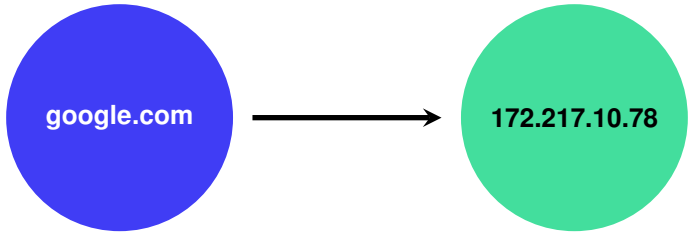
Domain Name System

Name resolution in a network

Richard Berger, 2021

Name resolution

Resolving a fully qualified domain name (FQDN) to its IP address



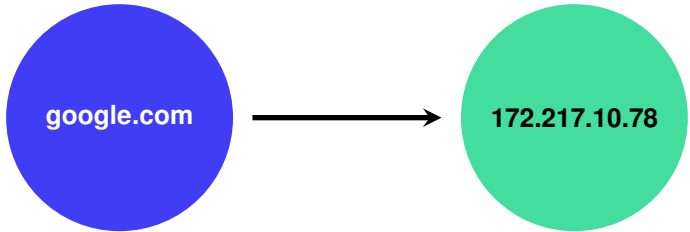
DNS: The Internet's Phonebook

Fully Qualified Domain Name (FQDN)	IPv4 Address
apple.com	17.253.144.10
amazon.com	176.32.103.205
google.com	142.250.64.78
microsoft.com	40.112.72.205

- networks use **Domain Name System (DNS) servers** to perform lookups
- a widely used DNS server implementation is BIND (Berkeley Internet Name Domain), also known as *named* (short for Name Daemon).
- UDP/TCP port 53

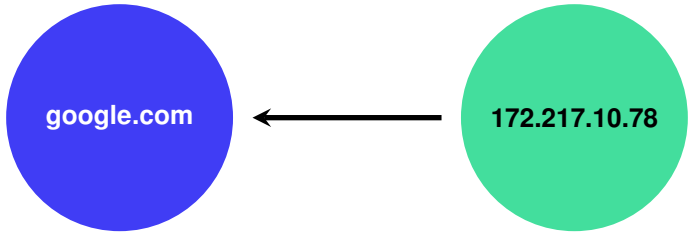
Forward Lookup

Resolving a fully qualified domain name (FQDN) to its IP address



Reverse Lookup

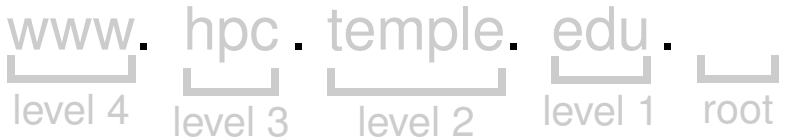
Finding the fully qualified domain name (FQDN) of an IP address



Fully Qualified Domain Name (FQDN)

www.hpc.temple.edu

Fully Qualified Domain Name (FQDN)

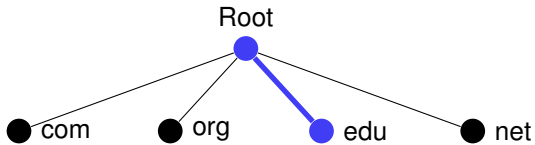


Fully Qualified Domain Name (FQDN)

www.hpc.temple.edu.

Fully Qualified Domain Name (FQDN)

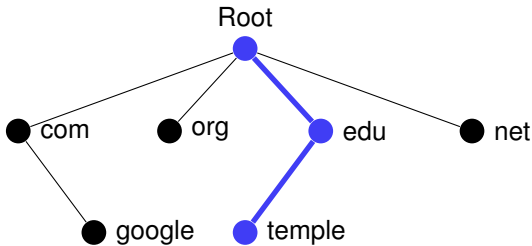
www.hpc.temple.edu.



Top-Level Domains

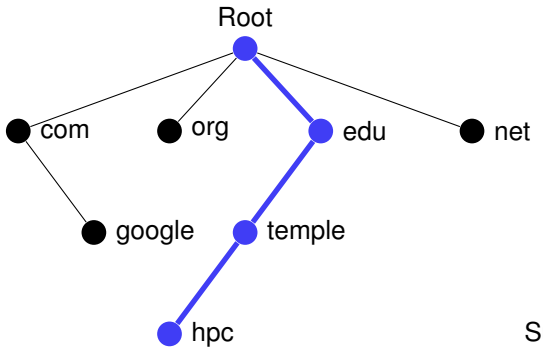
Fully Qualified Domain Name (FQDN)

www.hpc.temple.edu.



Fully Qualified Domain Name (FQDN)

www.hpc.temple.edu.



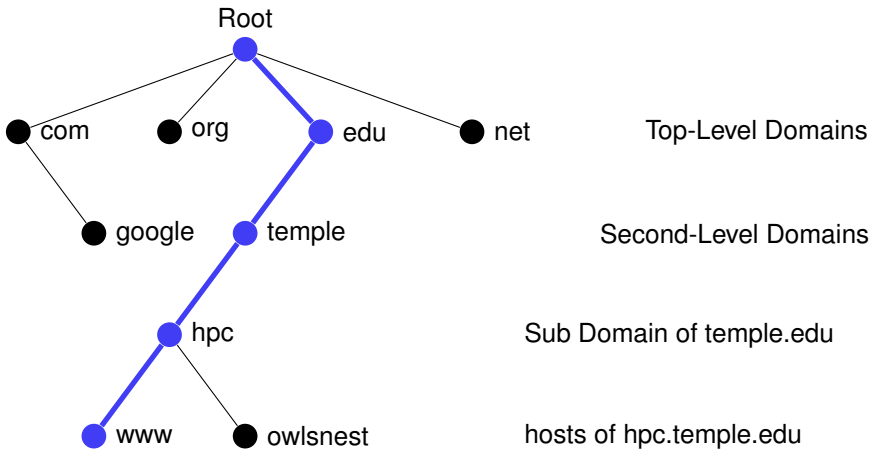
Top-Level Domains

Second-Level Domains

Sub Domain of temple.edu

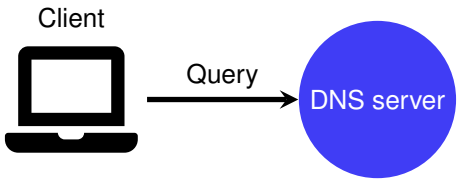
Fully Qualified Domain Name (FQDN)

www.hpc.temple.edu.

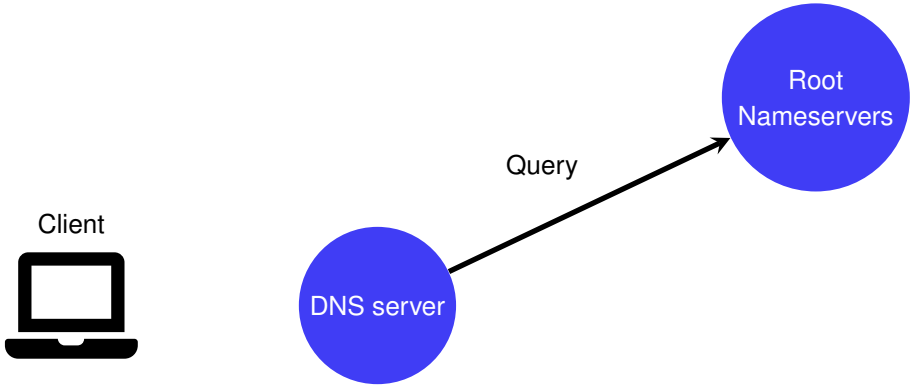


How a DNS query works: `www.google.com.`

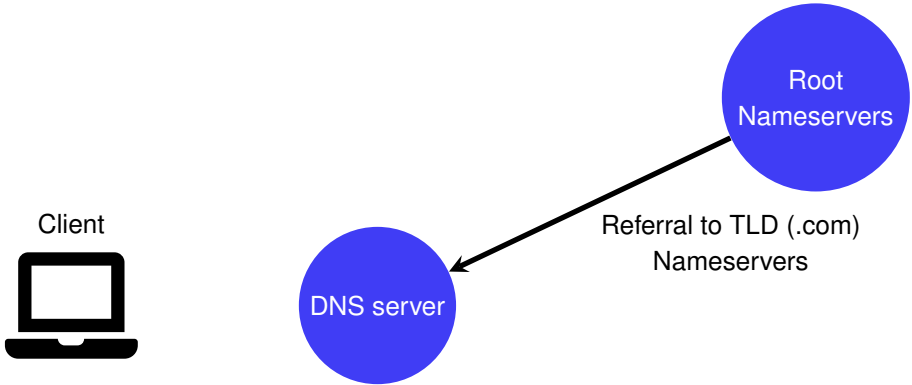
How a DNS query works: `www.google.com.`



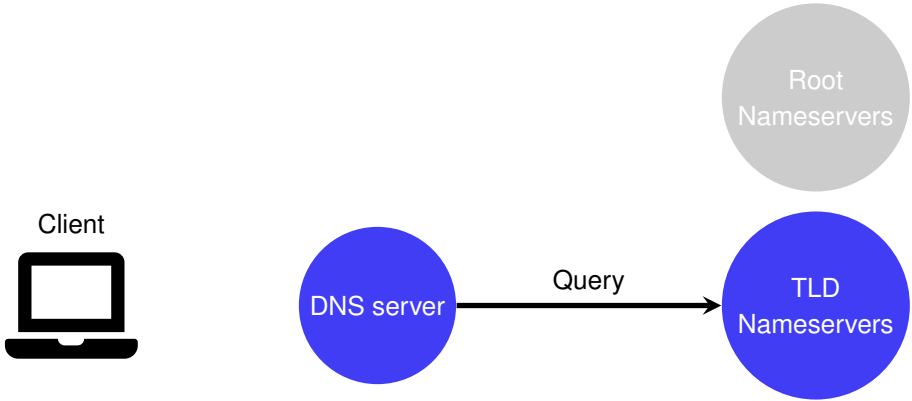
How a DNS query works: `www.google.com.`



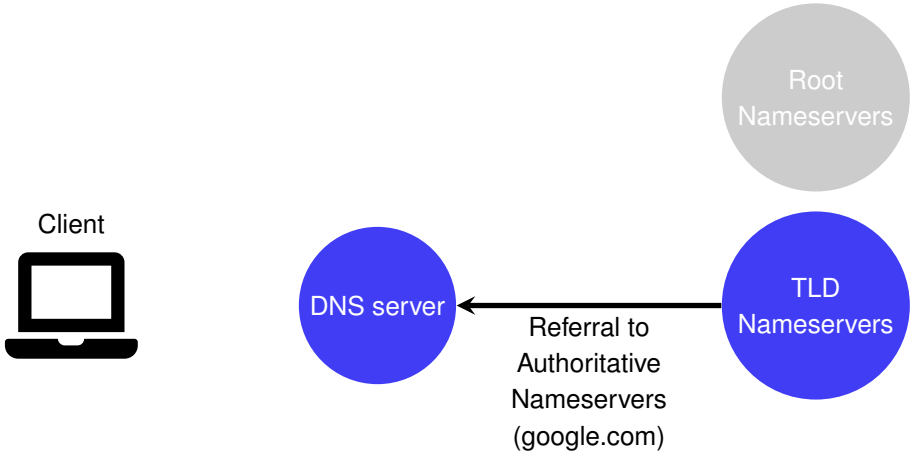
How a DNS query works: `www.google.com.`



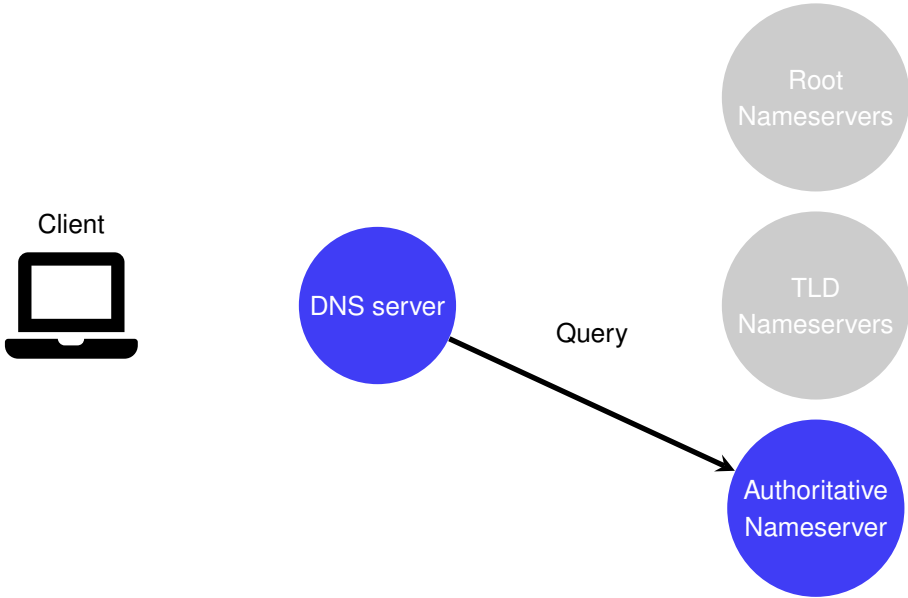
How a DNS query works: `www.google.com.`



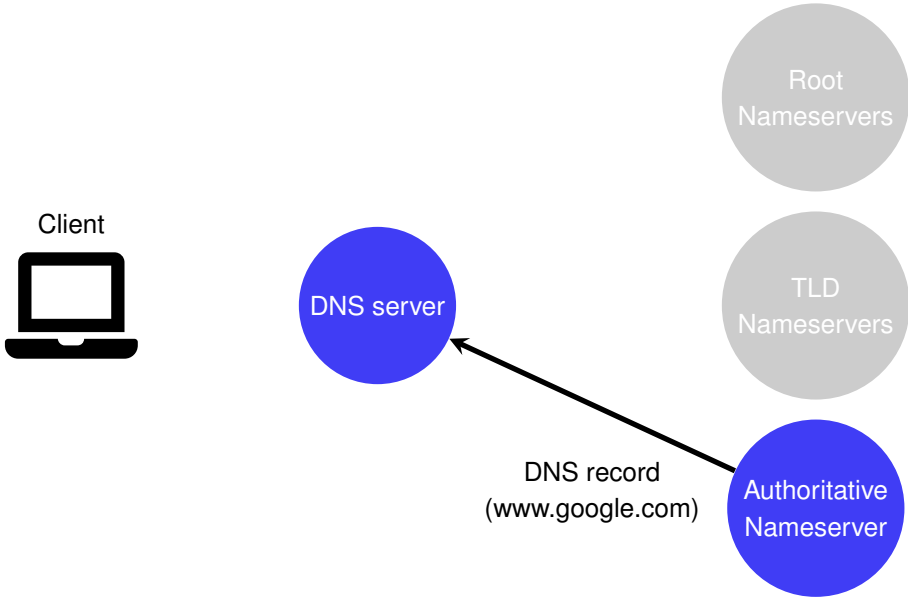
How a DNS query works: `www.google.com.`



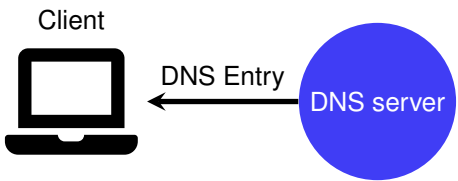
How a DNS query works: `www.google.com.`



How a DNS query works: `www.google.com.`



How a DNS query works: `www.google.com.`



Root Nameservers

TLD Nameservers

Authoritative Nameserver

Inspecting DNS queries with `host` and `dig`

```
[root@master ~]# host www.google.com
www.google.com has address 172.217.12.164
www.google.com has IPv6 address 2607:f8b0:4006:81a::2004

[root@master ~]# dig www.google.com
...
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         300     IN      A       172.217.12.164
...
```

DNS records

Address (A): Returns a 32bit IP address for a given name

```
; this defines www.google.com
www.google.com.      IN  A      172.217.12.164
```

IPv6 Address (AAAA): Returns a 128bit IPv6 address for a given name

```
; this defines the IPv6 address of www.google.com
www.google.com.  IN  AAAA     2607:f8b0:4006:81a::2004
```

DNS records

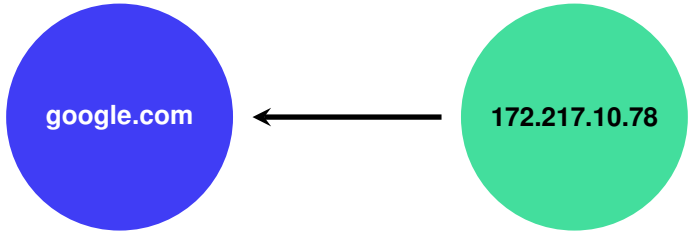
Name Server (NS): The authoritative nameserver for a given domain

```
google.com.   IN  NS  ns1.google.com.
google.com.   IN  NS  ns2.google.com.
google.com.   IN  NS  ns3.google.com.
google.com.   IN  NS  ns4.google.com.
```

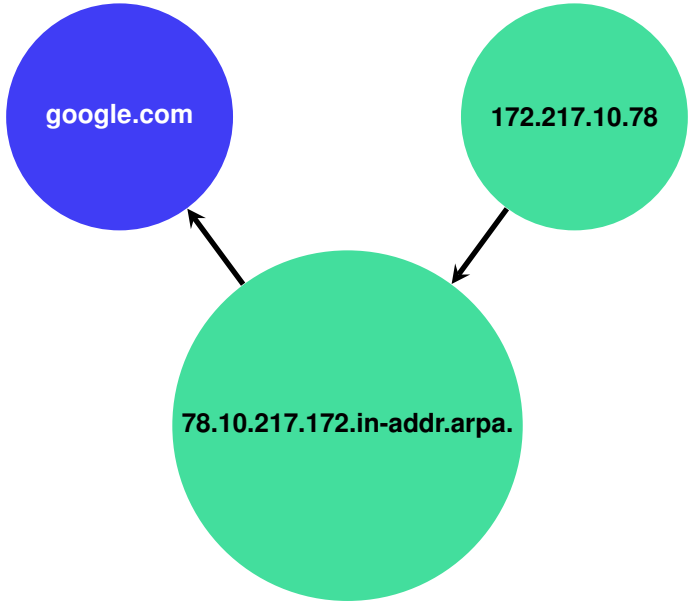
Canonical Name (CNAME): Alias one name to another

```
; ntp.example.com -> master.example.com
ntp.example.com.     IN  CNAME master.example.com.
```

Reverse Lookup



Reverse Lookup



DNS PTR records for reverse lookup

Pointer (PTR): Pointer records point an IP to a canonical name and are used in reverse DNS lookups.

```
; 192.168.1.1 -> master.hpc.
1.1.168.192.in-addr.arpa.  IN  PTR  master.hpc.
```

Inspecting reverse DNS queries with `host` and `dig`

```
[root@master ~]# host 192.168.17.1
1.17.168.192.in-addr.arpa domain name pointer t301.hpc.

[root@master ~]# dig -x 192.168.17.1
...
;; QUESTION SECTION:
;1.17.168.192.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
1.17.168.192.in-addr.arpa. 300  IN      PTR     c01.hpc.
...
```