DNS (Domain Name System)

What is DNS?

DNS translates a hostname to IP address. This is an application layer protocol. Whenever we search for a hostname the DNS comes into play. It acts like a dictionary that translates every hostname to the corresponding IP address.

Working:

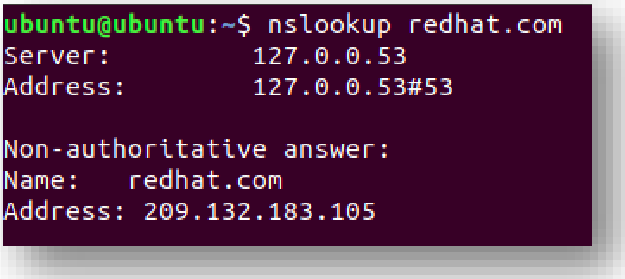
DNS is a distributed system all over the world. Our browser maintains a local DNS cache. They maintain all the hostnames to IP address translations of all the hostnames we browsed earlier. This improves performance, instead of resolving the hostname from outside DNS (which takes time) it can look into its cache and retrieve it faster.

If the searched hostname is not present in the local cache our browser sends the request for the local DNS server. If the local DNS has the IP address for the given hostname it sends the IP address otherwise it sends the request for the next level DNS server. This process goes on until the name is resolved and the name is then cached in the intermediate DNS servers.
The queries in DNS are processed in a recursive fashion. DNS has a recursive resolver that resolves the domain name recursively.

There are various kinds of domains.
Generic domain: .com(commercial), .edu(educational), .org(non-profit organization) and so on.
Country domain: .in(India) , .us, .uk
Inverse Domain: This is IP to domain name mapping.

nslookup:

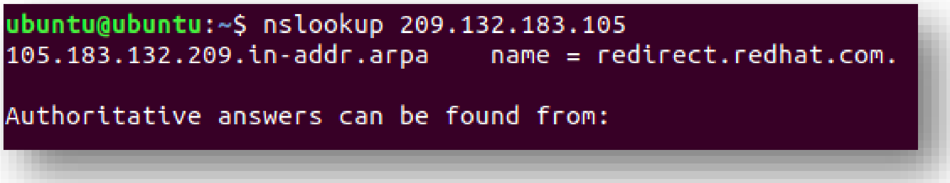
We can use the tool nslookup to get the information from the DNS server.
To get the address of any domain name we can type “nslookup <Domain name>” in the terminal.
To get the address for the redhat.com website we can type “nslookup redhat.com”



```
ubuntu@ubuntu:~$ nslookup redhat.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   redhat.com
Address: 209.132.183.105
```

Similarly to get the domain name from an address we can type “nslookup <IP address>”. If we type “nslookup 209.132.183.105” it will provide the domain name (i.e., redhat.com).

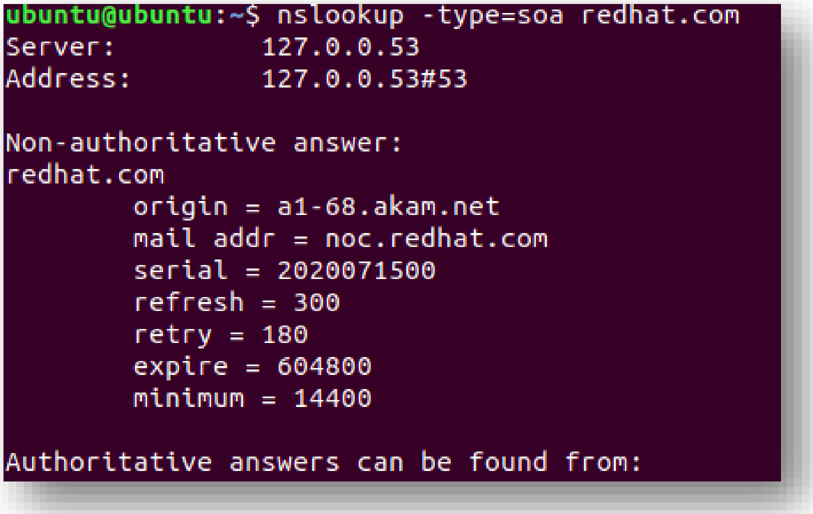


```
ubuntu@ubuntu:~$ nslookup 209.132.183.105
105.183.132.209.in-addr.arpa    name = redirect.redhat.com.

Authoritative answers can be found from:
```

There are a few options available in the nslookup command and the format of the command is “nslookup -type=<option> <domain name>”.

One of the options is “soa” (start of authority). This option provides authoritative information about the domain.

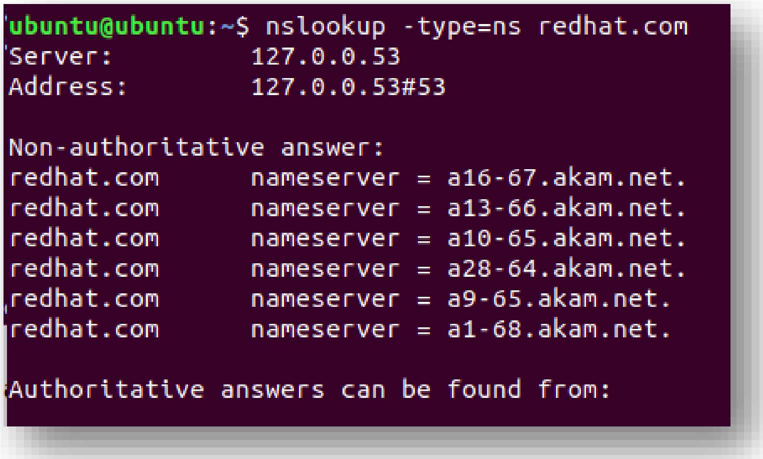


```
ubuntu@ubuntu:~$ nslookup -type=soa redhat.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
redhat.com
        origin = a1-68.akam.net
        mail addr = noc.redhat.com
        serial = 2020071500
        refresh = 300
        retry = 180
        expire = 604800
        minimum = 14400

Authoritative answers can be found from:
```

ns (Name Server): This option provides name servers that are associated with the domain.

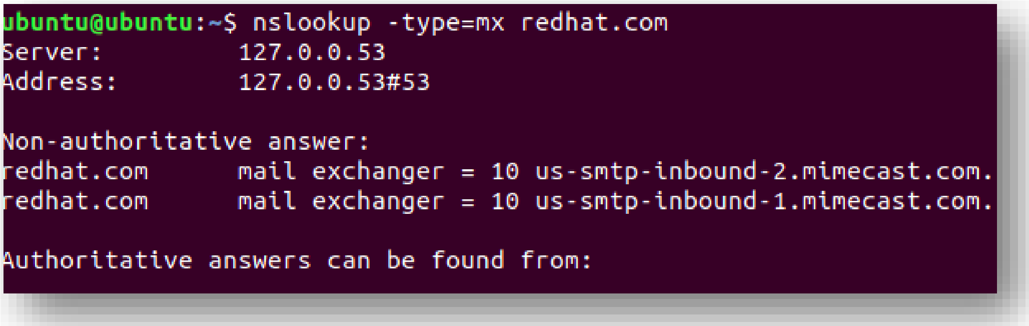


```
ubuntu@ubuntu:~$ nslookup -type=ns redhat.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
redhat.com      nameserver = a16-67.akam.net.
redhat.com      nameserver = a13-66.akam.net.
redhat.com      nameserver = a10-65.akam.net.
redhat.com      nameserver = a28-64.akam.net.
redhat.com      nameserver = a9-65.akam.net.
redhat.com      nameserver = a1-68.akam.net.

Authoritative answers can be found from:
```

mx (mail exchange): This option shows all mail exchange servers associated with the domain.

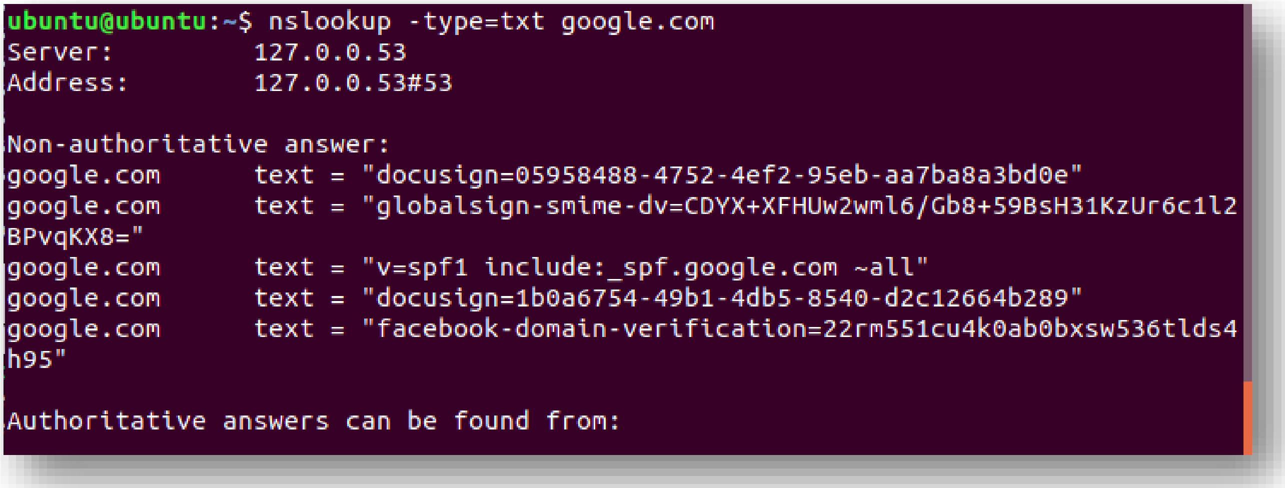


```
ubuntu@ubuntu:~$ nslookup -type=mx redhat.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
redhat.com      mail exchanger = 10 us-smtp-inbound-2.mimecast.com.
redhat.com      mail exchanger = 10 us-smtp-inbound-1.mimecast.com.

Authoritative answers can be found from:
```

txt: This shows all the text records configured for the specific domain.



```
ubuntu@ubuntu:~$ nslookup -type=txt google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      text = "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com      text = "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2
BPvqKX8="
google.com      text = "v=spf1 include:_spf.google.com ~all"
google.com      text = "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com      text = "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4
h95"

Authoritative answers can be found from:
```