The Domain Name System
Part One

● ● ●

Gautam Akiwate
Stanford University

Understand
the rationale, and operational workings of the

Domain Name System (DNS).

Problem

- Communication on the Internet via IP

- Hard to remember IP addresses

- Easier to remember names.

  - Slightly harder to type them in

    correctly!

- Map Names to IP addresses

  - stanford → 185.199.108.153

Centralized Solution: Historical Solution

- hosts.txt file that has mappings for all hosts
    - organization : host → IP address
    - /etc/hosts
- Stanford Research Institute (SRI) kept main copy
    - Single place to update records
    - Download hosts.txt file periodically

Centralized Solution: Historical Solution

- hosts.txt file that has mappings for all hosts
  - organization : host → IP address
  - /etc/hosts
- Stanford Research Institute (SRI) kept main copy
  - Single place to update records
  - Download hosts.txt file periodically
- Problems
  - Fragile
  - Hard to scale
  - Hard to keep in sync

Decentralized Solution: Intuition

hosts.txt | organization : host → IP address |

Decentralized Solution: Intuition

hosts.txt

organization : host → IP address

hosts.txt

organization→ IP address of organization.txt

organization.txt

host → IP address

Decentralized Solution: Intuition

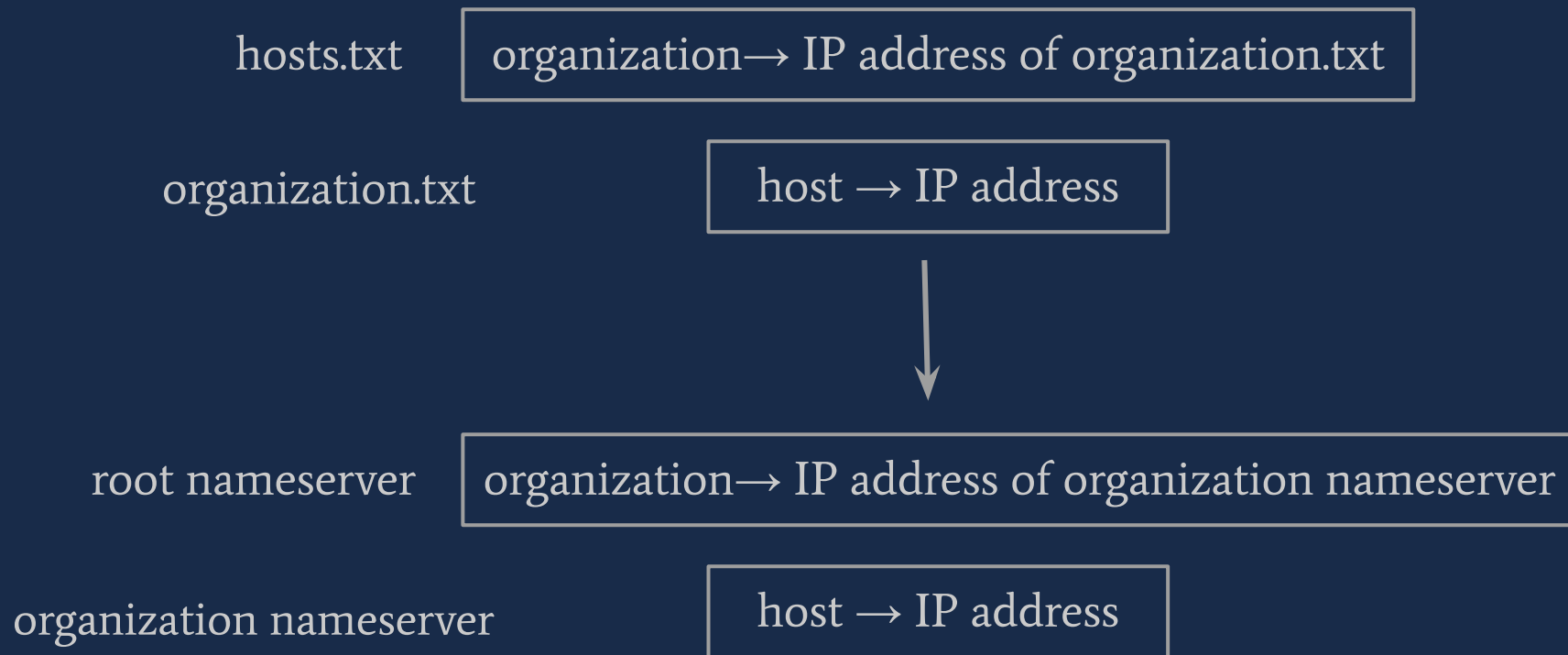hosts.txt | organization→ IP address of organization.txt |

organization.txt | host → IP address |

Decentralized Solution: Intuition

hosts.txt | organization→ IP address of organization.txt |

organization.txt | host → IP address |

root nameserver | organization→ IP address of organization nameserver |

organization nameserver | host → IP address |

DNS Hierarchical Namespace

DNS Root

DNS Root
.

root
authoritative
nameservers

ICANN

DNS Hierarchical Namespace
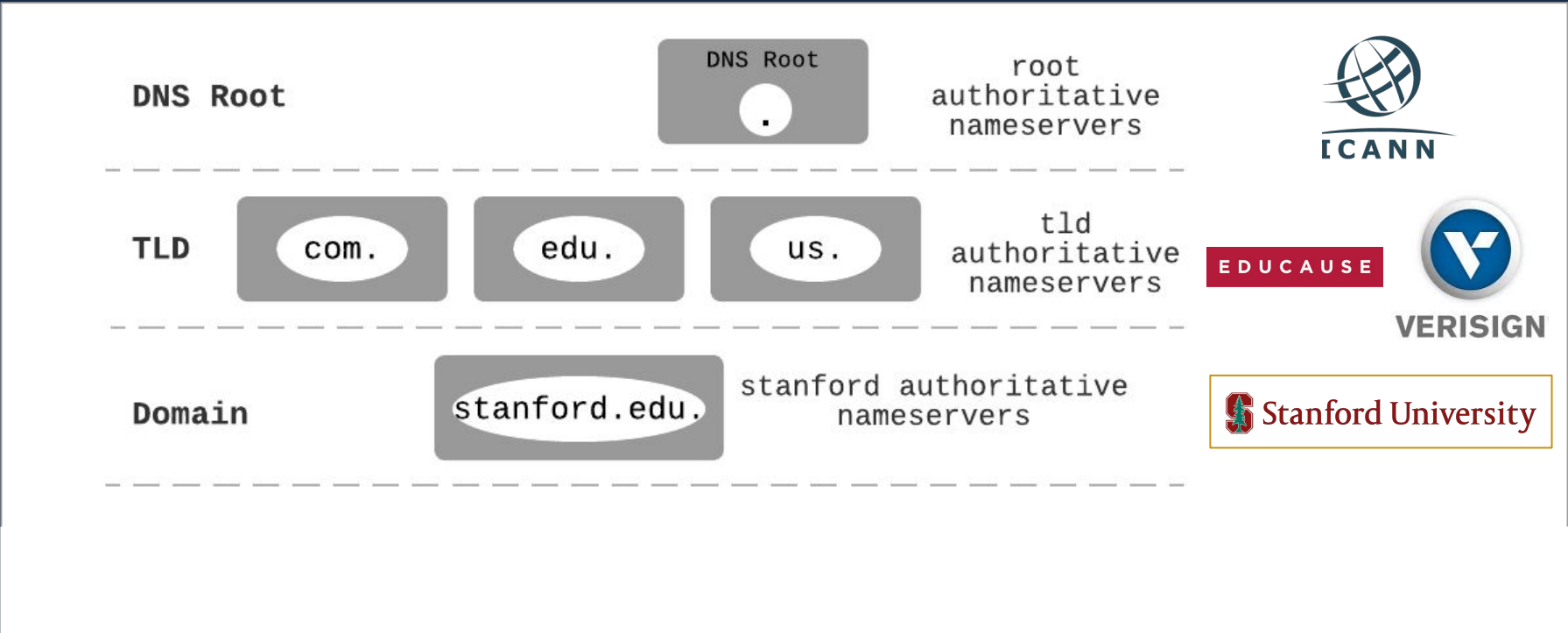
DNS Hierarchical Namespace
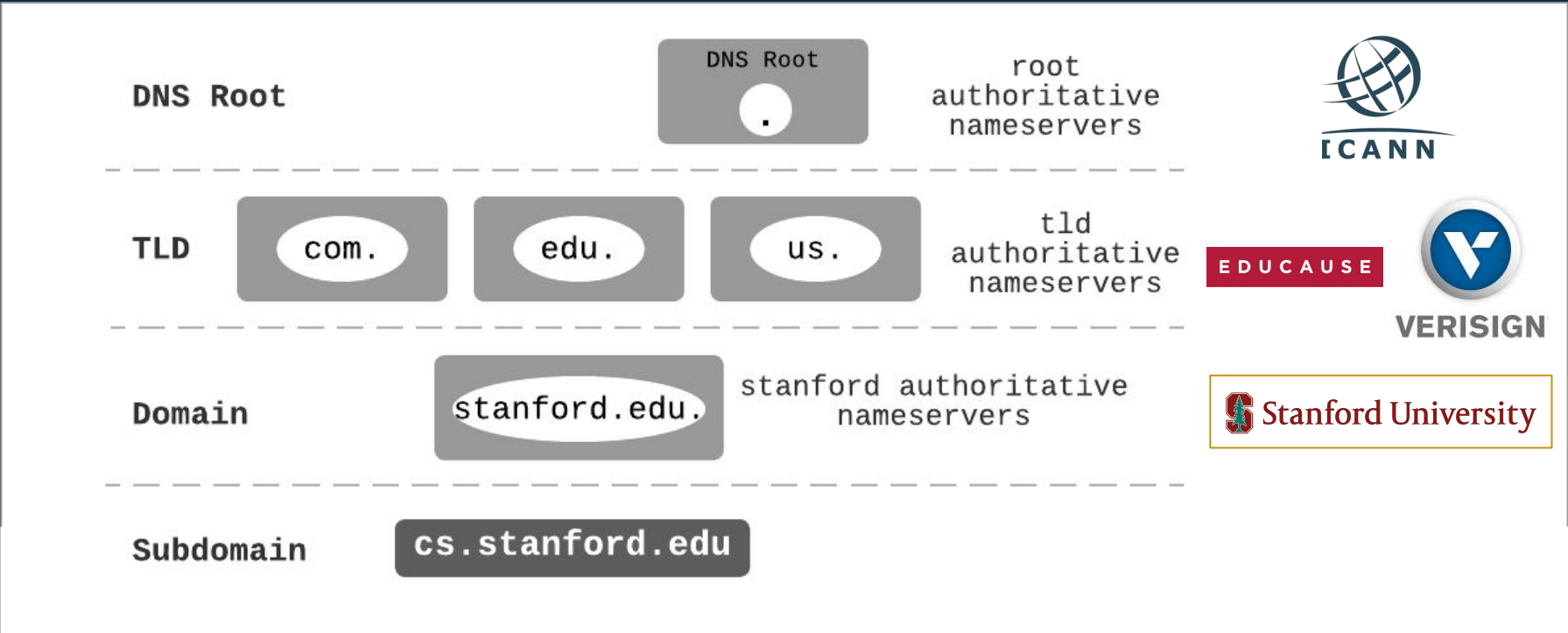
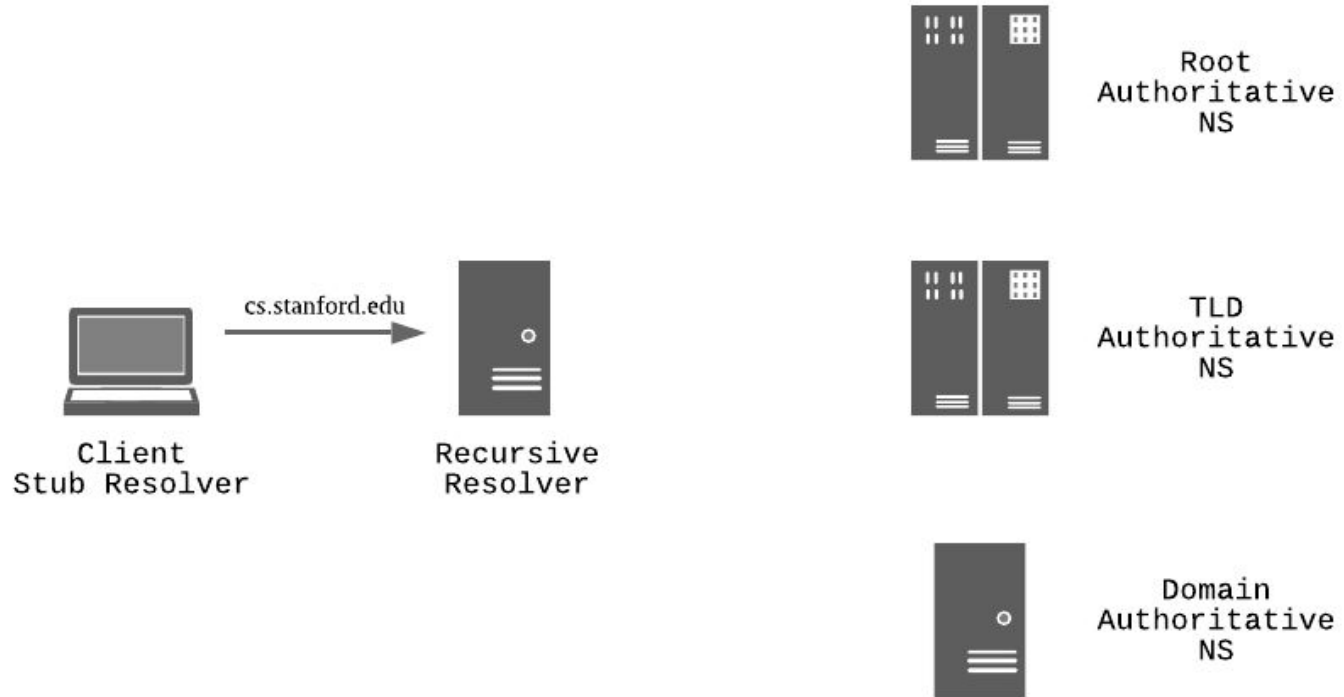# DNS Hierarchical Namespace
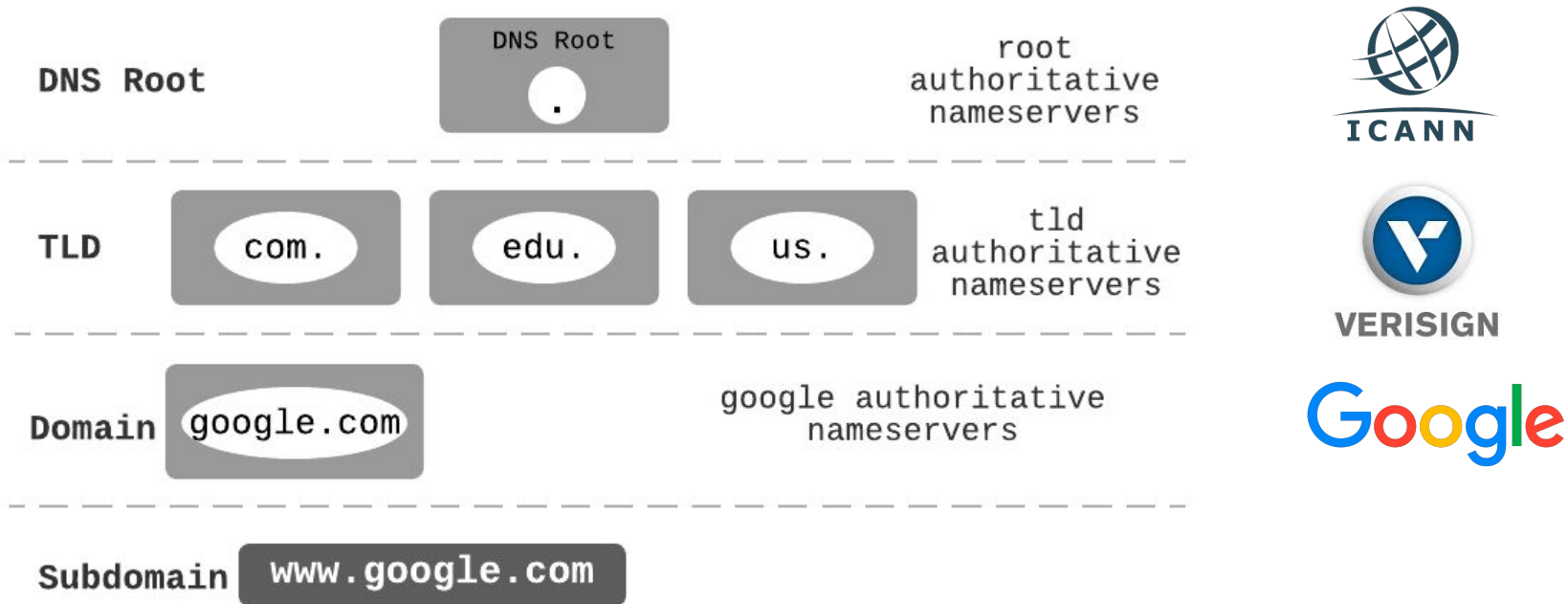
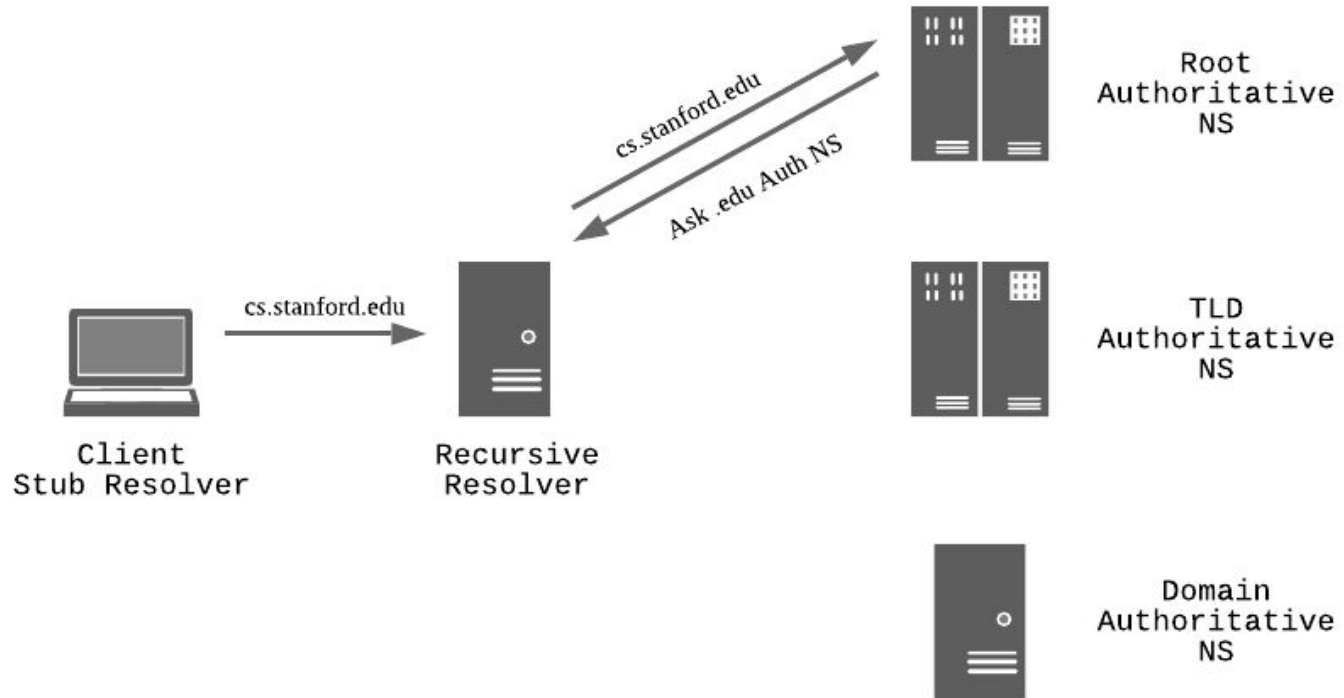# DNS Infrastructure
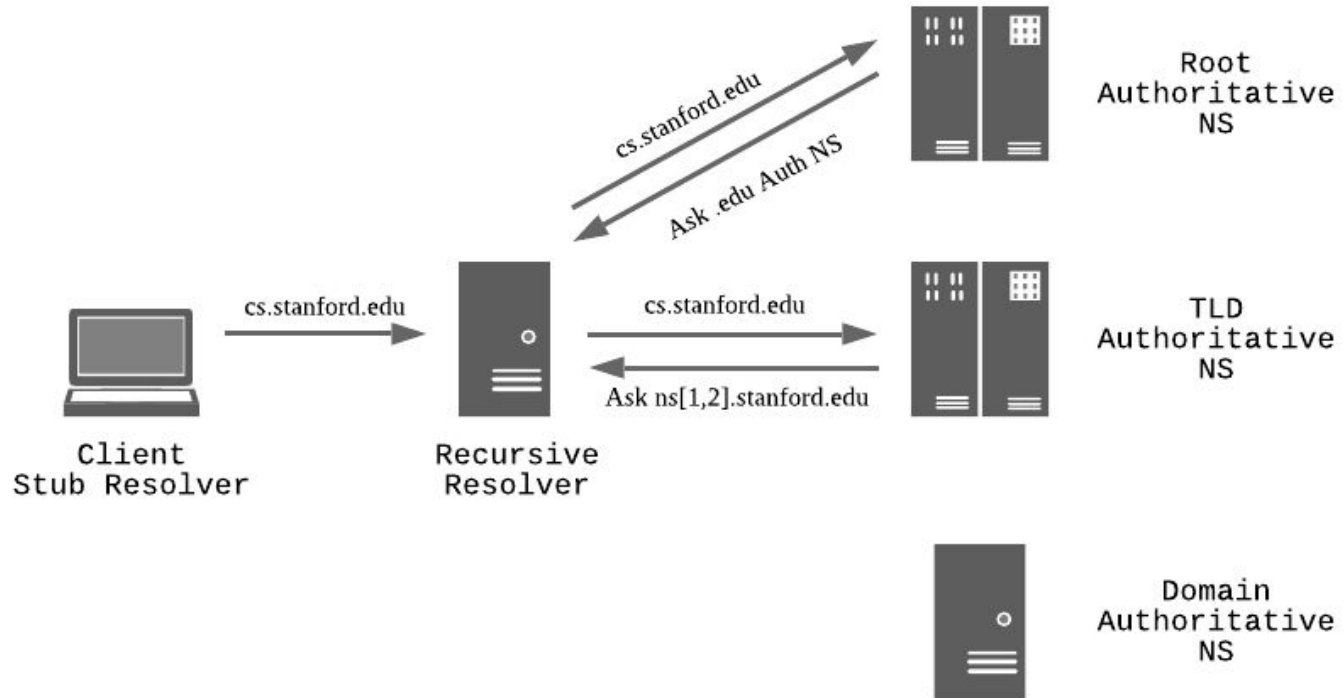

Root Authoritative NS
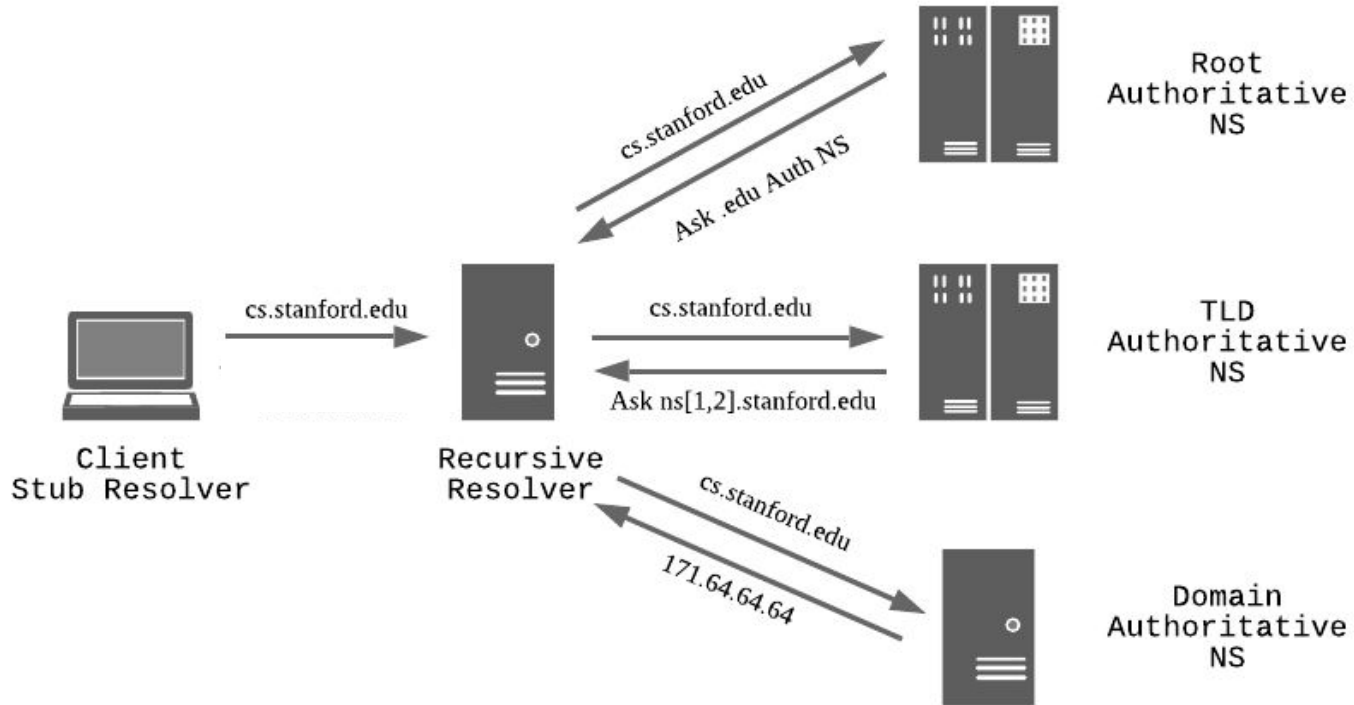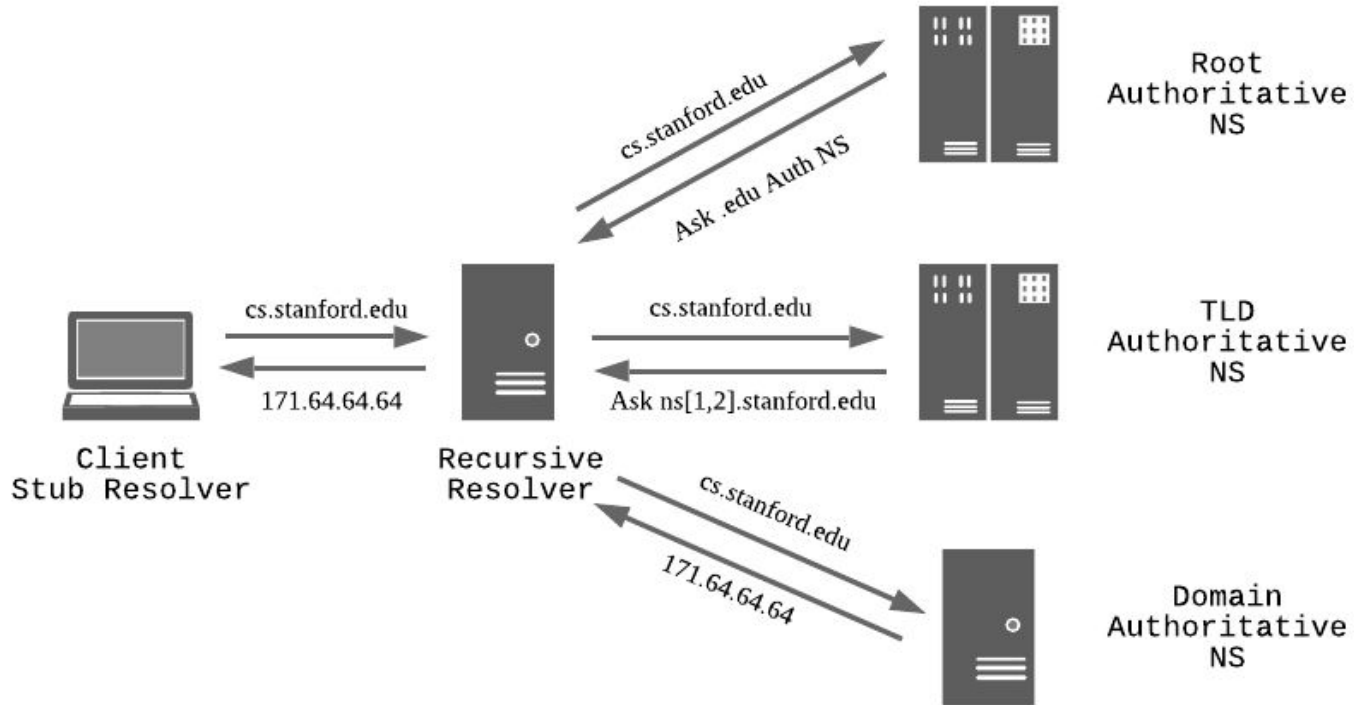
TLD Authoritative NS

Domain Authoritative NS

Life of a DNS Query

Life of a DNS Query
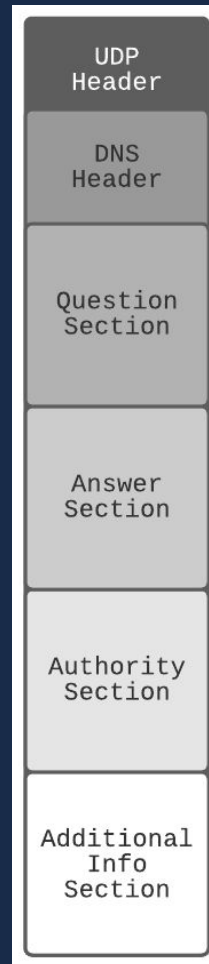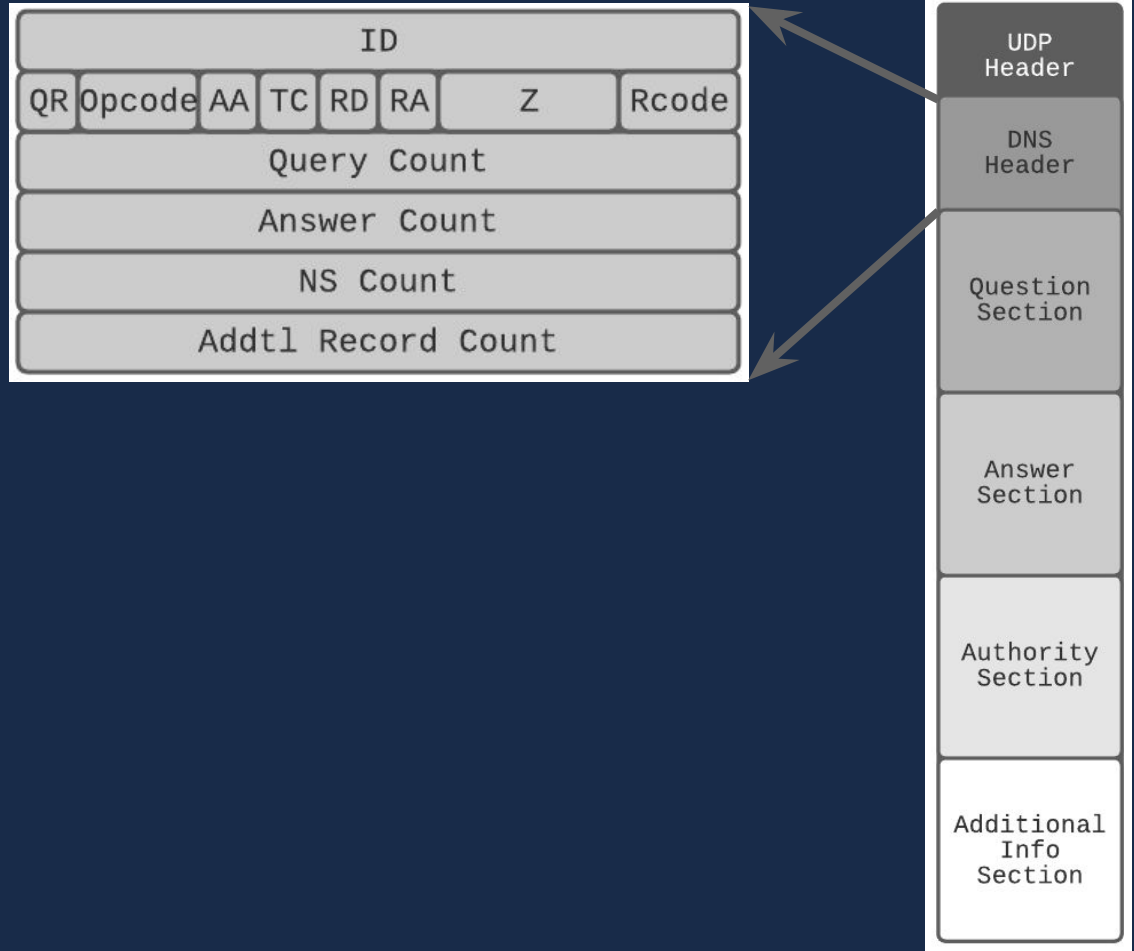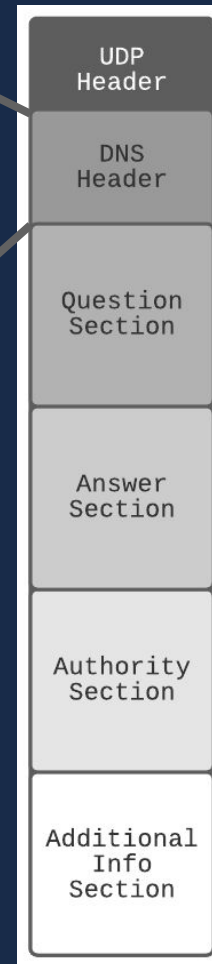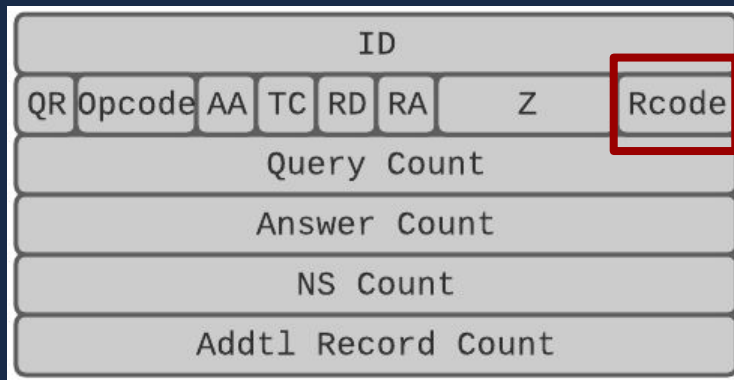
Life of a DNS Query

Life of a DNS Query

Life of a DNS Query

Life of a DNS Query

DNS Query Anatomy

UDP
Header

DNS
Header

Question
Section

Answer
Section

Authority
Section

Additional
Info
Section

DNS Query Anatomy

DNS Query Anatomy

	ID							
QR	Opcode	AA	TC	RD	RA	Z		Rcode
Query Count								
Answer Count								
NS Count								
Addtl Record Count								

UDP Header

DNS Header

Question Section

Answer Section

Authority Section

Additional Info Section

Rcode	Message	Function
0	NOERROR	Query Successful
2	SERVFAIL	Server failed to complete request
3	NXDOMAIN	Domain name does not exist
4	NOTIMP	Function not implemented
5	REFUSED	The server refused to answer the query

DNS Query Anatomy
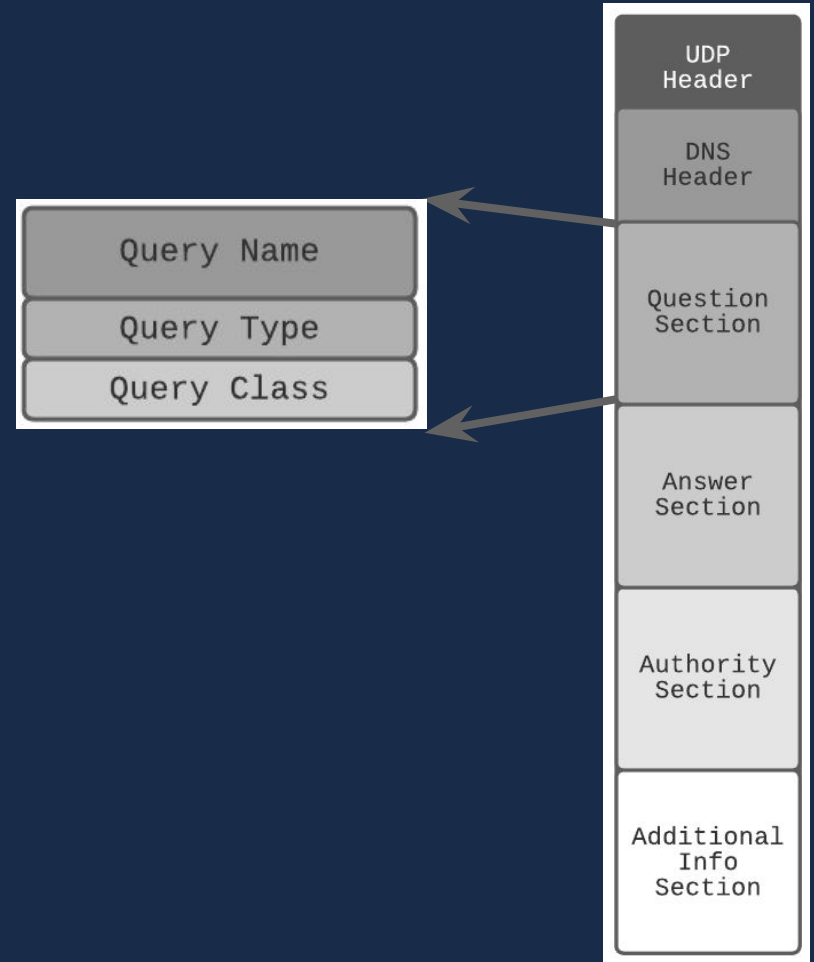
Query Name (QNAME) -- Domain to resolve!

| Query Name |
| Query Type |
| Query Class |

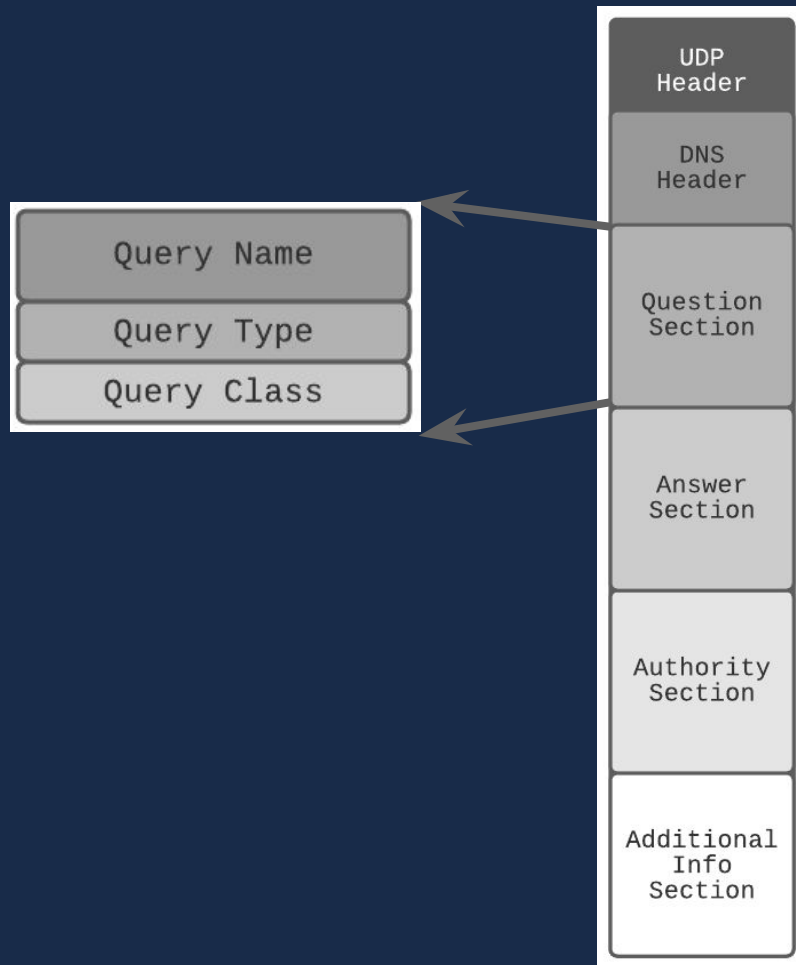| UDP Header |
| DNS Header |
| Question Section |
| Answer Section |
| Authority Section |
| Additional Info Section |

DNS Query Anatomy

Query Name (QNAME) -- Domain to resolve!

Query Class (QCLASS)

    CHAOS -- Used for debugging

    IN -- Internet

DNS Query Anatomy

Query Name (QNAME) -- Domain to resolve!

Query Class (QCLASS)
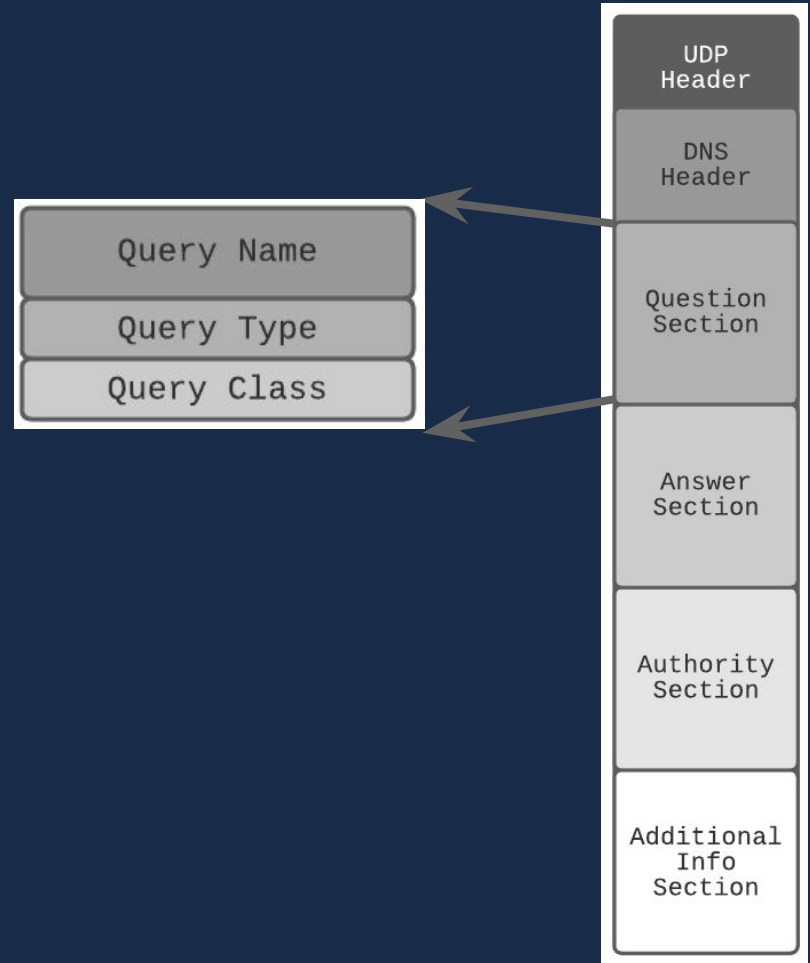
    CHAOS -- Used for debugging

    IN -- Internet

Query Type (QTYPE)

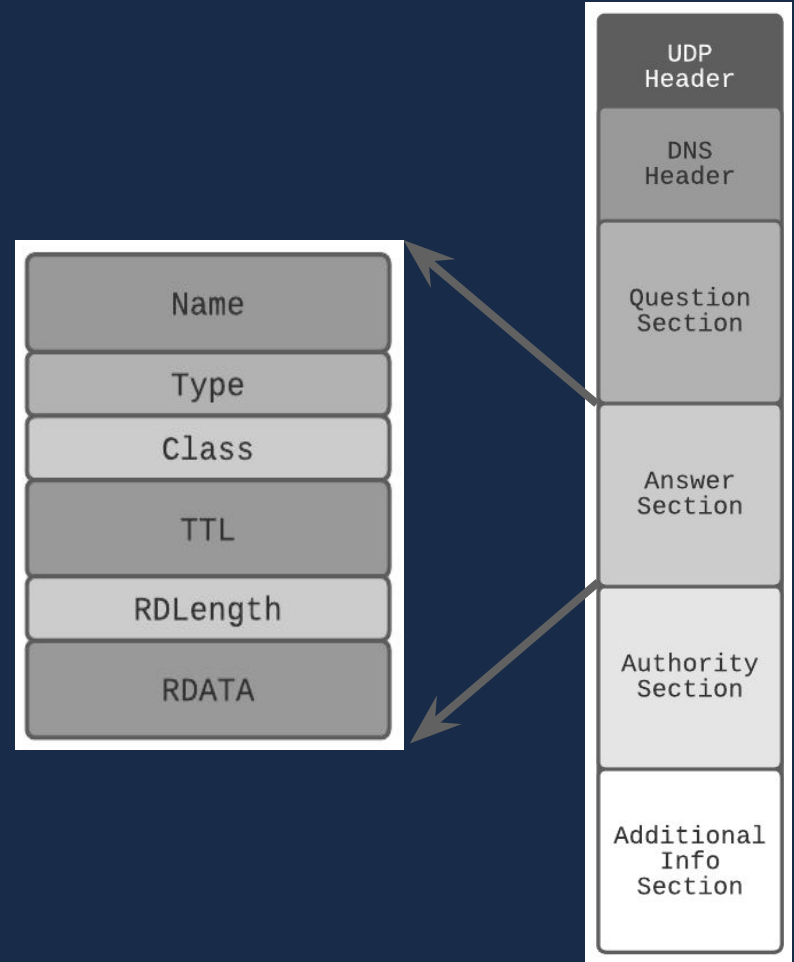   NS -- Authoritative nameserver for domain
    A -- IPv4 Address
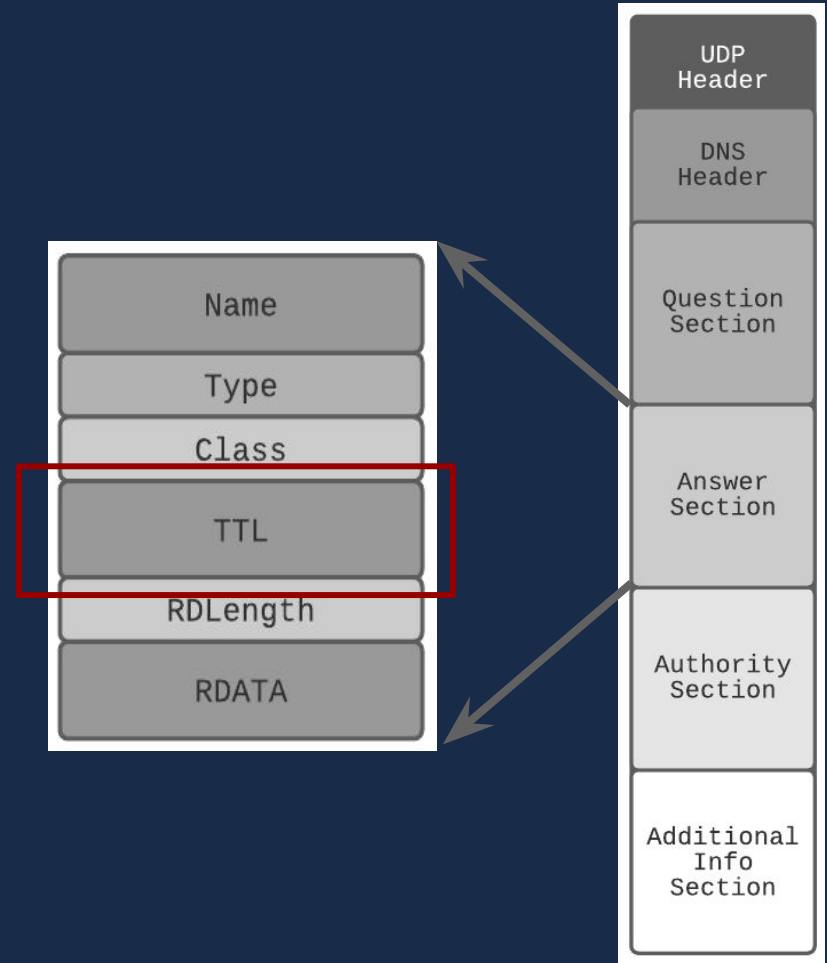   AAAA -- IPv6 Address
    MX -- Mail Exchange Records

Query Name
Query Type
Query Class

UDP Header
DNS Header
Question Section
Answer Section
Authority Section
Additional Info Section

DNS Query Anatomy

Name
Type
Class
TTL
RDLength
RDATA

UDP Header
DNS Header
Question Section
Answer Section
Authority Section
Additional Info Section

DNS Query Anatomy

TTL -- How long to cache answer

Caching

- Cache DNS Responses

  - Reduces load

  - Improves latency

  - Reuse of previous queries

- Negative Caching

- How long to cache?

  - Time To Live (TTL)

"The caching discipline of the
DNS works well, and
given the unexpectedly bad
performance of the
Internet, was essential to the
success of the system."

Live Demo

Discussion

Failures

Reliability

Integrity

Confidentiality

Discussion: Failures

- Why can a DNS query fail?

Discussion: Failures

- Misconfiguration?

  - Typos

  - Misconfigured authoritative nameserver

- Hardware/Network Failures

  - Unreachable Nameserver

- Large Traffic Volume

  - DoS Attacks

Discussion: Reliability

- Why use UDP? Why not TCP?

- Reliability through replication

    - Two authoritative nameserver per domain

    - What about root servers? TLD authoritative NS?

- Reliability across the entire life cycle?
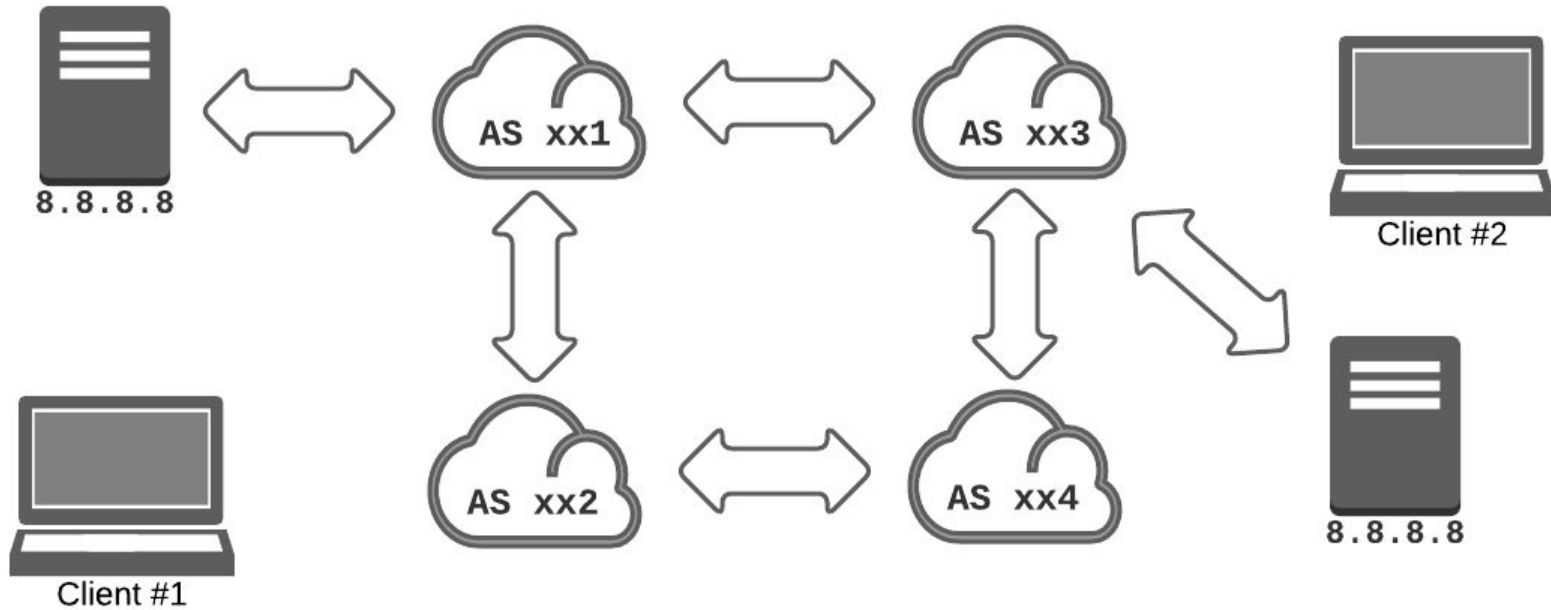
Discussion: Reliability

Root Servers

- Only 13 root servers?

Root Servers

- Only 13 root servers?

Anycast Primer

Anycast Primer
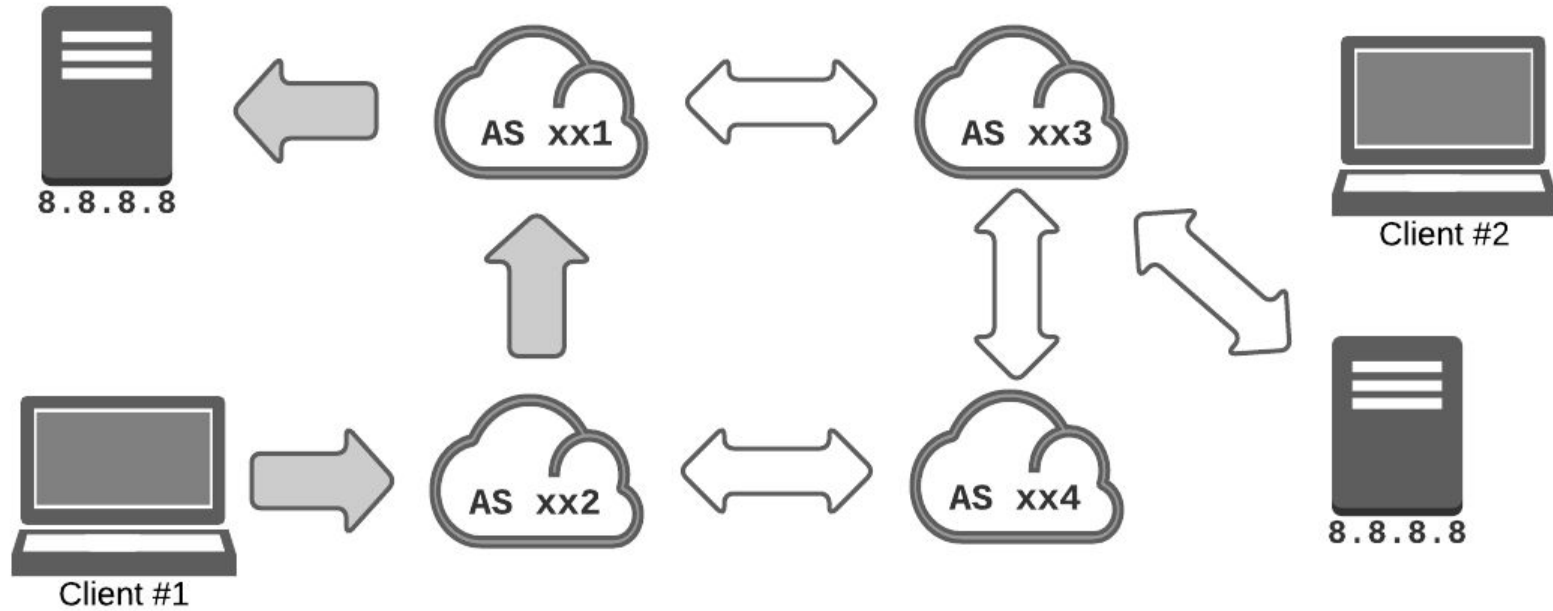
Anycast Primer

Discussion: Reliability

Discussion: Reliability
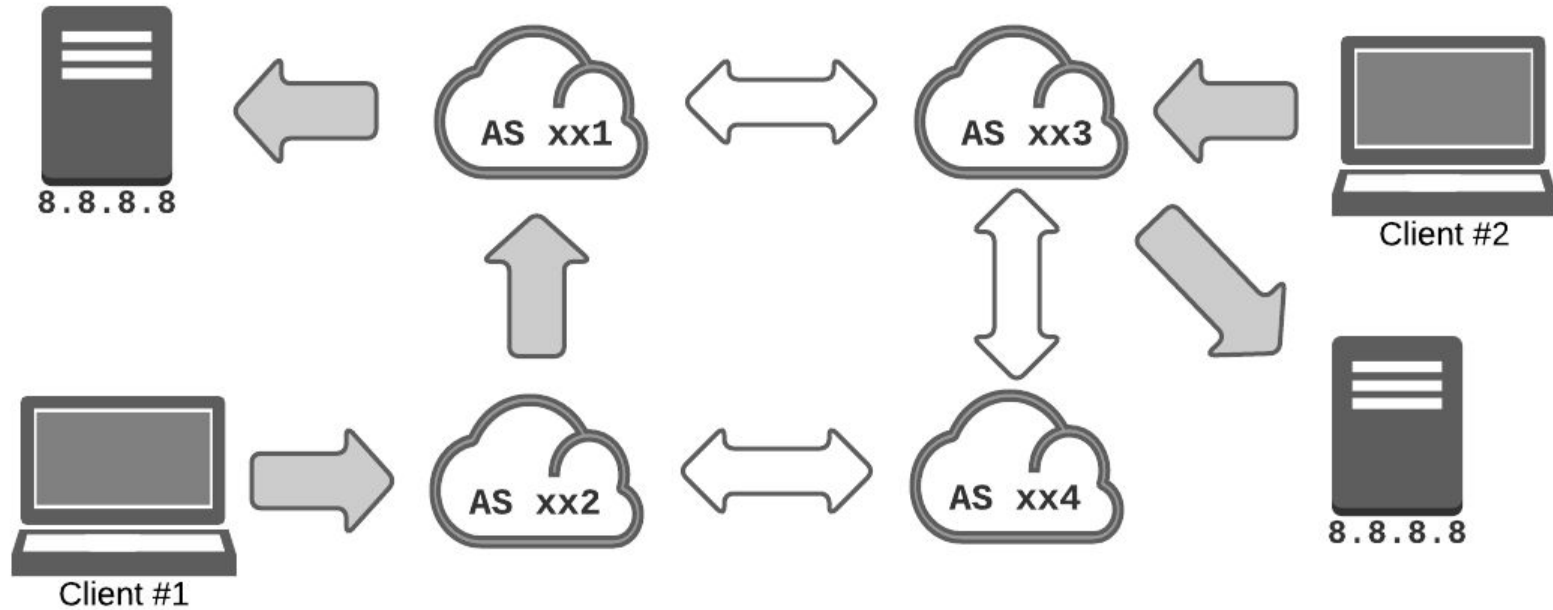
Discussion: Reliability

Client Stub Resolver — CPE Forwarder — Recursive Resolver

Root Authoritative NS

TLD Authoritative NS

Domain Authoritative NS

Discussion: Reliability

- Why use UDP? Why not TCP?

- Reliability through replication

  - Two authoritative nameserver per domain

  - What about root servers? TLD authoritative NS?

- Reliability across the entire life cycle?

- **Anycast adds another layer of reliability across the query life cycle!**

Discussion: Integrity

- Minimal security considerations in original DNS design.

- How to guarantee integrity of response?

  - Guarantee response has not been modified.

- But in order to do that, how to extend DNS?

# Extension Mechanisms for DNS (EDNS)
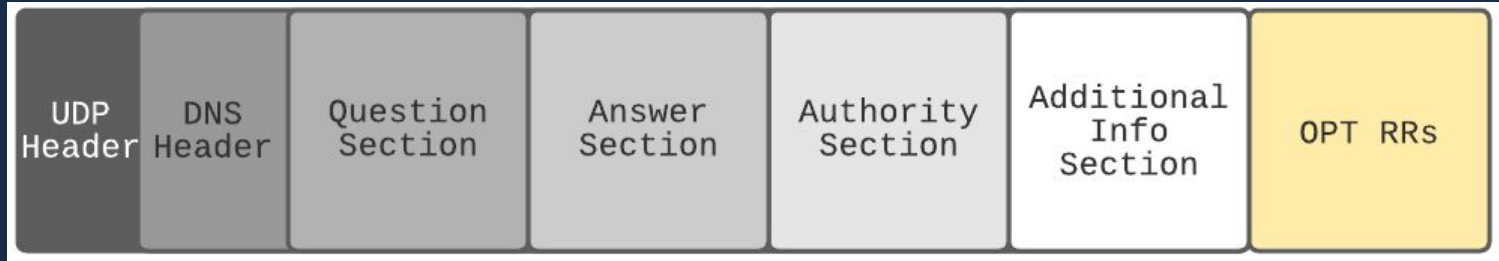
Add additional section to the end of a DNS packet.

EDNS sections skipped in old resolvers, and nameservers.

Used to implement DNSSEC, and ECS.

DNS Security Extension (DNSSEC)

- Add signature to DNS Records

  - Validate signature to ensure integrity of response

- Low adoption rate (though increasing)

- Not all resolvers support DNSSEC.

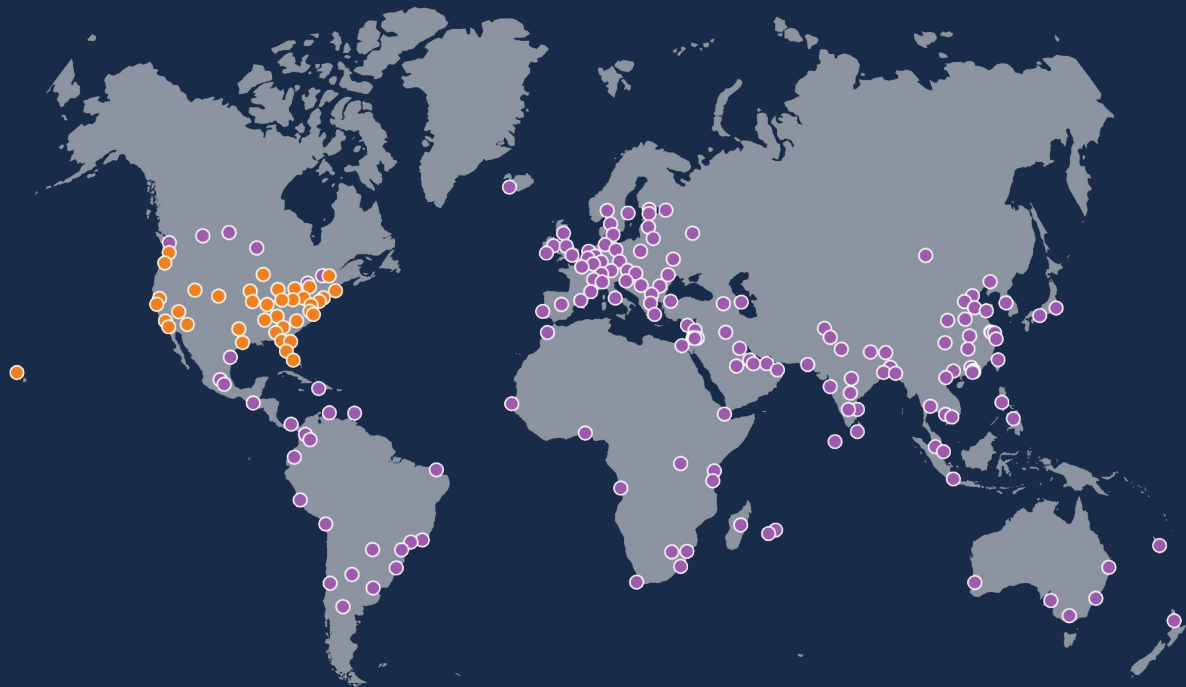 - Public DNS Resolvers support DNSSEC
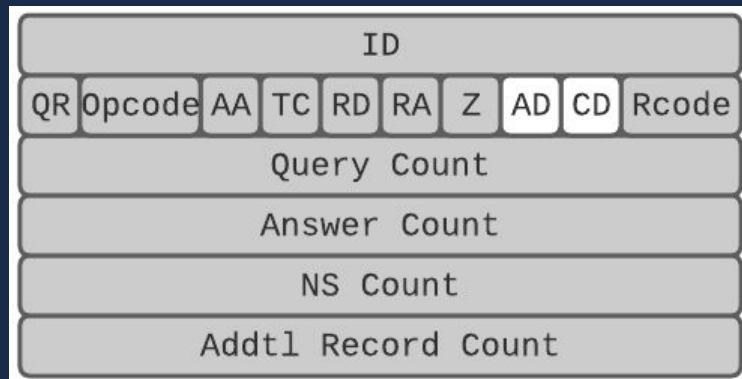
EDNS Client Subnet (ECS)

CDNs with large number of PoPs.

How to ensure response is mapped to closest PoP for client?

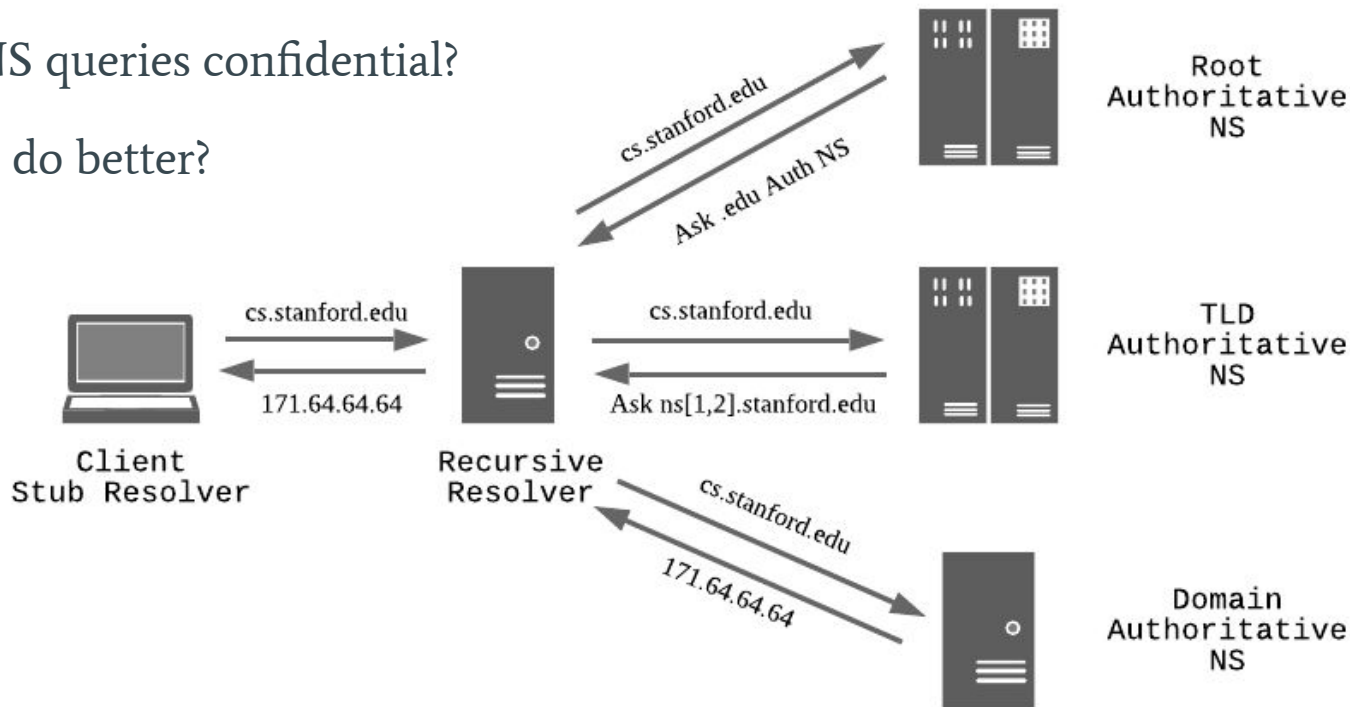ECS allows recursive resolvers to supply the prefix of client IP
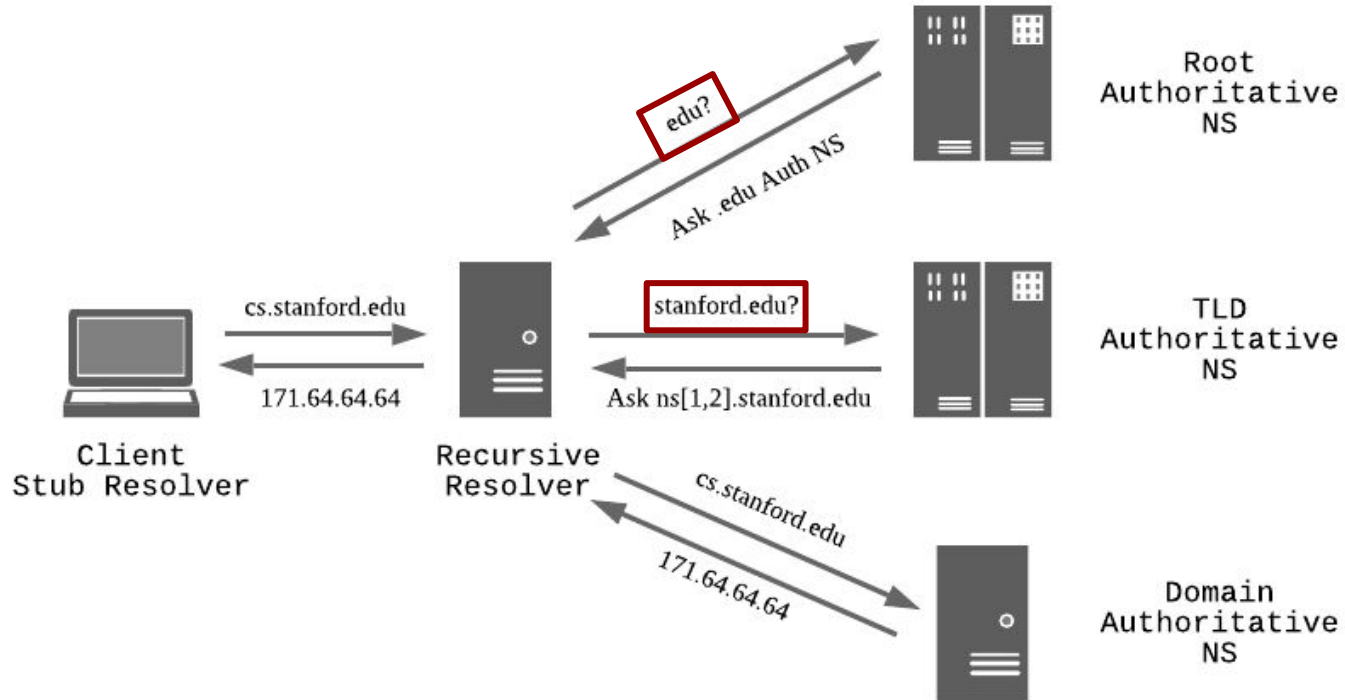
137.110.222.10 → 137.110.222.0/24

Discussion: Confidentiality

Are DNS queries confidential?

Can we do better?

QName Minimization

Encryption: DoH/DoT

DNS over HTTPs

DNS over TLS

Encrypted queries to recursive resolver?

Confidentiality? From whom?

What about ECS?

Questions?