# Understanding NetBIOS

By NeonSurge
Released through the rhino9 Team

**Preface**

Before you begin reading this paper, understand that this paper was written for the novice to the concept of NetBIOS, but - it also contains information the veteran might find educational. I am prefacing this so that I do not get e-mail like "Why did you start your paper off so basic?" - Simple, its written for people that may be coming from an enviroment that does not use NetBIOS, so they would need me to start with basics, thanks. -NeonSurge, rhino9 team.

**Whats is NetBIOS?**

NetBIOS (Network Basic Input/Output System) was originally developed by IBM and Sytek as an Application Programming Interface (API) for client software to access LAN resources. Since its creation, NetBIOS has become the basis for many other networking applications. In its strictest sense, NetBIOS is an interface specification for acessing networking services.

NetBIOS, a layer of software developed to link a network operating system with specific hardware, was originally designed as THE network controller for IBM's Network LAN. NetBIOS has now been extended to allow programs written using the NetBIOS interface to operate on the IBM token ring architecture. NetBIOS has since been adopted as an industry standard and now, it is common to refer to NetBIOS-compatible LANs.

It offers network applications a set of "hooks" to carry out inter-application communication and data transfer. In a basic sense, NetBIOS allows applications to talk to the network. Its intention is to isolate application programs from any type of hardware dependancies. It also spares software developers the task of developing network error recovery and low level message addressing or routing. The use of the NetBIOS interface does alot of this work for them.

NetBIOS standardizes the interface between applications and a LANs operating capabilities. With this, it can be specified to which levels of the OSI model the application can write to, making the application transportable to other networks. In a NetBIOS LAN enviroment, computers are known on the system by a name. Each computer on the network has a permanent name that is programmed in various different ways. These names will be discussed in more detail below.

PC's on a NetBIOS LAN communicate either by establishing a session or by using NetBIOS datagram or broadcast methods. Sessions allow for a larger message to be sent and handle error detection and correction. The communication is on a one-to-one basis. Datagram and broadcast methods allow one computer to communicate with several other computers at the same time, but are limited in message size. There is no error detection or correction using these datagram or broadcast methods. However, datagram communication allows for communication without having to establish a session.

All communication in these enviroments are presented to NetBIOS in a format called Network Control Blocks (NCB). The allocation of these blocks in memory is dependant on the user program. These NCB's are divided into fields, these are reserved for input and output respectively.

NetBIOS is a very common protocol used in todays enviroments. NetBIOS is supported on Ethernet, TokenRing, and IBM PC Networks. In its original induction, it was defined as only an interface between the application and the network adapter. Since then, transport like functions have been added to NetBIOS, making it more functional over time.

In NetBIOS, connection (TCP) oriented and connectionless (UDP) communication are both supported. It supports both broadcasts and multicasting and supports three distinct services: Naming, Session, and Datagram.

**NetBIOS Names**

NetBIOS names are used to identify resources on a network. Applications use these names to start and end sessions. You can configure a single machine with multiple applications, each of which has a unique NetBIOS name. Each PC that supports an application also has a NetBIOS station name that is user defined or that NetBIOS derives by internal means.

NetBIOS can consist of up to 16 aplhanumeric characters. The combination of characters must be unique within the entire source routing network. Before a PC that uses NetBIOS can fully function on a network, that PC must register their NetBIOS name.

When a client becomes active, the client advertises their name. A client is considered to be registered when it can successfully advertise itself without any other client claiming it has the same name. The steps of the registration process is as follows:

1. Uppon boot up, the client broadcasts itself and its NetBIOS information anywhere from 6 to 10 to ensure every other client on the network receives the information.

2. If another client on the network already has the name, that NetBIOS client issues its own broadcast to indicate that the name is in use. The client who is trying to register the already in use name, stop all attempts to register that name.

3. If no other client on the network objects to the name registration, the client will finish the registration process.

There are two types of names in a NetBIOS enviroment: Unique and Group. A unique name must be unique across the network. A group name does not have to be unique and all processes that have a given group name belong to the group. Each NetBIOS node maintains a table of all names currently owned by that node.

The NetBIOS naming convention allows for 16 characters in a NetBIOS name. Microsoft, however, limits these names to 15 characters and uses the 16th character as a NetBIOS suffix. A NetBIOS suffix is used by Microsoft Networking software to indentify the functionality installed or the registered device or service.

[QuickNote: SMB and NBT (NetBIOS over TCP/IP work very closely together and both use ports 137, 138, 139. Port 137 is NetBIOS name UDP. Port 138 is NetBIOS datagram UDP. Port 139 is NetBIOS session TCP. For further information on NetBIOS, read the paper at the rhino9 website listed above]

The following is a table of NetBIOS suffixes currently used by Microsoft WindowsNT. These suffixes are displayed in hexadecimal format.

| Name | Number | Type | Usage |
|---|---|---|---|
| <computername> | 00 | U | Workstation Service |
| <computername> | 01 | U | Messenger Service |
| <\\_MSBROWSE_> | 01 | G | Master Browser |
| <computername> | 03 | U | Messenger Service |
| <computername> | 06 | U | RAS Server Service |
| <computername> | 1F | U | NetDDE Service |
| <computername> | 20 | U | File Server Service |
| <computername> | 21 | U | RAS Client Service |
| <computername> | 22 | U | Exchange Interchange |
| <computername> | 23 | U | Exchange Store |
| <computername> | 24 | U | Exchange Directory |
| <computername> | 30 | U | Modem Sharing Server Service |
| <computername> | 31 | U | Modem Sharing Client Service |
| <computername> | 43 | U | SMS Client Remote Control |
| <computername> | 44 | U | SMS Admin Remote Control Tool |
| <computername> | 45 | U | SMS Client Remote Chat |
| <computername> | 46 | U | SMS Client Remote Transfer |
| <computername> | 4C | U | DEC Pathworks TCPIP Service |

| | | | |
|---|---|---|---|
| <computername> | 52 | U | DEC Pathworks TCPIP Service |
| <computername> | 87 | U | Exchange MTA |
| <computername> | 6A | U | Exchange IMC |
| <computername> | BE | U | Network Monitor Agent |
| <computername> | BF | U | Network Monitor Apps |
| <username> | 03 | U | Messenger Service |
| <domain> | 00 | G | Domain Name |
| <domain> | 1B | U | Domain Master Browser |
| <domain> | 1C | G | Domain Controllers |
| <domain> | 1D | U | Master Browser |
| <domain> | 1E | G | Browser Service Elections |
| <INet~Services> | 1C | G | Internet Information Server |
| <IS~Computer_name> | 00 | U | Internet Information Server |
| <computername> | [2B] | U | Lotus Notes Server |
| IRISMULTICAST | [2F] | G | Lotus Notes |
| IRISNAMESERVER | [33] | G | Lotus Notes |
| Forte_$ND800ZA | [20] | U | DCA Irmalan Gateway Service |

Unique (U): The name may have only one IP address assigned to it. On a network device, multiple occurences of a single name may appear to be registered, but the suffix will be unique, making the entire name unique.

Group (G): A normal group; the single name may exist with many IP addresses.

Multihomed (M): The name is unique, but due to multiple network interfaces on the same computer, this configuration is necessary to permit the registration. Maximum number of addresses is 25.

Internet Group (I): This is a special configuration of the group name used to manage WinNT domain names.

Domain Name (D): New in NT 4.0

For a quick and dirty look at a servers registered NetBIOS names and services, issue the following NBTSTAT command:

```
nbtstat -A [ipaddress]
```

**NetBIOS Sessions**

The NetBIOS session service provides a connection-oriented, reliable, full-duplex message service to a user process. NetBIOS requires one process to be the client and the other to be the server. NetBIOS session establishment requires a preordained cooperation between the two stations. One application must have issued a Listen command when another application issues a Call command. The Listen command references a name in its NetBIOS name table (or WINS server), and also the remote name an application must use to qualify as a session partner.  If the receiver (listener) is not already listening, the Call will be unsuccessful. If the call is successful, each application receives notification of session establishment with the session-id. The Send and Receive commands the transfer data. At the end of a session, either application can issue a Hang-Up command. There is no real flow control for the session service because it is assumed a LAN is fast enough to carry the required traffic.

**NetBIOS Datagrams**

Datagrams  can be sent to a specific name, sent to all members of a group, or broadcast to the entire LAN. As with other datagram services, the NetBIOS datagrams are connectionless and unreliable. The Send_Datagram command requires the caller to specify the name of the destination. If the destination is a group name, then every member of the group receives the datagram. The caller of the Receive_Datagram command must specify the local name for which it wants to receive datagrams. The Receive_Datagram command also returns the name of the sender, in addition to the actual datagram data. If NetBIOS receives a datagram, but there are no Receive_Datagram commands pending, then the datagram is discarded.

The Send_Broadcast_Datagram command sends the message to every NetBIOS system on the local network. When a broadcast datagram is received by a NetBIOS node, every process that has issued a Receive_Broadcast_Datagram command receives the datagram. If none of these commands are outstanding when the broadcast datagram is received, the datagram is discarded.

NetBIOS enables an application to establish a session with another device and lets the network redirector and transaction protocols pass a request to and from another machine. NetBIOS does not actually manipulate the data. The NetBIOS specification defines an interface to the network protocol used to reach those services, not the protocol itself. Historically, has been paired with a network protocol called NetBEUI (network extended user interface). The association of the interface and the protocol has sometimes caused confusion, but the two are different.

Network protocols always provide at least one method for locating and connecting to a particular service on a network. This is usually accomplished by converting a node or service name to a network address (name resolution). NetBIOS service names must be resolved to an IP address before connections can be established with TCP/IP. Most NetBIOS implementations for TCP/IP accomplish name address resolution by using either broadcast or LMHOSTS files. In a Microsoft enviroment, you would probably also use a NetBIOS Namer Server known as WINS.

**NetBEUI Explained**

NetBEUI is an enhanced version of the NetBIOS protocol used by network operating systems. It formalizes the transport frame that was never standardized in NetBIOS and adds additional functions. The transport layer driver frequently used by Microsofts LAN Manager. NetBEUI implements the OSI LLC2 protocol.  NetBEUI is the original PC networking protocol and interface designed by IBM for the LanManger Server. This protocol was later adopted by Microsoft for their networking products. It specifies the way that higher level software sends and receives messages over the NetBIOS frame protocol. This protocol runs over the standard 802.2 data-link protocol layer.

**NetBIOS Scopes**

A NetBIOS Scope ID provides an extended naming service for the NetBIOS over TCP/IP (Known as NBT) module. The primary purpose of a NetBIOS scope ID is to isolate NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID. The NetBIOS scope ID is a character string that is appended to the NetBIOS name. The NetBIOS scope ID on two hosts must match, or the two hosts will not be able to communicate. The NetBIOS Scope ID also allows computers to use the same computer namee as they have different scope IDs. The Scope ID becomes a part of the NetBIOS name, making the name unique.

==========================================================================
Thats it for NetBIOS. If you have any comments or questions... direct them to NeonSurge@abyss.com.

Rhino9: The WindowsNT Security Research Team:
www.x-treme.abyss.com/techvoodoo/rhino9

Peace.
NeonSurge
NeonSurge@abyss.com