Domain Name System (DNS)

CS 240 - The University of Illinois

Wade Fagen-Ulmschneider
November 9, 2021

DNS Translation

Up until now, we have been focused on delivering content and running web services. However, how does the user get to our service?!

- IP Address (Layer 3):

- User-Supplied Address:

DNS

Web Address   vs.   IP Address

Fully Qualified Domain Name (FQDN)

Does NOT contain protocol information:

Fully Qualified Domain Name (FQDN)

"Fully Qualified":

Fully Qualified Domain Name (FQDN)

Comprised of multiple hierarchical levels:

- TLD:

- SLD/2LD:

- Sub-domains:

DNS Record

DNS Records

A DNS record is a dictionary-like structure with a key ("record type") and an associated value and "Time to Live" (TTL) for caching.

- Time to Live (TTL) Value:

- A:

- AAAA:

- NS:

- MX:

- TXT:

DNS Record for illinois.edu

Record Type	Value	TTL
A		
AAAA		
MX		
NS		
TXT		

DNS Record for cs.illinois.edu

Record Type	Value	TTL
A		
AAAA		
MX		
NS		
TXT		

DNS Resolution

DNS Resolution

How do we retrieve DNS records so we can translate a domain name into an IP address?

DNS Root Servers

There are only **13** authoritative root DNS servers in the world (as of 2021), managed by the International Assigned Numbers Authority (IANA).

List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

https://www.iana.org/domains/root/servers

DNS Root Servers

Purpose:

TLD Name Servers

A collection of 1,514 (as of 2021) valid top-level domain name servers. (ICANN maintains registration and approval for all TLDs.)

Original TLDs: `.com .org .net .edu .mil .int .gov .arpa`

ccTLDs: `.ru .cn .de .uk .nl`

gTLDs: `.top .dev .xyz .site .me`

TLD Name Servers

Purpose:

SLD/2LD Name Servers

Any domain within a TLD.

When you "purchase" a domain name, part of the cost goes to maintaining your entry in the Domain Name System that points to your name server.

SLD/2LD Name Servers

Purpose:

When you connect to the Internet, the protocol that initializes your connection will provide the IP address to a local DNS server called your "**Preferred DNS Server**".

- Local:

- [Possibly] Private:

- Can be User-Defined:

A free, global DNS resolution service that you can use as an alternative to your current DNS provider.

Get started   Get Help

Why does DNS matter?

The Domain Name System (DNS) protocol is an important part of the web's infrastructure, serving as the Internet's phone book: every time you visit a website, your computer performs a DNS lookup. Complex pages often require multiple DNS lookups before they start loading, so your computer may be performing hundreds of lookups a day.

Try it out

- Configure your network settings to use the IP addresses 8.8.8.8 and 8.8.4.4 as your DNS servers.

- Or, read our configuration instructions (IPv6 addresses supported too).

If you decide to try Google Public DNS, your client programs will perform all DNS lookups using Google Public DNS.

In addition to traditional DNS over UDP or TCP, we also provide DNS over TLS (DoT) and DNS over HTTPS (DoH) for greater security and privacy.

Looking for Cloud DNS?

Public DNS is only a name resolver. If you are looking for a high-volume, programmable, authoritative name server using Google's infrastructure, try Google's Cloud DNS.

Why should you try Google Public DNS?

Speed up your browsing experience

Improve your security

Get the results you expect with absolutely no redirection

Issue Tracker
Something wrong? Send us a bug report!

User Forum
Discuss Google Public DNS-related issues

Announcements
Subscribe to our announcements

Videos
Kick back with Google Public DNS videos on YouTube

CLOUDFLARE

DNS   Families

1.1.1.1

The free app that makes your Internet safer.

Now available for even more devices.

App Store   Google Play

macOS   Windows   Linux

macOS Installation Instructions   Windows Installation Instructions   Linux Installation Instructions

IPv4
9.9.9.9

149.112.112.112

IPv6
2620:fe::fe

2620:fe::9

More options ▶

An open DNS recursive service for free security and high privacy

Quad9 is a free service that replaces your default ISP or enterprise Domain Name Server (DNS) configuration. When your computer performs any Internet transaction that uses the DNS (and most transactions do), Quad9 blocks lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve performance in addition to guaranteeing privacy. The Quad9 DNS service is operated by the Swiss-based Quad9 Foundation, whose mission is to provide a safer and more robust Internet for everyone.

Watch our short videos on how to set up Quad9 - Windows / MacOS ▶

60M
Average Daily Blocks

18+
Threats Intelligence Providers

150
Resolver Clusters in 90 countries

▶ Privacy

How Quad9 protects your privacy

When your devices use Quad9 normally, no data containing your IP address is ever logged in any Quad9 system. Connections can employ encryption if your system

Why Quad9 is dedicated to data privacy

Every transaction on the Internet starts with a DNS event. This name lookup reveals critically sensitive data about the person triggering that transaction. The nature of those name lookups has created a strong and dangerous motivation for commercialization
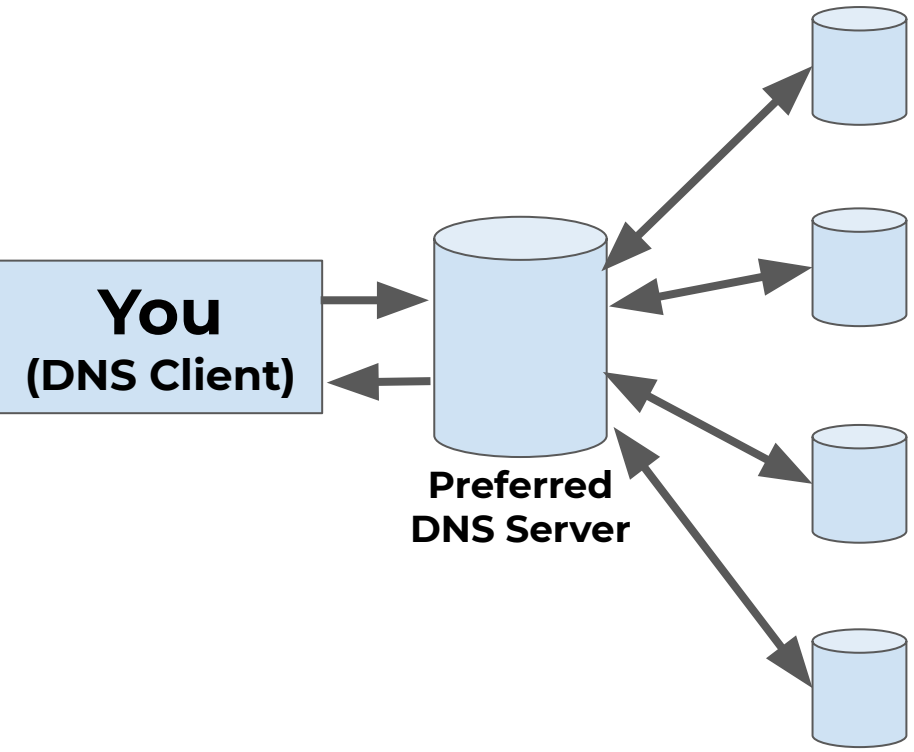
Q1: What servers must be contacted the first time that you visit **d7.cs.illinois.edu** if the cache is completely empty?

Q2: What servers must be contacted the second time that you visit **d7.cs.illinois.edu** after just a short time?

Q3: What servers must be contacted when you visit **waf.cs.illinois.edu** after the above requests?