

NBTSTAT (NetBios over TCP/IP Statistics)

This diagnostic command displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.

Syntax

```
nbtstat [-a RemoteName] [-A IP_address] [-c] [-n] [-R] [-r] [-S] [-s] [interval]
```

Parameters

- a**
Lists the remote computer's name table given its host name.
- A**
Lists the remote computer's name table given its IP address specified in dotted decimal notation.
- c**
Lists the contents of the NetBIOS name cache, with the IP address of each name.
- n**
Lists local NetBIOS names. In this listing, "Registered" indicates that the name has been registered on this network node, either by b-node broadcast or by a WINS server.
- R**
Reloads the LMHOSTS file after purging all names from the NetBIOS name cache.
- r**
Lists name resolution statistics for Windows networking. On a computer configured to use WINS, this option returns the number of names resolved and registered broadcast or WINS.
- S**
Displays both workstation and server sessions, listing the remote hosts by IP address only.
- s**
Displays both workstation and server sessions. It attempts to convert the remote host IP address to a name using the HOSTS file.

interval

Redisplays selected statistics, pausing *interval* seconds between each display. Press CTRL+C to stop redisplaying statistics. If this parameter is omitted, **nbtstat** prints the current configuration information once.

NetBIOS Names

Microsoft networking components, such as Windows NT Workstation and Windows NT Server services, allow the first 15 characters of a NetBIOS name to be specified by the user or administrator, but reserve the 16th character of the NetBIOS name (00-FF hex) to indicate a resource type. Following are some examples of NetBIOS names used by Microsoft components:

Unique Names

\\computer_name[00h]

Registered by the Workstation Service on the WINS Client

\\computer_name[03h]

Registered by the Messenger Service on the WINS Client

\\computer_name[06h]

Registered by the Remote Access Service (RAS), when started on a RAS Server.

\\computer_name[1Fh]

Registered by the Network Dynamic Data Exchange (NetDDE) services, will only appear if the NetDDE services are started on the computer. By default under Windows NT 3.51, the NetDDE services are not automatically started.

\\computer_name[20h]

Registered by the Server Service on the WINS Client.

\\computer_name[21h]

Registered by the RAS Client Service, when started on a RAS Client.

\\computer_name[BEh]

Registered by the Network Monitoring Agent Service—will only appear if the service is started on the computer. If the computer name is not a full 15 characters, the name will be padded with plus (+) symbols.

\\computer_name[BFh]

Registered by the Network Monitoring Utility (included with Microsoft Systems Management Server). If the computer name is not a full 15 characters, the name will be padded with plus (+) symbols.

\\username[03h]

User names for the currently logged on users are registered in the WINS database. The username is registered by the Server component so that the user can receive any “net send” commands sent to their username. If more than one user is logged on with the same username, only the first computer at which a user logged on with the username will register the name.

\\domain_name[1Bh]

Registered by the Windows NT Server primary domain controller (PDC) that is running as the Domain Master Browser and is used to allow remote browsing of domains. When a WINS server is queried for this name, a WINS server returns the IP address of the computer that registered this name.

\\domain_name[1Dh]

Registered only by the Master Browser, of which there can only be one for each subnet. This name is used by the Backup Browsers to communicate with the Master Browser to retrieve the list of available servers from the Master Browser.

WINS servers always return a positive registration response for domain_name[1D], even though the WINS server does not “register” this name in its database. Therefore, when a WINS server is queried for the domain_name[1D], the WINS server returns a negative response, which will cause the client to broadcast to resolve the name.

Group Names

\\domain_name[00h]

Registered by the Workstation Service so that it can receive browser broadcasts from LAN Manager-based computers.

\\domain_name[1Ch]

Registered for use by the domain controllers within the domain and can contain up to 25 IP addresses. One IP address will be that of the primary domain controller (PDC) and the other 24 will be the IP addresses of backup domain controllers (BDC's).

\\domain_name[1Eh]

Registered for browsing purposes and is used by the browsers to elect a Master Browser (this is how a statically mapped group name will register itself

\\--__MSBROWSE__[01h]

Registered by the Master Browser for each subnet