.168.x.200	-1
MYLONDON	<20> UNIQUE	192.168.x.200	-1

Using a Hosts File



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

Introduction

A Hosts file is a text file that provides a local method for resolution of host names into their respective IP addresses on a TCP/IP network. You can use Hosts files as an alternative to DNS servers, or together with DNS servers to resolve names on your TCP/IP network. You use a Hosts file on a small network or when it is not practical to maintain a DNS server.

Example of a table in the Hosts file

The following is a table of IP addresses and host names.

127.0.0.1	localhost
131.107.34.1	router
172.30.45.121	server1.central.microsoft.com s1

Note that the server at the IP address 172.30.45.121 can be referred to by either its FQDN, *server1.central.microsoft.com*, or the nickname, *s1*. Using a nickname allows a user to refer to the server without typing the entire FQDN.

Guidelines for using the Hosts file

Use the following guidelines to create and edit entries in the Hosts file:

- You can assign multiple host names to the same IP address.
- Entries in the Hosts file for Windows Server 2003 and Windows 2000 are not case sensitive.
- To create an entry, use the IP address of the computer followed by the FQDN. You can complete the entry with a comment. You use the pound sign (#) as a prefix for this optional comment.
- To locate the Hosts file, use the appropriate path as follows:
 - Microsoft Windows NT®, Windows 2000, and Windows XP:
%SystemRoot%\system32\drivers\etc\Hosts
 - Microsoft Windows 95 or Windows 98:
%WinDir%\Hosts

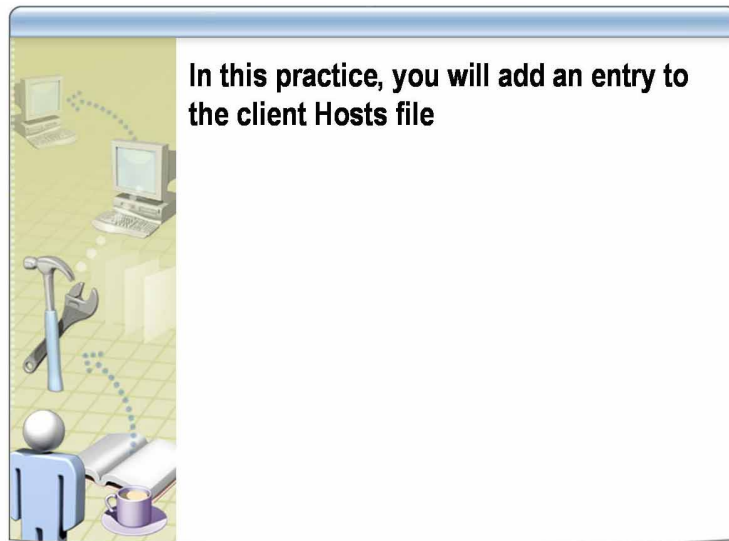
**Common causes of
Hosts file issues**

Connectivity issues associated with Hosts file are commonly caused by one or more of the following:

- The Hosts file does not contain the particular host name.
- The host name in the Hosts file or in the command is misspelled.
- The IP address for the host name in the Hosts file is invalid or incorrect.
- The Hosts file contains multiple entries for the same host on separate lines. Because the Hosts file is parsed from the top, the first entry found is used.

Tip Place the host names that need to be most frequently resolved near the top of the Hosts file, as the file is parsed linearly from the beginning.

Practice: Adding an Entry to the Hosts File



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

Introduction

In this practice, you will add an entry to a Hosts file.

Scenario

A client is unable to connect to a remote computer by its host name. The client is using a Hosts file for name resolution, and you have been asked to verify it and update it if necessary.

Practice

► Simulate the connectivity problem

1. At the command prompt, type **ping mocinstructor** and press ENTER.
2. Did you receive a reply?

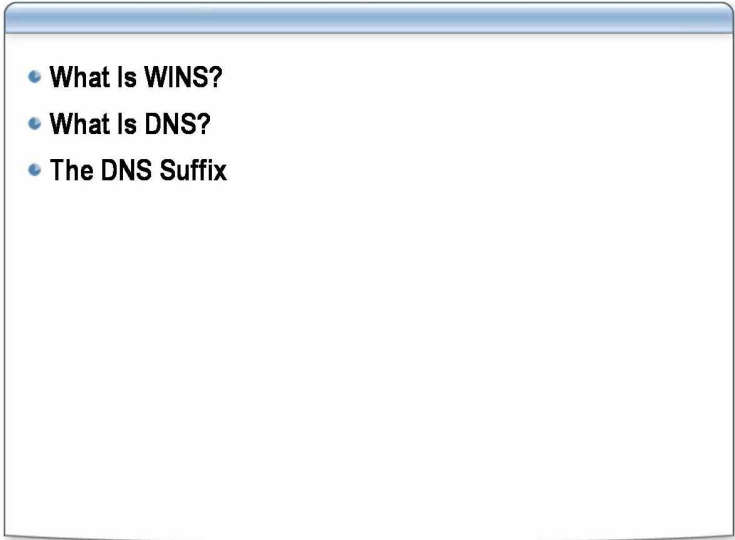
Answer: No, an error message is displayed stating Ping request could not find host mocinstructor. Please check the name and try again.

► Add an entry to a Hosts file

1. Using Run as open Notepad.exe as *Computer\Administrator*.
2. On the **File** menu, click **Open**.
3. In the **File name** box, type **c:\windows\system32\drivers\etc\hosts** and then click **Open**.
4. Add a new line at the end of the file, type **192.168.x.200 mocinstructor** and then press ENTER.
5. Save and close the Hosts file.
6. At the command prompt, type **ping mocinstructor** and then press ENTER.
7. Did you receive a reply?

Answer: Yes. The name is resolved using the Hosts file and a reply was received from 192.168.x.200.

Lesson: Using Dynamic Name Resolution

- 
- What Is WINS?
 - What Is DNS?
 - The DNS Suffix

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

Introduction

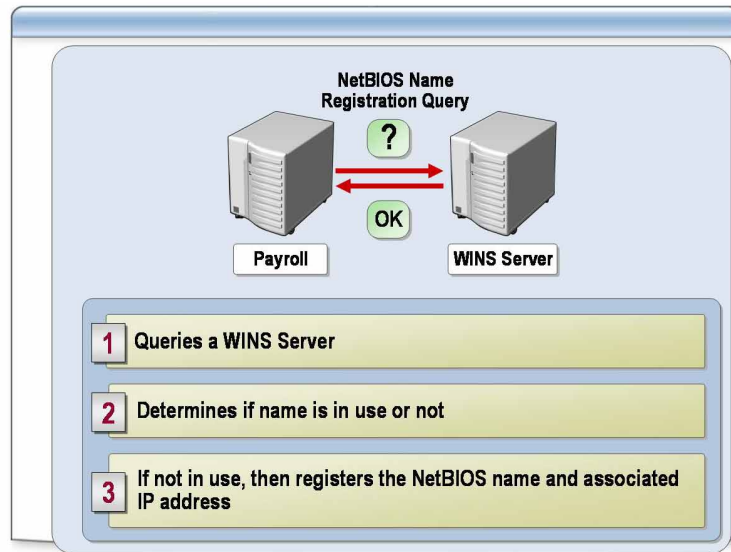
The advantage of using dynamic tables to store IP mappings is that the tables are updated automatically. To accomplish this, you use two Windows Server 2003 services: WINS and DNS. These services perform the same functions as the Lmhosts and Hosts files, but relieve you of the need to configure the files manually.

Lesson objectives

After completing this lesson, you will be able to:

- Describe WINS.
- Describe DNS.
- Use Ipconfig to manage the DNS client resolver cache.
- Configure a client to use a name server.

What Is WINS?



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

Introduction

WINS is a NBNS that you can use to resolve NetBIOS names to IP addresses when computers on your network are running Microsoft Windows Server 2003, Windows 2000, Windows NT 4.0, Windows 98, or Windows 95.

Benefits of using WINS

WINS provides a centralized database for registering dynamic mappings of NetBIOS names used on a network. WINS is built on a protocol that registers, resolves, and releases NetBIOS names by using unicast transmissions, rather than repeated transmissions of broadcast messages. This protocol allows the system to work across routers and eliminates the need for an Lmhosts file, restoring the dynamic nature of NetBIOS name resolution and allowing the system to work seamlessly with DHCP. For example, when dynamic addressing through DHCP creates new IP addresses for computers that move between subnets, the WINS database tracks the changes automatically.

Note WINS supports the NetBT mode of operation defined in Request for Comments (RFC) numbers 1001 and 1002 as p-node.

The WINS name resolution process

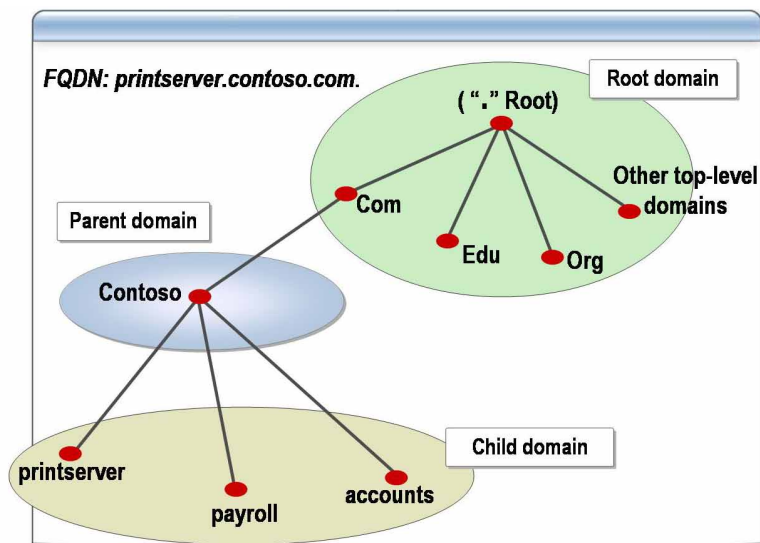
WINS is the Microsoft implementation of a NetBIOS name server. For WINS to function properly on a network, each client must:

- Register its NetBIOS name in the WINS database. When a client starts up, it will register its name with its configured WINS server.
- Renew its name registration at intervals. Client registrations are temporary, and from time to time a WINS client must renew its name or its lease will expire.
- Release names from the database when shutting down. When a WINS client no longer requires a name, for example when it is shut down, the client sends a message instructing the WINS server to release its name.

After it is configured with WINS as a name resolution method, the client will also use WINS to perform NetBIOS name queries. It does the following:

1. If the client cannot resolve the name from its cache, it sends a name query to its primary WINS server. If the primary WINS server does not respond, the client sends the request two more times.
2. If the client does not receive a response from its primary WINS server, the client resends the request to any additional WINS servers configured at the client. If a WINS server resolves the name, it responds to the client with the IP address of the requested NetBIOS name.
3. If no response is received, or if a Name not found message is received from the WINS server, the client then moves on to its next configured name resolution method.

What Is DNS?



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

Introduction

DNS provides a distributed database that is used to resolve FQDNs and other host names to IP addresses. All server versions of Windows 2003 include a DNS Server service. When you use DNS, you are enabling users on your network to apply user-friendly names, instead of IP addresses, to network resources.

How DNS resolves names to IP addresses

DNS uses a database of names and IP addresses to provide this service. DNS client software performs queries and updates to the DNS database. A user trying to locate a print server can use the DNS name *printserver.contoso.com*, for example, and have that name resolved to an IP address such as 172.16.23.55.

The DNS resolver cache

When DNS receives a positive response to a query, it adds that response to its client resolver cache. DNS always checks the cache before querying any other DNS servers. If a name is in the cache, DNS uses the name rather than querying other servers. This expedites queries and decreases network traffic for DNS queries.

Note For more information about DNS, see RFCs 1034 and 1035 under **Additional Reading** on the Student Materials compact disc.

The DNS namespace

The schema of the DNS database groups information about network resources into a hierarchical structure of alphanumeric *domains*. The hierarchical structure of domains is an inverted tree structure beginning with a *root domain* at its apex and descending into separate branches with common levels of *parent domains* and downward further into singular *child domains*. The representation of the entire hierarchical domain structure is known as a DNS *namespace*.

A DNS namespace may be created in any TCP/IP network by hosting the DNS root domain on a DNS server, but each DNS namespace must be separate from all other DNS namespaces as they are separate hierarchies. The DNS namespace on the Internet is the most common DNS namespace, but you may create a separate DNS namespace within your network with its own root domain that is entirely unrelated to the Internet DNS namespace. As may be expected, configuring hosts in separate DNS namespaces so that they can locate each other is complicated and requires separate devices such as proxy servers.

DNS nodes

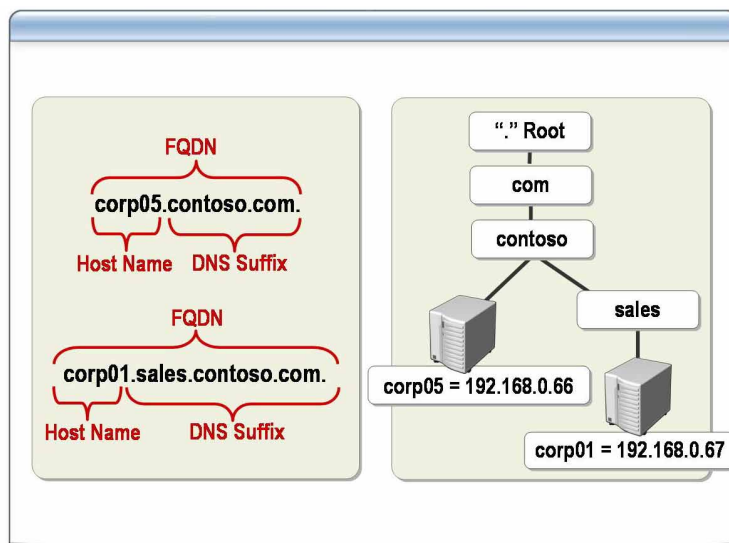
Each name in the DNS namespace is typically called a node. A DNS node, such as *ftp.contoso.com*, could represent a DNS domain, a host name, or a network service.

How DNS differs from WINS

DNS database records are replicated among DNS servers. The extensible nature and consequent size of the DNS database, along with the need to support frequent updates from multiple sources, requires that the DNS database be maintained in a distributed manner among DNS servers. In contrast, a WINS server is a flat database. Because WINS is a flat database it cannot be distributed and therefore does not have the scalability of a DNS database. Each DNS server hosts a portion of the DNS database and responds to queries for names in that portion with authoritative answers and then stores its answers in a cache. This local caching of query resolution information is used to improve performance.

Note For more information about DNS and the domain namespace, see Module 5, “Configuring DNS for Host Name Resolution,” in Course 2277A, *Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network: Network Services*.

The DNS Suffix



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

Introduction

In Windows Server 2003, you can enable users to locate and access a computer as identified by its FQDN using DNS.

The FQDN

The FQDN is a DNS name that uniquely identifies the computer on the network. By default, it is a concatenation of the host name, the primary DNS suffix, and a period. For example, an FQDN might be `corp01.sales.contoso.com.`

Primary DNS suffix

The primary DNS suffix name is the same as the domain name specified during installation of Windows Server 2003 and listed in **System Properties**. You can view the primary DNS suffix for your computer from the **Computer Name** tab of **System Properties**.

The primary DNS suffix is also known as the primary domain name. For example, the FQDN `corp05.contoso.com.` has the primary DNS suffix `contoso.com.`

Connection-specific DNS suffix

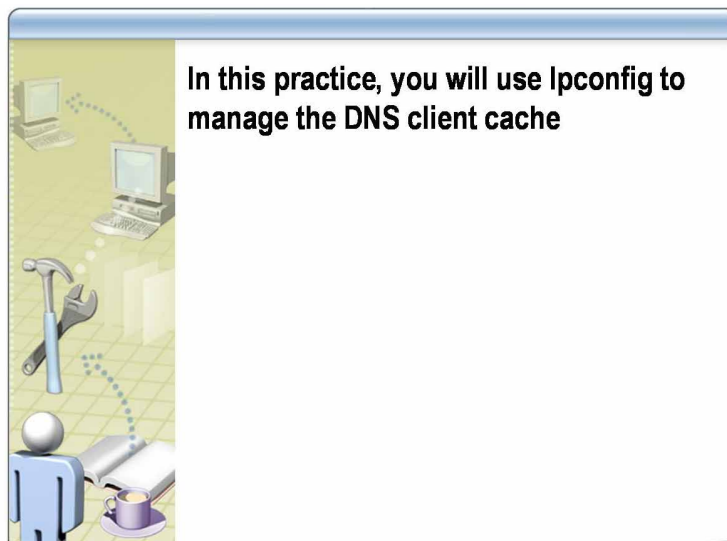
You can apply connection-specific DNS suffixes to the separate network adapter connections used by a *multihomed* computer to identify the host when it is connected to separate networks using different domain names. A multihomed computer is a computer with two or more network interfaces, such as network interface adapters. When using a connection-specific DNS suffix, a full computer name is also a concatenation of the host name and a connection-specific DNS suffix. For example, a connection-specific DNS suffix might be `sales.contoso.com.`

The connection-specific DNS suffix is also known as an adapter-specific DNS suffix.

Full computer name

The full computer name is a concatenation of the single-label host name, such as `corp01`, and a multi-label primary DNS suffix name, such as `sales.contoso.com.` Using the host and primary DNS suffix examples, the full computer name is `corp01.sales.contoso.com.` The host name is the same as the Computer Name specified during the installation of Windows Server 2003.

Practice: Using Ipconfig to Manage the DNS Client Resolver Cache



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

Introduction

In this practice, you will use Ipconfig to display and clear the DNS client resolver cache.

Scenario

You are isolating client connectivity issues that seem to involve incorrect DNS name resolution. You suspect that an expired entry is present in the client resolver cache and decide to clear it.

Practice

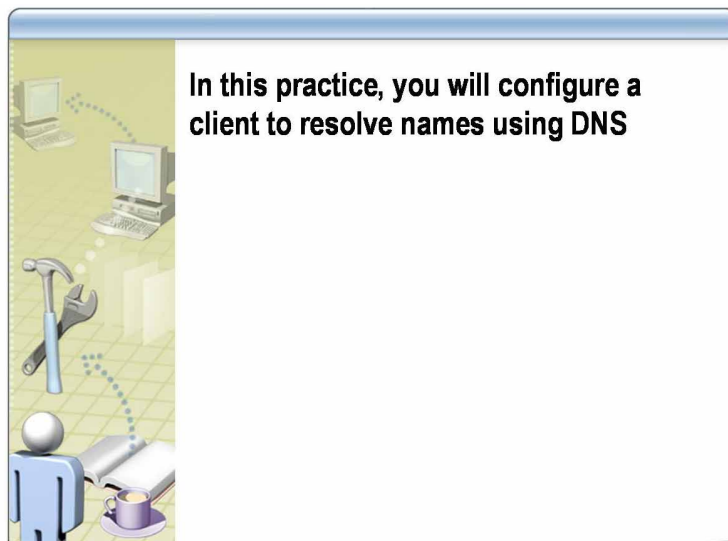
► View the DNS client resolver cache

1. At the command prompt, type **ipconfig /displaydns** and press ENTER.
2. Observe the DNS entries displayed. You may need to scroll up in the command window.
3. Type **ipconfig /flushdns** and press ENTER.
4. A message appears stating the cache was successfully flushed.
5. Type **ipconfig /displaydns** and press ENTER.
6. What entries are displayed?

Answer: The number and type of entries will vary; however, an entry for mocinstructor should be displayed since it is an entry in the Hosts file and the london.nwtraders.msft entry should have been removed from the cache.

7. Close all windows and log off.

Practice: Configuring a Client to Use a Name Server



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

Introduction

In this practice, you will configure the DNS client to use static DNS and WINS server addresses by using the Local Area Connections property sheet. This configuration would need to be performed on all computers that require Internet or intranet access where DHCP is not used.

Scenario

Your organization is opening a new satellite office that will have only 15 workstations and a router to connect to the Internet. This router will also be used to connect to the corporate network, but will continue using the same DNS server configuration. Because there will be no DHCP services in use by this office, you must configure static IP addresses and static DNS server addresses.

Practice

► Document your current Internet Protocol TCP/IP settings

1. Log on as administrator with a password of **P@ssw0rd**.
2. Open a command prompt, type **ipconfig /all** and then press ENTER.
3. Document your current TCP/IP settings:
 - a. IP address
 - b. Subnet mask
 - c. Default gateway
 - d. DNS servers
 - e. Primary WINS server

► **Configure the local area connection to use a static TCP/IP address**

1. Click **Start**, point to **Control Panel**, point to **Network Connections**, and then click **Local Area Connection**.
2. Click **Properties**.
3. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. Click **Use the following IP address**, and then use the settings that you documented in the previous procedure.
5. In the **Use the following DNS server addresses** section, enter the DNS server addresses that you documented in the previous procedure.
6. Click **OK** to accept the new settings, click **Close** to close the **Local Area Connection Properties** dialog box, and then click **Close** to close the **Local Area Connection Status** dialog box.
7. At the command prompt, type **ipconfig /all** and then press ENTER.
8. Verify that settings match those recorded in the previous procedure.

► **Configure the local area connection to use a WINS server**

1. At the command prompt, locate the Primary WINS Server attribute. Is it displayed?

Answer: No, it has not been configured.

2. Click **Start**, point to **Control Panel**, point to **Network Connections**, and then click **Local Area Connection**.
3. Click **Properties**.
4. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
5. On the **General** tab, click **Advanced**.
6. Click **WINS**, and then click **Add**.
7. In the **TCP/IP WINS Server** dialog box, type **192.168.x.200** and then click **Add**.
8. To close the **Advanced TCP/IP Settings** dialog box, click **OK**.
9. To close the **Internet Protocol (TCP/IP) Properties** dialog box, click **OK**.
10. To close the **Local Area Connection Properties** dialog box, click **Close**.
11. To close the **Local Area Connection Status** dialog box, click **Close**.
12. At the command prompt, type **ipconfig /all** and press ENTER.
13. Does the Primary WINS Server attribute appear?

Answer: Yes, it has been configured with 192.168.x.200 as the IP address.

14. Close all windows and log off.

Lesson: Summarizing the Name Resolution Process



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

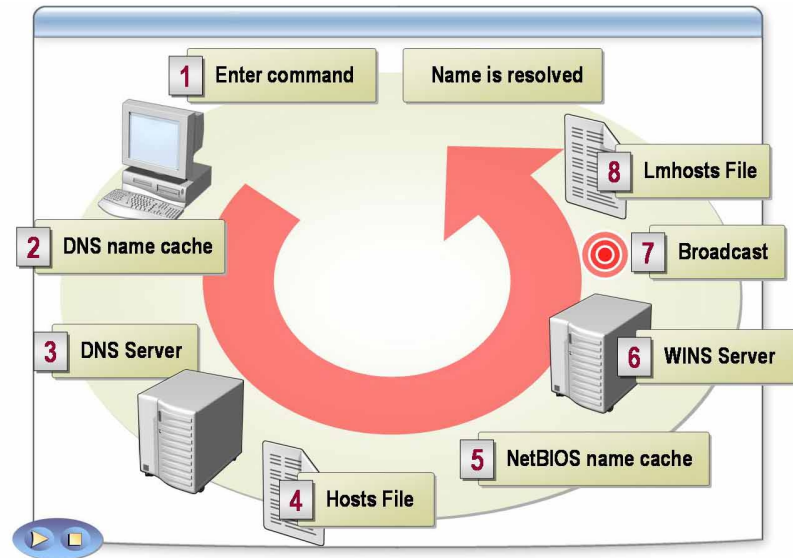
Introduction

TCP/IP identifies source and destination computers by their IP addresses. Name resolution methods attempt to determine the IP address associated with a name.

Objective

After completing this lesson, you will be able to describe the process of resolving client names to IP addresses.

How Client Names Are Resolved



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

Introduction

For hosts on your network to communicate with each other, their user-friendly names must be resolved to IP addresses.

What is name resolution?

Name resolution is the process by which the user-friendly name of a computer is resolved to its IP address on a TCP/IP network. Name resolution enables hosts to communicate with each other by using TCP/IP. After a host's name has been resolved to its IP address, ARP can then be used to resolve the next hop IP address into its corresponding MAC address. After the MAC address of the next hop address is known, frames may be placed on the network.

Name resolution in Windows

For clients running Windows Server 2003, Windows 2000, and Windows XP, you primarily use DNS to resolve names. Clients running previous versions of Windows primarily use NetBIOS names for network communication. As a result, these clients require a method of resolving NetBIOS names to IP addresses.

How it works

When you go to the command prompt of a machine running Microsoft Windows and type a Net Use command to map a drive to a network shared folder, you can type the NetBIOS name of the target host in the command. For example, *net use x: \\servername\sharename*. For this command to be fulfilled, the NetBIOS name of the remote host must first be resolved into its IP address so that it can be contacted on the network. This process is called NetBIOS name resolution.

You can use a number of different methods to perform NetBIOS name resolution. By default, a Windows Server 2003–based computer that is not configured as a WINS client or WINS server uses broadcast mode for name resolution.

Each method is successively tried until the name is resolved into its IP address or name resolution fails. Some methods will not be available—for example, when there is no NBNS or DNS server on the network.

Example of NetBIOS name resolution

The following table shows the order in which methods of name resolution are attempted when the NetBT node type of the client is H-node, **Enable Lmhosts Lookup** is checked on the **WINS** tab of **Advanced TCP/IP Properties** and **Enable DNS** registry setting is set to 1, as described in the following table.

Method in the order applied	Comments
1. Check local NetBIOS name cache	The cache contains recently resolved NetBIOS names.
2. Contact NBNS	This method works only if NBNS is configured. WINS is usually the NBNS on a Microsoft network. The requestor tries three times to contact the name server, and then tries three times to contact a secondary WINS server if there is one.
3. Perform local broadcast	The requestor broadcasts a NetBIOS name query request packet. The requestor tries three times before giving an error.
4. Check local Lmhosts file	The requestor checks if an Lmhosts file exists.
5. Check DNS client cache	The requestor checks its DNS client cache for the name.
6. Check local hosts file	On Windows Server 2003, the requestor checks the Hosts file if Enable DNS For Windows Resolution is selected on the WINS Address tab of the TCP/IP property sheet. This option is not available for Windows 2000.
7. Contact DNS server (if all methods fail, an error message states that the computer could not be found on the network)	The requestor contacts the DNS server if Enable DNS For Windows Resolution is selected on the WINS Address tab of the TCP/IP property sheet and the DNS tab has a DNS server specified on it. The requestor also tries 5, 10, 20, and 40 seconds later.

Note The name resolution process stops when the first IP address is found for the name.
