Abstract

The Server Message Block (SMB) is a presentation layer protocol providing file and print sharing functions for LAN Manager, and other network operating systems.

The Network Basic I/O System (NetBIOS) NetBIOS was developed in the early 1980s to allow applications to communicate over a network. The TCP/IP version called NetBIOSoverTCP/IP (NetBT), was developed to support communications between symbolically named stations and transfer of arbitrary data. NetBT supports all three services (Name, Datagram and Session) supported by NetBIOS.

This document attempts to provide, Control and Operational details on SMB over NetBT session, which is otherwise not clearly explained in the RFCs [Netbios concepts] and [Netbios specification] or any available documentation.

This document is intended for documentation purpose and for informational use only. This document does not attempt to define a standard, rather tries explaining an existing implementation.

This document puts together pieces of information scattered in multiple documents and offers a single complete documentation for this specific application (smb over NetBT).

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1 Introduction ............................................. 3
  1.1 Terminology ......................................... 3
2. Overview ................................................. 3
3. Server Message Block packet structure ..................... 4
4 Netbios Session Service Packet structure .................. 5
5 File and Printer Sharing Operations ....................... 6
6 Security Considerations ................................... 9
7 IANA Considerations ..................................... 9
8 References ................................................ 9
    8.1 Normative References ............................... 9
    8.2 Informative References ............................ 9
Authors’ Addresses .......................................... 9
1 Introduction

NetBIOS over TCP/IP (NBT, or sometimes NetBT) is a networking protocol that allows legacy node applications relying on the NetBIOS API to scale for the modern TCP/IP networks. This shall support all the three NetBIOS services (given below) over secured tcp/ip connections.

* Name service for name registration and resolution (port: 137)
* Datagram distribution service for connectionless communication (port: 138)
* Session service for connection-oriented communication (port: 139)

The file and printer sharing services are provided by the Server Message Block (SMB) protocol. This shall run on top of NetBT session or run directly over TCP.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Overview

In NetBIOS, the following three services are supported.

Name Service : Each participant must register on the network using a unique name of at most 16 characters. NetBT Name Service handles and records all name registrations. (Port: 137/UDP or 137/TCP)

Datagram Service: Datagram mode is connectionless. A datagram is sent to unique or multiple NetBIOS participants on the network. (Port 138/UDP)

Session Service : Session mode lets two hosts in the network to access and transfer data in a secured way. (Port 139/TCP)

Direct hosted "NetBIOS-less" SMB traffic uses port 445 (TCP and UDP) and SMB over NetBT uses the nbsession service Port (139/TCP).

NetBT allows handling of larger messages, while also providing error detection and recovery. This document is focused on the NetBT Session service for message transfer between hosts, and hence shall discuss SMB and SMB over NetBT in detail.
3. Server Message Block packet structure

Server Message Block (SMB) allows hosts to control sessions like share files, printers, disks etc. SMB thus enables access of shared resources between nodes across the network. SMB packet structure is given below.

1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        0xff   |       S       |       M       |     B         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Command   |       Status  ..                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    .. Status  |       Flags                   |    Flags2 ..  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    .. Flags2  |       TreeID                  |     PID ..    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    .. PID     |       User                    |  MultiplexID..|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| ..MultiplexID |     WordCount |   ParameterWords[Wordcount]   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Byte count         |         DATA                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+/                              /
/+                                                                 |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

A successful connection from a client machine to the server returns a Treeid that identifies the transactions through this particular connection. Each of the operations from the client is identified by the caller process id (PID) and the userid (UID) is used for the authenticated requests/operations.

Multiplexing the single client and server connection among the client’s multiple processes, threads, and requests per thread is identified by the Multiplex id (MID).

The Size of the data portion of the packet is given by Bytecount and the actual data follows this field.
4 Netbios Session Service Packet structure

The [Netbios specification] describes the session service packet structure. File and printer services are the primary uses of the NetBIOS Session service. All session packets are of the following general structure:

```
1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| TYPE | FLAGS | LENGTH |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/ TRAILER (Packet Type Dependent) /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The TYPE, FLAGS, and LENGTH fields are present in every session packet.

<table>
<thead>
<tr>
<th>TYPE - Message Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SESSION MESSAGE</td>
</tr>
<tr>
<td>SESSION REQUEST</td>
</tr>
<tr>
<td>POSITIVE SESSION RESPONSE</td>
</tr>
<tr>
<td>NEGATIVE SESSION RESPONSE</td>
</tr>
<tr>
<td>RETARGET SESSION RESPONSE</td>
</tr>
<tr>
<td>SESSION KEEP ALIVE</td>
</tr>
</tbody>
</table>

4.1 Session Message

The actual data transfer in NetBT session is through session messages. The Session service Packet Type "Session message" is represented in hexadecimal as 00.

```
00 - SESSION MESSAGE
```

```
1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| TYPE | FLAGS | LENGTH |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/ USER_DATA /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The NetBT session is established on TCP port 139 and the data transfer is done through the session messages. The connection is then closed after the data transfer. There may be one or more session messages during an active session based on the size of data.
5 File and Printer Sharing Operations

The file and printer sharing services are provided by the Server Message Block (SMB) protocol. This shall run on top of NetBT session or run directly over TCP. SMB fits well with the client-server topology, where client makes specific requests and the server responds accordingly.

5.1 Direct hosted SMB

Direct hosted SMB traffic uses port 445. This does not use NetBT. Here, a four-byte header precedes the SMB traffic. The first byte of this header is always 0x00, and the next three bytes are the length of the data.

This is useful in systems that do not support NetBT and in network where NetBT is not preferred.

If the Client has NetBT disabled, it will always try to connect to the server at port 445 only. If the server answers on port 445, the session shall be established and continued on that port. If it doesn’t answer, the session will fail completely. When the server has NetBT disabled, it shall listen on port 445 only and respond to requests to this port.

5.2 SMB over NetBT

If both the direct hosted and NetBT interfaces are enabled, both methods are tried at the same time and the first to respond is used. This allows interoperability with operating systems that do not support direct hosting of SMB traffic or NetBT.

5.2.1. NetBT Session Establishment

When the client and the remote machine have NetBT enabled, the Netbios Sessions are established by exchanging packets on TCP port 139. The node establishing the session attempts to make a TCP connection to port 139 on the remote node/server.

On establishing the TCP connection, the client then sends over this connection a "Session Request" packet with the NetBIOS names of the client to the NetBIOS name to remote machine/server. The remote node shall respond with a "Positive Session Response" indicating that a session can be established or a "Negative Session Response" indicating that no session can be established.

Multiple sessions, each identified with a unique Transaction id, may exist between any pair of calling and called names.
5.2.2 NetBT session Data Transfer

Data is transmitted during an established session by Session Message packets. NetBIOS keep-alives are used on each connection to verify that both the server and workstation are still able to maintain their session.

For file sharing or printer sharing services, the data transfer shall be through the SMB packets that are exchanged as NetBT session message packets.

5.2.3 SMB Data transfer on NetBT

On an established NetBT session, the client through SMB negotiates the SMB capabilities with the remote machine/server. This is done through SMB command "Negotiate protocol request" on NetBT session message which is responded by a "Negotiate protocol response". The negotiated SMB capabilities includes understanding long file names, extended attributes, and so on.

All the SMB command messages go on top of the NetBT session message on port 139. The flags field in the SMB header shall indicate the type of SMB command as request to the server or as response to the client or the redirector. SMB shall follow this with "Session setup and x request" command. The User and domain information of the connecting machine shall be recorded in the local system. The session setup request shall have the same process id (PID) as the Negotiate protocol request/response. This command is replied with a "session setup and x response" command for the same PID.

SMB "Tree connect and X request" command shall follow the session setup. The "Path" field of this command shall contain the path of the shared resource in the remote machine/server, the client is requesting access. The remote machine shall respond with a "Tree connect and X response" for a successful tree connection with a unique TreeID.

On establishing the tree connection, further network traffic shall be generated based on the operation performed including displaying directory, accessing data files, launching applications, etc. The subsequent transactions on this tree connection shall have matching TID, PID, UID information.

The SMB data transfer typically uses "Read and x request", "Read and x response", "Write and x request" and "Write and x response" commands. "No more data from sender" flag set in these commands shall indicate that there is no more data to follow.
The client machine sends a "close request" command and the server shall acknowledge with a "close response". This may be followed by a further set of transactions on the same tree.

The client may then request to close the tree connection with a "tree disconnect request". The remote machine/server releases the TID and responds with a "tree disconnect response".

5.2.4 NetBT Session Close The NetBT Sessions are closed by closing the TCP connection. When a user requests to close a session, the service first attempts a graceful close of the TCP connection. If the connection does not close within the SSN_CLOSE_TIMEOUT the TCP connection is aborted. No matter how the TCP connection is terminated, the NetBIOS session service always closes the NetBIOS session.
6 Security Considerations

Security considerations discussed in [Netbios concepts] and [Netbios specification] apply to this document.

7 IANA Considerations

This document does not require any IANA action.

8 References

8.1 Normative References


8.2 Informative References


Authors’ Addresses

Palanivelan Appanasamy
Principal Software Engineer,
Networking/WAN, EMC Corporation,
Bangalore-560048.
India.
EMail: Palanivelan.Appanasamy@emc.com