

Resolving Names to IP Addresses

You've learned a lot about TCP/IP in previous chapters. You know that TCP/IP uses IP addresses to route traffic from one computer to another. However, if you're like most people, you don't want to memorize IP addresses. Computers are much easier to identify when they have names.

Computers are named with host names and NetBIOS names. Each of these name types has special features. For example, computers on the Internet use host names, but internal networks can use either host names or NetBIOS names. Additionally, TCP/IP uses several different methods to resolve these names to IP addresses. The primary method used to resolve host names to IP addresses is with Domain Name System (DNS) servers. The primary method used to resolve NetBIOS names to IP addresses is with Windows Internet Naming System (WINS) servers. However, additional methods exist. This chapter covers the different types of names, the types of name resolution, and the steps TCP/IP uses to resolve names to IP addresses.

- ▶ **Exploring types of names used in networks**
- ▶ **Exploring types of name resolution**
- ▶ **Identifying the steps in name resolution**

Exploring Types of Names Used in Networks

Computers work with numbers. At the lowest level, the computers use ones and zeros assigned to individual bits. Every single piece of data that flows through a computer is reduced to simply ones and zeros.

However, you and I just don't think that way. Instead, we think in words. If someone asked you to memorize the MAC addresses or IP addresses of your favorite websites, you may find it a little challenging. However, if someone asked you to name your favorite websites, you could do so easily.

Thankfully, computers can also use names. However, there are many different elements built into networking to convert these names into the numbers used by the computers.

The following list shows the progression of how names are resolved to different types of addresses:

Name Computers are assigned names, and you can usually reach a computer in a network using the name. These names can be either *host names* or *NetBIOS names*, or both, depending on where they are located. Only host names are utilized on the Internet, but both host names and NetBIOS names can be used on internal networks.

IP Address IP addresses are assigned to the network interface cards of computers. The IP address is used at the Network layer of the OSI Model to route traffic between subnetworks. Name resolution methods resolve the computer name to an IP address.

MAC Address The media access control (MAC) address or physical address uniquely identifies the NIC. Each device on a network has an interface with a different MAC address. The MAC address is used at the lower levels of the OSI Model.

Bits Bits are the lowest level of data. Data streams to and from computers using bits of ones and zeros.

The types of names given to computers and other network devices are either host names or NetBIOS names. As an introduction, Table 10.1 outlines some of the characteristics and differences of host names and NetBIOS names.

TABLE 10.1 Comparing host names and NetBIOS names

Characteristics	Host names	NetBIOS names
Length	Up to 255 characters	15 readable characters; 16th character identifies a service
Location	On Internet and internal networks	Only on internal networks
Primary name resolution method	Domain Name System (DNS)	Windows Internet Naming Service (WINS)
Namespace	Hierarchical (part of fully qualified domain name)	Flat namespace (single level names only)

Chapter 3 covered the seven layers of the Open Systems Interconnect (OSI) model.

Understanding Host Names

A host name is a user-friendly string of characters, or label, assigned to a computer or other network device. Host names are the primary name type used today. They are the only types of names used on the Internet and the primary name type used on many internal networks.

Host names can be as long as 255 characters. They can contain letters, numbers, periods, and hyphens.

When a host is part of a domain, the full computer name is the fully qualified domain name (FQDN). Figure 10.1 shows the host name and FQDN of a Windows Server 2008 server. The FQDN in a Windows system can be up to 255 characters as long as no more than 63 characters are used between each period.

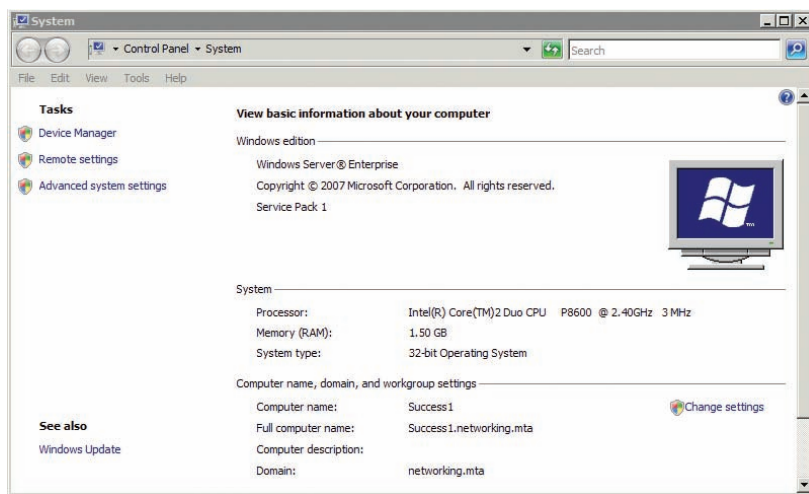


FIGURE 10.1 Viewing the computer name on Windows Server 2008

Notice that the computer name is Success1. This is the host name. The computer is a member of a domain named networking.mta. The full computer name (or FQDN) is success1.networking.mta.

Understanding NetBIOS Names

Network Basic Input/Output System (NetBIOS) names are 15 characters long. Even when the actual name is shorter (such as PC1), the NetBIOS name is padded with trailing spaces to make the name 15 characters long.

Windows limits the length of host names in Windows systems to 63 characters. However, it's recommended to limit the length to 15 characters for compatibility with NetBIOS names.

You can also view the host name of your computer from the command prompt by typing `hostname` and pressing Enter.

HOST NAMES, URLs, AND FQDNS

A uniform resource locator (URL) is the address used to access Internet resources such as websites. It includes the protocol and the fully qualified domain name (FQDN). For example, if you wanted to reach the website **www.bing.com**, you would use this URL: **http://www.bing.com**. The protocol is HTTP, and the FQDN is **www.bing.com**.

www is the host name, and it represents a web farm of computers that respond to that name. You probably know that you don't even have to use **www**, though. Instead, you can simply enter the address as **http://bing.com**, and it'll work. Of course, you can also skip the protocol in your web browser. For example, if you're using Internet Explorer (IE), you can simply enter **bing.com**. IE assumes you're using HTTP and fills that in for you.

DNS supports multiple computers with the same name and can resolve name requests to different servers in a round-robin fashion. DNS also supports alias names to allow computers to respond to different names. A single computer can be registered in DNS with multiple different names, and each name will resolve to the same IP address.

Chapter 6 presented the hexadecimal numbering system. As a reminder, it includes the numbers 0 to 9 and the letters A to F.



The NetBIOS name includes a hidden 16th byte. This 16th byte is a hexadecimal number that identifies services running on the system. Other systems and applications on the network use this information to determine how they can communicate with a system.

Table 10.2 shows common values for the 16th byte of a computer's NetBIOS name. These values identify services running on desktop and server operating system computers or provide other information about the computer.

In addition to tracking the name of the computer, NetBIOS tracks the name of the workgroup or domain that a computer has joined.

You can view NetBIOS names registered by a system using the `nbtstat` command. The following steps show how:

1. Launch a command prompt by clicking Start > Run; then enter `cmd` in the Run box, and press Enter.
2. Enter `nbtstat -n`, and press Enter.

Listing 10.1 shows the output of the `nbtstat -n` command on a Windows Server 2008 server named `success1`. This computer is a domain controller within the `networking.mta` domain.

TABLE 10.2 Examples of the value and meaning of NetBIOS 16th byte for computer names

Hexadecimal value	Meaning	Comments
00	Workstation service	Used to create and maintain client network connections to other computers on the network
20	File server service	Indicates the computer can share files and printers over the network
23/24	Microsoft Exchange	Identifies a server hosting Microsoft Exchange

Microsoft Exchange is used in Windows environments for email.

Listing 10.1 Output of `nbtstat -n` command

```
C:\>nbtstat -n
```

```
Local Area Connection:
```

```
Node IpAddress: [192.168.3.1] Scope Id: []
```

```
NetBIOS Local Name Table
```

Name	Type	Status
SUCCESS1	<00> UNIQUE	Registered
NETWORKING	<00> GROUP	Registered
NETWORKING	<1C> GROUP	Registered
SUCCESS1	<20> UNIQUE	Registered
NETWORKING	<1B> UNIQUE	Registered

Notice the output for the computer name (`SUCCESS1`) has specific hex values listed. Similarly, the output for the domain name (`NETWORKING` from `networking.mta`) has hex values listed. Table 10.2 showed the meaning of these values for a computer name. Table 10.3 shows the meaning of some values for the domain.

The value <00> means something different when it's a UNIQUE type and when it's a GROUP type. UNIQUE <00> indicates the workstation service, and GROUP <00> indicates the domain name.

TABLE 10.3 Examples of the value and meaning of NetBIOS 16th byte for domain names

Hexadecimal value	Meaning	Comments
00	Domain name	Indicates the name of the domain
1C	Domain controller	Indicates that the server is a domain controller in the domain
1B	Domain master browser	Indicates the computer is hosting the Domain Master Browser role, which is used by NetBIOS services in the network

Note that the value 00 means domain name when associated with GROUP, but it can also mean the workstation service when associated with UNIQUE.

Many more NetBIOS services can be assigned to any computer. The important point to grasp from this section is that each computer can have multiple NetBIOS names. Different NetBIOS names have different hex values to provide information about the computer.

Creating NetBIOS Names from Host Names

A Windows Server 2008 server's name is Success1. Is this a host name or a NetBIOS name? The answer is that it's both. When you name a computer, the name is used for both the host name and the NetBIOS name.

If the name is 15 characters long or less, the computer will have the same host name and NetBIOS name. However, if the host name is more than 15 characters, Windows truncates the name to the first 15 characters for use as the NetBIOS name. This is important because it's possible to inadvertently give different computers duplicate NetBIOS names.

As an example, consider Table 10.4, which shows the host names and the resulting NetBIOS name derived from the host name. Some of the host names are more than 15 characters, resulting in duplicate NetBIOS names.

TABLE 10.4 NetBIOS names derived from host names

Host name	NetBIOS name	Comment
CPU1	CPU1	No problem
CPU2	CPU2	No problem
NetworkingComputer1	NETWORKINGCOMPU	Name truncated

(Continues)

Duplicate NetBIOS names result in errors and communication problems with these computers. All computers on the same network need unique names.

TABLE 10.4 (Continued)

Host name	NetBIOS name	Comment
NetworkingComputer2	NETWORKINGCOMPU	Duplicate name
DC1	DC1	No problem
DC2	DC2	No problem
DomainController1	DOMAINCONTROLLE	Name truncated
DomainController2	DOMAINCONTROLLE	Duplicate name

Notice that the shorter computer names are identical as both host names and NetBIOS names. However, since NetBIOS truncates the longer computer names to only the first 15 characters, some of the computers have duplicate NetBIOS names.

Viewing and Modifying a Computer Name

You can use the following steps to view a computer's host name, view its NetBIOS name, and modify the computer's name:

1. Log onto the computer. If you plan on changing the computer name, you will need to log on with an administrative account.
2. Click Start, type `cmd` in the Start Search box, and press Enter. This will launch a command prompt.
3. Enter **hostname** at the command prompt, and press Enter. This returns the host name of the computer.
4. Click Start, right-click Computer, and select Properties. This will display a page similar to Figure 10.1 shown earlier in this chapter.
Notice that you can view the computer name, the FQDN (as the full computer name), and the domain on this page. In Figure 10.2, the computer name is `Success1`, the FQDN is `success1.networking.mta`, and the domain is `networking.mta`.
5. On the System properties page, click Advanced System Settings. If prompted by UAC, click Yes or provide appropriate credentials.
6. Select the Computer Name tab. Click Change. Click More. Your display will look similar to Figure 10.2.

Notice that you can view the DNS suffix of the computer and the NetBIOS computer name on this page. The suffix is automatically

Although Windows host names can be 63 characters, you should limit them to no more than 15 characters for compatibility with NetBIOS.

These steps are written for a Windows Server 2008 server. However, they will also work on Windows 7 and some other Windows systems.

You can modify the primary DNS suffix. However, you cannot modify the NetBIOS name.

added when a computer joins a domain, and the NetBIOS name is automatically created from the computer name.

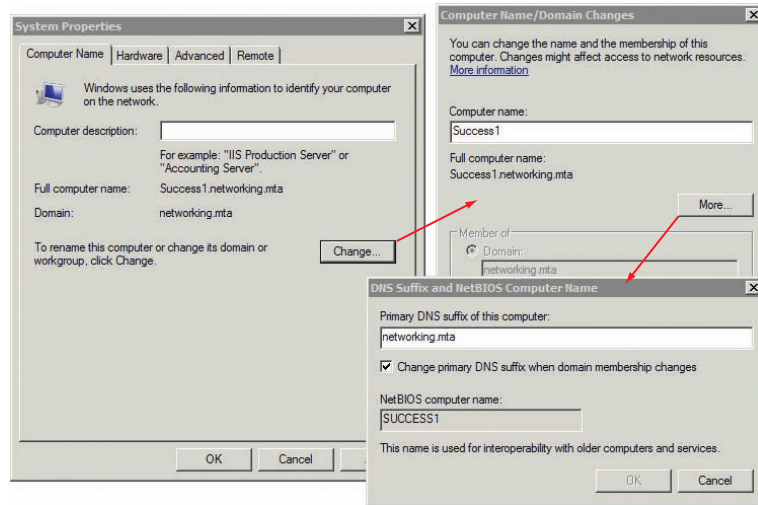


FIGURE 10.2 Viewing computer names

7. Click Cancel. If desired, you can modify the computer name by changing it on the Computer Name/Domain Changes page.
8. Close all windows.

Exploring Types of Name Resolution

Names have to be resolved to IP addresses on the Internet and within internal networks. Eight types of name resolution can be used. Table 10.5 introduces the different types, and the following sections describe them in more detail.

TABLE 10.5 Name resolution methods

Name resolution method	Resolves (host names, NetBIOS names, or both)	Comments
Domain Name System (DNS) server	Host names (Windows Server 2008 DNS can be configured to resolve NetBIOS names using GlobalNames zones)	DNS servers are on the Internet and internal networks; Microsoft domains require DNS.

(Continues)

TABLE 10.5 (Continued)

Name resolution method	Resolves (host names, NetBIOS names, or both)	Comments
Host cache	Host names	Host cache can be viewed with the <code>ipconfig /displaydns</code> command.
Hosts file	Host names	Located in <code>c:\windows\system32\drivers\etc\</code> folder by default.
Windows Internet Name Service (WINS)	NetBIOS names	WINS servers are located only on internal networks.
NetBIOS cache	NetBIOS names	NetBIOS cache can be viewed with the <code>nbtstat -c</code> command.
Lmhosts file	NetBIOS names	Located in <code>c:\windows\system32\drivers\etc\</code> folder when used.
Broadcasts	Both	The system simply sends a broadcast with the name asking the owner to reply with its IP address.
Link-local multicast name resolution (LLMNR)	Host names	This is a newer method similar to broadcast that works on internal networks.

Understanding Domain Naming Service

The *Domain Naming System (DNS)* is a service that resolves host names to IP addresses. These can be names of computers within an internal network or names of computers on the Internet. Clients send name resolution requests to a DNS server, and the DNS server responds with the IP address. The client computer then uses the returned IP address as the destination IP address for data traffic.



DNS is essential on a Microsoft domain. Active Directory requires DNS to locate servers running specific services, such as domain controllers.

▶
Host records are sometimes listed as host (A) and other times as A (host). However, they are the same.

▶
Reverse lookup zones are optional. Some DNS servers don't host reverse lookup zones or support reverse lookups.

▶
SRV records are used for host names similar to how the 16th byte of NetBIOS names is used. Both identify specific services running on computers.

Figure 10.3 shows the DNS console on a Windows Server 2008 server. It shows several host (A) records with their names and IP addresses. When a system queries a DNS server with the name of a computer, the DNS server checks to see whether it has a matching host (A) record for the requested name in its database, and if so, it returns the IP address to the requesting client.

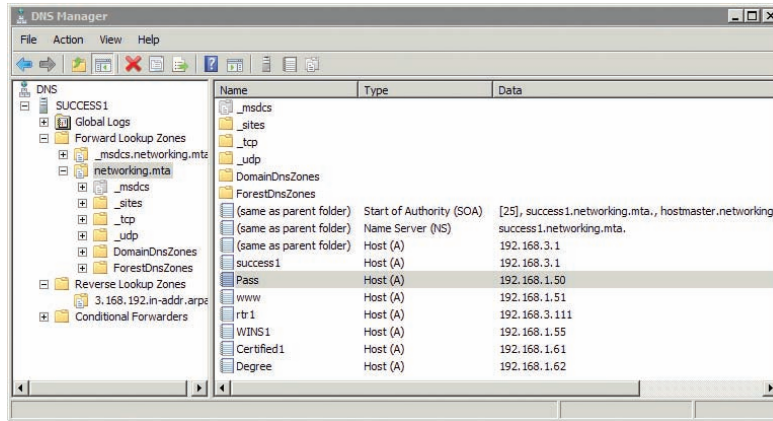


FIGURE 10.3 Viewing the DNS console

Notice that the server in Figure 10.3 also has a reverse lookup zone. Reverse lookup zones use pointer (PTR) records to do reverse lookups. In other words, you can pass the IP address to the DNS server and retrieve the name of the computer with that IP address.

DNS servers host multiple types of records beyond the A records. For example, an Active Directory domain must have service (SRV) records to locate domain controllers in the network. Table 10.6 outlines many of these records.

TABLE 10.6 Common DNS records

Record type	Usage
A (host)	Resolves host names to IPv4 IP addresses
AAAA (host)	Resolves host names to IPv6 addresses
PTR (pointer)	Resolves IP addresses to host names
CNAME (alias)	Resolves one host name to another host name, which allows multiple computer names to be resolved to the same IP address
MX	Used for mail exchange servers (email servers)

(Continues)

TABLE 10.6 (Continued)

Record type	Usage
SRV	Required by Active Directory to locate servers running specific services (such as domain controllers)
NS	Identifies DNS name servers

A DNS server that holds records for a specific namespace (such as the networking.mta namespace) is authoritative for that namespace. In other words, it knows all the computers and the IP addresses in that namespace. If it doesn't have a record for one of these computers, no one else will either.

If a DNS server is not authoritative for a namespace, it can still resolve names by forwarding the name request to other DNS servers.

DNS is hierarchical. No single server knows the names and IP addresses for all the computers on the Internet. Instead, DNS servers are authoritative for different namespaces. Consider Figure 10.4, which shows the hierarchy of DNS servers on the Internet. They are explained as follows:

DNS Root Servers At the top of the hierarchy are DNS root servers. There are only 13 DNS root servers in the world. These servers know only the addresses of DNS servers that are authoritative for top-level domains such as .com, .net, .org, and so on. If you ask it for the address of training.microsoft.com, it won't know. However, it will know the address of the DNS servers that are authoritative for the .com namespace.

Top-Level Domain DNS Servers Next are the top-level domain DNS servers. Top-level domain DNS servers know the addresses of second-level domain DNS servers in their namespace. For example, a .com DNS server knows the addresses of servers that are authoritative for the Microsoft.com namespace. However, a .com DNS server doesn't know anything at all about .net, .org, or any other top-level domain namespace.

Second-Level Domain DNS Servers Below the top-level domain DNS servers are the second-level domain DNS name servers. These servers are authoritative in the second-level DNS namespace. For example, Microsoft has several servers that are authoritative in the Microsoft.com domain. The DNS servers in the Microsoft.com namespace know only about Microsoft.com. They wouldn't know anything about other namespaces such as sybex.com.

Third- and Lower-Level Domain DNS Servers Third-level and lower-level domain DNS servers are possible. However, these are needed only when the FQDN includes these lower levels. For example, Microsoft may have a DNS server dedicated to the

Multiple DNS servers are available for each of the top-level domains. If one DNS server in the .com namespace fails, others in the .com namespace can still answer queries.

training.microsoft.com namespace. This DNS server can resolve all the host names in the training.microsoft.com namespace. Other companies may not have third-level DNS servers. Instead, the second-level server resolves the names for all the company's resources on the Internet.

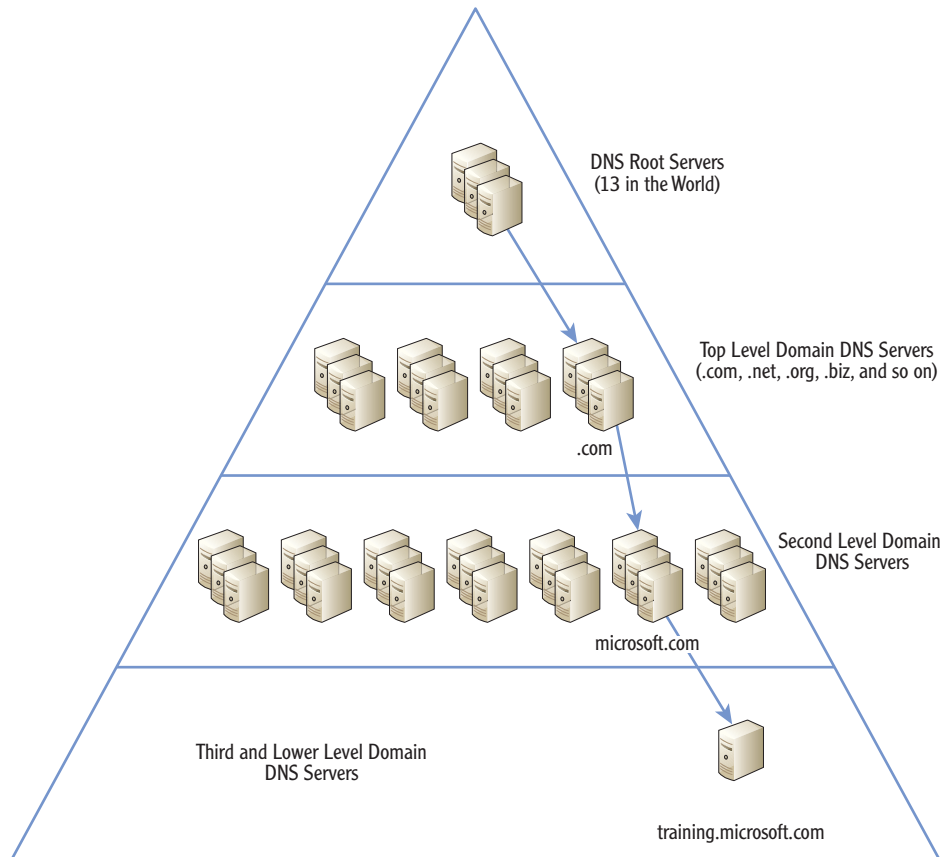


FIGURE 10.4 DNS hierarchy

DNS queries to the Internet start with a query to one of the DNS root servers. For example, imagine if a client is trying to reach a web server named **www.sybex.com** from an internal network named **networking.mta**. The record for the **www.sybex.com** web server won't be on the internal DNS server. However, the internal DNS server can make queries to the Internet to retrieve the name.

Figure 10.5 and the following steps show how this works in practice.

1. The client passes the request to the DNS server to resolve `www.sybex.com`. Assume that the DNS server has just turned on and doesn't have any information except for the address of the DNS root servers.
2. Since the top-level domain is `.com` and the DNS server doesn't have the IP address of a DNS server in the `.com` domain, it queries a DNS root server. The DNS root server responds with the IP address of a DNS server that is authoritative for the `.com` namespace.

◀ If the DNS server has been on for a while, it will have cached information, and it may be able to skip some of the steps.

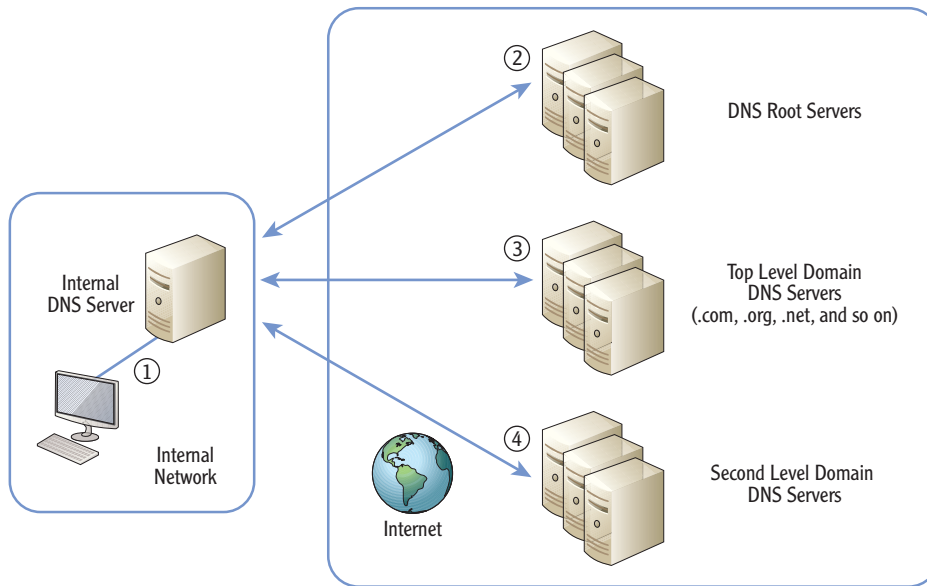


FIGURE 10.5 Resolving a DNS query on the Internet

3. Next, the internal DNS server queries the `.com` DNS server for the address of a DNS server that is authoritative in the `sybex.com` domain. The top-level domain DNS server responds with an IP address.
4. Finally, the internal DNS server queries the `sybex.com` DNS server for the IP address of the web server named `www`.

DNS servers cache responses in their internal memory. In other words, after a DNS server queries a root DNS server for an address of a `.com` DNS server, it keeps this information. The next time it needs to query the `.com` server for an address, it just looks in cache for this information.

RESOLVING NETBIOS NAMES WITH DNS

Windows Server 2008 supports a new type of zone called a GlobalNames zone. In networks where there are very few NetBIOS applications, you can use GlobalNames zones for single label names, just as if they were NetBIOS names.

When a GlobalNames zone is used, DNS can resolve both host names and NetBIOS names. GlobalNames zones are used only on internal Microsoft networks. On the Internet, DNS can only resolve host names.

Viewing the Host Cache

Every time a computer receives a name resolution response from a DNS server, it places the result in the local host cache. The host cache is an area of memory on any computer that is dynamically updated with host name and their corresponding IP addresses.

The host cache is also called the *DNS resolver cache*, since many of the entries are created when DNS is queried to resolve a host name. However, the host cache also includes data from the hosts file (described in the next section).

You can view the host cache on any computer from the command prompt by using the following steps:

1. Launch a command prompt by clicking Start > Run; enter `cmd` in the Run box, and press Enter.
2. Enter `ipconfig /displaydns`, and press Enter.

Listing 10.2 shows the partial output of the `ipconfig /displaydns` command on a Windows Server 2008 server.

Listing 10.2 Output of `ipconfig /displaydns` command

```
C:\>ipconfig /displaydns

Windows IP Configuration

    1.0.0.127.in-addr.arpa
    -----
    Record Name . . . . . : 1.0.0.127.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live . . . . . : 86400
    Data Length . . . . . : 4
    Section . . . . . : Answer
```

The host cache on an end user's computer is different from the DNS cache on a DNS server. However, they work the same. Cached data doesn't need to be queried again.

The actual output includes many more entries. However, only a few entries are shown here to conserve space.

```

PTR Record . . . . . : localhost

localhost
-----
Record Name . . . . . : localhost
Record Type . . . . . : 1
Time To Live . . . . . : 86400
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 127.0.0.1

bing.com
-----
Record Name . . . . . : bing.com
Record Type . . . . . : 1
Time To Live . . . . . : 580
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 65.55.175.254

```

Notice the first record is a PTR record (reverse lookup record) for the local computer using the loopback address of 127.0.0.1. The second record is an A (host) record for localhost record that is mapped to the loopback address of 127.0.0.1. You will usually see these two entries for any Windows 2008 computer.

The third record for bing.com is a record returned from a DNS server and placed in cache. Notice that it has a Time To Live section. Every record returned from a DNS server includes this, and it indicates how long the data will remain in cache. The value of 580 indicates that it will remain in cache for another 580 seconds. Any queries to bing.com will use this IP address as long as it remains in cache. After the timeout period, it is removed from the cache and requires another query to DNS to resolve it.

Viewing the Hosts File

The hosts file is a simple text file located in the `c:\windows\system32\drivers\etc` folder by default. The hosts file maps the names of computers to IP addresses. The benefit is that mapped records in this file are automatically placed in the host cache.

Listing 10.3 shows the contents of a host file on a Windows Server 2008 server.

Listing 10.3 Hosts file

```

# Copyright (c) 1993-2006 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

```

The 127.0.0.1 and localhost records come from the hosts file on Windows computers.

You can remove cached items from the host cache with the `ipconfig / flushdns` command. However, this does not remove items in cache from the hosts file.

You can place entries in a hosts file to bypass DNS queries for specific hosts. If the entry is in the hosts file or in cache, DNS is not queried.

If you enter `ping localhost` at the command prompt, the localhost name is resolved to either `127.0.0.1` or `::1`, depending on whether `ping` is using IPv4 or IPv6.

```
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1      localhost
::1           localhost
```

Notice that the beginning of the file consists of comments preceded by hash marks (#). The only two entries are the `127.0.0.1` and `::1` lines. These lines map the localhost name to the IPv4 loopback address of `127.0.0.1` and to the IPv6 loopback address of `::1`.

All entries in the hosts file are immediately placed in cache, and they stay there constantly. Hosts file entries do not time out and fall out of cache.

Understanding WINS

Windows Internet Name Service (WINS) is a service you can add to a server to resolve NetBIOS names to IPv4 addresses. A WINS server can resolve only NetBIOS names, not host names.

You'll find WINS servers on internal Microsoft networks. Non-Microsoft networks may include NetBIOS servers to resolve NetBIOS names, but they can be other types of NetBIOS servers. WINS is Microsoft's implementation of a NetBIOS server.

You may remember that DNS is hierarchical. It uses multilevel names such as root level, top level, and so on. Because of this, DNS is highly scalable. DNS on the Internet efficiently resolves the IP addresses of billions of computers. It works as efficiently with these billions of computers as it will on an internal network with just a few dozen computers.

In contrast, WINS is not hierarchical. Instead, it's a flat database that supports only single-level names. WINS does not scale well and couldn't possibly work with billions of computers. As more computers are added to a WINS server, it can get bogged down.

Don't be fooled by the word *Internet* in WINS. WINS is not used on the Internet at all. It is used only on internal Microsoft networks.

Since DNS performs so much better than WINS and because WINS does not support IPv6, WINS is being phased out. However, it is still being used in many networks today since many applications still use NetBIOS names.

Figure 10.6 shows the TCP/IP properties for a network interface card (NIC) on a Windows system. Notice that you can configure the name of a DNS server on the same page as you configure the IP address of the NIC. However, you have to click the Advanced button and select the WINS tab to add the IP address of a WINS server.

If your network includes multiple WINS servers, you can add the IP addresses of each one.

Although you can configure the IP address of DNS and WINS servers manually, most networks use DHCP to configure these addresses automatically.

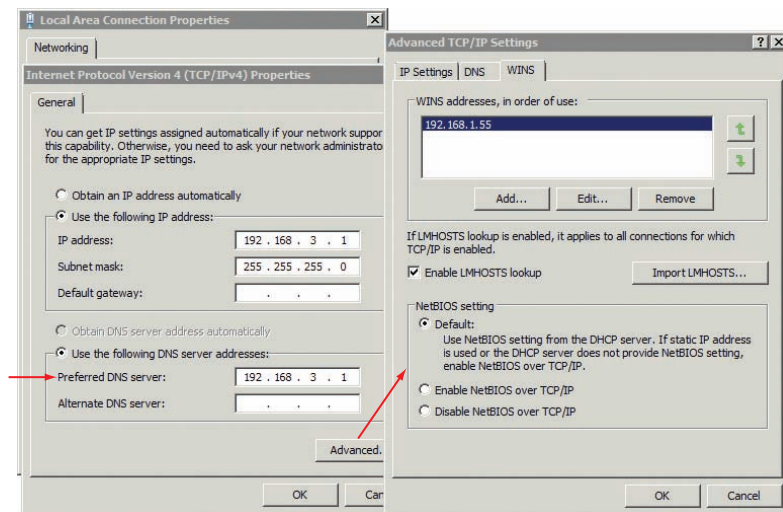


FIGURE 10.6 Configuring a computer to use WINS

Viewing the NetBIOS Cache

Just as any host name that is resolved by DNS is placed in cache, NetBIOS names resolved by WINS are also placed in cache. DNS names are placed in the host cache, and WINS names are placed in the NetBIOS cache.

You can view the NetBIOS cache using the `nbtstat -c` command, as follows:

1. Launch a command prompt by clicking Start > Run; then enter `cmd` in the Run box, and press Enter.
2. Enter `nbtstat -c`, and press Enter.

Listing 10.4 shows the cache of a Windows 2008 server that recently resolved the name of a file server (named FS1) to the address of 192.168.1.117.

Listing 10.4 Output of `nbtstat -c`

```
C:\>nbtstat -c
```

```
Local Area Connection:
```

```
Node IpAddress: [192.168.3.1] Scope Id: []
```

```
NetBIOS Remote Cache Name Table
```

Name	Type	Host Address	Life [sec]
FS1	<20> UNIQUE	192.168.1.117	562

Notice that the table in Listing 10.4 includes a *Life (sec)* column. This lists how long (in seconds) the entry will remain in cache. It is similar to the *Time To Live* entry for the hosts cache. After the time expires, the entry will fall out of cache, and another NetBIOS query will be needed to resolve the IP address. You can flush the NetBIOS cache with the `nbtstat -R` command.

Understanding the Lmhosts File

The `lmhosts` file is similar to the `hosts` file except that you map NetBIOS names to IP addresses. The `hosts` file maps host names to IP addresses. Although the `lmhosts` file was used quite often in the early days of Microsoft networking, it is rarely used today. Windows 7 and Server 2008 products don't even include a working `lmhosts` file in operating systems.

You can view the `lmhosts.sam` file (a sample `lmhosts` file) in the same location as the `hosts` file: `c:\windows\system32\drivers\etc`. If you want to use an `lmhosts` file, you need to create one. The name of the file must be `lmhosts` without any extension.

Understanding Broadcast Name Resolution

Another method of name resolution is *broadcast*. In other words, a system can simply send a request on the segment with a name. Any host that has that name replies with its IP address.

Remember, though, that broadcasts don't pass routers, so the use of broadcasts for name resolution works only when the computers are on the same segment.

Understanding Link-Local Multicast Name Resolution

Link-local multicast name resolution (LLMNR) is similar to broadcast, but it can resolve both IPv4 and IPv6 addresses. It works for hosts on the same local link.

The **R** in the `nbtstat -R` command must be uppercase. This is one of the few times when a command prompt command is case sensitive.

The last popular use of the `lmhosts` file was in Windows NT 4.

LLMNR has been available in Windows since Windows Vista and Windows Server 2008.

Chapter 5 described Automatic Private IP Addresses (APIPA) in the 169.254.0.0 range. APIPA addresses are assigned to DHCP clients when a DHCP server can't be reached. APIPA addresses don't include DNS addresses, and the primary method of name resolution for APIPA clients is via broadcasts. Chapter 6 described link-local addresses that are similar to APIPA addresses but for IPv6. Link-local addresses have a prefix of fe80 hexadecimal.

If a system is using a link-local IPv6 address, LLMNR can be used in place of DNS for name resolution. It will work for other hosts that have the same link-local address prefix of fe80.

Identifying the Steps in Name Resolution


Applications and services on networks resolve computer names to IP addresses. Some of the applications and services are host based, and some are NetBIOS based. In other words, some expect that the computers have host names, and some expect that the computers have NetBIOS names. This is important because it affects the steps in name resolution.


The following two sections show the steps in name resolution for host names and NetBIOS names.

Identifying Steps in Host Name Resolution

When an application or service assumes that a name is a host name, it will take the following steps to resolve it:

1. Windows first checks to see whether the queried name is the same as its host name. If so, it uses its own IP address.
2. Next, Windows checks the host cache. If the name is in cache, it doesn't check any further.
3. If the name isn't in cache, Windows queries DNS. If a system is configured with both a preferred and an alternate DNS server, it queries the preferred DNS server. An alternate DNS server is queried only if the preferred DNS server doesn't respond.
4. Next, Windows checks the NetBIOS name cache.
5. If the name isn't in the NetBIOS name cache, Windows will query a WINS server. If multiple WINS servers are configured, Windows will query each WINS server until it either resolves the name or runs out of WINS servers to query.

 The application or service determines the steps used in name resolution, based on whether it expects a host name or a NetBIOS name.

 These first three steps are the primary steps for host name resolution. If necessary, NetBIOS methods can be used to resolve the name.

6. If WINS doesn't resolve the name, Windows will attempt to resolve the name using broadcast. This succeeds only if the computer is on the local subnet.
7. Last, Windows will check the `lmhosts` file, if it exists.

The preceding steps are used if the application assumes that the name is a host name. However, if the application assumes that the name is a NetBIOS name, then it performs the steps in a different order, as shown in the next section.

Identifying Steps in NetBIOS Name Resolution

If the application or server assumes that the name is a NetBIOS name, it will use the following steps by default:

1. First, Windows checks the NetBIOS name cache.
2. If the name isn't in the NetBIOS name cache, Windows will query DNS for a name in a GlobalNames zone (GNZ).
3. If a GNZ isn't being used or can't resolve the name, then Windows will query a WINS server. If multiple WINS servers are configured, Windows will query each WINS server until it either resolves the name or runs out of WINS servers to query.
4. If WINS doesn't resolve the name, Windows will attempt to resolve the name using broadcast. This succeeds only if the computer is on the local subnet.
5. If the broadcast can't resolve the name, Windows then checks to see whether the queried name is the same as the computer's NetBIOS name.
6. Next, Windows checks the host cache.
7. Last, Windows queries DNS.

Although the preceding steps are the default, different steps and orders are possible. Windows systems use NetBIOS over TCP/IP (NetBT). The NetBT node type can be modified to use different combinations. Table 10.7 shows the different node types available in Windows.

You can view which NetBT node type your system is configured to use with the `ipconfig /all` command. Listing 10.5 shows a partial output of the `ipconfig /all` command. Notice the node type is listed as Hybrid. This shows that it will use WINS by default and then use broadcast.

TABLE 10.7 NetBIOS over TCP/IP (NetBT) node types

Type	Comments
B-node (broadcast)	Sends only a broadcast
P-node (peer-to-peer)	Queries only a WINS server
M-node (mixed)	Combines B-node and P-node Uses broadcast by default
H-node (hybrid)	Combines B-node and P-node Uses WINS by default
Microsoft enhanced B-node	Uses broadcast and then the lmhosts file

Windows 7 and Windows Server 2008 use the H-node (hybrid) by default.

Listing 10.5 Partial output of ipconfig /all

```
C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Success1
Primary Dns Suffix . . . . . : networking.mta
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : networking.mta
```

THE ESSENTIALS AND BEYOND

The two types of computer names are host names and NetBIOS names. Computers on the Internet use host names. Internal networks use either host names or NetBIOS names. The primary name resolution method for host names is DNS. The primary name resolution method for NetBIOS names in Microsoft networks is WINS. Other name resolution methods include the host cache, hosts file, NetBIOS cache, lmhosts cache, broadcast, and LLMNR.

ADDITIONAL EXERCISES

- ▶ Identify the host name and FQDN (if applicable) of your computer.
- ▶ Identify the NetBIOS name of your computer.

(Continues)

THE ESSENTIALS AND BEYOND *(Continued)*

- ▶ View the host cache on your computer.
- ▶ View the NetBIOS cache on your computer.

To compare your answers to the author's, please visit www.sybex.com/go/networkingessentials.

REVIEW QUESTIONS

1. What is the type of name used for computers on the Internet?
A. DNS name **C.** WINS name
B. NetBIOS name **D.** Host name
2. What type of computer names are assigned to Microsoft systems on a Microsoft network? (Choose all that apply.)
A. DNS names **C.** WINS names
B. NetBIOS names **D.** Host names
3. True or false. The primary name resolution method for NetBIOS names is DNS.
4. True or false. Any entries in the Windows hosts file automatically appears in the host cache.
5. How can you view the host cache (or DNS resolver cache)?
A. Enter **nbtstat -n** at the command prompt. **C.** Enter **ipconfig /displaydns** at the command prompt
B. Enter **nbtstat -c** at the command prompt. **D.** Enter **ipconfig /flushdns** at the command prompt.
6. True or false. The Windows Internet Naming Service (WINS) operates on the Internet.
7. What command can you enter at the command prompt to remove DNS resolved entries from the host cache?
A. Enter **ipconfig /flushdns** at the command prompt. **C.** Enter **nbtstat -n** at the command prompt.
B. Enter **ipconfig /displaydns** at the command prompt. **D.** Enter **nbtstat -c** at the command prompt.
8. A system has an IPv6 address with a prefix of fe80. It does not have an IPv4 address. How is the computer name resolved to an IP address for this computer?