Microsoft®

Module 4: Configuring a Client for Name Resolution

Contents

Instructor Notes

Presentation:
85 minutes

Lab:
15 minutes

As part of the Microsoft® Windows Server™ 2003 installation process, systems administrators specify a name by which the computer is known to the network. The Microsoft 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 into media access control (MAC) addresses, which are needed for TCP/IP communication. This module describes the various types of name resolution mechanisms provided by the Windows operating systems and how students can use them for clients on the network.

After completing this module, students will be able to:

- Describe how name resolution occurs.
- Describe how host names are used and resolved.
- Describe how NetBIOS names are used and resolved.

Required materials

To teach this module, you need the Microsoft Office PowerPoint® file 2276C_04.ppt.

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 of the materials for this module.
- Complete the practices.
- Review the referenced RFCs.

How to Teach This Module

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

Lesson: Overview of Name Resolution

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 the students. Emphasize that a comprehensive understanding of DNS is beyond the scope of this course.

Types of Names That Computers Use

Emphasize to students that host names are used by most newer applications. NetBIOS names are generally used Windows NT and Windows 98 and earlier operating systems and applications.

Lesson: Resolving Host Names

This section describes the instructional methods for teaching this lesson.

Purpose of a Hosts File

Emphasize that students would only use a Hosts file for a small network or when there is no DNS server, because maintaining a Hosts file is awkward. Consider demonstrating how a host name is added to a Hosts file and pinging the new host name to show that it works.

What Is DNS?

Use the graphic to review the hierarchy of the DNS namespace, and make sure that students understand that they must include a period after *com* in an FQDN. Remind students that DNS is essential for the Active Directory® directory service.

How Windows Clients Use the DNS Suffix

Emphasize to students that in most cases, clients are configured with only one DNS suffix. Demonstrate how to add additional DNS suffixes.

DNS Resolver Cache

Review the benefits of the DNS resolver cache. Be sure that students understand that the content of the Hosts file is loaded into the DNS resolver cache. This is a change from earlier versions of Windows. Demonstrate how to use Ipconfig to display and clear the DNS resolver cache.

The Host Name Resolution Process

Review the host name resolution process to be sure that students understand how all of the host name resolution methods work together as part of an overall system. Indicate to students that the NetBIOS name resolution methods will be covered in more depth in the next lesson.

Practice: Resolving Host Names

Monitor the students during this practice to ensure that they understand the results that they are seeing. This practice should take about 10 minutes.

Lesson: Resolving NetBIOS Names

This section describes the instructional methods for teaching this lesson.

What Is NetBIOS?

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

What Is NetBT?

Emphasize the three NetBIOS naming functions. Students should understand that these functions need to be performed for any NetBIOS name resolution method.

Types of NetBT Nodes

Emphasize to students which are the default node types and when they are used, because most companies do not change the default node settings.

What Is Nbtstat?

Use your computer to demonstrate Nbtstat, specifying the **–n** switch, and explain the statistics that are displayed.

What Is Lmhosts?

Review how the Lmhosts file is used to resolve names and why it would be used. Use your computer to demonstrate adding an entry to the Lmhosts file on your DEN-CL1 virtual machine.

What Is WINS?

Emphasize that the Microsoft Windows Internet Naming Service (WINS) is used to resolve NetBIOS names. Tell students that WINS is usually used instead of an Lmhosts file.

The NetBIOS Name Resolution Process

Emphasize to students that while this process can vary depending on the NetBT node type, most companies do not change the default node settings.

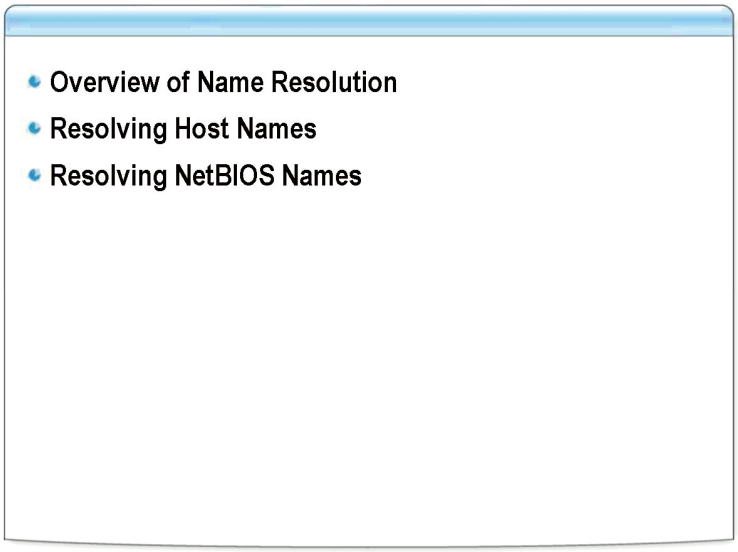
Practice: Resolving NetBIOS names

In this practice, students add an entry to the Lmhosts file on their client. The entry uses #PRE to make the entry visible when viewing the NetBIOS name cache. Ensure that students understand that this is not always a requirement when adding entries to Lmhosts. This practice should take about 10 minutes.

Lab: Configuring a Client for Name Resolution

Remind the students that they can review the module for assistance in completing the lab. Tell students that a detailed answer key for each lab is provided in the Labdocs folder on the Student Materials compact disc.

Overview



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 Microsoft 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 into media access control (MAC) addresses, which are 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.

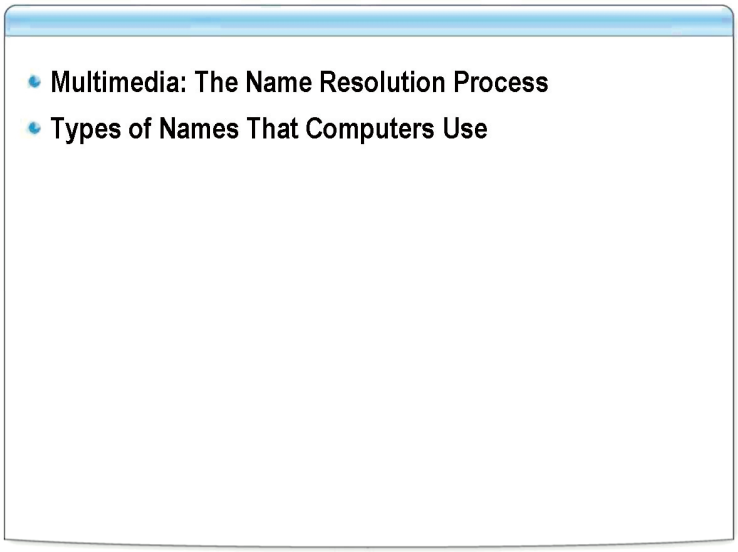
Note In this module, the term *client* refers to a computer running a Windows operating system on a network running TCP/IP. The term *host* includes clients and refers to any device on the network that has an IP address.

Objectives

After completing this module, you will be able to:

- Describe how name resolution occurs.
- Describe how host names are used and resolved.
- Describe how NetBIOS names are used and resolved.

Lesson: Overview of Name Resolution



Introduction

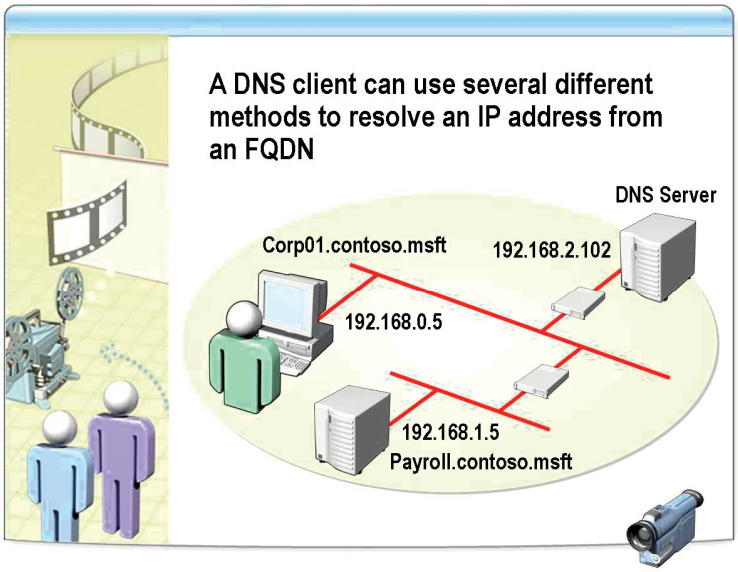
You must configure the client computers on your network so that their computer names can be resolved into IP addresses. When you configure clients for name resolution, you are ensuring that they can communicate with other computers using computer names. For two hosts to communicate on a network, the 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 objectives

After completing this lesson, you will be able to:

- Describe the name resolution process used by Windows clients.
- Describe why computers use names and the two types of names that they use.

Multimedia: The Name Resolution Process



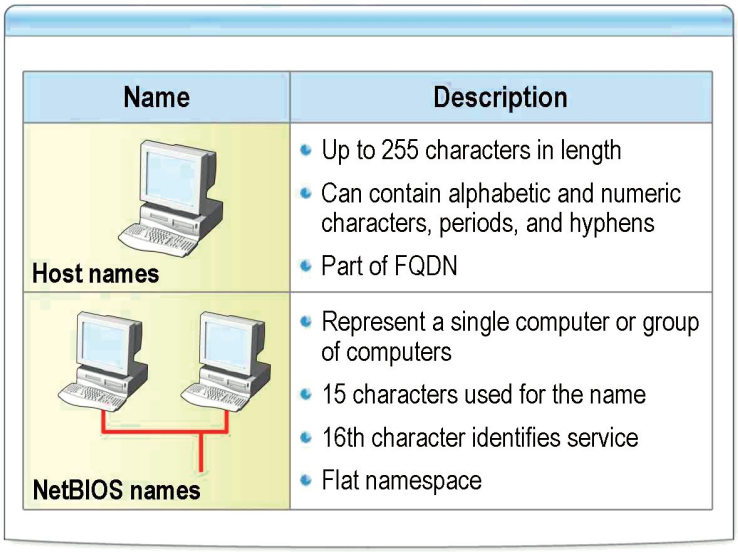
File location

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 that a DNS client can use to resolve an IP address from a fully qualified domain name (FQDN).

Types of Names That Computers 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 computer's IP address. These names are either NetBIOS names or host names.

Note Earlier versions of Windows require NetBIOS to support networking capabilities. Windows 2000, Windows XP, and Windows Server 2003 support NetBIOS for backward compatibility with earlier versions of Windows, but they do not require NetBIOS.

Choosing a name type

The name type used by an application is determined by the application developer. Windows operating systems allow applications to request network services through either Windows Sockets or NetBIOS. If an application requests network services through Windows Sockets, host names are used. If an application requests services through NetBIOS, a NetBIOS name is used.

Most current applications, including Internet applications, use Windows Sockets to access network services. NetBIOS is used by many earlier Windows applications. Windows 98 and earlier versions of Windows use only NetBIOS for file sharing. Windows 2000, Windows XP, and Windows Server 2003 use both Windows Sockets and NetBIOS for file sharing.

Note Windows Sockets applications allow users to specify the destination host by IP address or host name. NetBIOS applications require the use of a NetBIOS name.

Host name

A host name is a user-friendly name that is associated with 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, periods, and hyphens.

Note Although a host name can be up to 255 characters long, Windows Server 2003 and Windows XP support host names only up to 63 characters in length. The maximum number of characters between periods in a host name is 63.

Host names can be used in various forms. The two most common forms are an alias and an FQDN. An alias is a single name associated with an IP address, such as *payroll*. An alias can be combined with a domain name to create an FQDN. An FQDN is structured for use on the Internet and includes periods as separators. An example of an FQDN is *payroll.contoso.com*.

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 are used for the name. The final character is used to identify the resource or service that is being referred to on the computer.

The NetBIOS namespace is flat, meaning that names can be used only once within a network. NetBIOS names cannot be organized into a hierarchical structure, as can be done with FQDNs.

How NetBIOS names are constructed

The 15-character name can include the computer name, the domain name, and the name of the user who is logged on. 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, the Messenger service would be uniquely identified on the network with the NetBIOS name SERVER12 [03h]. (Note: the extra spaces make the name 15 characters long.) A NetBIOS name is also distinguished by whether it is:

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

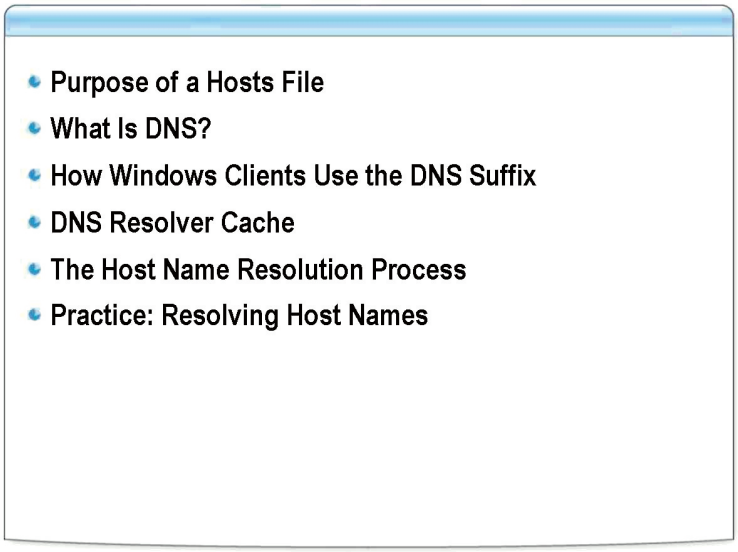
Common suffixes for NetBIOS names

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.

Lesson: Resolving Host Names



Introduction

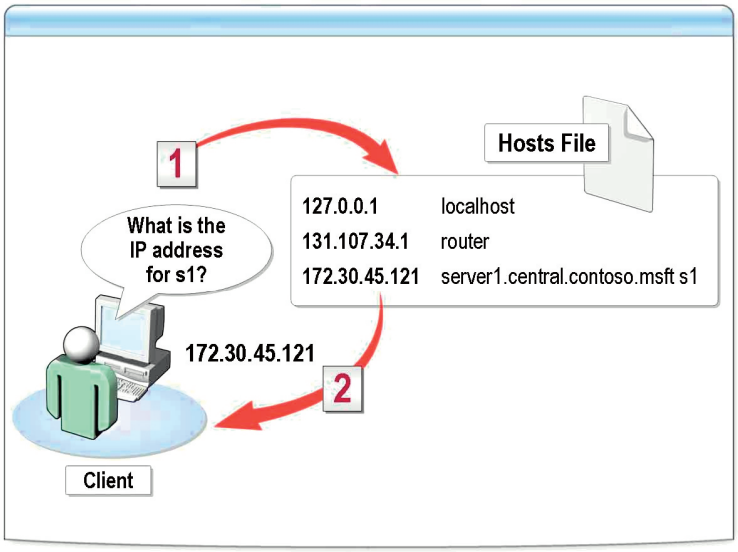
Host names are used for basic network services in Windows 2000, Windows XP, and Windows Server 2003. Proper resolution of host names to IP addresses is essential to the proper functioning of a Windows-based network. Network administrators must understand host name resolution in Windows to troubleshoot problems with host name resolution.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the purpose of a Hosts file.
- Describe what DNS is and how DNS is used to provide name resolution.
- Describe how Windows clients use the DNS suffix.
- Describe the DNS resolver cache.
- Describe the host name resolution process.
- Configure host name resolution.

Purpose of a Hosts File



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. Most networks do not use a Hosts file because maintaining the file on each individual computer and server is difficult. However, a Hosts file is often used during troubleshooting because adding an entry to a Hosts file is faster than reconfiguring a DNS server.

Hosts file entries

The following example shows three Hosts file entries:

```
127.0.0.1        localhost
131.107.34.1     router
172.30.45.121    server1.central.contoso.msft s1
```

The server with the IP address 172.30.45.121 can be referred to by its FQDN, *server1.central.contoso.msft*, or alias, *s1*. Using an alias 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
  - Windows 95 or Windows 98:

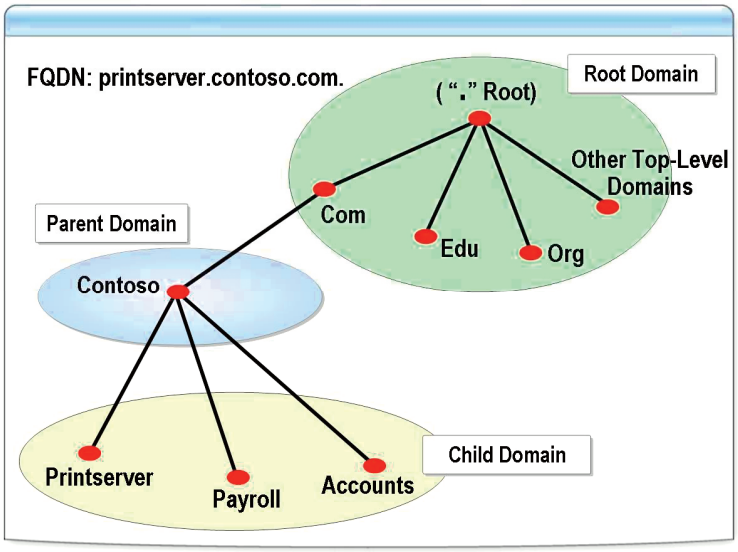
    \%WinDir%\Hosts

Common causes of Hosts file problems

Connectivity issues associated with the 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.

What Is DNS?



Definition

DNS is a service that uses a distributed database to resolve FQDNs and other host names to IP addresses. All server versions of Windows 2003 include a DNS 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 on 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.

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

The DNS namespace

DNS groups information about network resources into a hierarchical structure of *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*.

The Internet uses a single DNS namespace with multiple root servers. To participate in the Internet DNS namespace, a domain name must be registered with a DNS registrar. This ensures that no two organizations attempt to use the same domain name.

If hosts located on the Internet do not need to resolve names in your domain, you can host a domain internally, without registering it. However, you must still ensure that the domain name is unique from Internet domain names, or connectivity to Internet resources might be affected. A common way to ensure uniqueness is to create an internal domain in the .local domain. The .local domain is reserved for internal use in much the same way that private IP addresses are reserved for internal use.

A DNS namespace can 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 can create a separate DNS namespace within your network with its own root domain that is entirely unrelated to the Internet DNS namespace.

DNS nodes

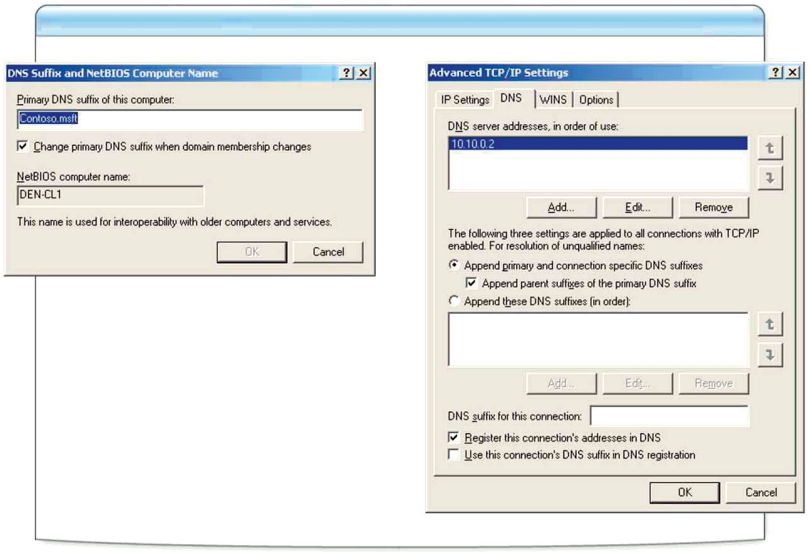
Each name in the DNS namespace is typically called a *node*. A DNS node, such as *ftp.contoso.com*, could represent a DNS domain, a host name, or a network service.

DNS and Active Directory

DNS is essential to the proper functioning of the Active Directory® directory service. Active Directory stores service location information in DNS. Clients require access to the service information in DNS to locate domain controllers and global catalog servers. Active Directory domains use the same naming structure as DNS domains.

Note For more information about DNS and the domain namespace, see Module 4, "Resolving Host Names by Using Domain Name System," in Course 2277, *Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure: Network Services*.

How Windows Clients Use the DNS Suffix



Introduction

A DNS suffix is used by a client for both resolving and registering DNS names. During host name resolution, the client attempts to resolve the host name by appending all configured DNS suffixes to the host name. During DNS name registration, the client registers its host name in DNS domains matching each configured DNS suffix.

In most cases, only a single DNS suffix, the *primary* DNS suffix, is configured. However, the ability to add additional DNS suffixes allows users to resolve resource host names in multiple domains without using FQDNs.

Primary DNS suffix

For clients that are members of an Active Directory domain, the primary DNS suffix is the same as the Active Directory domain. Client computers register their host names in DNS by using the primary DNS suffix. Client computers also resolve host names by using the primary DNS suffix.

If the "Append parent suffixes of the primary DNS suffix" option is selected, all parent domains of the primary DNS suffix will be used to resolve host names. For example, if a client is configured with the primary DNS suffix *contoso.msft*, that client will attempt to resolve host names by appending *contoso.msft* and *msft*.

The primary DNS suffix is configured in the **DNS Suffix and Netbios Computer Name** dialog box, which can be opened from the **Computer Name** tab in the **System Properties** dialog box. Other DNS suffix settings are configured on the **DNS** tab in the **Advanced TCP/IP Settings** dialog box.

Connection-specific DNS suffix

On a multihomed computer, you can apply a DNS suffix to a single adapter with a connection-specific DNS suffix. The connection-specific DNS suffix will be used in addition to the primary DNS suffix when host names are resolved.

When a multihomed computer registers its host name in DNS, only the IP address of the specified connection is registered in the domain specified in the connection-specific DNS suffix. In the domain specified in the primary DNS suffix, all IP addresses on the multihomed computer are registered. The "Use this connection's DNS suffix in DNS registration" option must be selected.

A connection-specific DNS suffix is typically used when a service is bound to only a single IP address on a multihomed computer. For example, a developer might have configured a test Web server to use only the IP address on the second network adapter in his client.

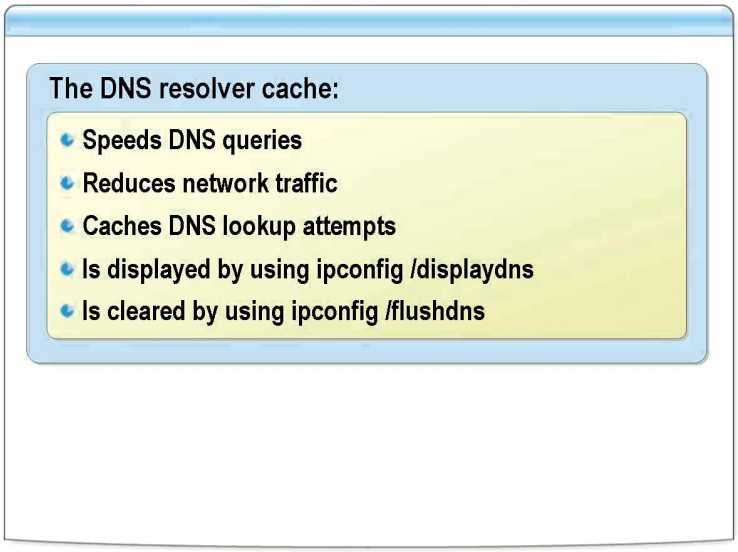
Additional DNS suffixes

In complex environments with many DNS domains, you can configure DNS suffixes in addition to the primary DNS suffix and any connection-specific DNS suffixes. Many large companies have several DNS domains for backward compatibility with earlier systems. These companies would configure additional DNS suffixes to enable host name resolution in several domains.

Full computer name

The full computer name of a Windows client is the concatenation of the single-label host name, such as *corp01*, and a multilabel 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.

DNS Resolver Cache



Introduction

The DNS resolver cache is used to speed up DNS queries and reduce network traffic. Clients always check the DNS resolver cache before sending a query to a DNS server. If a name is in the cache, the cached information is used rather than querying the DNS server.

DNS resolver cache contents

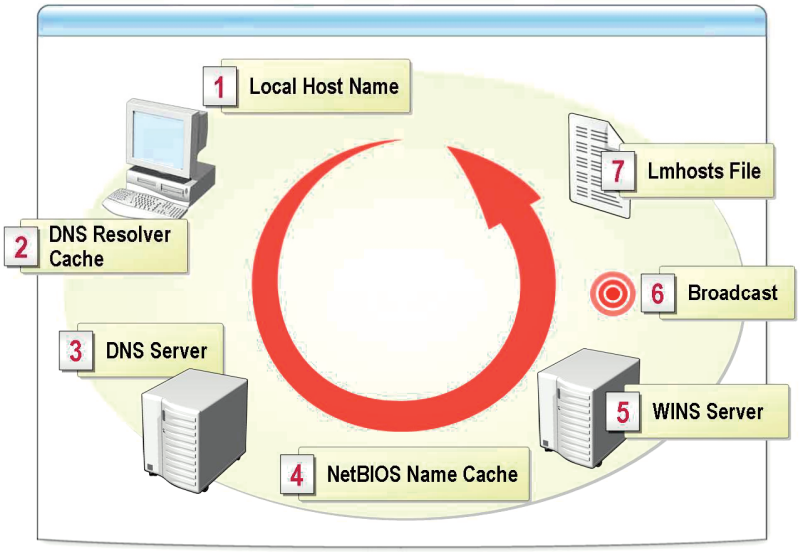
Each time a client attempts to resolve a host name through DNS, the result is added to the DNS resolver cache. If the query result is positive, the name stays in the cache for the period of time specified by the DNS server that hosts the record. In most cases, this is about 24 hours. If the result is negative, the failed attempt is cached for 300 seconds (5 minutes).

The DNS resolver cache also contains all host names specified in the Hosts file. If the Hosts file is modified, the contents are reloaded. Caching the Hosts file is more efficient than reading it each time a host name is resolved. Cache entries loaded from the Hosts file do not expire.

Controlling the DNS resolver cache

You can use Ipconfig to view and clear the DNS resolver cache. The command **ipconfig /displaydns** displays the contents of the DNS resolver cache. The command **ipconfig /flushdns** clears the contents of the DNS resolver cache. Clearing the DNS resolver cache is useful when an incorrect DNS record has been fixed but the incorrect result is still cached on the client.

The Host Name Resolution Process



Introduction

When an application uses Windows Sockets and a host name is specified, TCP/IP will use the DNS resolver cache and DNS when attempting to resolve the host name. If NetBIOS over TCP/IP is enabled, TCP/IP will also use NetBIOS name resolution methods when resolving host names. NetBIOS over TCP/IP is enabled by default.

The host name resolution process

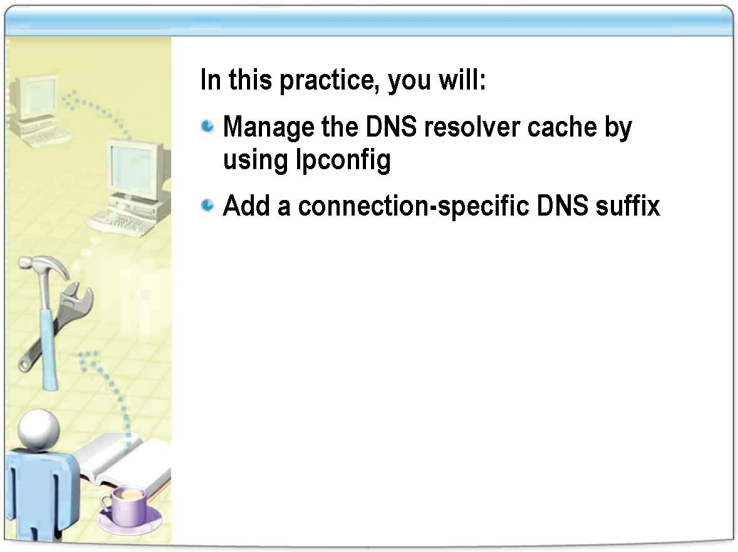
When NetBIOS over TCP/IP is enabled, the host name resolution process is as follows:

1. Windows checks whether the host name is the same as the local host name.
2. Windows searches the DNS resolver cache.
3. Windows sends a DNS request to its configured DNS servers.
4. Windows converts the host name to a NetBIOS name and checks the local NetBIOS name cache.
5. Windows contacts its configured Microsoft Windows Internet Naming Service (WINS) servers.
6. Windows broadcasts as many as three NetBIOS Name Query Request messages on the directly attached subnet.
7. Windows searches the Lmhosts file.

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

Note For more information about host name resolution, see Chapter 7, "Host Name Resolution," in *TCP/IP Fundamentals for Microsoft Windows* on the Microsoft Web site.

Practice: Resolving Host Names



Objectives

In this practice, you will:

- Manage the DNS resolver cache by using Ipconfig.
- Add a connection-specific DNS suffix.

Instructions

Be sure that the DEN-DC1 and DEN-CL1 virtual machines are started.

Practice

► **Manage the DNS resolver cache by using Ipconfig**

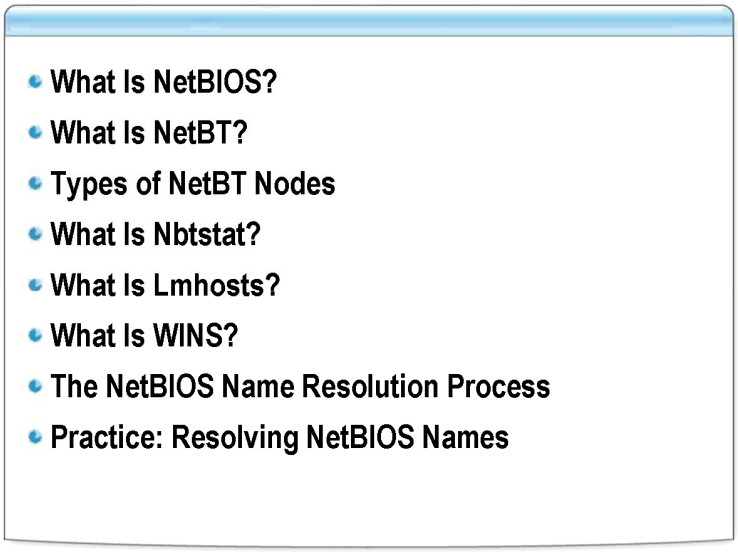
1. On DEN-CL1, log on as **Paul**, with a password of **Pa$$w0rd**.
2. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
3. At the command prompt, type **ipconfig /displaydns** and then press ENTER. Observe the DNS entries displayed. You might need to scroll up in the command prompt window. Notice that DEN-DC1 is in the list.
4. Type **ipconfig /flushdns** and then press ENTER.
5. Type **ipconfig /displaydns** and then press ENTER. Notice that DEN-DC1 is no longer in the list.
6. Click **Start**, point to **All Programs**, point to **Accessories**, and then click **Notepad**.
7. Click **File**, and then click **Open**. In the **Files of type** box, select **All Files**, browse to **C:\Windows\system32\drivers\etc\hosts**, and then click **Open**.
8. Scroll to the bottom of the Hosts file, and then type **127.0.0.5 testhost**.
9. Click **File**, click **Save**, and then close Notepad.
10. At the command prompt, type **ipconfig /displaydns**, and then press ENTER. Notice that **testhost** is now listed.
11. Close the command prompt window.

► **Add a connection-specific DNS suffix**

1. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **ipconfig /all** and then press ENTER. Notice that the primary DNS suffix is **contoso.msft**.
3. Type **ping DEN-DC1.contoso.msft** and then press ENTER. This test is successful because a DNS record has been created for DEN-DC1 in contoso.msft.
4. Type **ping DEN-CL1.testdom.msft** and then press ENTER. This test is unsuccessful because a DNS record has not been created for DEN-CL1 in testdom.msft.
5. Click **Start**, click **Control Panel**, double-click **Network Connections**, right-click **Local Area Connection**, and then click **Properties**.
6. Click **Internet Protocol (TCP/IP)**, click **Properties**, click **Advanced**, and then click the **DNS** tab.
7. In the **Suffix for this connection** box, type **testdom.msft**.
8. Select the **Use this connection's DNS suffix in DNS registration** check box.
9. Click **OK** twice, click **Close**, and then close Network Connections.
10. At the command prompt, type **ipconfig /registerdns** and then press ENTER. This command forces your client to reregister its host name with the DNS server.
11. Type **ping DEN-CL1.testdom.msft** and then press ENTER. This time, the ping is successful because a DNS record has been created for DEN-CL1 in testdom.msft.
12. Close the command prompt window.

Important Do not shut down the virtual machines.

Lesson: Resolving NetBIOS Names



Introduction

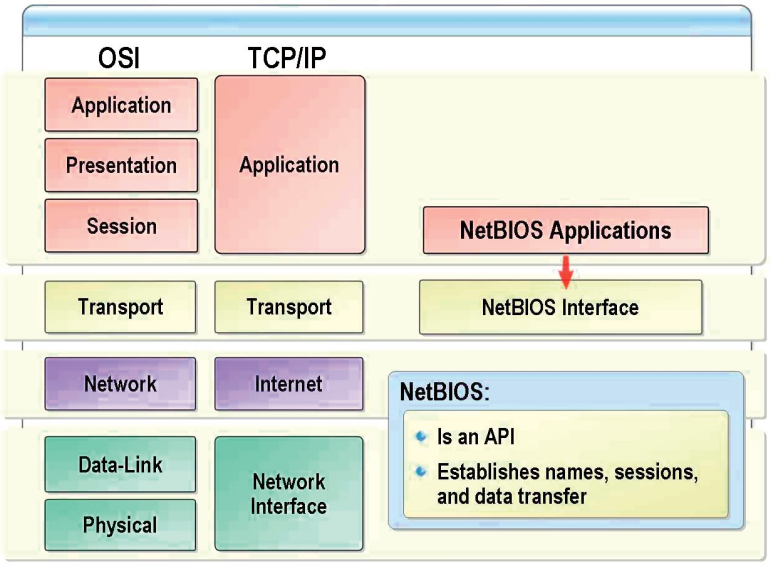
NetBIOS acts to connect applications in the session and transport layers of TCP/IP, providing messaging and resource allocation. NetBIOS establishes logical names on the network, establishes sessions between two logical names on the network, and supports reliable data transfer between computers that 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 NetBIOS.
- Describe NetBT and why it is necessary.
- List the types of NetBT nodes.
- Describe Nbtstat.
- Describe an Lmhosts file and when to use it.
- Describe WINS.
- Describe the NetBIOS name resolution process.
- Configure a client to use Lmhosts and WINS.

What Is NetBIOS?



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.

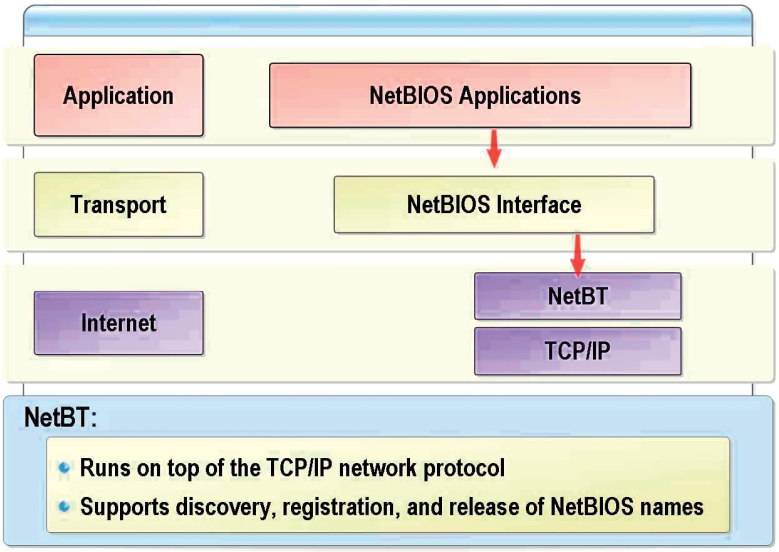
Definition of NetBIOS

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 allow 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 this course.

What Is NetBT?



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 composed of the NetBIOS session-layer protocol and the 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 NetBT determines the method for naming functions

There are several ways that NetBT can perform naming functions. For example, NetBT can use a broadcast, a NetBIOS Name Server (NBNS) such as a WINS server, or 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

Introduction

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

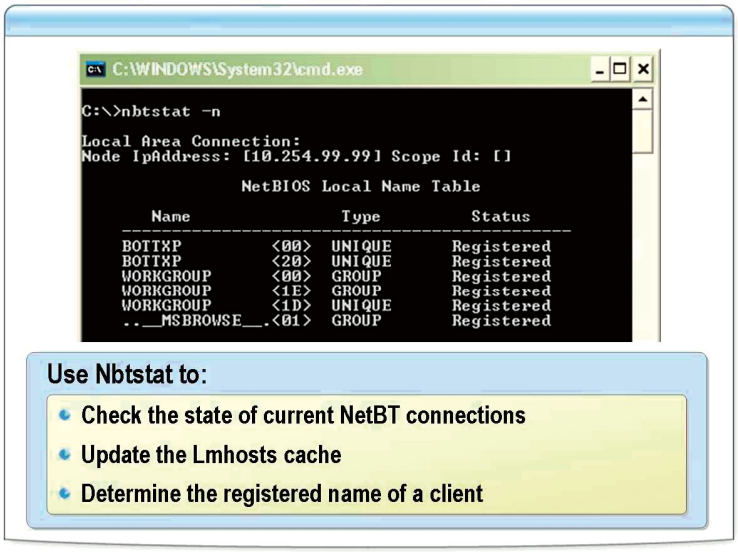
NetBT node types

The NetBT node types are listed in the following table.

Node type	Method (in the order applied)	Description
B-node (broadcast)	Broadcast only	Uses broadcast NetBIOS name queries for name registration and name resolution. Typically not forwarded by routers, so limited to the local subnet. Can create excessive broadcast traffic for large subnets.
P-node (peer-to-peer)	NBNS only	Uses NBNS only. WINS is the Microsoft implementation of an NBNS.
M-node (mixed)	Broadcast, NBNS	A combination of B-node and P-node. Uses broadcast by default. If unable to resolve a name, 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 uses 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 Windows Server 2003 by using the registry, but the preferred way is to configure the Dynamic Host Configuration Protocol (DHCP) to specify the node type to the client.

What Is Nbtstat?



Introduction

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

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 correspond 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 a command prompt window.

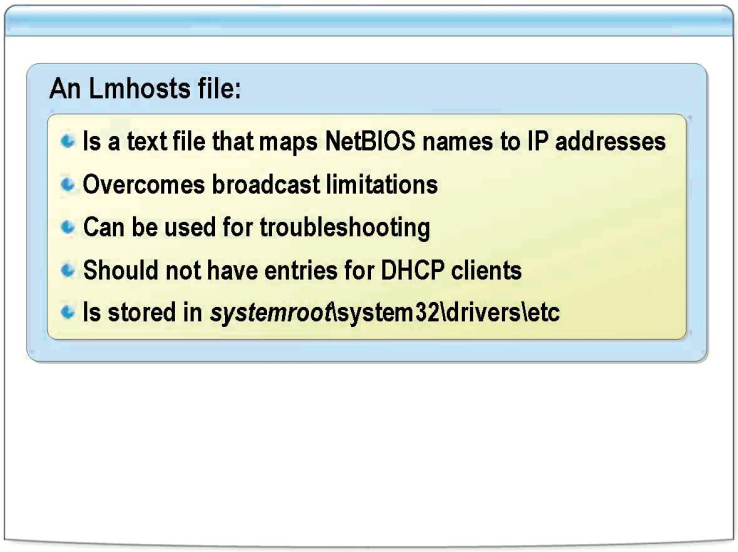
Examples of Nbtstat displays

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 the 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* as well as its MAC address.

What Is Lmhosts?



Definition

Lmhosts is a text file that allows you to map NetBIOS names to IP addresses. Lmhosts is not used in most networks because it is difficult to maintain on many computers. The Lmhosts file has no file extension.

Why use Lmhosts?

Early networks that required NetBIOS name resolution used broadcasts to resolve NetBIOS names to IP addresses. However, as networks became larger and incorporated multiple subnets, NetBIOS name resolution did not work because broadcasts are not propagated across routers. Lmhosts eliminates the issue by allowing the client to resolve the name locally rather than requiring broadcasts.

Another reason to use Lmhosts is for troubleshooting. Adding a NetBIOS name to Lmhosts is a quick and easy way to ensure that a client can properly resolve a NetBIOS name.

Guidelines for editing Lmhosts

Use the following guidelines when editing Lmhosts:

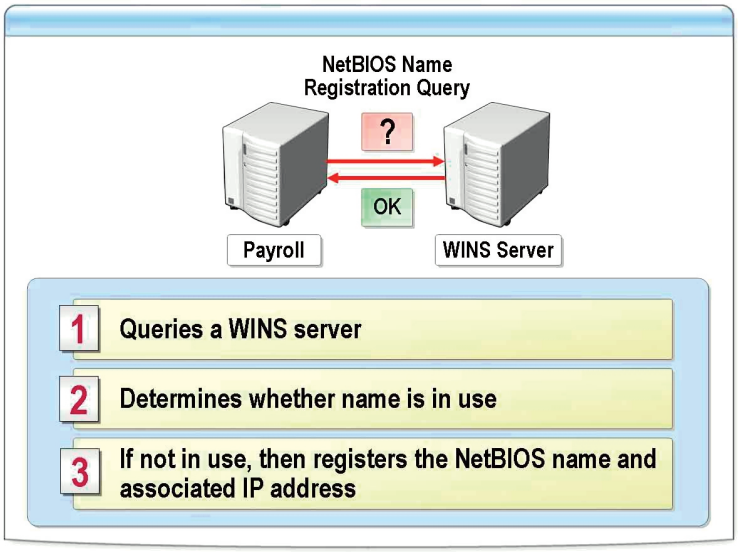
- Use the default location of the *systemroot*\system32\drivers\etc folder.
- View the Lmhosts example file Lmhosts.sam for configuration information.
- To create an entry, use the IP address of the computer, followed by at least one space or tab and the NetBIOS name of the computer.

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. For example, *AccountingDC* is a mixed-case name, and *HumanRscSr\0x03* specifies a name with a special character. If a name is enclosed in double quotation marks, it is used exactly as entered.
- 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, the keyword #PRE 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 the *Microsoft Windows 2000 Resource Kit* on the Microsoft Web site.

What Is WINS?



Introduction

WINS is an NBNS that you can use to resolve NetBIOS names to IP addresses when computers on your network are running 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.

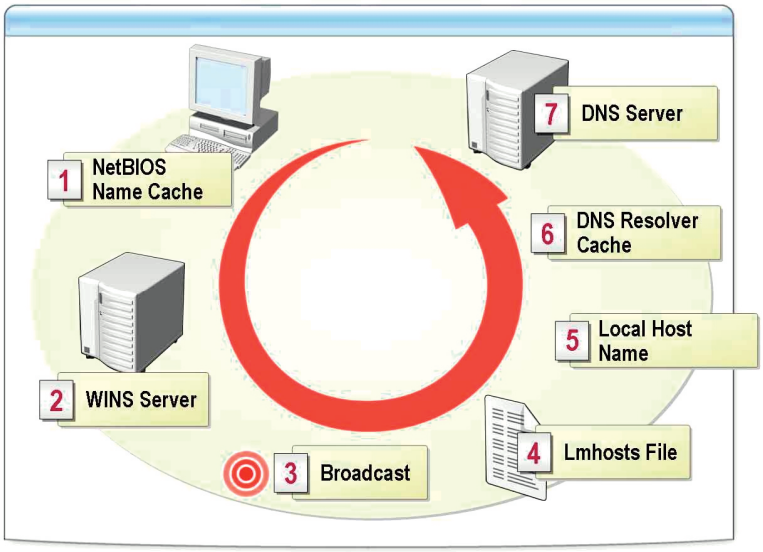
Note WINS supports the NetBT mode of operation defined in RFCs 1001 and 1002 as *p-node*.

WINS client requirements

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.

The NetBIOS Name Resolution Process



Introduction

The NetBIOS name resolution process varies, depending on the NetBT node type that is specified. However, in most cases, the default NetBT node type is not altered. If all NetBIOS name resolution methods fail, clients will attempt to use host name resolution methods to resolve NetBIOS names.

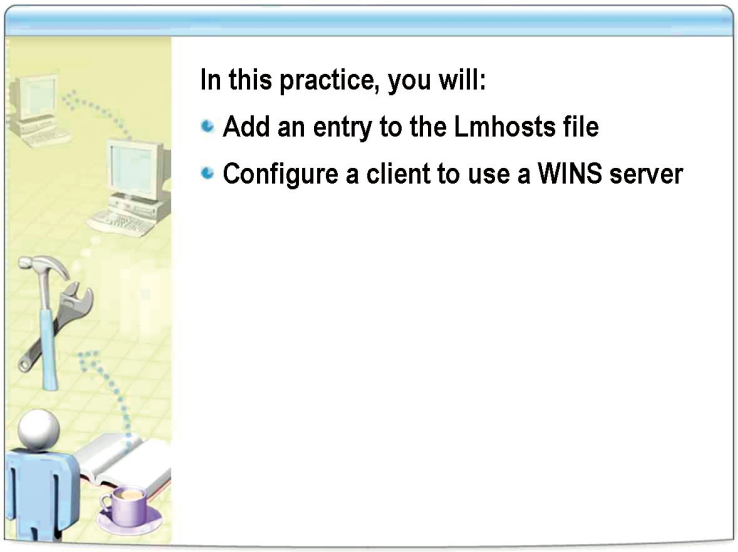
The host name resolution process

When a WINS server is configured on the client, the NetBIOS name resolution process is as follows:

1. Windows checks the local NetBIOS name cache.
2. Windows contacts its configured WINS servers.
3. Windows broadcasts as many as three NetBIOS Name Query Request messages on the directly attached subnet.
4. Windows searches the Lmhosts file.
5. Windows checks whether the NetBIOS name is the same as the local host name.
6. Windows searches the DNS resolver cache.
7. Windows sends a DNS request to its configured DNS servers.

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

Practice: Resolving NetBIOS Names



Objectives

In this practice, you will:

- Add an entry to the Lmhosts file.
- Configure a client to use a WINS server.

Instructions

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

Practice

► **Add an entry to the Lmhosts file**

1. On DEN-CL1, log on as **Paul**, with a password of **Pa$$w0rd**.
2. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
3. Type **nbtstat –c** and then press ENTER. Notice that **testserver** is not listed.
4. Click **Start**, click **Control Panel**, and then click **Folder Options**.
5. Click the **View** tab, clear the **Hide extensions for known file types** check box, and then click **OK**.
6. At a command prompt, type **copy C:\Windows\system32\drivers\etc\lmhosts.sam C:\Windows\system32\drivers\etc\lmhosts** and then press ENTER.
7. Click **Start**, point to **All Programs**, point to **Accessories**, and then click **Notepad**.
8. Click **File**, and then click **Open**.
9. In the **Files of type** box, select **All Files**.
10. Browse to **C:\Windows\system32\drivers\etc**, click **lmhosts**, and then click **Open**.
11. Scroll to the bottom of Lmhosts, type **10.10.0.58 testserver #PRE**, and then press ENTER.
12. Click **File**, click **Save**, and then close Notepad.

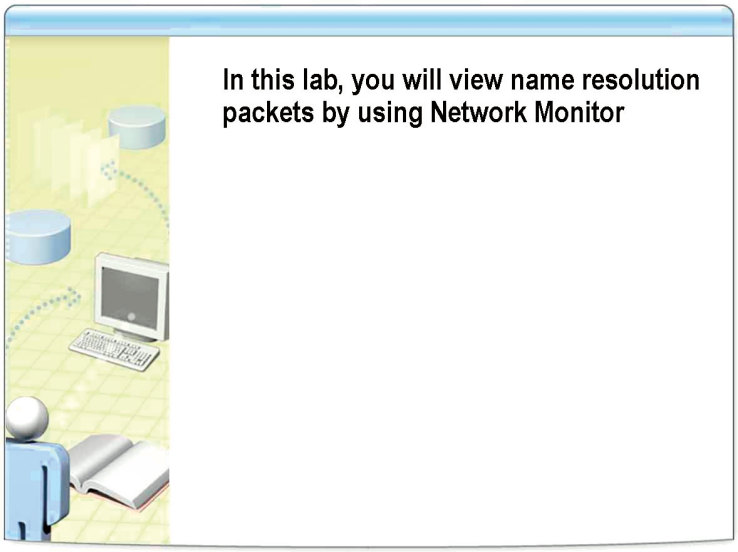
13. At the command prompt, type **nbtstat –R** and then press ENTER. This reloads the NetBIOS name cache, including entries in Lmhosts marked with **#PRE**.
14. Type **nbtstat –c** and then press ENTER. Notice that **testserver** is now listed.
15. Close the command prompt window.

► **Configure a client to use a WINS server**

1. Click **Start**, click **Control Panel**, click **Network Connections**, right-click **Local Area Connection**, and then click **Properties**.
2. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. Click **Advanced**, and then click the **WINS** tab.
4. Click the **Add** button, type **10.10.0.2** and then click **Add**.
5. Click **OK** twice, and then click **Close**.
6. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
7. Right-click **Local Area Connection**, and then click **Status**.
8. Click the **Support** tab, and then click **Details**. Notice that the WINS server is now configured.
9. Click **Close** twice, and then close Network Connections.

Important Do not shut down the virtual machines.

Lab: Configuring a Client for Name Resolution



Objective

After completing this lab, you will be able to view name resolution packets by using Network Monitor.

Instructions

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

Estimated time to complete this lab: 15 minutes

Exercise 1
Viewing DNS Packets

In this exercise, you will view the DNS packets sent between a client and a DNS server. This is useful for troubleshooting host name resolution problems.

Scenario

A client computer on your network has been intermittently having problems resolving host names. You will view the DNS packets between the client and the DNS server to verify that the proper communication process is occurring. To do this, you use Network Monitor.

Tasks	Detailed steps
1. Start capturing packets on DEN-DC1.	**a.** Open Network Monitor. **b.** If necessary, select **Local Area Connection** for the network. **c.** Start a capture.
2. Clear the DNS cache on DEN-CL1.	**a.** Open a command prompt window. **b.** Clear the DNS cache by using Ipconfig.
3. On DEN-CL1, ping DEN-DC1.	▪ Ping DEN-DC1.
4. View the DNS packets in Network Monitor.	**a.** Stop and view the capture. **b.** Filter the capture to show only DNS packets. **c.** View the details of each DNS packet.
5. Start capturing packets on DEN-DC1.	▪ Start a capture.
6. On DEN-CL1, ping DEN-DC2.	**a.** Ping DEN-DC2. **b.** Close the command prompt window.
7. View the DNS packets in Network Monitor.	**a.** Stop and view the capture. **b.** Filter the capture to show only DNS packets. **c.** View the details of each DNS packet. **d.** Close Network Monitor.
8. Complete the lab exercise.	**a.** Close all programs and shut down all computers. Do not save changes. **b.** To prepare for the next module, start the DEN-DC1 and DEN-CL1 virtual computers.