The DNS Root Server System

An Introduction intended for a non-technical public policy audience

Jeff Osborn, RSSAC Chair

ICANN 79, San Juan, Puerto Rico

February 2024

Introduction: Newcomers at ICANN79

- For today, imagine you are regulators and lawmakers:
  - You need to learn how DNS works
  - You need to learn the role that the root server system plays in DNS
  - You need to learn the (relative) significance of the root server system
  - You want to make good decisions
- The Root Server System Advisory Committee (RSSAC)
  - Advises the ICANN community on matters related to the root server system
  - Each RSO appoints 1 member and 1 alternate; plus multiple lisiasons

Introducing DNS (the Domain Name System)

- DNS uses human names to find computer addresses
  - Humans know the domain names like: www.amazon.com
  - Computers know IP addresses like: 18.239.62.181
  - DNS translates “www.amazon.com” into “18.239.62.181”
  - For the most part, numbers change, but names don’t
- Most connected devices need DNS to find things
  - Computers & servers
  - Smart phones
- Questions use a domain name; answers use IP addresses

Benefits of DNS

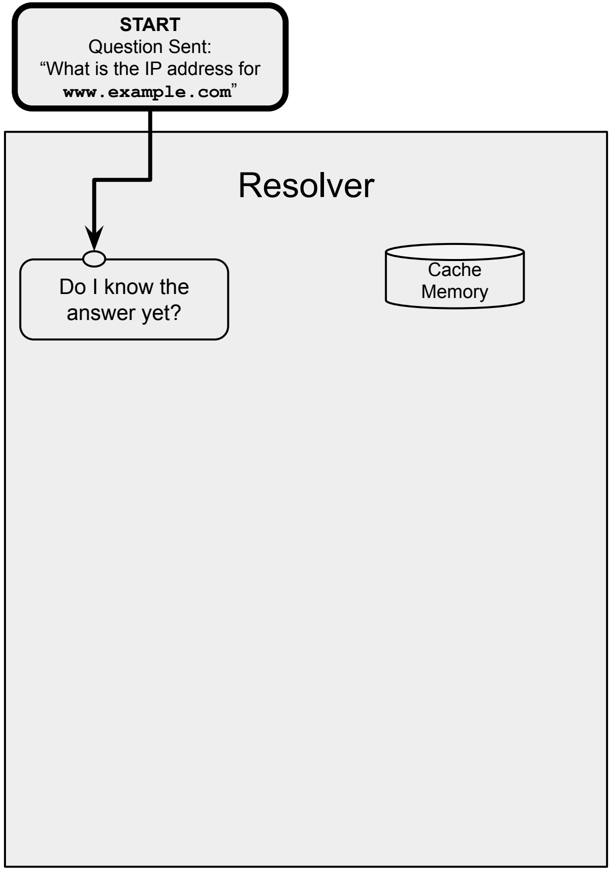
- Service portability
  - Resource owners control address mapping in their domain
  - DNS follows you to your new online home
- It’s how registrants enjoy the use of their domain name
  - Flexible delegated management of hundreds of millions of directories
  - World’s largest distributed database
- Human-friendly identifiers
  - **`www.example.com`** is easier to use than **`192.168.45.99`**

Devices get addresses from resolvers

- There are millions of resolvers around the world
- It’s like resolvers can read all the world’s phone books
    - The phone books are authoritative servers
    - The phone book listings are zone data
    - What is the number for www.amazon.com?
    - The number for www.amazon.com (for now) is 18.239.62.181
        - This happens in milliseconds
        - This happens about 500 trillion of times every day

Resolvers get addresses from authoritative servers

- The resolver remembers addresses
  - This is called caching
  - This is where answers come from most of the time
- Once in a while, it needs a new number or to confirm an old one
- Depending how much it needs, it will ask:
  1. A domain name’s authoritative server
  2. A domain name’s authoritative server, and a TLD’s authoritative server
  3. A domain name’s authoritative server, and a TLD’s authoritative server, and a root server

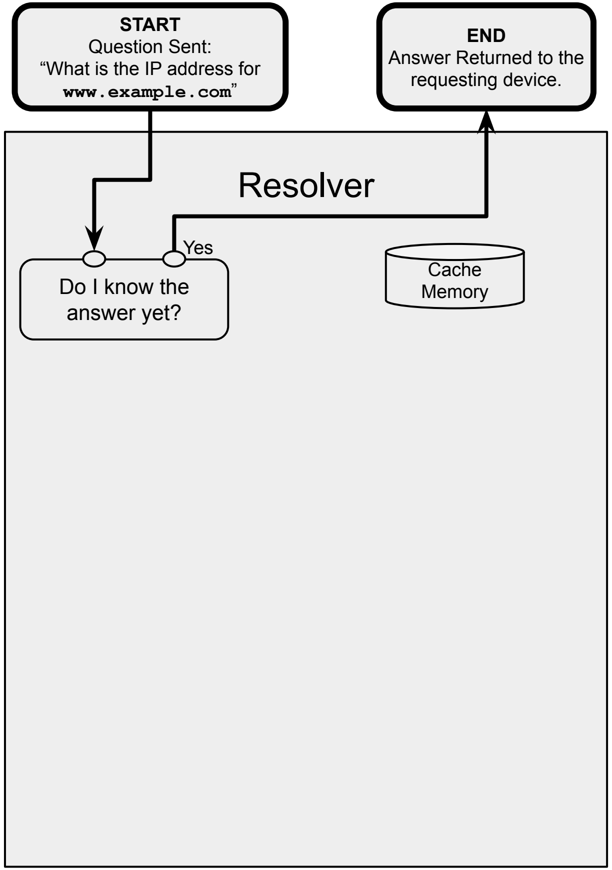


START
Question Sent:
“What is the IP address for
`www.example.com`”

Resolver

Do I know the answer yet?

Cache Memory

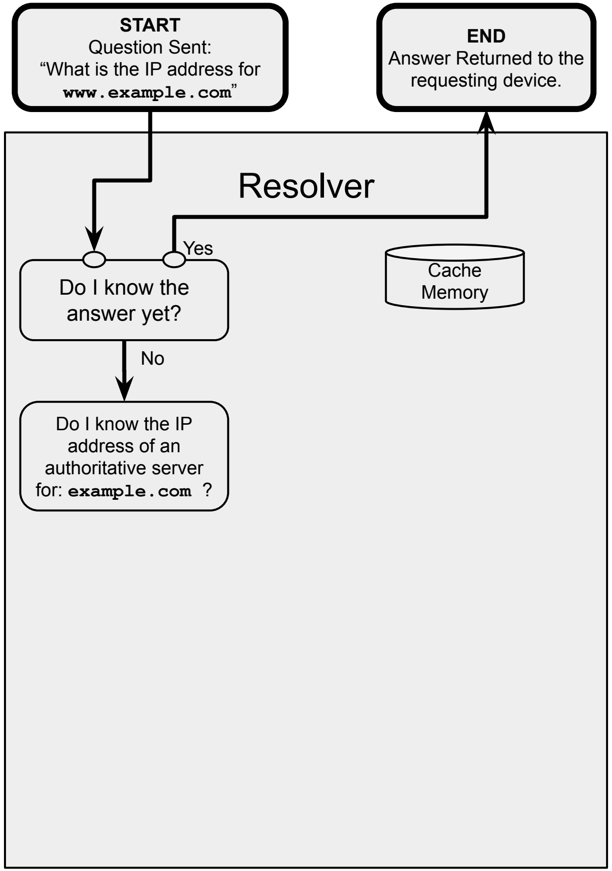


Frequency (estimates):

On average, how often do Resolvers consult at this level to answer a question?

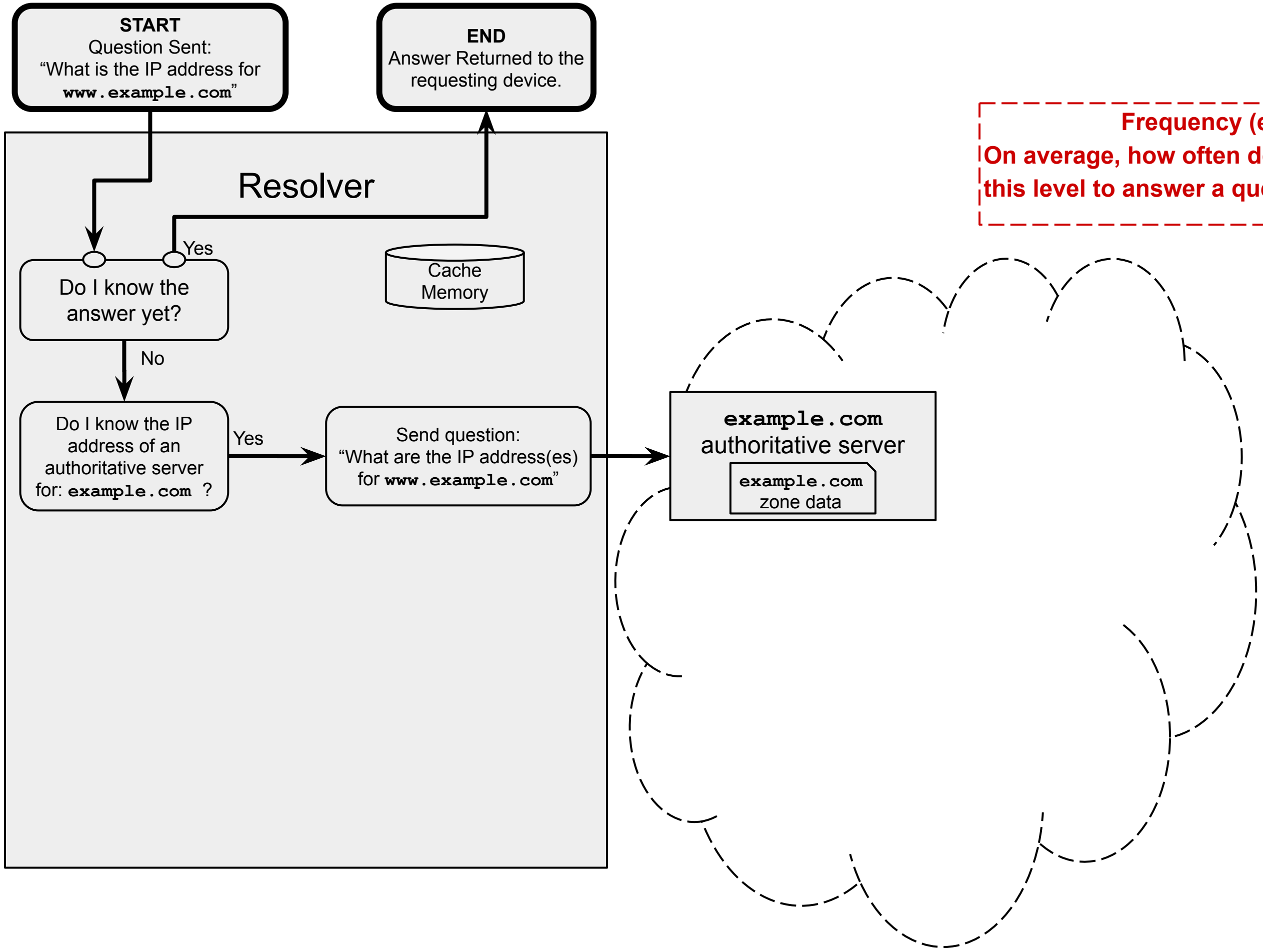
Routine:

> 90 of every 100 answers are returned needing cache memory only



Frequency (estimates):
On average, how often do Resolvers consult at this level to answer a question?

Routine:
> 90 of every 100 answers are returned needing cache memory only



START
Question Sent:
"What is the IP address for `www.example.com`"

END
Answer Returned to the requesting device.

Resolver

Do I know the answer yet?

Yes

No

Cache Memory

Do I know the IP address of an authoritative server for: `example.com` ?

Yes

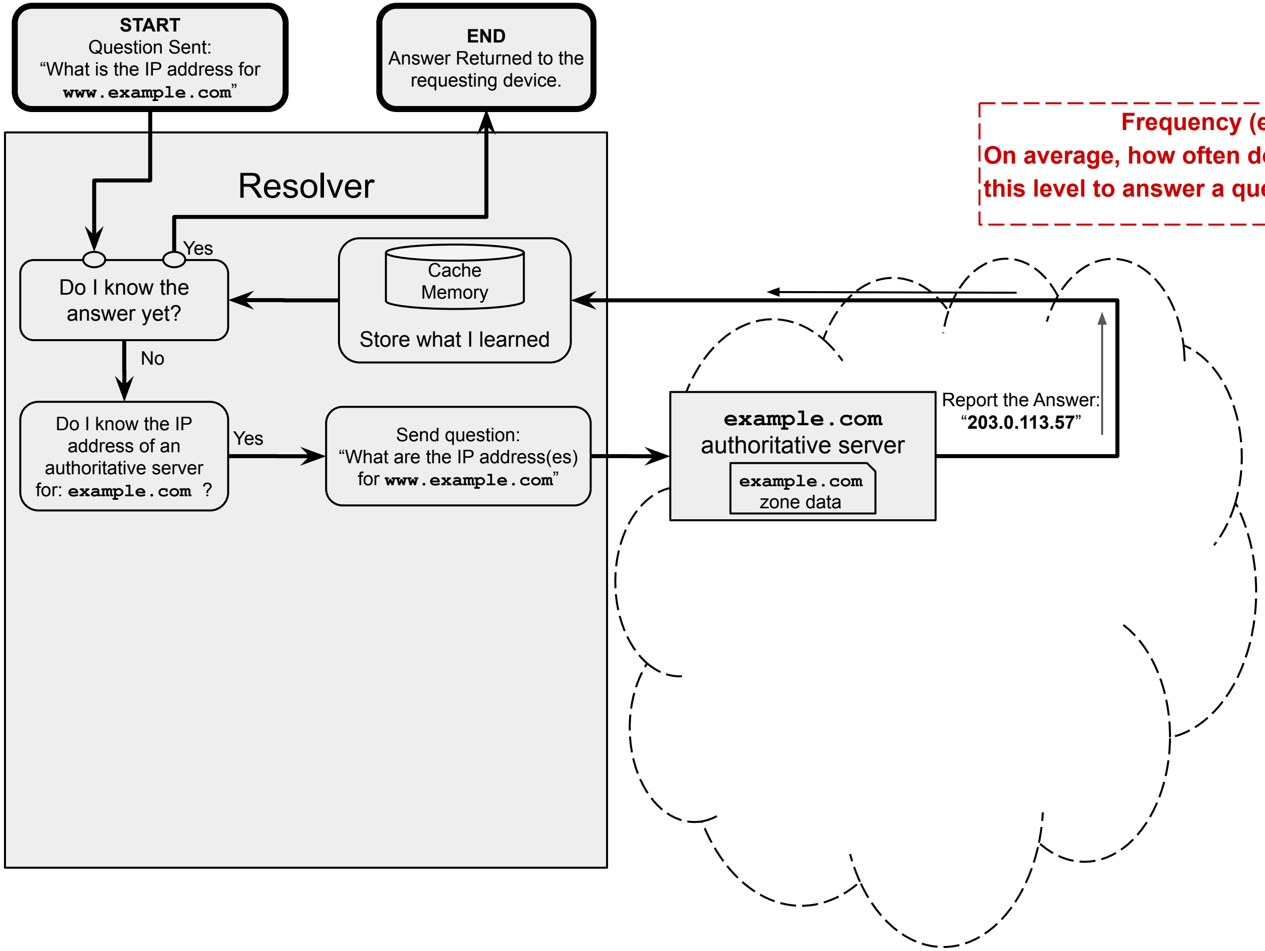
Send question:
"What are the IP address(es) for `www.example.com`"

`example.com` authoritative server

`example.com` zone data

Frequency (estimates):
On average, how often do Resolvers consult at this level to answer a question?

Routine:
> 90 of every 100 answers are returned needing cache memory only



START
Question Sent:
"What is the IP address for **`www.example.com`**"

END
Answer Returned to the requesting device.

Resolver

Do I know the answer yet?

Yes

No

Cache Memory

Store what I learned

Do I know the IP address of an authoritative server for: **`example.com`** ?

Yes

Send question:
"What are the IP address(es) for **`www.example.com`**"

`example.com`
authoritative server

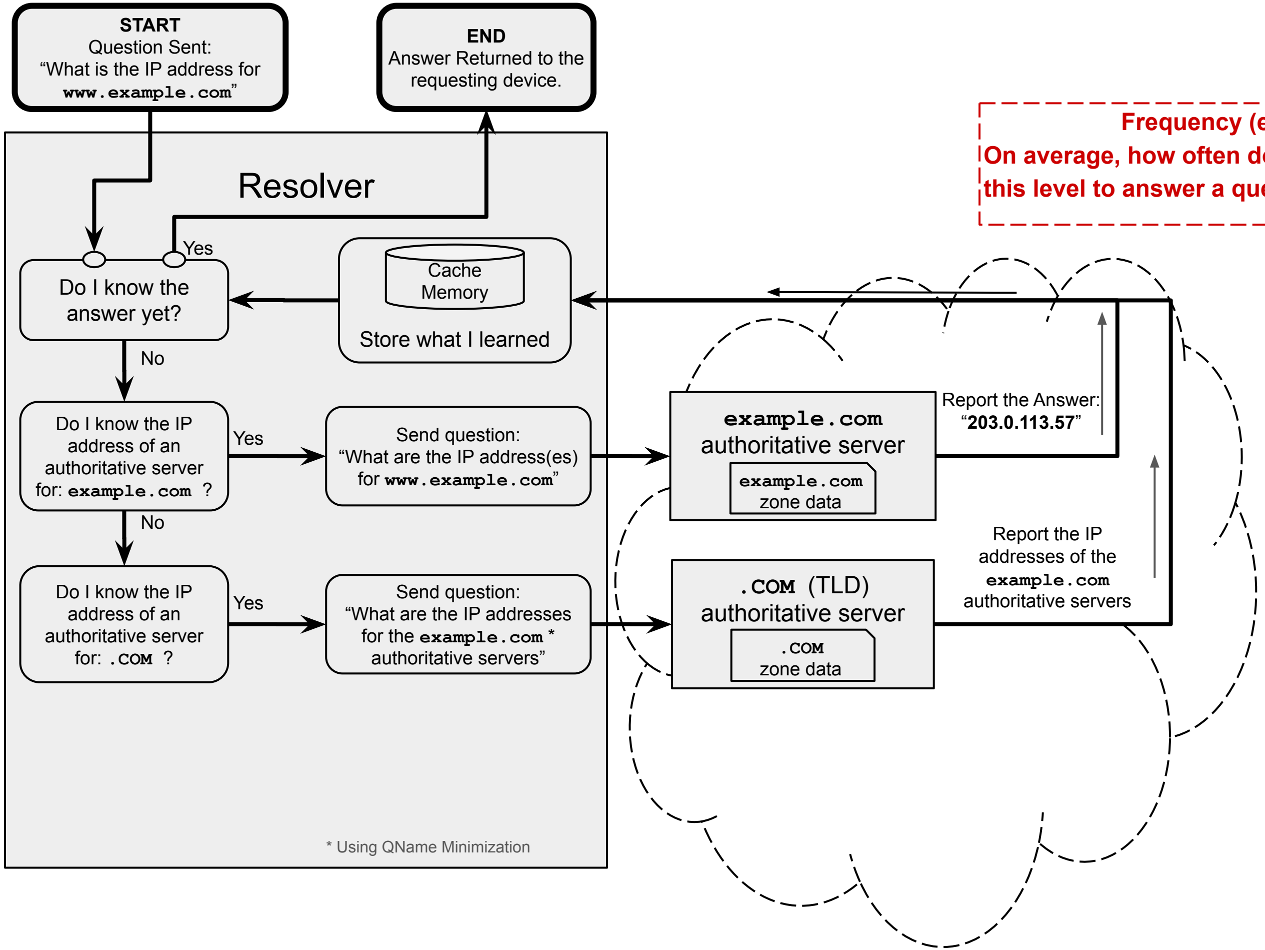
`example.com`
zone data

Report the Answer:
"**203.0.113.57**"

Frequency (estimates):
On average, how often do Resolvers consult at this level to answer a question?

Routine:
> 90 of every 100 answers are returned needing cache memory only

Ocasional:
~5 of every 100 answers require a question to the domain name's authoritative server



START
Question Sent:
“What is the IP address for `www.example.com`”

END
Answer Returned to the requesting device.

Resolver

Yes

Do I know the answer yet?

Cache Memory

Store what I learned

No

Do I know the IP address of an authoritative server for: `example.com` ?

Yes

Send question:
“What are the IP address(es) for `www.example.com`”

No

Do I know the IP address of an authoritative server for: `.COM` ?

Yes

Send question:
“What are the IP addresses for the `example.com`* authoritative servers”

`example.com` authoritative server

`example.com` zone data

Report the Answer:
“**203.0.113.57**”

`.COM` (TLD) authoritative server

`.COM` zone data

Report the IP addresses of the `example.com` authoritative servers

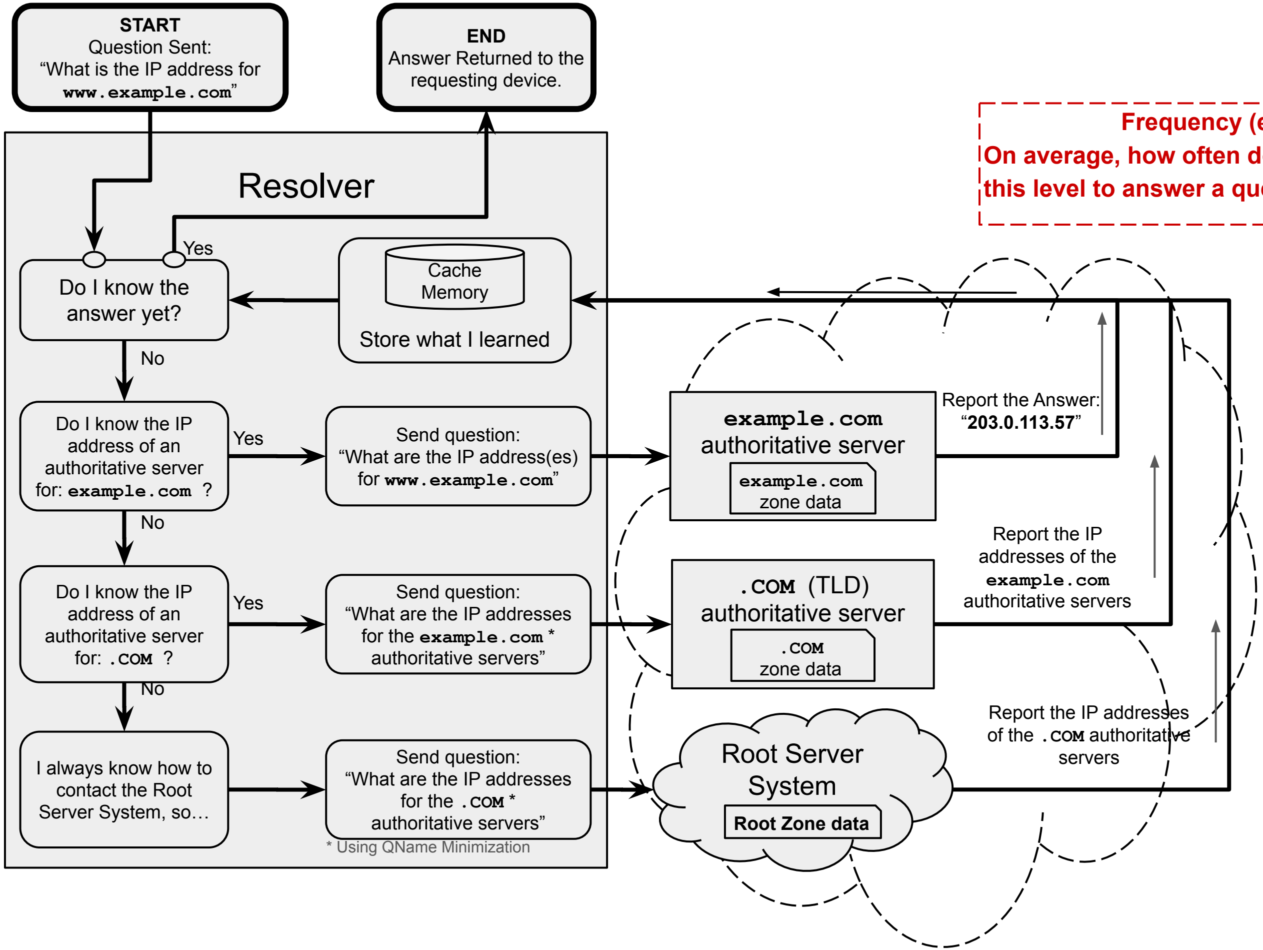
* Using QName Minimization

Frequency (estimates):
On average, how often do Resolvers consult at this level to answer a question?

Routine:
> 90 of every 100 answers are returned needing cache memory only

Ocasional:
~5 of every 100 answers require a question to the domain name’s authoritative server

Uncommon:
~2 of every 100 answers require a question to the TLD authoritative server



START
Question Sent:
“What is the IP address for
`www.example.com`”

END
Answer Returned to the
requesting device.

Resolver

Do I know the answer yet?

Yes

No

Cache Memory

Store what I learned

Do I know the IP address of an authoritative server for: `example.com` ?

Yes

Send question:
“What are the IP address(es) for `www.example.com`”

No

Do I know the IP address of an authoritative server for: `.COM` ?

Yes

Send question:
“What are the IP addresses for the `example.com` * authoritative servers”

No

I always know how to contact the Root Server System, so…

Send question:
“What are the IP addresses for the `.COM` * authoritative servers”

* Using QName Minimization

`example.com` authoritative server

`example.com` zone data

Report the Answer:
“**203.0.113.57**”

`.COM` (TLD) authoritative server

`.COM` zone data

Report the IP addresses of the `example.com` authoritative servers

Root Server System

Root Zone data

Report the IP addresses of the `.COM` authoritative servers

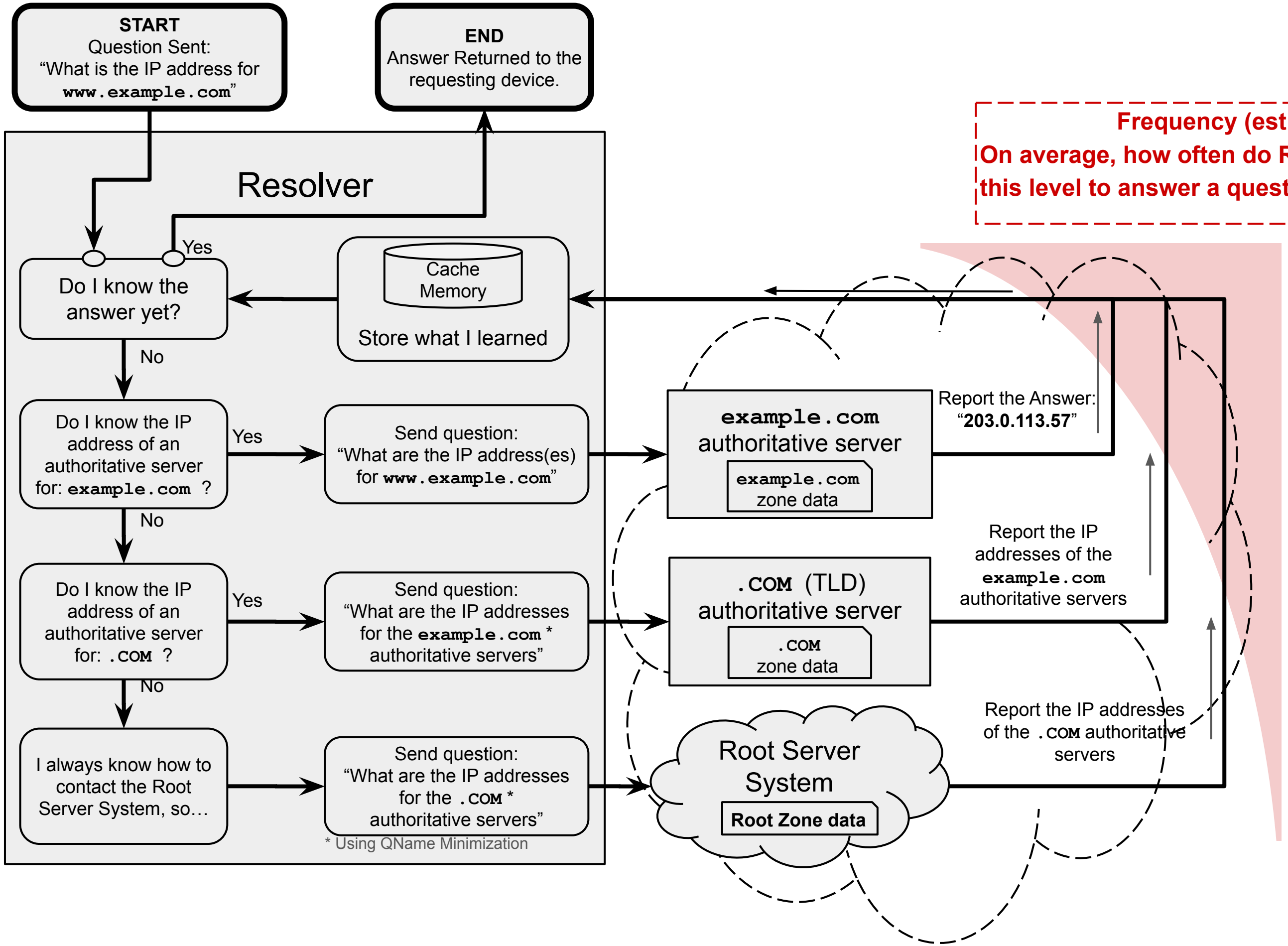
Frequency (estimates):
On average, how often do Resolvers consult at this level to answer a question?

Routine:
> 90 of every 100 answers are returned needing cache memory only

Ocasional:
~5 of every 100 answers require a question to the domain name’s authoritative server

Uncommon:
~2 of every 100 answers require a question to the TLD authoritative server

Rare:
~1 in every 5,000 answers requires a question to the RSS



START
Question Sent:
“What is the IP address for **`www.example.com`**”

END
Answer Returned to the requesting device.

Resolver

Do I know the answer yet?

Yes

No

Cache Memory

Store what I learned

Do I know the IP address of an authoritative server for: **`example.com`** ?

Yes

Send question:
“What are the IP address(es) for **`www.example.com`**”

No

Do I know the IP address of an authoritative server for: **`.COM`** ?

Yes

Send question:
“What are the IP addresses for the **`example.com`** * authoritative servers”

No

I always know how to contact the Root Server System, so…

Send question:
“What are the IP addresses for the **`.COM`** * authoritative servers”

* Using QName Minimization

`example.com` authoritative server

`example.com` zone data

Report the Answer:
“**203.0.113.57**”

`.COM` (TLD) authoritative server

`.COM` zone data

Report the IP addresses of the **`example.com`** authoritative servers

Root Server System

Root Zone data

Report the IP addresses of the **`.COM`** authoritative servers

Frequency (estimates):
On average, how often do Resolvers consult at this level to answer a question?

Routine:
> 90 of every 100 answers are returned needing cache memory only

Ocasional:
~5 of every 100 answers require a question to the domain name’s authoritative server

Uncommon:
~2 of every 100 answers require a question to the TLD authoritative server

Rare:
~1 in every 5,000 answers requires a question to the RSS

In review

- A root server holds a copy of “Root Zone” data
  The Root Zone holds addresses for TLD’s like:
  - .com
  - .nl
  - .jobs (and on and on)
- A TLD authoritative server knows the address for the next step
  - All names that end in .com, like amazon.com or tiktok.com
  - All names that end in .nl, like tulips.nl or herring.nl
  - All names that end in .jobs, like tech.jobs or highpay.jobs
- A domain name’s authoritative server knows
  - The answer to the question about www.amazon.com or mail.amazon.com or info.amazon.com
- The resolver finds and returns the answer

In the millisecond world of a resolver, queries to the Root Server System are rare.

How often does this happen (on average)?

(estimates, Jan 2024)

- All of the world's resolvers put together:
  - Answer about 500 TRILLION address questions per day
    - Q: How do I contact **`www.example.com`**
    - A: Try **`203.0.113.57`**
  - Ask the root server system about 100 BILLION questions per day
    - Q: How do I contact the authoritative server for **`.COM`** TLD?
    - A: Try **`192.168.231.45`**

- Questions to the RSS
  - Volume is big (100 Billion / day)
  - Frequency is small (1 in every 5,000 or less)

Root Server System Operation

- Massively redundant 1700+ globally distributed server instances
  - Each server instance holds 100% of the Root Zone content
  - Diverse hardware platforms
  - Diverse operating systems
  - Diverse DNS applications
  - Diverse data routing

- Result: No single point of technological failure

Root Server System Operation

- Co-operated by 12 autonomous Root Server Operators (RSO)
    - Each RSO is independent of the others
    - Force majeure event suffered by one (court injunction, etc) has no operational impact on the others

- Result: No single point of institutional failure

Root Server Operators do not choose the content of Root Zone data

- Where does zone data from?
  - Registrants maintain the zone data for their own domain
  - Registrants provide their authoritative server addresses to TLD registries, via registrars
  - TLD registries provide their authoritative server addresses to IANA for inclusion in the root zone
  - IANA authenticates and sends root zone data changes to the Root Zone Maintainer (RZM), an outsourced service
  - The RZM generates DNSSEC signatures and makes the root zone data available in the RSS by transmitting it to the RSOs
- The RSOs serve up what IANA sends

40 years of stability, security, and resilience

- The Root Server System has operated since the 1980’s
- It has never suffered a service outage.
    - DDoS attackers have tried; they failed, by design

Summary

- The root server system is an important, if infrequent, component of address resolution
  - Most DNS queries are answered from cache memory
  - Most remaining DNS queries go straight to domain name authoritative servers
- Root server operators do not decide the content of the Root Zone
- The root server system
  - Is massively redundant
  - Is technologically diverse
  - Is institutionally resilient
- The root system works