nbtscan(1) — nbtscan — Debian testing — Debian Manpages

By AUTHOR¶

Archived: 2026-04-05 15:58:35 UTC

Scroll to navigation

NAME¶

nbtscan - scan networks for NetBIOS name information

SYNOPSIS¶

```
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q]

        [-s separator] [-h] [-m retransmits] [-f filename | target]
```

DESCRIPTION¶

NBTscan is a program for scanning IP networks for NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address (such as Ethernet).

NBTscan produces a report like that:

```
    IP address      NetBIOS Name  Server    User          MAC address

    ------------------------------------------------------------------------

    192.168.1.2     MYCOMPUTER              JDOE          00-a0-c9-12-34-56

    192.168.1.5     WIN98COMP     <server>  RROE          00-a0-c9-78-90-00
```

```
192.168.1.123  DPTSERVER     <server>  ADMINISTRATOR  08-00-09-12-34-56
```

First column lists IP address of responded host. Second column is computer name. Third column indicates if this computer shares or is able to share files or printers. For NT machine it means that Server Service is running on this computer. For Windows 95 it means that "I want to be able to give others access to my files" or "I want to be able to allow others to print on my **printer**(s)" checkbox is ticked (in Control Panel/Network/File and Print Sharing). Most often it means that this computer shares files. Third column shows user name. If no one is logged on from this computer it is same as computer name. Last column shows adapter MAC address.

If run with **-v** switch NBTscan lists whole NetBIOS name table for each responded address. The output looks like that:

```
NetBIOS Name Table for Host 192.168.1.123:

Name             Service          Type

---------------------------------------

DPTSERVER        <00>             UNIQUE

DPTSERVER        <20>             UNIQUE

DEPARTMENT       <00>             GROUP

DEPARTMENT       <1c>             GROUP

DEPARTMENT       <1b>             UNIQUE

DEPARTMENT       <1e>             GROUP

DPTSERVER        <03>             UNIQUE

DEPARTMENT       <1d>             UNIQUE
```

```
    ??__MSBROWSE__?  <01>            GROUP

    INet~Services    <1c>            GROUP

    IS~DPTSERVER     <00>            UNIQUE

    DPTSERVER        <01>            UNIQUE

    Adapter address: 00-a0-c9-12-34-56

    ----------------------------------------
```

OPTIONS¶

A summary of options is included below.

-v

Verbose output. Print all names received from each host.

-d

Dump packets. Print whole packet contents. Cannot be used with **-v**, **-s** or **-h** options.

-e

Format output in /etc/hosts format.

-l

Format output in lmhosts format.

-t <*timeout*>

Wait *timeout* seconds for response. Default 1.

-b <*bandwidth*>

Output throttling. Slow down output so that it uses no more that *bandwidth* bps. Useful on slow links, so that outgoing queries don't get dropped.

-r

Use local port 137 for scans. Win95 boxes respond to this only. You need to be root to use this option.

-q

Suppress banners and error messages.

-s <*separator*>

Script-friendly output. Don't print column and record headers, separate fields with *separator*.

-h

Print human-readable names for services. Can only be used with **-v** option.

-m <*retransmits*>

Number of *retransmits*. Default 0.

-f <*filename*>

Take IP addresses to scan from file "*filename*"

target

NBTscan is a command-line tool. You have to supply at least one argument, the address range, in one of three forms:

xxx.xxx.xxx.xxx

Single IP in dotted-decimal notation. Example: 192.168.1.1

xxx.xxx.xxx.xxx/xx

Net address and subnet mask. Example: 192.168.1.0/24

xxx.xxx.xxx.xxx-xxx

Address range. Example: 192.168.1.1-127. This will scan all addresses from 192.168.1.1 to 192.168.1.127

EXAMPLES¶

Scans the whole C-class network:

```
nbtscan 192.168.1.0/24
```

Scans the whole C-class network, using port 137:

```
nbtscan -r 192.168.1.0/24
```

Scans a range from 192.168.1.25 to 192.168.1.137:

```
nbtscan 192.168.1.25-137
```

Scans C-class network. Prints results in script-friendly format using colon as field *separator*:

```
nbtscan -v -s : 192.168.1.0/24
```

The last command produces output like that:

```
192.168.0.1:NT_SERVER:00U

192.168.0.1:MY_DOMAIN:00G

192.168.0.1:ADMINISTRATOR:03U

192.168.0.2:OTHER_BOX:00U

...
```

Scans IP addresses specified in file iplist:

```
nbtscan -f iplist
```

NETBIOS SUFFIXES¶

NetBIOS Suffix, aka NetBIOS End Character (endchar), indicates service type for the registered name. The most known codes are listed below. (U = Unique Name, G = Group Name)

```
Name                Number(h)  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(MSMail Connector)

<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 Clients Remote Control

<computername>          44       U    SMS Administrators Remote Control Tool

<computername>          45       U    SMS Clients Remote Chat

<computername>          46       U    SMS Clients Remote Transfer

<computername>          87       U    Microsoft Exchange MTA

<computername>          6A       U    Microsoft Exchange IMC
```

```
    <computername>          BE       U    Network Monitor Agent

    <computername>          BF       U    Network Monitor Application

    <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    IIS

    <IS~computer name>      00       U    IIS
```

FAQ¶

1.

NBTscan lists my Windows boxes just fine but does not list my Unixes or routers. Why?

R: That is the way it is supposed to work. NBTscan uses NetBIOS for scanning and NetBIOS is only implemented by Windows (and some software on Unix such as Samba).

2.

Why do I get "Connection reset by peer" errors on Windows 2000?

R: NBTscan uses port 137 UDP for sending queries. If the port is closed on destination host destination will reply with ICMP "Port unreachable" message. Most operating system will ignore this message. Windows 2000 reports it to the application as "Connection reset by peer" error. Just ignore it.

3.

Why NBTscan doesn't scan for shares? Are you going to add share scanning to NBTscan?

R: No. NBTscan uses UDP for what it does. That makes it very fast. Share scanning requires TCP. For one thing, it will make **nbtscan** more slow. Also adding share scanning means adding a lot of new code to **nbtscan**. There is a lot of good share scanners around, so there is no reason to duplicate that work.

4.

Why do I get 00-00-00-00-00-00 instead of MAC address when I scan a Samba box?

R: Because that's what Samba send in response to the query. Nbtscan just prints out what it gets.

NBTscan was created by Alla Bezroutchko <alla@inetcat.org>. Currently is maintained by some volunteers at https://github.com/resurrecting-open-source-projects/**nbtscan**

This manual page was written for the first time by Ryszard Lach <rla@debian.org> and rewritten, from scratch, by Joao Eriberto Mota Filho <eriberto@debian.org> for the Debian GNU/Linux system (but may be used by others).
