

# Nslookup 命令使用说明

Nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令行工具。只有在已安装 TCP/IP 协议的情况下才可以使用 nslookup 命令行工具。

## 1 基本使用方法

### 1.1 语法

```
nslookup [-opt ...]
```

#使用默认 DNS 进入交互模式。

```
nslookup [-opt ...] - server
```

#使用指定 DNS 进入交互模式。

```
nslookup [-opt ...] host
```

#使用默认 DNS 查询 host。

```
nslookup [-opt ...] host server
```

#使用指定 DNS 查询 host。

### 1.2 参数

-opt ... : 将一个或多个 nslookup 子命令指定为命令行选项。

例:

```
C:\>nslookup www.baidu.com
```

```
Server: nameserver1.domain.com
```

```
Address: 10.0.0.1
```

```
Non-authoritative answer:
```

```
Name: www.baidu.com
```

```
Addresses: 61.135.169.125, 61.135.169.105
```

61.135.169.125, 61.135.169.105 是 www.baidu.com 对应的 IP 地址.

## 2 交互式模式:

要在交互模式下启动 Nslookup.exe, 只需在命令提示符下输入 nslookup:

```
C:\> nslookup
```

```
Default Server: nameserver1.domain.com
```

Address: 10.0.0.1

>

在命令提示符下输入 **help** 或 **?** 将生成可用的命令列表。在命令提示符下输入的任何内容，如果它不是有效命令，则假设它是主机名，尝试使用默认服务器来解析它。要中断交互命令，请按 **CTRL+C**。要退出交互模式并返回到命令提示符下，并在命令提示符下输入 **exit**。

以下是帮助输出，其中包含选项的完整列表：

Commands: (identifiers are shown in uppercase, [] means optional)

NAME - print info about the host/domain NAME using default server

NAME1 NAME2 - as above, but use NAME2 as server

help or ? - print info on common commands

set OPTION - set an option

all - print options, current server and host

[no]debug - print debugging information

[no]d2 - print exhaustive debugging information

[no]defname - append domain name to each query

[no]recurse - ask for recursive answer to query

[no]search - use domain search list

[no]vc - always use a virtual circuit

domain=NAME - set default domain name to NAME

srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1, N2, etc.

root=NAME - set root server to NAME

retry=X - set number of retries to X

timeout=X - set initial time-out interval to X seconds

type=X - set query type (for example, A, ANY, CNAME, MX, NS, PTR, SOA, SRV)

querytype=X - same as type

class=X - set query class (for example, IN (Internet), ANY)

[no]msxfr - use MS fast zone transfer

ixfrver=X - current version to use in IXFR transfer request

server NAME - set default server to NAME, using current default server

lserver NAME - set default server to NAME, using initial server

finger [USER] - finger the optional NAME at the current default host

root - set current default server to the root

ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)

-a - list canonical names and aliases

-d - list all records

-t TYPE - list records of the given type (for example, A, CNAME, MX, NS, PTR, etc.)

view FILE - sort an 'ls' output file and view it with pg

exit - exit the program

通过在命令提示符下运行 set 命令，可以在 Nslookup.exe 中设置许多不同的选项。要得到这些选项的完整列表，只需输入 set all。请参见以上内容，在 set 命令下，得到可用选项的打印输出

查找不同的数据类型：

要在域名空间中查找不同的数据类型，请在命令提示符下使用 set type 或 set q[querytype] 命令。

例如，要查询邮件交换器数据，请输入：

```
C:\> nslookup
```

```
Default Server: ns1.domain.com
```

```
Address: 10.0.0.1
```

```
> set q=mx
```

```
> mailhost
```

```
Server: ns1.domain.com
```

```
Address: 10.0.0.1
```

```
mailhost.domain.com MX preference = 0, mail exchanger =  
mailhost.domain.com
```

```
mailhost.domain.com internet address = 10.0.0.5
```

```
>
```

第一次查询是查找远程名称，答案是权威的，但随后的查询是非权威的。第一次查询远程主机时，本地 DNS 服务器与作为该域权威的 DNS 服务器取得联系。然后，本地 DNS 服务器缓存该信息，以便从本地服务器缓存中非权威地回答随后的查询。

直接从另一个名称服务器中进行查询：

要直接查询另一个名称服务器，请使用 server 或 lserver 命令切换到该名称服务器。lserver 命令使用本地服务器得到要切换的服务器地址，而 server 命令使用当前默认服务器得到该地址。

例如：

```
C:\> nslookup
Default Server: nameserver1.domain.com
Address: 10.0.0.1
> server 10.0.0.2
Default Server: nameserver2.domain.com
Address: 10.0.0.2
>
```

使用 Nslookup.exe 转移整个区域：

使用 ls 命令，Nslookup 可以用于转移整个区域。查看远程域中的所有主机，这是有用的。ls 命令的语法如下：

```
ls [-a | d | t type] domain [> filename]
```

不带参数使用 ls 命令将返回所有地址和名称服务器数据的列表。-a 参数将返回别名和正式名称，-d 将返回所有数据，而 -t 将按类型进行筛选。

例如：

```
>ls domain.com
[nameserver1.domain.com]
nameserver1.domain.com. NS server = ns1.domain.com
nameserver2.domain.com NS server = ns2.domain.com
nameserver1 A 10.0.0.1
nameserver2 A 10.0.0.2
>
```

在 DNS 服务器中可以按块转移区域，以便只有授权的地址和网络才可以执行此操作。如果设置了区域安全，将返回以下错误消息：

```
*** Can't list domain example.com .: Query refused
```

## 3 Nslookup.exe 的疑难解答

### 3.1 默认服务器超时

当启动 Nslookup.exe 工具时，以下错误可能出现：

```
*** Can't find server name for address w.x.y.z : Timed out
```

备注： w.x.y.z 是在“DNS 服务搜索顺序”列表中列出的第一个 DNS 服

务器。

\*\*\* Can't find server name for address 127.0.0.1: Timed out

第一个错误指出不能连接 DNS 服务器，或者该计算机上的服务没有运行。要解决此问题，启动该服务器上的 DNS 服务，或检查可能存在的连接问题。

第二个错误指出在“DNS 服务搜索顺序”列表中还没有定义服务器。要解决此问题，请将有效 DNS 服务器的 IP 地址添加到此列表中。

### 3.2 启动 Nslookup.exe 时找不到服务器名

启动 Nslookup.exe 工具时，可能出现以下错误：

\*\*\* Can't find server name for address w.x.y.z: Non-existent domain

当没有域名服务器 IP 地址的 PTR 记录时，会出现此错误。当 Nslookup.exe 启动时，它执行反向搜索，以得到默认服务器的名称。如果没有 PTR 数据，则返回此错误消息。要解决此问题，请确保反向搜索区域存在，并包含名称服务器的 PTR 记录。

### 3.3 Nslookup 在子域上无法执行

当在子域上执行查询或进行区域转移时，Nslookup 可能返回以下错误：

\*\*\* ns.domain.com can't find child.domain.com.: Non-existent domain

\*\*\* Can't list domain child.domain.com.: Non-existent domain

在 DNS Manager 中，可以在主区域下添加一个新域，这样就创建了一个子域。用这种方法创建子域并不为该域创建一个单独的 db 文件，这样在该域进行查询或在该域进行区域转移时将会产生以上错误。在父域上进行区域转移时将同时列出父域数据和子域数据。要解决此问题，请在 DNS 服务器上为该子域创建一个新主域。

## 4 附录：常用的域名服务器

1. 阿里云 DNS: 223.5.5.5，备用 223.6.6.6
2. 比较权威的老牌 DNS: 114.114.114.114
3. 谷歌老大哥的全球解析 DNS 服务器: 8.8.8.8
4. 腾讯公共 DNS: 119.29.29.29
5. 百度公共 DNS: 180.76.76.76