

How to Use Ping and Ipconfig to Test DNS

Objective

Ping is a very basic utility to troubleshoot DNS. It is only able to lookup A and PTR records. Nslookup and digger should be used for any advanced DNS query. On the other hand most users are very familiar and comfortable with the utility and, therefore, it is extremely easy to learn. Ping is also widely available in all operating systems.

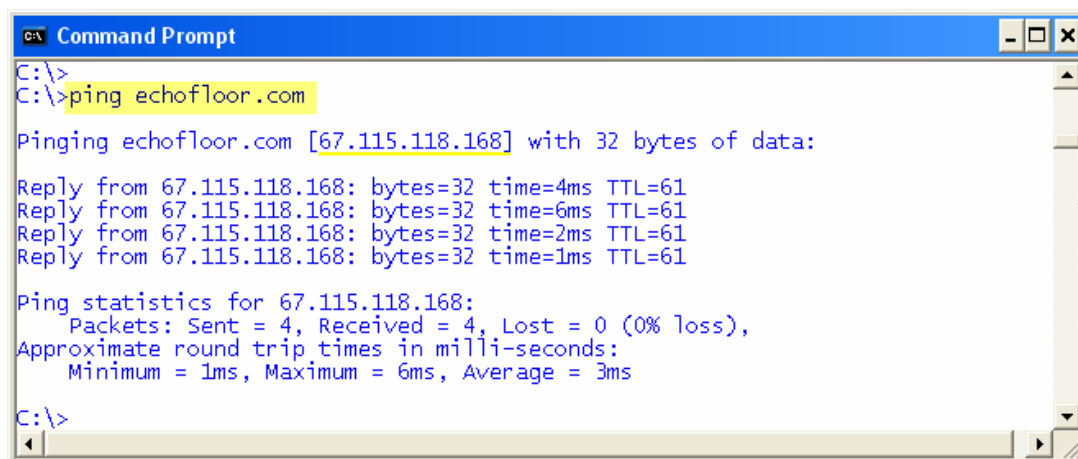
Table of Contents

PING: A RECORD LOOK-UP	2
PING: PTR RECORD (REVERSE DNS) LOOK-UP	3
IPCONFIG: DNS CACHE DISPLAY	5
IPCONFIG: DNS FLUSHING	6
IPCONFIG: DNS REGISTER	7
ADDITIONAL RESOURCES	7

Ping: A Record Look-Up

A records map names to IP addresses. This is the default behavior when using ping.

```
Ping echofloor.com
```



```
C:\>
C:\>ping echofloor.com

Pinging echofloor.com [67.115.118.168] with 32 bytes of data:

Reply from 67.115.118.168: bytes=32 time=4ms TTL=61
Reply from 67.115.118.168: bytes=32 time=6ms TTL=61
Reply from 67.115.118.168: bytes=32 time=2ms TTL=61
Reply from 67.115.118.168: bytes=32 time=1ms TTL=61

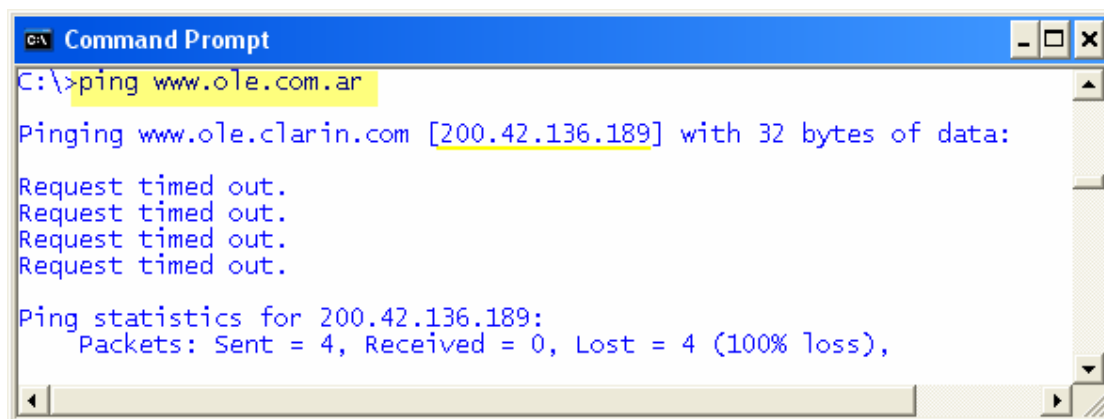
Ping statistics for 67.115.118.168:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 3ms

C:\>
```

In this example the ping utility performs two tasks. It first performs a DNS query to lookup the IP address corresponding to echofloor.com. Then, it then pings successfully the resolved 67.115.118.168 IP address.

It is also possible to resolve a name address into an IP address successfully but then fail the ping connectivity test.

```
ping www.ole.com.ar
```



```
C:\>ping www.ole.com.ar

Pinging www.ole.clarin.com [200.42.136.189] with 32 bytes of data:

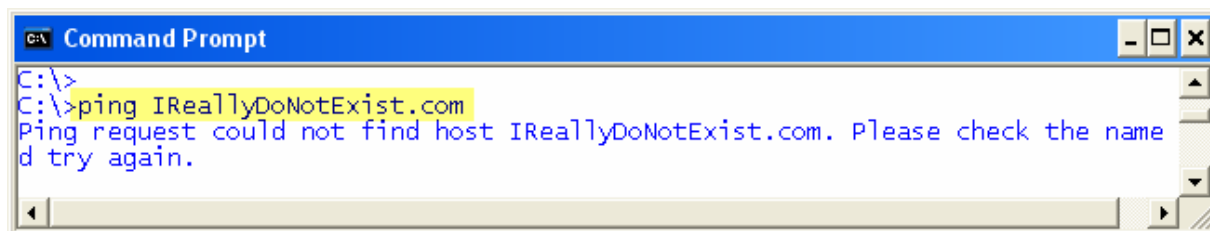
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.42.136.189:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Finally the A Record look-up may fail all together.

```
ping IReallyDoNotExist.com
```



```
C:\>
C:\>ping IReallyDoNotExist.com
Ping request could not find host IReallyDoNotExist.com. Please check the name
d try again.

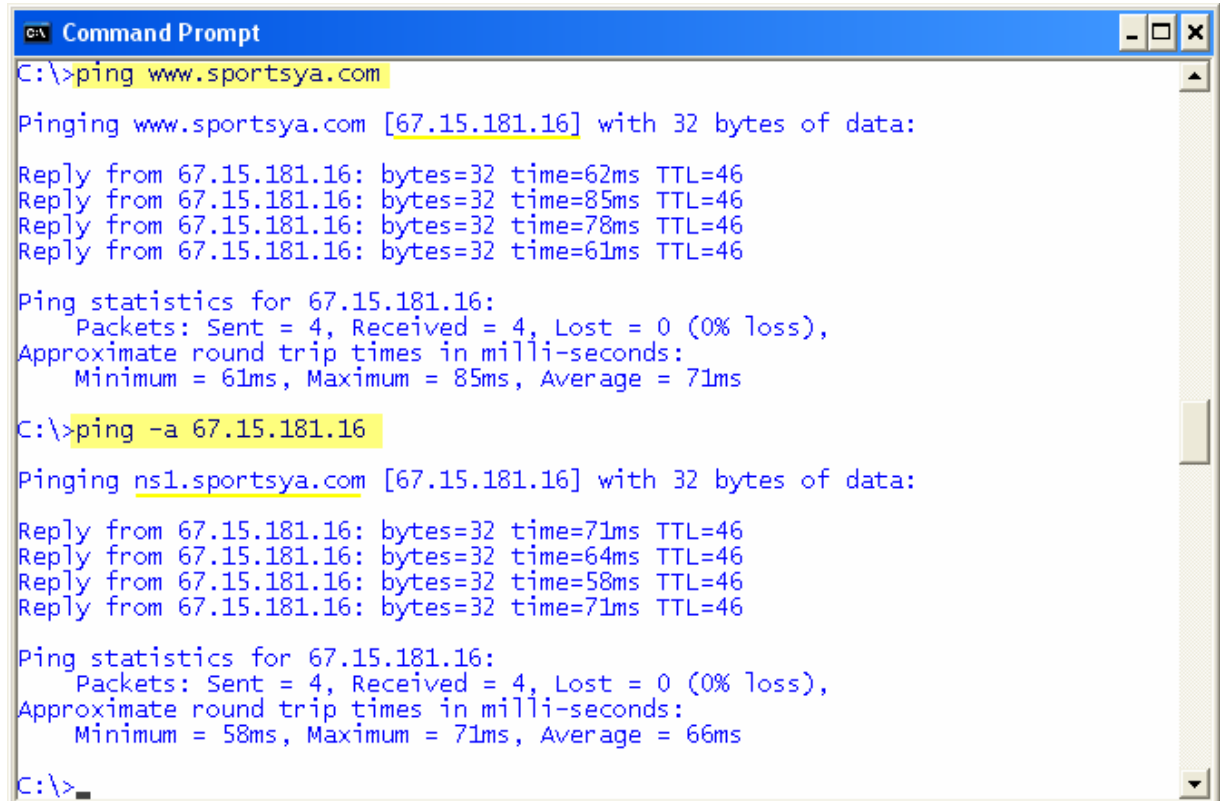
C:\>
```

Ping: PTR Record (Reverse DNS) Look-Up

PTR records resolve an IP address to a name address. This process is also known as reverse DNS lookup. This can be done with ping by using the `-a` flag.

```
ping -a 67.15.181.16
```

Sportsya.com domain resolves to 67.15.181.16. A reverse DNS lookup of this IP address resolves to ns1.sportsya.com name. IP addresses and domain names do not have a one-to-one relationship. Many names can be mapped to the same IP address whereas only one name can be reverse resolved from a given IP address.



```
C:\>ping www.sportsya.com

Pinging www.sportsya.com [67.15.181.16] with 32 bytes of data:

Reply from 67.15.181.16: bytes=32 time=62ms TTL=46
Reply from 67.15.181.16: bytes=32 time=85ms TTL=46
Reply from 67.15.181.16: bytes=32 time=78ms TTL=46
Reply from 67.15.181.16: bytes=32 time=61ms TTL=46

Ping statistics for 67.15.181.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 61ms, Maximum = 85ms, Average = 71ms

C:\>ping -a 67.15.181.16

Pinging ns1.sportsya.com [67.15.181.16] with 32 bytes of data:

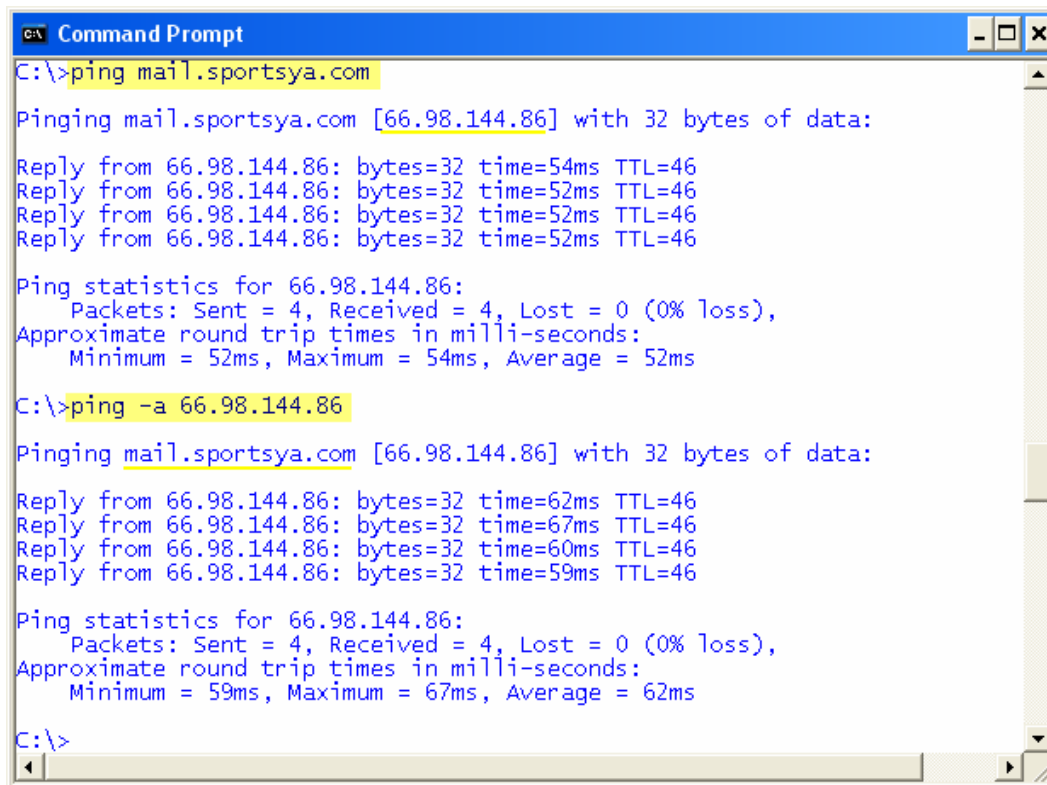
Reply from 67.15.181.16: bytes=32 time=71ms TTL=46
Reply from 67.15.181.16: bytes=32 time=64ms TTL=46
Reply from 67.15.181.16: bytes=32 time=58ms TTL=46
Reply from 67.15.181.16: bytes=32 time=71ms TTL=46

Ping statistics for 67.15.181.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 58ms, Maximum = 71ms, Average = 66ms

C:\>
```

The MX record for sportsya.com is mail.sportsya.com which resolves to 66.98.144.86. The reverse DNS of this IP address resolves back to mail.sportsya.com. The reverse PTR record matching the forward lookup may be important to ensure mail delivery.

Companies such as AOL perform a reverse DNS on the IP address of the connecting SMTP server and compared the resolved name to the announced domain name at connection (in the EHLO/HELO command). If these do not match, the connection is dropped.



```
C:\>ping mail.sportsya.com

Pinging mail.sportsya.com [66.98.144.86] with 32 bytes of data:

Reply from 66.98.144.86: bytes=32 time=54ms TTL=46
Reply from 66.98.144.86: bytes=32 time=52ms TTL=46
Reply from 66.98.144.86: bytes=32 time=52ms TTL=46
Reply from 66.98.144.86: bytes=32 time=52ms TTL=46

Ping statistics for 66.98.144.86:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 52ms, Maximum = 54ms, Average = 52ms

C:\>ping -a 66.98.144.86

Pinging mail.sportsya.com [66.98.144.86] with 32 bytes of data:

Reply from 66.98.144.86: bytes=32 time=62ms TTL=46
Reply from 66.98.144.86: bytes=32 time=67ms TTL=46
Reply from 66.98.144.86: bytes=32 time=60ms TTL=46
Reply from 66.98.144.86: bytes=32 time=59ms TTL=46

Ping statistics for 66.98.144.86:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 59ms, Maximum = 67ms, Average = 62ms

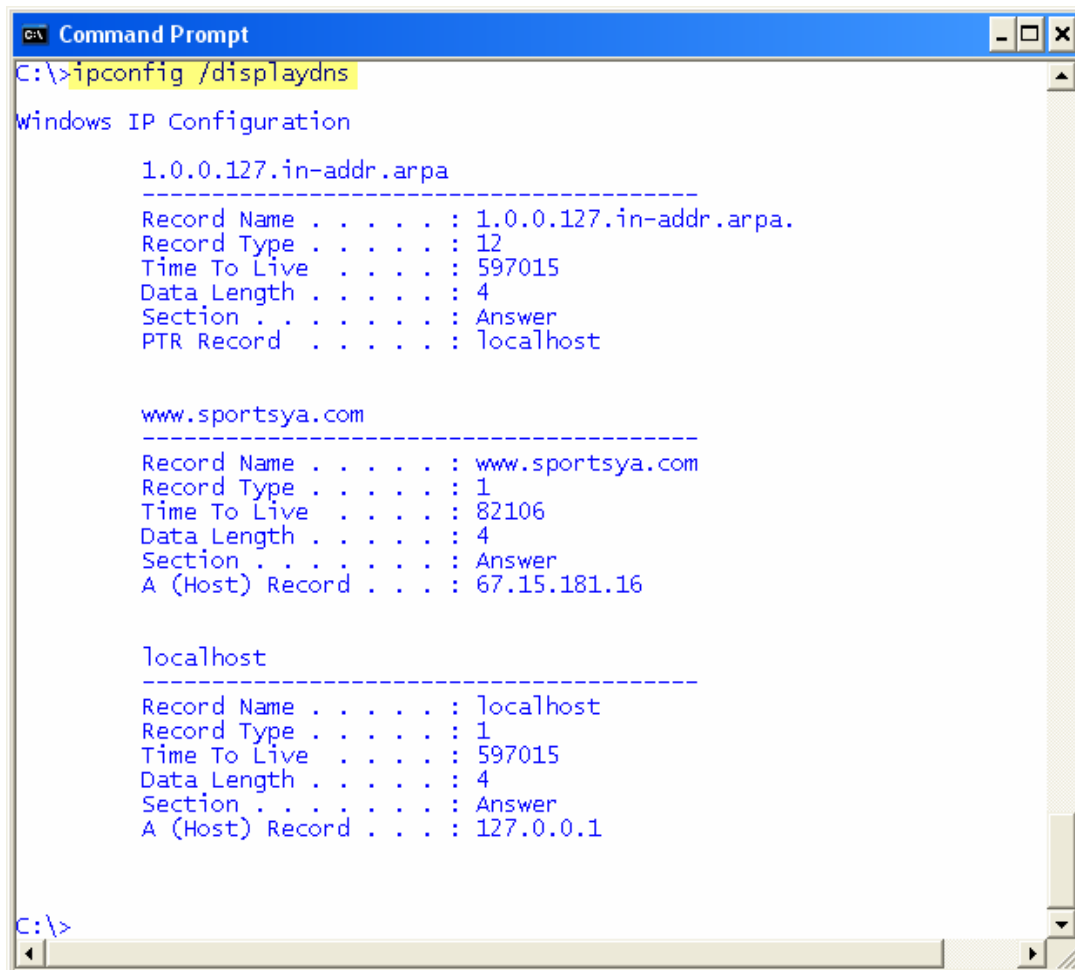
C:\>
```

Ipconfig: DNS Cache Display

Windows will cache DNS information as it is looked up. This process is done to speed up repeated identical queries. DNS responses from a DNS server include a "Time to Live" in seconds that is used to age out the entry from the DNS cache.

The `ipconfig /displaydns` command displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

The result here shows three DNS entries. The `www.sportsya.com` entry shows an IP address of `67.15.181.16`. The time to live is `82,106` or 22 hours.



```
Command Prompt
C:\>ipconfig /displaydns

Windows IP Configuration

1.0.0.127.in-addr.arpa
-----
Record Name . . . . . : 1.0.0.127.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 597015
Data Length . . . . . : 4
Section . . . . . : Answer
PTR Record . . . . . : localhost

www.sportsya.com
-----
Record Name . . . . . : www.sportsya.com
Record Type . . . . . : 1
Time To Live . . . . . : 82106
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 67.15.181.16

localhost
-----
Record Name . . . . . : localhost
Record Type . . . . . : 1
Time To Live . . . . . : 597015
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 127.0.0.1

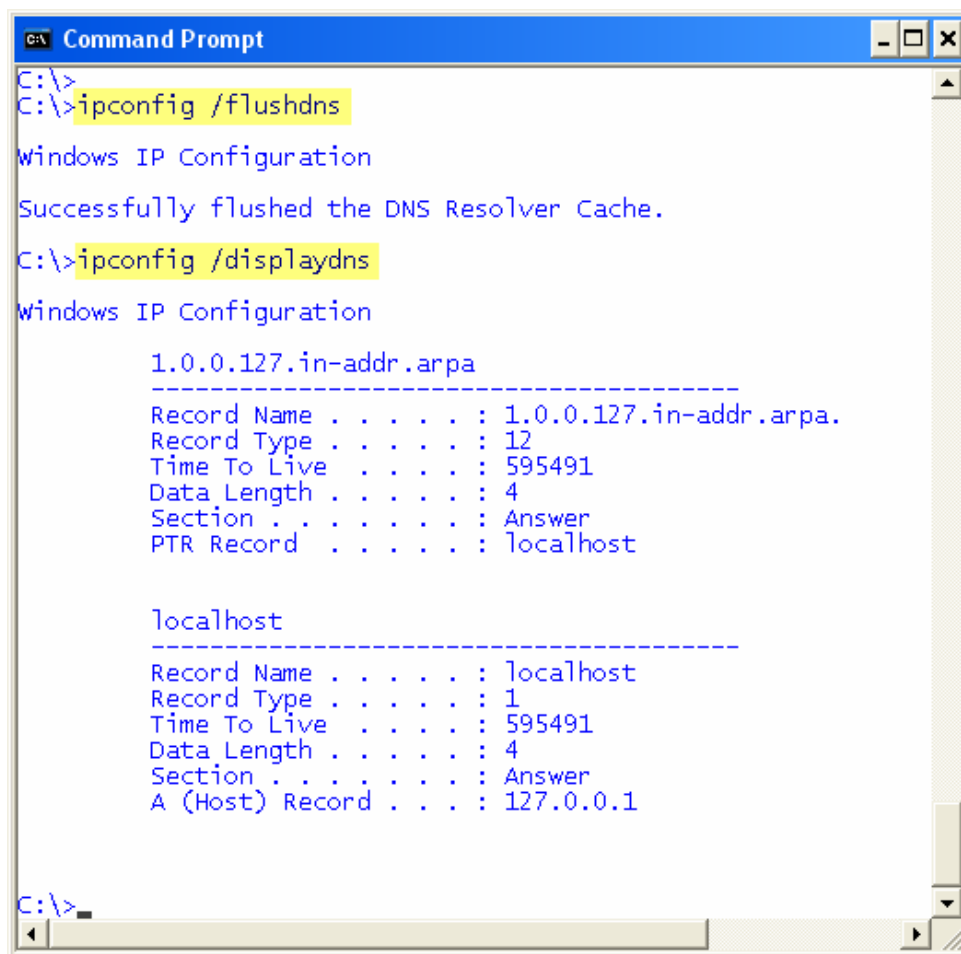
C:\>
```

Ipconfig: DNS Flushing

Entries in the dns cache can be manually flushed using ipconfig. The “ipconfig /flushdns” command flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically. Flushing may also be necessary when DNS entries have been updated but the PC still holds the old DNS information in its cache.

The DNS flush is run successfully in the example below. Note that localhost entry always populates the DNS cache.

```
Ipconfig /flushdns
```



```
C:\> ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\> ipconfig /displaydns
Windows IP Configuration

    1.0.0.127.in-addr.arpa
    -----
    Record Name . . . . . : 1.0.0.127.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live . . . . . : 595491
    Data Length . . . . . : 4
    Section . . . . . : Answer
    PTR Record . . . . . : localhost

    localhost
    -----
    Record Name . . . . . : localhost
    Record Type . . . . . : 1
    Time To Live . . . . . : 595491
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 127.0.0.1

C:\>
```

Ipconfig: DNS Register

The `ipconfig /registerdns` command instructs the network host to register its hostname and IP dynamically to the local DNS servers. Command initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

Note that this features mainly works with the Windows DNS Server.

For more information on renewing DNS client registration using the `ipconfig` command, see the following article: <http://technet2.microsoft.com/WindowsServer/en/library/792cc8f3-15f2-4f87-b83a-3a12d12c6b5b1033.mspx?mfr=true>

Additional Resources

More information can be found at the following Microsoft web pages.

- **Ping**
 - <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ping.mspx?mfr=true>
- **Ipconfig**
 - <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ipconfig.mspx?mfr=true>
- **Ipconfig /diplaydns**
 - <http://technet2.microsoft.com/WindowsServer/en/library/7356d145-e8ee-4dae-9edb-8b08a37e53841033.mspx?mfr=true>
- **Ipconfig /flushdns**
 - <http://207.46.196.114/WindowsServer/en/library/a184e334-2c9f-48c4-abe7-804188200dd91033.mspx?mfr=true>
- **ipconfig /registerdns**
 - <http://technet2.microsoft.com/WindowsServer/en/library/792cc8f3-15f2-4f87-b83a-3a12d12c6b5b1033.mspx?mfr=true>

Contacting SonicWALL Sales

- Toll free US: +1 888.557.6642
- Local US: +1 408.745.9600
- Local Fax US: +1 408.745.9300
- If you wish to be contacted, use this form: http://www.sonicwall.com/us/How_to_Buy.html

Created: 04/01/07

Updated: 05/08/07

Created by: Jean-Marc Catalaa

Version 2.0