

WINS Overview

WINS Defined

Windows Internet Name Service (WINS) provides a distributed database for registering and querying dynamic mappings of NetBIOS names for computers and groups used on your network. WINS maps NetBIOS names to IP addresses and was designed to solve the problems arising from NetBIOS name resolution in routed environments. WINS is the best choice for NetBIOS name resolution in routed networks that use NetBIOS over TCP/IP.

NetBIOS names are used by earlier versions of Microsoft operating systems to identify and locate computers and other shared or grouped resources needed to register or resolve names for use on the network.

NetBIOS names are a requirement for establishing networking services in earlier versions of Microsoft operating systems. Although the NetBIOS naming protocol can be used with network protocols other than TCP/IP (such as NetBEUI or IPX/SPX), WINS was designed specifically to support NetBIOS over TCP/IP (NetBT).

WINS simplifies managing the NetBIOS namespace in TCP/IP-based networks. Figure 6-1 shows a typical series of events involving WINS clients and servers.

In this example, the following occurs:

1. A WINS client, HOST-A, registers any of its local NetBIOS names with WINS-A, its configured WINS server.
2. Another WINS client, HOST-B, queries WINS-A to locate the IP address for HOST-A on the network.
3. WINS-A replies with the IP address for HOST-A, 192.168.1.20.

In addition, you can also use the WINS console to perform the following optional or advanced setup tasks:

- View and modify WINS properties, such as the **Renew Interval** and other intervals that are used when registering, renewing, and verifying name records stored in the server database.
- Add and configure static WINS mappings, if they are needed for use on your network.
- Delete or tombstone WINS records that appear in WINS server data used throughout your network.

For Windows 2000 Server, WINS administration can also be performed using command-line based tools. For information about Netshell commands for WINS and using WINS command-line tools, see Chapter 7.

New Features

For Windows 2000, WINS provides the following feature enhancements:

- *Persistent connections.* You can now configure each WINS server to maintain a persistent connection with one or more replication partners. This increases the speed of replication and eliminates the overhead of opening and terminating connections. For more information, see “Persistent Connections” in this chapter.
- *Manual tombstoning.* You can manually mark a record for eventual deletion, or *tombstoning*. The tombstone state of the record replicates to other WINS servers, preventing any replicated copies of the deleted records from re-appearing at the same server where they were originally deleted. For more information, see “Deleting and Tombstoning Records” in this chapter.
- *Improved management utility.* The WINS console is fully integrated with the MMC, a powerful and more user-friendly environment you can customize for your efficiency. Because all server administrative utilities included for your use in Windows 2000 Server are part of MMC, new MMC-based utilities are easier to use, as they operate more predictably and follow a common design.
- *Improved ease of use for both using and managing advanced WINS features.* Several useful WINS features from earlier versions of Windows NT Server that were only configurable through the registry are now more directly usable. These include the ability to block records by a specific owner or WINS replication partner (formerly known as *Persona Non Grata*), or allow override of static mappings (formerly known as *Migrate On/Off*). For more information, see “Blocking Rep-

HOW A NETBIOS NAME IS USED

For example, the Server service uses a NetBIOS name. When the server computer starts, this service registers a unique NetBIOS name, based on its configured NetBIOS computer name—SERVER1, in this example—on the network. The exact name registered is a combination of the characters SERVER1, assigned for the NetBIOS computer name, plus a 16th character that contains the hexadecimal byte value of 20 (or [20h], as it appears when viewing records in the WINS console).

When other computers on the network use the net use command to attempt to connect to SERVER1, a name-query request searches for this NetBIOS name. The query uses direct contact with a WINS server or a broadcast to the local network to process the query. When the matching named server process is found—for example, a NetBIOS name entry of SERVER1 with a name suffix value of 20 for the 16th character—the IP address contained in this name record is returned to the requesting computer. Communications can then be established using underlying network transport protocol services.

NETBIOS BEFORE WINDOWS 2000

In earlier versions of Windows NT, all network services were registered using only NetBIOS names. For Windows 2000, the Netlogon service, and potentially other network services, will register in DNS instead. Also, legacy network command-line applications (such as the various **net** commands) use NetBIOS names to access these services.

NetBIOS names are also used by other NetBIOS-based computers, such as Windows for Workgroups, LAN Manager, and LAN Manager for UNIX hosts. For more information on NetBIOS names and how they are used to register and indicate named types of service on the network, see Appendix C, “WINS Resources and Troubleshooting.”

INSIDE NETBIOS

NetBIOS defines two components.

- *A session-level interface.* The NetBIOS interface is a standard API that applications can use. These applications submit network input and output and control directives to underlying network protocol software for transfer through the network. You can run any application program using the NetBIOS API for network communication on any protocol software that supports the NetBIOS interface.
- *A protocol for session management and data transport.* The protocol used here can be any networking protocol and its related software used to perform the actual transport and communication of the NetBIOS interface command set. Two examples are TCP/IP and NetBEUI protocol software, both of which are generally provided with earlier versions of Windows operating systems.

Lmhosts Files

The `lmhosts` file is a static file that assists with remote NetBIOS name resolution on computers that cannot respond to NetBIOS name-query broadcasts. It contains NetBIOS name-to-IP addresses mappings. Its function is similar to that of the `Hosts` file; the difference is that the `Hosts` file can be used to map DNS domain names for host computers to their IP addresses.

Computers in a Microsoft-based network can resolve NetBIOS names in several ways. If one method fails, they try the next method, in a fixed order. In a broadcast-based network, the computer first checks its NetBIOS name cache. Normally, the cache contains the name only if it was used recently, but names can be preloaded from an `lmhosts` file into the cache.

If static name-to-address mappings are entered in the `lmhosts` file using the `#pre` notation, then these names are considered to be preloaded into the NetBIOS names cache and are used first to resolve name query, before a NetBIOS subnet broadcast or WINS query are used.

After checking the local cache, WINS servers are contacted (if they are configured and reachable) first before the name query is broadcast locally on the client subnet to further attempt resolution of the name. If these methods fail, the client (if enabled to do so) can later refer to an `lmhosts` file again to further search for and obtain the name-to-IP address mapping; for example, to resolve a name used by another computer located on another subnet located across a router from the client.

LIMITATIONS OF LMHOSTS FILES

Despite the many uses of the `lmhosts` file, there are some limitations to its design. Its greatest limitation is that it is a static file. Because of this, entries must be updated if the name or the IP address of the computer changes.

An IP address for a client might change for several reasons, such as

- It changes (physically moves) to another subnet within your routed LAN.
- The computer is a portable and changes to another site location, such as a remote dial-up user dialing in from home through remote access to your network.
- The DHCP server leases the client a different IP address after its lease expires.

When such changes occur, they must also be propagated to all the computers that need access to the resource with the changed name-to-IP-address mapping. A centrally maintained `lmhosts` file can reduce some of the manual administration needed to propagate new or revised mappings to the required computers. However, entering and changing the mappings is still a manual, labor-intensive process. While maintaining an `lmhosts` file

TABLE 6.1

Computer Browser Service Functions

Browser role	Description
Domain master browser	Used only in domain environments. By default, the Primary Domain Controller for a domain operates in this role. Collects and maintains the master browse list of available servers for its domain, as well as any names for other domains and workgroups used in the network. Distributes and synchronizes the master browse list for master browsers on other subnets that have computers belonging to the same domain.
Master browser	Collects and maintains the list of available network servers in its subnet. Fully replicates its listed information with the domain master browser to obtain a complete browse list for the network. Distributes its completed list to backup browsers located on the same subnet.
Backup browser	Receives a copy of the browse list from the master browser for its subnet. Distributes the browse list to other computers upon request.
Potential browser	Under normal conditions, operates similarly to a non-browser. Capable of becoming a backup browser if instructed to by the master browser for the subnet.
Non-browser	Does not maintain a browse list. Can operate as a browse client, requesting browse lists from other computers operating as browsers on the same subnet. Configured so it cannot become a browser.

Under some conditions, such as failure or shutdown of a computer designated a specified browser role, browsers (or potential browsers) may change to a different role of operation. This is typically performed through a process known as a *browser election*.

Browsing services in earlier versions of Windows operating systems can be understood in terms of three key processes:

- *Collection of browsing information.* Browse lists are made up of computers that share resources through the use of the Server service. Periodically, every computer running this service broadcasts a host announcement message for its configured domain or workgroup name to the local subnet. These announcements are collected and processed on an ongoing basis by the master browser for each subnet.

When the master browser on a subnet receives a host announcement, it compares the name of the sending computer to its current browse list. If the name already appears, it is refreshed in the list. If the name does not appear, it is added to the list.

- *Distribution of browsing information.* Browse lists are distributed to backup browsers by the master browser for the subnet. Periodically, the master browser must broadcast an announcement message for its

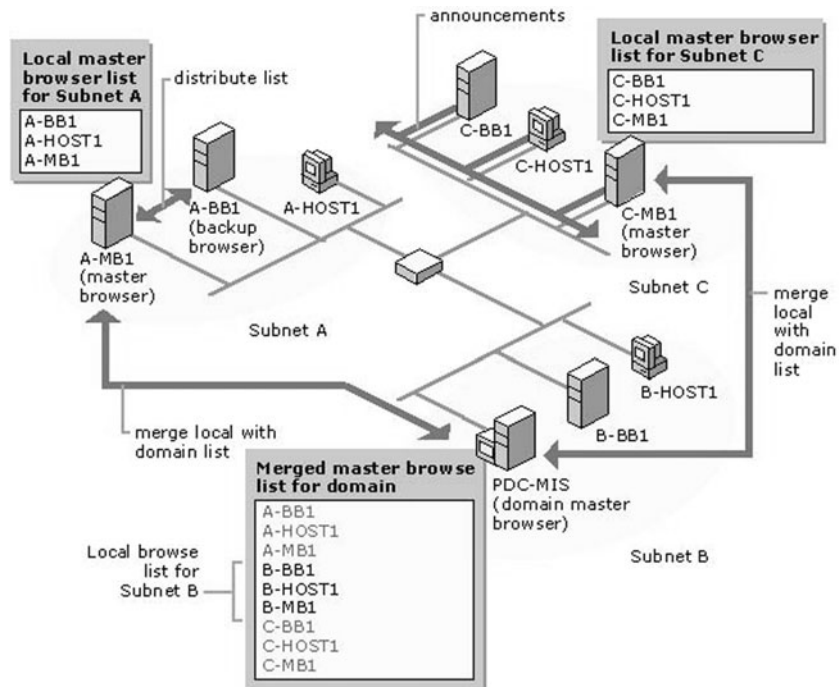


FIGURE 6-2

How browsing works to collect, distribute, and merge lists

Browsing WANs With TCP/IP

The Computer Browser service relies almost entirely on using broadcast communication on each subnet in a network. In a WAN that uses TCP/IP, where domains can be separated by routers, special problems for browsing can occur. Most IP routers are not configured to forward broadcasts.

For browsing in these environments, there are two issues to consider.

- How browsers separated by a router perform browser functions, such as updating and maintaining a complete browse list of all network servers, domains, and workgroups.
- How local browse clients on each subnet browse remote domains not present on the same subnet.

These issues can be addressed in three possible ways: using WINS, maintaining an `lmhosts` file for each subnet master browser, or enabling Net-BIOS broadcasts through IP routers.

The last option, enabling broadcasts across IP routers, is not recommended for most routed TCP/IP networks. The second option, using `lmhosts` files, offers a partial solution to these issues by providing a way to

Locating Domain Controllers Using NetBT

A domain is a logical grouping of network servers and other computers that share common security and user account information. In a domain-based network, Windows NT computers are configured as members of a specified domain.

When domain computers require access, such as network logon or access to a shared resource in the domain, authentication of the user in the domain security database is needed to control access. Domain controllers are computers running Windows NT Server that perform the specialized function of controlling this access. If a domain controller for the domain cannot be located, the user is denied access. For this reason, it is critical that member computers in each domain be able to locate domain controllers.

For environments with domains running Windows NT Server 4.0 and earlier versions, the process of locating domain controllers involves the resolution of the <domain> [1C] name. This name is registered for use by the domain controllers within each domain and can contain up to 25 IP addresses.

The first IP address is always for the PDC. The additional (up to 24) IP addresses are for Backup Domain Controllers (BDCs). Because this name is treated as a domain group by WINS, each member of the group (a domain controller) must renew its name individually in WINS, or its IP address entry in the list is released and can be eventually overwritten.

Each time a domain controller starts, it registers its <domain>[1Ch] name. This record can then be updated dynamically in the WINS database and replicated to other WINS servers located throughout the network.

In addition to locating domain controllers, some domain functions are reserved for handling only by the domain master browser or PDC. Because the PDC or domain master browser is a single server computer, locating it involves resolution of a special record type, the <domain> [1B] name. This record can be registered by the PDC in WINS and is used to map the domain name to a single IP address of the server computer performing in this domain role.

Note

For Windows 2000 Server, domains are established with Active Directory, which uses a method based on DNS query to locate Windows 2000 domain controllers.

HOW <DOMAIN> [1B] NAMES ARE USED

Queries for <domain> [1B] names are made by,

- *Domain-based password changes.* When a user in a Windows NT domain attempts to change their password at a domain member computer, a WINS query is used to locate the configured <domain>[1B]

WINS DATABASE FILES

WINS uses the Jet database format for storing its data. Jet produces *J<n>.log* and other files in the *systemroot\System32\Wins* folder to increase the speed and efficiency of data storage.

Table 6.2 describes the files that are created and used by the Jet database in each WINS server.

TABLE 6.2
Files Created and Used by the Jet Database

File	Description
J50.log and J50#####.log	<p>A log of all transactions done with the WINS database. This file is used by WINS to recover data if necessary.</p> <p>To increase speed and efficiency of data storage, the Jet database writes current transactions to log files rather than directly to the database. Therefore, the most current view of the data includes both the database and any transactions in the log files. Both of these files are used for recovery if the WINS service abruptly or unexpectedly stops. If the service stops in an unexpected manner, the log files are automatically used to re-create the correct state of the WINS database.</p> <p>Log files maintain a specific size; however, they can grow quickly on a busy WINS server. Inevitably, WINS writes more transactions to a log than the log size can accommodate. When a log file is filled, it is renamed, indicating that it is an older log and not in use. A new transaction log is created with the <i>J<n>.log</i> file name, where <i><n></i> is a decimal number, such as <i>J50.log</i>. The naming format of the previous log file is <i>JetXXXXX.log</i>, where each <i>X</i> denotes a hexadecimal number from 0 to F. Previous log files are maintained in the same folder as the current log files.</p> <p>The log files are processed (all entries written to the database) and deleted when a successful backup occurs or when the WINS server is shut down properly. If many <i>J<n>.log</i> files accumulate, you should schedule frequent backups to maintain the logs. After the entries are processed, you can manually delete the log files; however, this prevents a successful recovery of the database if it should be needed. For this important reason, do not manually delete or remove the log files from the system until a backup has been performed.</p>
J50.chk	<p>A checkpoint file that indicates the location of the last information successfully written from the transaction logs to the database. In a data recovery scenario, the checkpoint file indicates where the recovery or replaying of data should begin. This checkpoint file is updated every time data is written to the database file (<i>Wins.mdb</i>).</p>
Wins.mdb	<p>The WINS server database file, which contains two tables: the IP address-to-Owner ID mapping table and the Name-to-IP address mapping table.</p>
Winstmp.mdb	<p>A temporary file that is created by the WINS server service. This file functions as a swap file during index maintenance operations and can remain in the <i>systemroot\System32\Wins</i> directory after a system failure.</p>
Res#.log	<p>These are reserved log files, which function in emergencies when the server runs out of disk space. If a server attempts to create another transaction log file and there is insufficient disk space, the server flushes any outstanding transactions into these reserved log files. The service then shuts down and logs an event to Event Viewer.</p>

Renewing Names

Periodic name renewal is required for WINS client computers to renew their NetBIOS name registrations with the WINS server. The WINS server treats name renewal requests similarly to new name registrations.

When a client computer first registers with a WINS server, the WINS server returns a message with a TTL value that indicates when the client registration expires or needs to be renewed. If renewal does not occur by that time, the name registration expires on the WINS server and the name entry is eventually removed from the WINS database. However, static WINS name entries do not expire, and therefore do not need to be renewed in the WINS server database. For information about using static mappings, see Chapter 7.

The default **Renew interval** for entries in the WINS database is six days. Renewal occurs every three days for most WINS clients because WINS clients attempt to renew their registrations when 50 percent of the TTL value has elapsed.

A name must be refreshed before this interval ends, or it will be released. Names are refreshed by sending a name refresh request to the WINS server, as shown in Figure 6-14.

It is the responsibility of the client (HOST-C) to refresh its name before the Renew interval expires. If the WINS server, WINS-A, does not respond to the refresh request, the client, HOST-C, can increase the rate at which it attempts to refresh its name.

Important

In most cases, the default value is the appropriate Renew interval. You should always set the same Renew interval for all server replication partners whenever multiple WINS servers are used.

Incorrectly adjusting the Renew interval can adversely affect system and network performance.

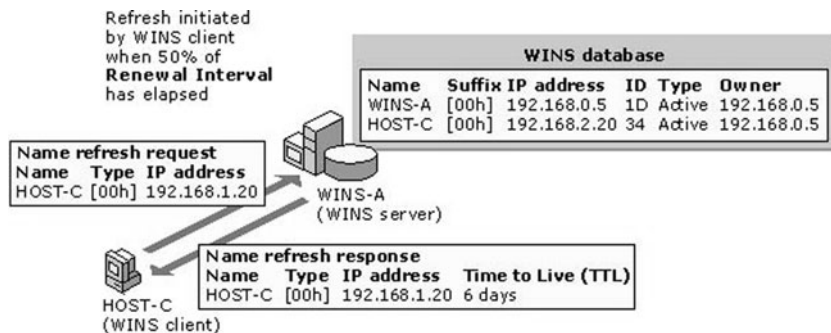


FIGURE 6-14

How clients refresh names in WINS

Using the WINS console, you can choose to configure the level of burst handling used by the server, which modifies the size of the burst queue to accommodate either a low, medium, or large burst situation.

Note

Any WINS server running either Windows 2000 Server or Windows NT Server 4.0 (with Service Pack 3 or later installed) can use burst handling.

Deleting and Tombstoning Records

WINS now provides improved database management through support for the following deletion operations:

- Simple deletion, for deleting WINS database records stored on a single server database.
- Tombstoned deletion, for deleting WINS database records replicated to databases on other WINS servers.
- Multiple-group selection of displayed database records, for either simple or tombstoned deletion.

The WINS console also provides a simple and convenient utility for administratively removing records of any type, regardless of whether they are statically or dynamically added. In previous releases of Windows NT Server, other available WINS management tools could only administratively delete entries (such as static mappings) that were added in the same way.

HOW SIMPLE DELETION WORKS

Simple deletion removes the records that are selected in the WINS console only from the local WINS server you are currently managing. If the WINS records deleted in this way exist in WINS data replicated to other WINS servers on your network, these additional records are not fully removed. Also, records that are simply deleted on only one server can reappear after replication between the WINS server where simple deletion was used and any of its replication partners.

HOW TOMBSTONING WORKS

Tombstoning marks the selected records as *tombstoned*, that is, marked locally as *extinct* and immediately released from active use by the local WINS server. This method allows the tombstoned records to remain present in the server database for purposes of subsequent replication of these records to other servers.

When the tombstoned records are replicated, the tombstone status is updated and applied by other WINS servers that store replicated copies of these records. Each replicating WINS server then updates and tombstones