NetBIOS over TCP/IP, and WINS

NetBIOS over TCP/IP

NetBIOS over TCP/IP (NetBT or NBT) was implemented to allow Windows 2000 and Windows XP computers to communicate with devices and share resources on the network running older Windows operating systems. In Windows 7, the default NetBIOS setting is to use the NetBIOS setting provided via DHCP. If a Windows 7 computer uses a static IPv4 address, it will automatically use NetBIOS over TCP/IP.

Broadly speaking, NetBIOS works by maintaining a list of unique names assigned to network resources; providing the services to establish, defend, and resolve these names; and carrying the necessary communications between applications that make use of these network resources. Named resources include files, services (processes), users, computers, and Windows workgroups and domains. NetBIOS ensures that names are accurate, current, and unique, and it provides the APIs with access to these resources. An application makes a call to the NetBIOS API to access a named resource or discover the names of available resources. Depending on the precise configuration of NetBIOS on the particular machine, NetBIOS may take a variety of steps to resolve the name to an address. It can then send messages to query the named resource, or it can open and maintain a session.

Traditionally, for most Windows clients, NetBIOS was the native method used to access network resources and share their own resources with others. A network with Windows 2000 or clients and servers didn't require NetBIOS. In practice, however, there are still some networks that require NetBIOS to share resources with clients.

Drawbacks to NetBIOS

NetBIOS has two serious drawbacks. The most serious is that it does not have a network component to its namespace. NetBIOS names are only names, not addresses. This differs from IP addresses, which have a host portion and a network portion. Because NetBIOS names only have a host portion, they are considered nonroutable. (Another way of saying this is that NetBIOS uses a flat namespace.) IP, by contrast, uses a hierarchical namespace, such as server.domain.com. NetBIOS requires TCP/IP or some other network-aware protocol to be useful across network boundaries.

The second drawback is less serious but seems even more intractable. NetBIOS is a chatty protocol, constantly sending short messages for a wide variety of purposes. This characteristic, which was trivial on the 20- to 40-machine networks of the 1980s, can be a significant weakness on networks with hundreds of clients, particularly when WAN connections are used for name resolution.

NBT

NBT is defined by RFC 1001, "Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods," and RFC 1002, "Protocol Standard for NetBIOS Service on a TCP/UDP Transport: Detailed Specifications." NBT was implemented to correct the shortcomings of NetBIOS. NBT is typically used on networks that do not have access to a DNS server, are not operating in a domain, and are using older versions of Windows and Microsoft applications and services. Under these circumstances, NBT allows a computer to browse the network and locate other computers and services. It also allows file sharing across the network and provides name resolution services.

If the Windows computers on your network require NBT and if the device providing DHCP, such as a DSL modem, does not have a configuration setting that can provide NBT, you may have to manually enable NBT on your Windows computer. This task is performed

in the Internet Protocol Version 4 (TCP/IPv4) Properties box. On the General tab, click the Advanced button. On the Advanced TCP/IP Settings box, click the WINS tab. And then, under NetBIOS setting, select the Enable NetBIOS over TCP/IP radio button.

On the vast majority of today's networks, it will be unnecessary to enable NBT, given that DNS use is ubiquitous, even in small office/home office (SOHO) environments. Also, the use of Windows 7 and modern Microsoft applications and services is rapidly rendering NBT unnecessary. NBT is not supported in IPv6, and there is no method of configuring the use of NBT in the properties of an IPv6 protocol for a network adapter.

WINS

Windows Internet Name Service (WINS) is a service that resolves NetBIOS names to IP addresses in routed networks. This requires the use of a WINS server on the network, such as Windows Server 2003. A Windows client computer must be configured to look for the IP address of one or more WINS servers on the network. WINS is ideally used in networks that require NBT for name resolution, which typically means a network using older versions of Windows or a mix of modern and older Windows computers.

The use of a WINS server on a network automates dynamic name resolution. For instance, when a DHCP server changes the IP address of a WINS-enabled network node, the WINS data for the computer is updated on the WINS server database. This reduces the need for nodes to issue IPv4 requests for NetBIOS name resolution.

How WINS Works

If a Windows network node requires NetBIOS name resolution, it will first check its local NetBIOS computer name. It then looks at its local NetBIOS name cache for remote names. If the name-to-address mapping isn't found, the node forwards its NetBIOS query to the primary WINS server configured in the IPv4 properties of its network adapter. If the primary WINS server does not respond, it will query any other WINS servers it is configured for, if they exist. Only if no WINS server responds will the node send a broadcast NetBIOS query to the local subnet. Finally, if these attempts have been unsuccessful, the node will check its LMHOSTS file and then its HOST file for the mapping.

WINS servers rely on direct communications (unicasts) between themselves and the clients (end nodes) attempting to register and resolve NetBIOS names. WINS clients configured as p-nodes, m-nodes, or h-nodes may attempt to register or resolve NetBIOS names by contacting the WINS server(s) configured for their use. When interacting with the WINS server, all three node types behave the same way.

WINS-enabled clients can be configured to use more than one WINS server. Older WINS clients could only be configured to use one primary and one secondary WINS server. Windows 2000 and Windows XP clients can be configured to use 11 secondary WINS servers. The client attempts to use the primary WINS server first. (This is the first in the list, if you are configuring the client from the Advanced TCP/IP Settings dialog box.) If the primary WINS server does not respond, the client uses any secondary WINS server(s) configured for it, using them in the order listed in the Advanced TCP/IP Settings dialog box. You should avoid using more than one or two secondary WINS servers, because the WINS client will query each WINS server in its list, attempting name resolution until the list is exhausted. This can cause an unnecessary increase in network traffic.

When a node, user, or process with a NetBIOS name signs on to the network or starts up, it attempts to register its name. If it is configured to use WINS, it sends a Name Registration Request packet to the WINS server. If the name is in the proper form for NetBIOS names and no record for that name already exists in the WINS server's database, the WINS server

sends a positive Name Registration Reply packet to the node and enters the name in its database. The WINS server's response includes the TTL (six days by default) for the name. The node attempts to renew this name at half the TTL value—three days' time if it received the default TTL. If a name is not renewed within the TTL, the name is released and made available for use by the next entity attempting to register it.

If the name already exists in the database, the WINS server sends a Wait Acknowledgment (WACK) to the node attempting to register. This message acknowledges the receipt of the Name Registration Request packet without either granting or denying it, but asks the node to wait. At the same time, the WINS server attempts to contact the registered owner of the name to see if the name is still in use. If the owner responds, then the WINS server sends a negative Name Registration Reply packet to the node attempting to register the name. If the registered owner does not respond, then the WINS server grants the name to the node attempting to register, sending it a positive Name Registration Reply packet. (In earlier versions of WINS, the server responded to an apparent name conflict by asking the registering node itself to send a challenge to the name holder.)

In some circumstances, the WINS server may issue either a Name Conflict Demand packet or a Name Release Demand packet to a name holder or a node, attempting to register a name in conflict. These so-called "demand" packets are requests that have no response associated with them. They are treated as imperatives, and a node must comply. The Name Conflict Demand packet tells a node that its name is in conflict. The node notifies the user of this situation, and the node eventually releases the name. The Name Release Demand packet tells the receiving node to remove the name immediately from its name table. Typically, these types of packets are only sent when, for example, you are reconfiguring your network and names and addresses are being assigned and reassigned in rapid succession.

Burst Mode

WINS servers support a special name registration regime called burst mode. When a large network first comes to life at the start of the workday, for example, many hundreds or thousands of Name Registration Requests may pour in within a few seconds. To prevent the WINS server from being overwhelmed by a sudden spike in utilization, WINS servers can go into burst mode. In burst mode, the server responds to every Name Registration Request packet with a positive Name Registration Reply without attempting to resolve any conflicts. The trick is this: It includes in each positive response a small TTL, and it gives a slightly different TTL to each node. Because the nodes will attempt to renew their names in half the TTL, name conflict resolutions can be deferred until the spike passes. In this way, the server itself can fan out the queue, spreading the workload over a longer time period.

You can change the queue size that triggers burst mode handling (it's set to 500 registrations by default) in the WINS Server Console. WINS servers have a maximum capacity of 25,000 name resolution/refresh queries. For example, if the burst queue is set for 500 entries and more than 500 requests arrive, the next 100 WINS name registration requests will be responded to with a TTL of 5 minutes. Each additional 100 requests will add another 5 minutes to the TTL, up to a maximum of 50 minutes. If WINS client registration requests continue to arrive at burst levels, the next set of 100 queries is answered with the starting TTL of 5 minutes, repeating the entire process until the maximum intake level is reached.

WINS, NetBIOS, and Linux Samba

Linux and UNIX machines can also access NetBIOS resources using the Samba suite of applications for those operating systems. Samba uses SMB and NetBT for resource sharing on IP networks. When properly configured, Samba hosts can access resources through any

WINS server, and Windows clients can access resources through the Samba server, all using a core of NetBT. Samba, like Linux, is Open Source software (it can be altered and redistributed without fees or restrictions).

WINS No Longer in General Use

As with the use of NBT, WINS services are largely unnecessary in modern Windows network environments because of the widespread use of DNS servers for name resolution. The versions of Windows that once utilized NBT and WINS are no longer supported by Microsoft and are considered obsolete. WINS is not supported in IPv6, and there is no method for configuring the IPv6 protocol properties of the network adapter of a Windows 7 computer to point to a WINS server. DNS is the primary method of name resolution for IPv6-enabled computers.

Tools for Troubleshooting NetBIOS and WINS Problems

When the network itself is in good shape, the failure of NetBIOS services is most often the result of misconfiguration of end nodes or server failure. Poor performance, on the other hand, is more likely to be the cumulative result of minor configuration errors in the server, or in some significant number of end nodes. Server topology also has a large impact on overall performance. Setting up WINS services for a network with many subnets requires not only considerations of security and availability but of load optimizing across WAN links. Push-type replication partners, in true NetBIOS fashion, can be very chatty. You have to weigh the frequency of WINS server updates against the frequency of incorrect positive Name Query responses. Incorrect name resolutions can also generate significant traffic and generally degrade performance.

The tools that are useful for diagnosing and troubleshooting TCP/IP networks in general are also useful in maintaining NetBIOS and WINS services. Ping is an excellent way to test connectivity, for example. Traceroute and Netstat are also useful diagnostic tools. The following sections look more closely at several tools that are useful in troubleshooting name resolution problems.

Nbstat

Nbtstat is a command-line program that returns statistics on NetBIOS, using NetBT if TCP/IP is installed on the machine from which it is run. Nbtstat is available on all Windows 7 and Windows 10 client computers and on Windows Server 2012 and Windows Server 2016 servers. This is a simple tool that gives you instant feedback on the state of particular NetBIOS clients and on NetBIOS name resolution in general.

The -n argument returns a list of all the local NetBIOS names in a tabular form similar to what is shown in Table 1. The -r argument returns a list of names resolved by broadcast and by WINS, and includes a summary count of name resolutions and registrations by each method. The -s argument returns the NetBIOS sessions table, showing open sessions with their destination IP address. The -S (uppercase "S") argument shows the same thing, but it attempts to resolve the remote host name using the HOSTS file. The NetBIOS suffixes in Table 8-1 are from Windows networking, but applications such as Microsoft Exchange can also use NetBIOS names.

Table 1 NetBIOS suffixes and meanings

NetBIOS Suffix (Hex)	Meaning	Used with This Name	Used with This Name Type
00	Workstation service	*Computername*	Unique name

01	**Messenger service**	***Computername***	**Unique name**
03	**Messenger service**	***Computername***	**Unique name**
06	**Remote Access Server (RAS)**	***Computername***	**Unique name**
1F	**NetDDE service**	***Computername***	**Unique name**
20	**Server service**	***Computername***	**Unique name**
21	**RAS Client service**	***Computername***	**Unique name**
BE	**Network Monitor Agent service**	***Computername***	**Unique name**
BF	**Network Monitor Application service**	***Computername***	**Unique name**
00	**Registers the computer as a member of the Windows or workgroup**	***Domainname***	**Group name**
1B	**Registers the computer as the domain**	***Domainname***	**Group name**
1C	**Domain controllers**	***Domainname***	**Group name**
1E	**Used to facilitate browser elections**	***Domainname***	**Group name**
03	**Messenger service**	***Username***	**Unique name**

Note: For a full list of the arguments and their syntaxes, type nbtstat with no argument at a command prompt.

Nbtstat is a fast way to check the status of a particular NetBIOS host or get a quick snapshot of NetBIOS name resolution activity on the local network segment. If, for example, a node appears to have trouble communicating with the WINS server, issuing the `nbtstat` command may show it is actually attempting to use broadcast name resolution.