

Check and Troubleshoot DNS

Here are a collection of Windows Command Prompt commands for working with an troubleshooting DNS

ipconfig /displaydns

```
ipconfig /displaydns
```

```
C:\Windows\system32>ipconfig /displaydns
```

```
Windows IP Configuration
```

```
www.cisco.com
```

```
-----  
Record Name . . . . . : www.cisco.com  
Record Type . . . . . : 5  
Time To Live . . . . . : 9  
Data Length . . . . . : 8  
Section . . . . . : Answer  
CNAME Record . . . . . : www.cisco.com.akadns.net
```

```
Record Name . . . . . : www.cisco.com.akadns.net  
Record Type . . . . . : 5  
Time To Live . . . . . : 9  
Data Length . . . . . : 8  
Section . . . . . : Answer  
CNAME Record . . . . . : wwwds.cisco.com.edgekey.net
```

```
Record Name . . . . . : wwwds.cisco.com.edgekey.net  
Record Type . . . . . : 5  
Time To Live . . . . . : 9  
Data Length . . . . . : 8  
Section . . . . . : Answer  
CNAME Record . . . . . : wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

```
Record Name . . . . . : wwwds.cisco.com.edgekey.net.globalredir.akadns.net  
Record Type . . . . . : 5  
Time To Live . . . . . : 9  
Data Length . . . . . : 8  
Section . . . . . : Answer  
CNAME Record . . . . . : e2867.dsca.akamaiedge.net
```

```
Record Name . . . . . : e2867.dsca.akamaiedge.net  
Record Type . . . . . : 1  
Time To Live . . . . . : 9  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . . : 23.7.24.10
```

Output of DNS Cache Explained

Output	Description
Record Name	This is the name that was queried for and resolved via a DNS request

Record Type	<p>1 = A record for IPv4 5 = CNAME record 15 = MX record 16 = Text record 28 = AAAA record for IPV6 12 = PTR (pointer) record</p> <p>These are just a few of the DNS resource types with their associated numbers. For more check this Wikipedia article.</p>
Time to Live	The time in seconds after which the cached DNS entry will expire.
Data Length	The data length refers to the size of the data stored in the cache for a particular domain name. This data can include information such as the IP address associated with the domain name, the time to live (TTL) for the record, and other details about the DNS query. The data length is typically measured in bytes, and is used by the DNS resolver to determine how much space to allocate for the record in its cache.
Section	This is a header designating the 'Answer', which is what follows as the A (Host) Record
A (Host) Record	This is the corresponding resolved IPv4 address for the domain name.

Adding the pipe with clip to the command copies the output to the clipboard and you can copy that into a text editor to make it easier to search and filter the results.

```
ipconfig /displaydns | clip
```

Windows IP Configuration

www.google.com

Record Name : www.google.com

Record Type : 1

Time To Live : 172

Data Length : 4

Section : Answer

A (Host) Record . . . : 142.250.72.68

www.cnn.com

Record Name : www.cnn.com

Record Type : 5

Time To Live : 5

ipconfig /flushdns

```
ipconfig /flushdns
```

This command clears the DNS cache

```
C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>ipconfig /displaydns

Windows IP Configuration

C:\Windows\system32>_
```

nslookup <domain name>

```
nslookup <domain name>
```

```
C:\Windows\system32>nslookup www.google.com
Server: UnKnown
Address: 192.168.2.10

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:400f:807::2004
          142.250.69.228
```

You can add the DNS server you want to query to the end of the command.

```
nslookup <domain name> <dns server IP>
```

```
C:\Windows\system32>nslookup www.google.com 1.1.1.1
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:400f:802::2004
          142.250.69.228
```

```
C:\Windows\system32>nslookup www.google.com 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:400f:803::2004
          142.250.69.228
```

If there are specific DNS records like mail, text, or pointer records you can add type to the query.

```
nslookup -type=mx <domain name>
```

```
C:\Windows\system32>nslookup -type=mx google.com
Server: UnKnown
Address: 192.168.2.10

Non-authoritative answer:
google.com      MX preference = 10, mail exchanger = smtp.google.com
```

```
nslookup -type=txt <domain name>
```

```
C:\Windows\system32>nslookup -type=txt google.com
Server: UnKnown
Address: 192.168.2.10

Non-authoritative answer:
google.com      text =

        "apple-domain-verification=30afIBcvSuDV2PLX"
google.com      text =

        "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cp0JM0nikft0jAgjmsQ"
google.com      text =

        "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com      text =

        "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59Bsh31KzUr6c1l2BPvqKX8="
google.com      text =

        "v=spf1 include:_spf.google.com ~all"
google.com      text =
```

```
nslookup -type=ptr <domain name>
```

```
C:\Windows\system32>nslookup -type=ptr google.com
Server: UnKnown
Address: 192.168.2.10

google.com
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial = 504224200
    refresh = 900 (15 mins)
    retry = 900 (15 mins)
    expire = 1800 (30 mins)
    default TTL = 60 (1 min)
```

Revision #1

Created 17 November 2022 14:17:12 by Glen Taylor

Updated 25 January 2023 17:35:26 by Glen Taylor