Removing NetBIOS From Windows 2000

Reduced traffic, easier network support and enhanced security are the three major advantages of removing NetBIOS from the Windows 2000 network. We explain the issues and how to decommission NetBIOS.

By Dave Cook

Designing a network can be a complex operation. There are many decisions to be made, all of which will have a direct bearing on the manageability of the network, its future expansion capabilities, and its interoperability with other operating systems.

One of the biggest challenges facing administrators involves the use of protocols. Which protocols should be employed, for instance, and what combination of protocols is likely to give the best results for greater network integration.

In the past it has often been a case of the more protocols supported, the greater the possibility that two or more devices will be able to communicate with each other, and without any type of restriction. But at what cost to the network? Due to the additional memory and processing power required, each and every protocol used will have a direct impact on performance.

The ideal solution would be to have every device use the same protocol. Networks would retain the same broad connectivity, and they would do so without having to suffer the wasteful burden of supporting multiple protocols.

This scenario is fast becoming a reality, made possible by the remarkable growth of the Internet and its underlying method of transport, the Transfer Control Protocol/Internet Protocol (TCP/IP). Novell, for example, has recently ended its dependence on the Internetwork Packet eXchange/Sequenced Packet eXchange (IPX/SPX) by making its NetWare operating system capable of native IP communication.

Leftovers

TCP/IP, of course, is the default choice of Windows 2000. But, unlike previous Microsoft operating systems, Network Basic Input/Output System (NetBIOS) support is no longer required to communicate with other Microsoft network clients. Nevertheless, even with the extensive use of TCP/IP-based protocols, a few remnants of the NetBIOS background still exist.

This is hardly surprising, really, because all Microsoft networks prior to Windows 2000 required NetBIOS support over each transport protocol. Most often these protocols would be in the form of TCP/IP, IPX/SPX and the Network Basic Extended User Interface (NetBEUI). Basically, administrators had no option but to accept multiple protocols because, without them, Microsoft clients simply could not communicate with one another.

Now that Microsoft has decided to end the reliance on NetBIOS in Windows 2000, there are numerous advantages to be gained by removing it from the network. Even though, in practical terms, this can only be achieved once all downlevel Microsoft clients and servers have been purged from the network. The advantages of removing NetBIOS include:

- You can wave goodbye to WINS. Once NetBIOS is retired, clients can end their reliance on the problematic WINS and employ the more advanced Active Directory's Dynamic Domain Name Service (DDNS) for name registration and resolution.
- Easier, more efficient network support. With NetBIOS removed, there are far fewer protocols to manage.
- Improved network performance. The removal of NetBIOS will drastically reduce traffic over the network. Without having to wait for broadcast results, Windows should react more rapidly.
- Increased security. Under NetBIOS, Windows computers are not entirely secure. Removing NetBIOS from systems, especially those ma-

"The NetBIOS standard allows applications on different computers to communicate across a variety of local area network (LAN) protocols, including the Internet Protocol (IP)."

chines directly connected to the Internet, will gain users an added level of security.

But before we get too involved with the practicalities of removing NetBIOS, a brief overview of some of its most important characteristics is in order.

NetBIOS Overview

NetBIOS is an application program interface. It was designed by IBM and Sytek in 1984 for their PC Network program, and later adapted by Microsoft and included in MS-DOS version 3.1. Since then NetBIOS has become a worldwide network standard.

The NetBIOS standard allows applications on different computers to communicate across a variety of local area network (LAN) protocols, including the Internet Protocol (IP). However, it is not in itself a routing mechanism; applications communicating across a wide area network (WAN) will typically require the assistance of another mechanism, such as TCP.

NetBIOS is a Session-layer protocol, rather than a Network- or Transport-layer protocol. It specifies the interface for programs to communicate with it, and then relies on lower-level protocols like NetBEUI to transport the NetBIOS information between machines. NetBEUI was purpose-built to transport NetBIOS across a network. As with NetBIOS, NetBEUI is unaware of subnets.

Machines with NetBIOS enabled identify one another using names made up of text, rather than IP addresses. These names can include the upper case letters of the alphabet, the numbers from zero to nine, and numerous special characters including an underscore, brackets and the tilde sign.

Although the NetBIOS naming convention allows 16 bytes in a name, Microsoft limits these names to 15 bytes and uses the 16th byte to designate a service, such as a Workstation, File Server and so forth. This combination of NetBIOS name and service ID forms a unique identifier, which is similar to the way an IP address and the User Datagram Protocol (UDP) port numbers combine to form a socket.

Services

There are three categories of NetBIOS services: the name service, the session service and the datagram service:

Name Service

The name service allows an application to verify that its own NetBIOS name is unique. The application issues an add name query request containing the name, and NetBIOS broadcasts it. Other NetBIOS applications receiving that query will return either an add name response, or a name-in-conflict response. If there is no response to the query after approximately six broadcasts, then the name is regarded as unique.

Using the NetBIOS name service it is possible to delete a name that an application no longer requires, and to use a server's NetBIOS name to determine the server's address. In the case of the latter, the application issues a name query request containing the target server's name, and NetBIOS broadcasts it. The server that recognises the name will return a name query response that contains its network address.

Session Service

The NetBIOS session service lets two computers establish a reliable connection so that they can exchange messages with one another. Error detection and recovery options are provided, and messages can be up to 131,071 bytes long.

Datagram Service

The datagram service allows applications to communicate without having to acknowledge a connection. Messages can be sent independently and broadcast to every computer on the LAN. However, it is the application itself that is responsible for error protection and recovery.

WINS

Prior to Windows 2000, the Windows Internet Naming Service (WINS) made it possible to dynamically register computer names on the network. WINS is required mainly for two reasons: to provide a centralised location for name resolution within the network - because NetBIOS encounters problems when used with multiple subnets - and to reconcile the static nature of the Domain Name Service (DNS).

To overcome both difficulties in Windows 2000, Microsoft has introduced Dynamic DNS (DDNS). The biggest difference between DDNS and WINS is that WINS translates NetBIOS names to IP addresses, while DDNS translates host names to IP addresses. Support for dynamic update is essential, since most of today's medium-to-large TCP/IP networks rely on the Dynamic Host Configuration Protocol (DHCP) to allocate their clients' IP addresses.

Like NetBIOS, WINS isn't required in a pure Windows 2000 TCP/IP environment. So, unless there are Windows-based clients still using NetBIOS, WINS can be retired from Windows 2000. Typically, WINS would be retained for mixed environments that include legacy clients such

"The benefits of removing NetBIOS include easier network support, and improved network performance due to reduced traffic. Security will also be enhanced."

Removing NetBIOS

"If any critical applications are found to be reliant on NetBIOS and there are no alternatives available, the only solution is to leave NetBIOS active, albeit in a reduced role."

as Windows for Workgroups and Windows 95.

Windows 2000 WINS includes numerous server enhancements, as well as an improved management tool and additional client functions. Support is there for manual tombstoning, persistent connections, enhanced filtering, record searching, and dynamic re-registration. The end result is a more robust and easier solution for mapping NetBIOS names to IP addresses on TCP/IP networks. Although WINS and DDNS can co-exist indefinitely, a significant decrease in traffic will be achieved if Windows 2000 clients can be made to rely only on DDNS.

In order to resolve the NetBIOS name of a downlevel client to an IP address by querying DDNS only, Windows 2000 DHCP Servers need to be implemented. This procedure, which allows DDNS-enabled clients to resolve downlevel NetBIOS names without WINS, is called downlevel registration.

Apart from a new-look Microsoft Management Console and provisions for some vendor-specific options and class IDs, the DHCP service in Windows 2000 is practically identical to the one provided with Windows NT 4.0 Service Pack 5. Before installing DHCP, however, be sure to make an inventory of current IP address assignments, and to ensure that all hosts have static addresses.

Pre-Removal Testing

When moving away from NetBIOS and WINS, it is important to determine which machines and applications still require NetBIOS. The first port of call should be to the WINS console: click Start, point to Programs, Administrative Tools, and then click on WINS.

Assuming the entire system is to be upgraded to Windows 2000, all entries shown that are OS-specific may be deleted. Typically, these entries would look like the following: computername<00>, computername<01>, domain<00>, domain<1B>, \\—_MSBROWSE_<01>, and computername<23>, among others. For further information on NetBIOS names, Microsoft maintains a list of more than 30 different service types and their hex identifiers on the Web at: **support.Microsoft.com/support/kb/articles/q163/4/09.asp**.

Once any OS-specific entries have been removed, any remaining entries will need to be investigated further. The system or application requiring those entries will need tracing, and a non-NetBIOS alternative will have to be provided.

It is possible that not all clients will register with WINS. If this is the case, then each machine will need investigating individually before NetBIOS can be removed. One way to achieve this is to enlist the help of a network sniffer, such as the Intel sniffer in SMS or Sniffer Pro from Network Associates.

On the other hand, the command-line utility NBTSTAT is a useful little tool, and perfectly capable of querying remote machines for their registered names. If the name of the remote computer is known, for example, then:

```
NBTSTAT - A computername
```

performs a NetBIOS adapter status command against the machine specified. Likewise, if the IP address is known, then use:

```
NBTSTAT - A address
```

To search for applications using NetBIOS directly across the network, use:

```
NBTSTAT - S - 1
```

at the command line. This will display the current NetBIOS sessions and their status - including statistics - once every second. With the application running and creating network activity, analysing the NBTSTAT output will determine whether NetBIOS is still present.

After performing the aforementioned tests, the network administrator should then determine the

Disabling NetBIOS-over-TCP/IP

Once the transition to Windows 2000 Servers and desktops is complete, it makes good sense to disable the NetBIOS-over-TCP/IP (NetBT) name resolution and to use DDNS exclusively. The benefits of removing NetBIOS include easier network support, and improved network performance due to reduced traffic. Security will also be enhanced, since Windows computers using NetBIOS can be vulnerable to attack, especially when connected to the Internet.

Before NetBIOS is removed, however, it is important to note that the following conditions must apply:

- All downlevel operating systems such as Windows for Workgroups, Windows 9x and Windows NT that use NetBIOS and are connected to the network must be upgraded to Windows 2000.
- Any applications still using NetBIOS must be upgraded, replaced with a similar application that doesn't require NetBIOS, or withdrawn.

consequences of removing NetBIOS from the system. With luck, only the operating systems will be NetBIOS-dependant, in which case the transition can go ahead as planned.

If any critical applications are found to be reliant on NetBIOS and there are no alternatives available, the only solution is to leave NetBIOS active, albeit in a reduced role. In the vast majority of cases, however, other solutions will be to hand and the migration away from NetBIOS can proceed to the next stage, which is implementing DDNS.

Implementing DDNS

Because DDNS completely replaces the functionality of WINS, the replacement system must be fully prepared and operational before any Windows 2000 clients are deployed. Be aware, though, that DDNS and Active Directory designs are closely related.

Getting the design right at the first attempt is essential if major problems are to be avoided later. Further information regarding the deployment of DDNS and Active Directory can be found in the resources section of Microsoft's Windows 2000 Web site at **www.microsoft.com/windows2000/library**.

Once DDNS is up and running, the deployment of Windows 2000 can commence in earnest. During the upgrade it should be ensured that all NetBIOS applications existing on downlevel systems are replaced. Obviously, both DDNS and WINS will be required during this time. Unfortunately, until the removal of WINS, this is likely to make the network as inefficient as it was before.

Decommissioning

With Windows 2000 fully deployed, WINS can be removed from the network. This process is called decommissioning. DHCP clients, for example, can be configured not to use WINS simply by deleting the NBNS/-WINS option from each scope. Machines with static addresses, meanwhile, will also need to have WINS server addresses removed from the machine's TCP/IP properties window.

To decommission a WINS server click on Start, and select Programs, Administrative tools, and WINS. From the WINS console, open the applicable WINS server and click on Active Registration. On the Action menu, click Delete Owner, and then, from Delete This Owner, click the IP address of the WINS server to be decommissioned. Be aware that it could take some time to load the records for the selected server if it is not running locally.

Note also that, when removing a WINS server, it is important that records wherever possible are tombstoned at the server. Tombstoning ensures that any replication partners associated with the decommissioned WINS server are updated, with all records suitably released.

At the option "Use this operation to delete the selected owner and its records", click on "Replicate deletion to other WINS servers (tombstone)" and click OK. When prompted to confirm Tombstoning, click Yes. In the console tree, click Replication Partners and, on the Action menu, click Replicate Now. Once replication has been verified, WINS can be safely removed from the decommissioned server.

Assuming no other WINS servers remain in commission, it is now possible to disable NetBIOS-over-TCP/IP. To remove the NetBIOS name resolution, right-click on My Network Places, select Properties and then right-click the Local Area Connection icon and select Properties from the fly-out menu. This will open the Local Area Connection Properties window.

Double-click the Internet Protocol (TCP/IP) entry and the Internet Protocol Properties window will open. Now click on the Advanced button. From the Advanced TCP/IP Settings window, select the WINS tab and check the Disable NetBIOS Over TCP/IP radio button. It is worth noting that Dynamic Host Configuration Protocol (DHCP) clients can also distribute this setting.

With NetBIOS disabled, click OK to save the change, click OK to return to the Local Area Connection Properties window and, finally, click OK to save all changes and close the window. Once NetBIOS has been successfully removed from the network, all parallel connections will end and only direct hosting will be used from that point onwards.

Further Information

www.microsoft.com/windows2000/library
Microsoft Windows 2000 technical library
support.microsoft.com/support/kb/articles/q163/4/09.asp
A useful list of NetBIOS name types
www.atr.net/faq/ras/q11949~1.htm
NetBIOS Name Resolutions and WINS
www.faqs.org/rfcs/rfc1001.html
More on NetBIOS protocols
www.con.wesleyan.edu/~triemer/network/docservs.html
Some well-known port numbers
www.cis.ohio-state.edu/hypertext/information/rfc.html
Internet Request For Comments (RFC) documents
www.codd.com/vbonline/apiary/netbios.htm
Help for VB programmers regarding NetBIOS

PCNA

The Author

Dave Cook is a freelance journalist and technical consultant. You can contact him by email as dave.cook@itp-journals.com.

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.