CSCI 466: Networks

DNS

Reese Pearsall

Fall 2024

*All images are stolen from the internet

Announcements

Wireshark Lab 1 due **this Friday @ 11:59 PM**

PA1 Posted, due on **Sunday September 22nd**

OSI Model

Application Layer

Presentation Layer *

Session Layer *

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Application Layer

Messages from Network Applications

↓

Physical Layer

Bits being transmitted over a copper wire

**In the textbook, they condense it to a 5-layer model, but 7 layers is what is most used*

DNS

Humans browse the web using hostnames
- (They need English)

Computers understand numbers
- (They need IP addresses)

DNS

Humans browse the web using hostnames
- (They need English)

Computers understand numbers
- (They need IP addresses)

→ ??? → `153.90.127.197`

DNS

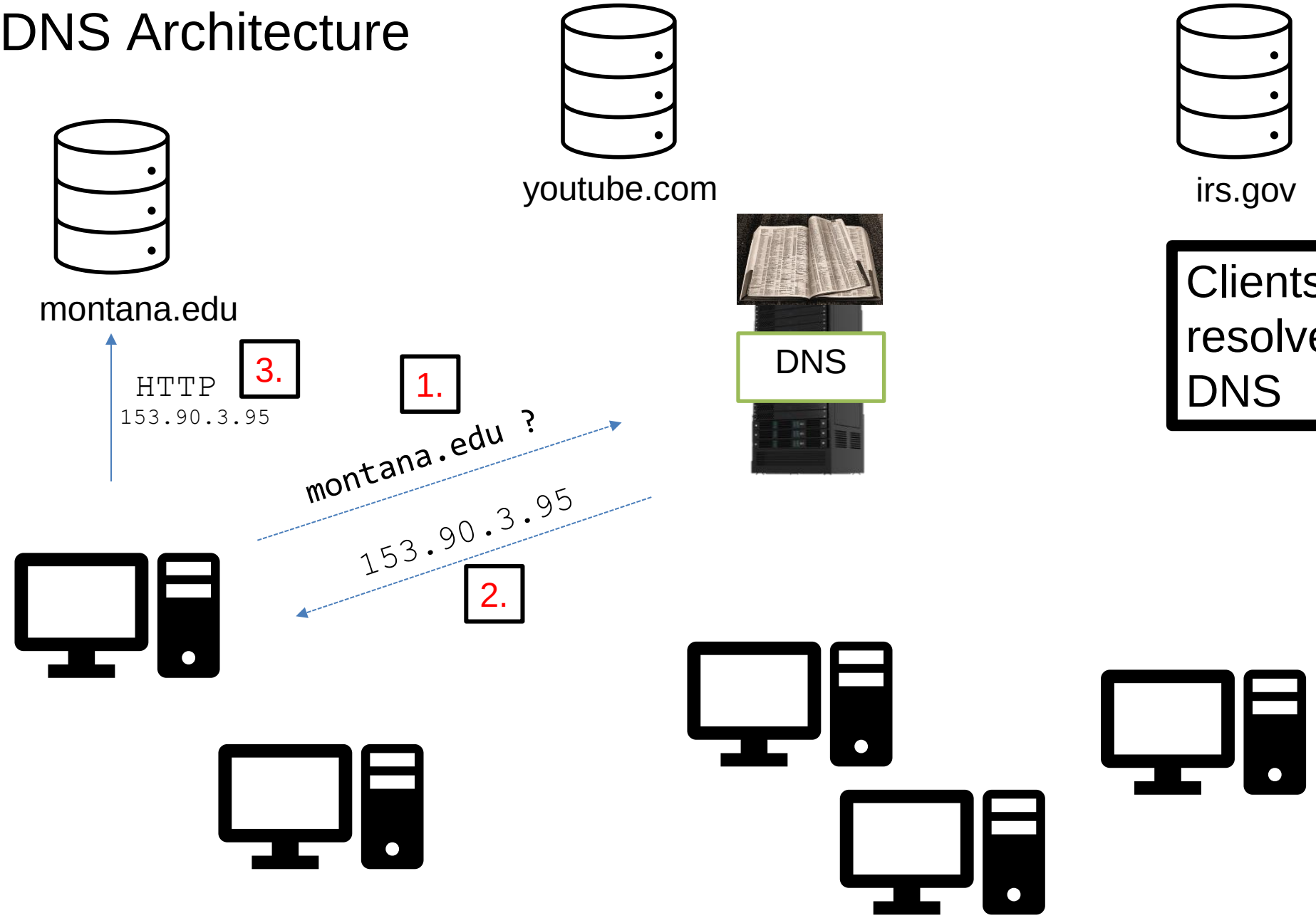
Humans browse the web using hostnames
- (They need English)

Computers understand numbers
- (They need IP addresses)

→ **DNS** → `153.90.127.197`

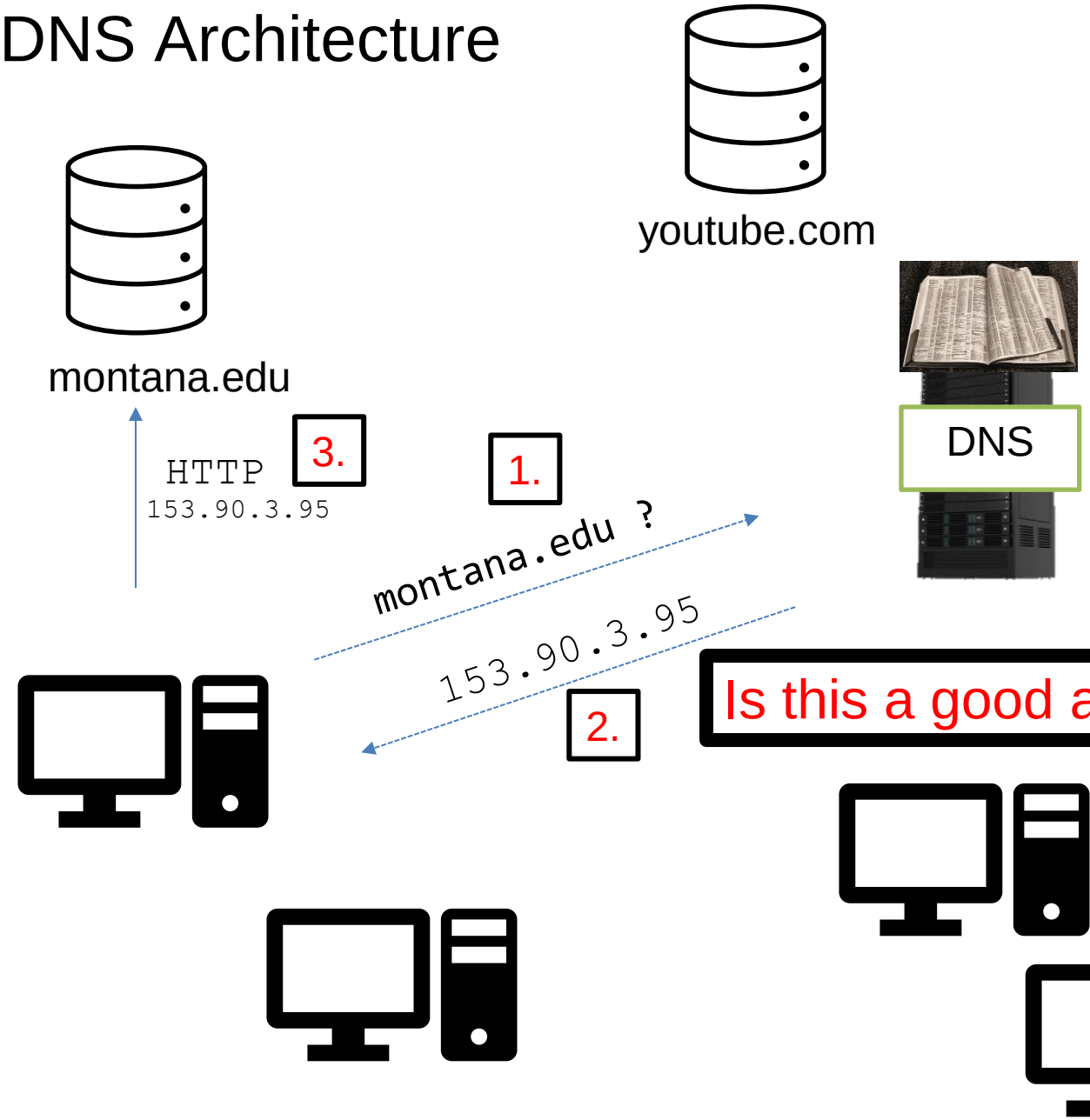
Domain Name System (DNS) is a database of mappings between hostnames and IP addresses

DNS Architecture



Clients will first need to resolve hostnames with DNS

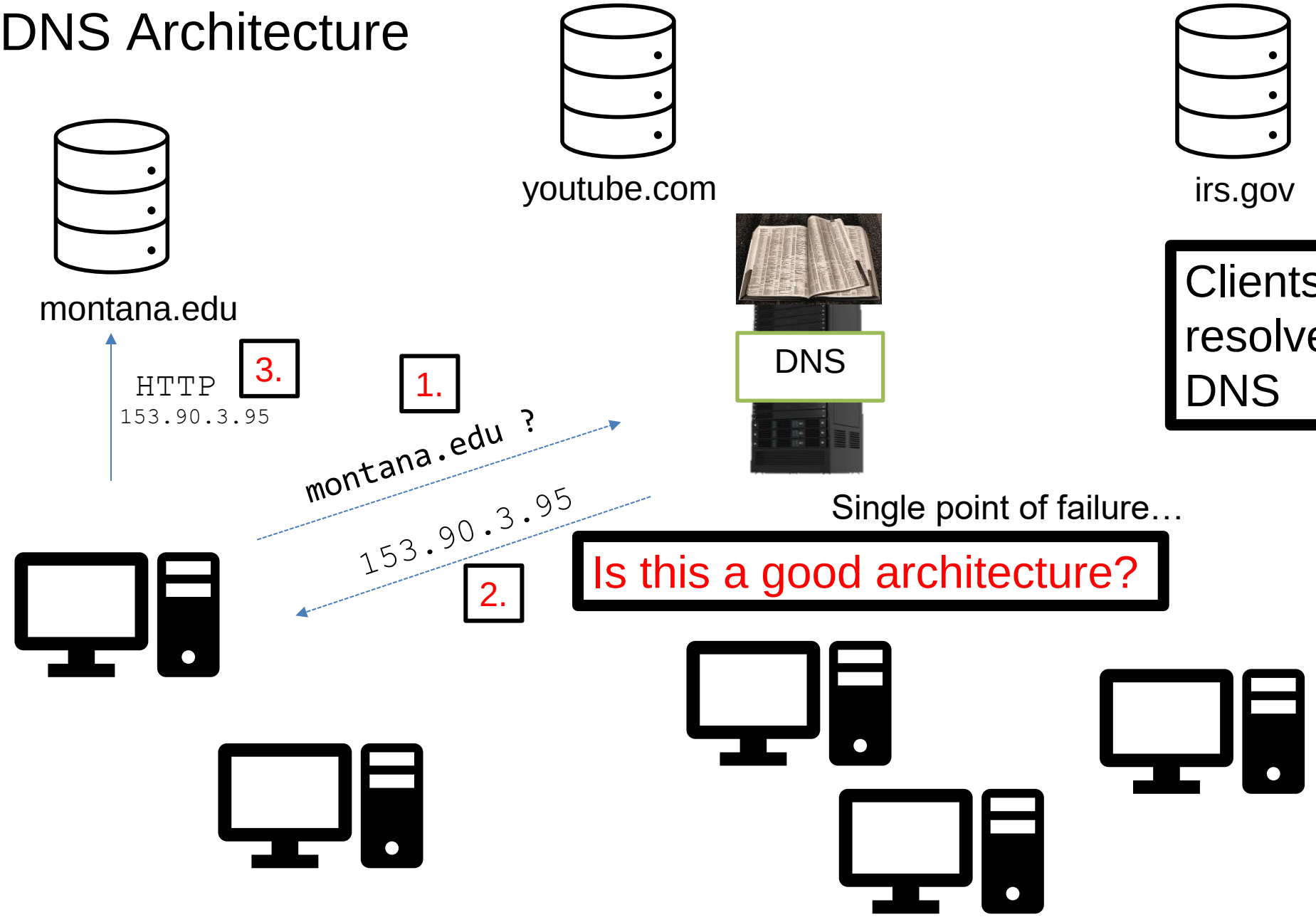
DNS Architecture



Clients will first need to resolve hostnames with DNS

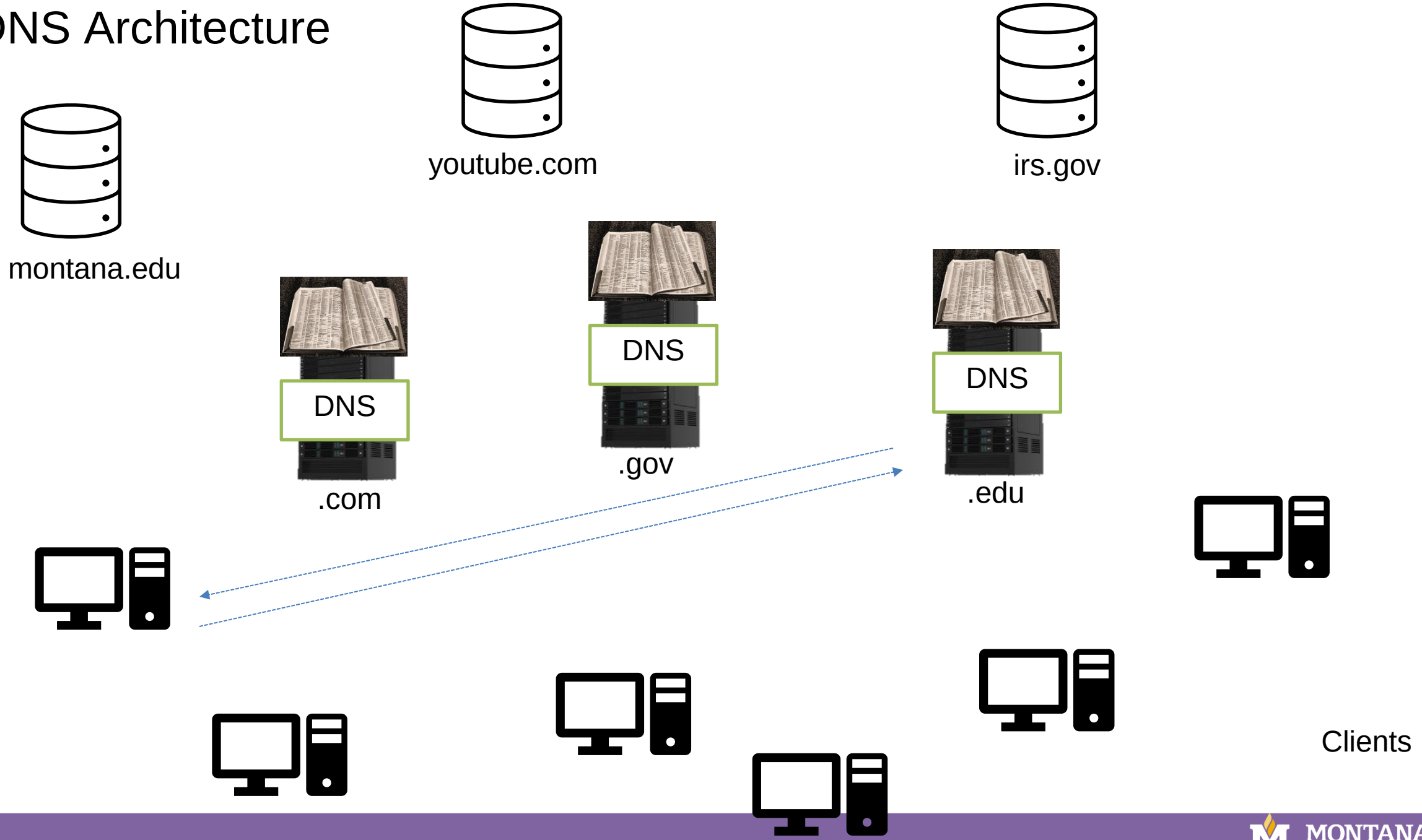
Is this a good architecture?

DNS Architecture



Clients will first need to resolve hostnames with DNS

DNS Architecture



DNS Architecture

(how big would that map be?)

- DNS is a **distributed**, **hierarchical** database (no DNS server has all the records!)

Hierarchy consists of different types of DNS servers:

DNS Architecture

- DNS is a **distributed**, **hierarchical** database (no DNS server has all the records!)

Hierarchy consists of different types of DNS servers:

Authoritative DNS servers- Organization's own DNS with up-to-date records

facebook.com DNS

amazon.com DNS

montana.edu DNS

harvard.edu DNS

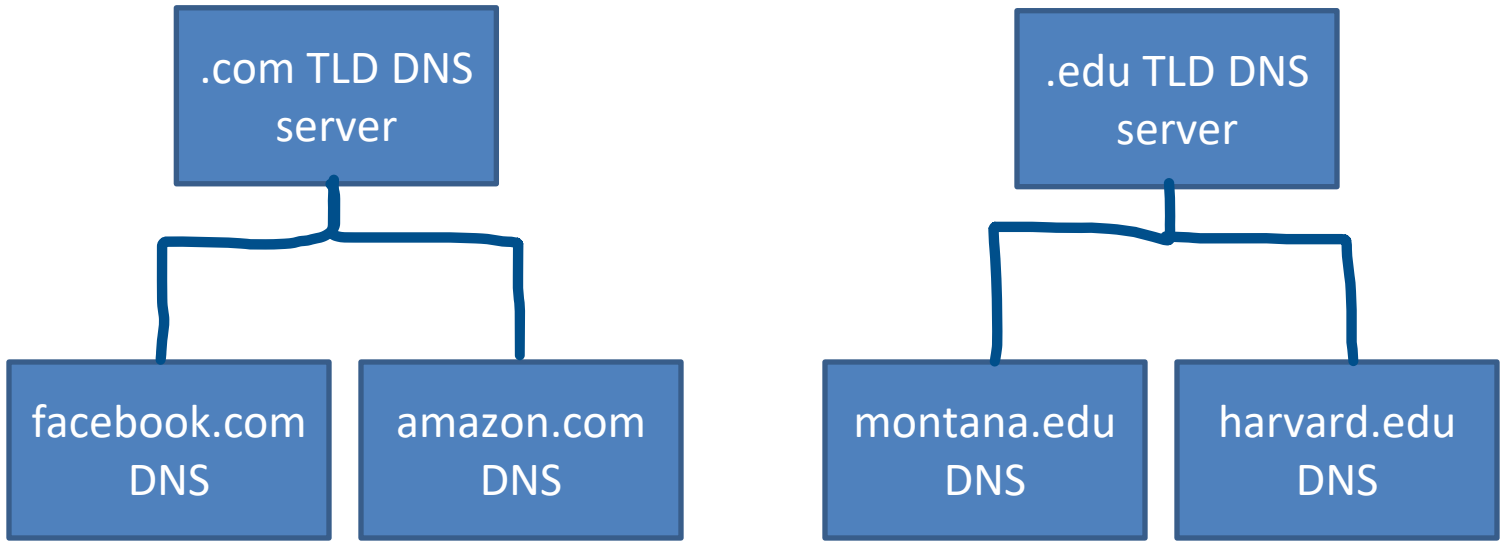
DNS Architecture

- DNS is a **distributed**, **hierarchical** database (no DNS server has all the records!)

Hierarchy consists of different types of DNS servers:

Authoritative DNS servers- Organization's own DNS with up-to-date records

Top-level domain (TLD) servers- responsible for keeping IP addresses for authoritative DNS servers for each top-level domain (.com, .edu, .jp, etc)



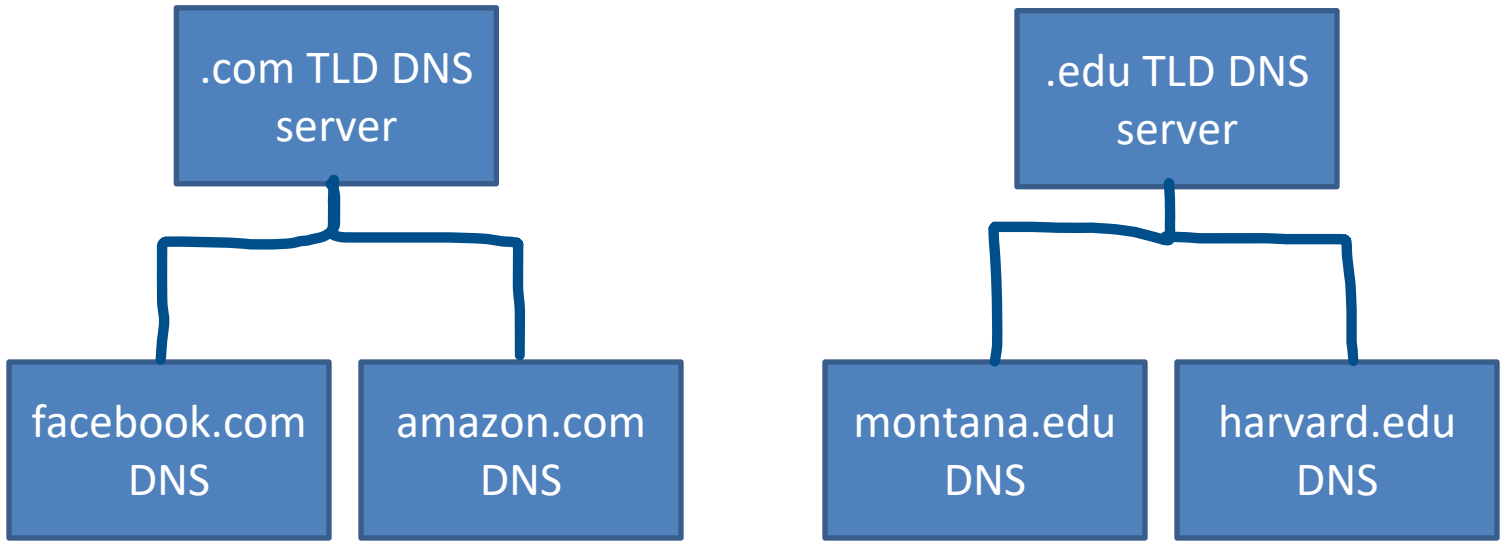
DNS Architecture

- DNS is a **distributed**, **hierarchical** database (no DNS server has all the records!)

Hierarchy consists of different types of DNS servers:

Authoritative DNS servers- Organization's own DNS with up-to-date records

Top-level domain (TLD) servers- responsible for keeping IP addresses for authoritative DNS servers for each top-level domain (.com, .edu, .jp, etc)



DNS Architecture

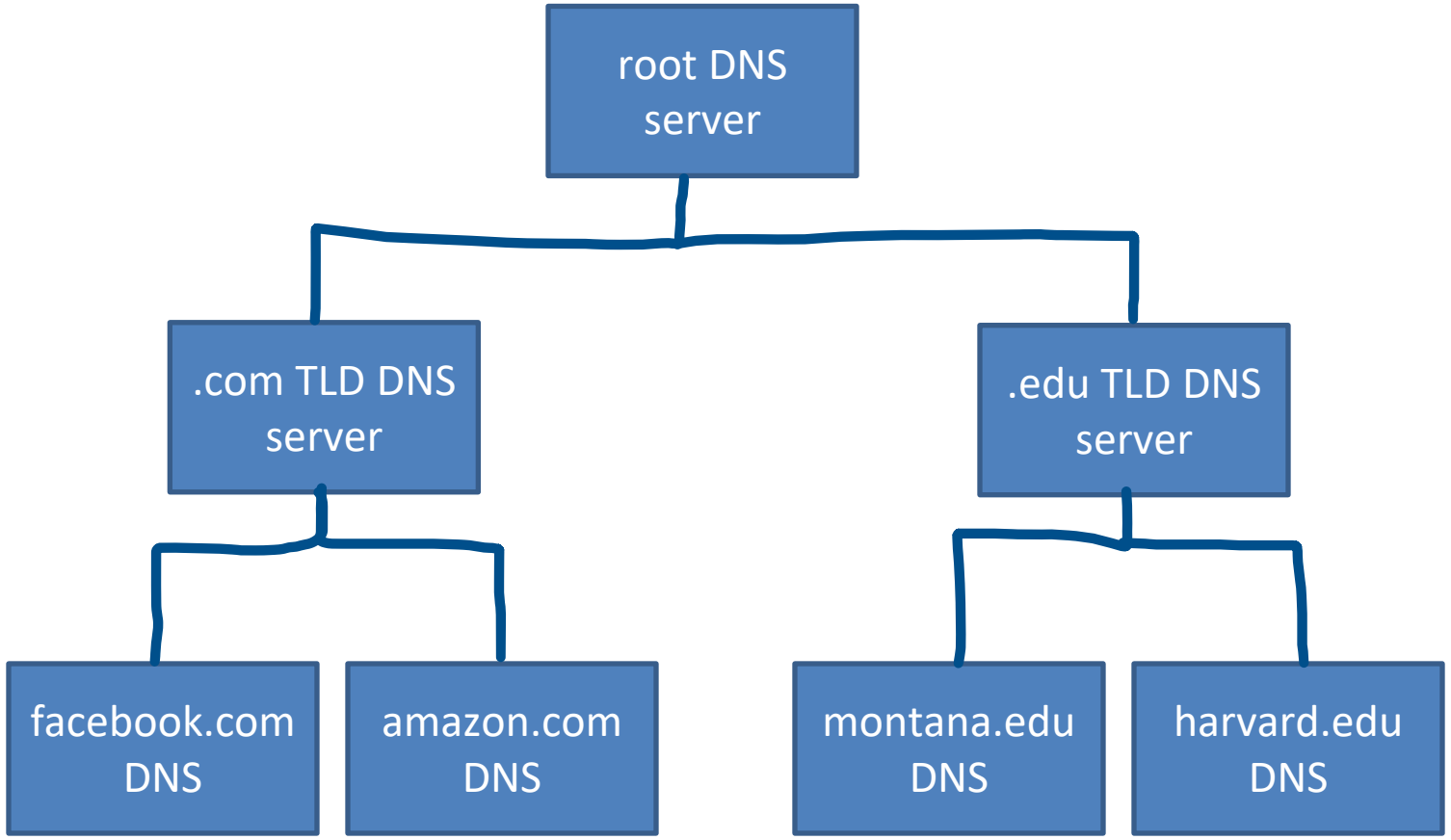
- DNS is a **distributed**, **hierarchical** database (no DNS server has all the records!)

Hierarchy consists of different types of DNS servers:

Authoritative DNS servers- Organization's own DNS with up-to-date records

Top-level domain (TLD) servers- responsible for keeping IP addresses for authoritative DNS servers for each top-level domain (.com, .edu, .jp, etc)

Root DNS servers- responsible for maintaining IP addresses for TLD servers



DNS Architecture

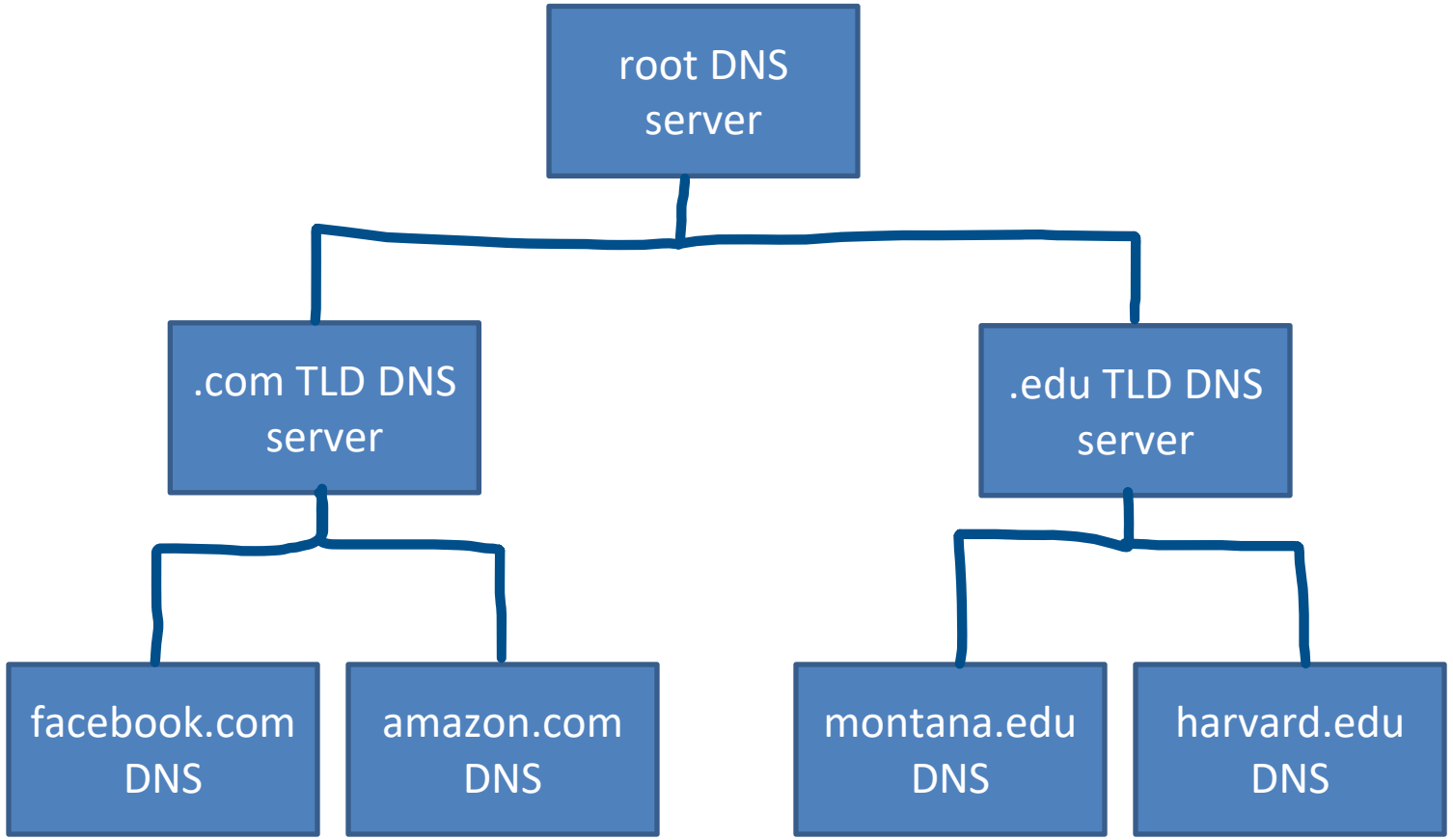
- DNS is a **distributed**, **hierarchical** database (no DNS server has all the records!)

Hierarchy consists of different types of DNS servers:

Authoritative DNS servers- Organization's own DNS with up-to-date records

Top-level domain (TLD) servers- responsible for keeping IP addresses for authoritative DNS servers for each top-level domain (.com, .edu, .jp, etc)

Root DNS servers- responsible for maintaining IP addresses for TLD servers



DNS Root server locations

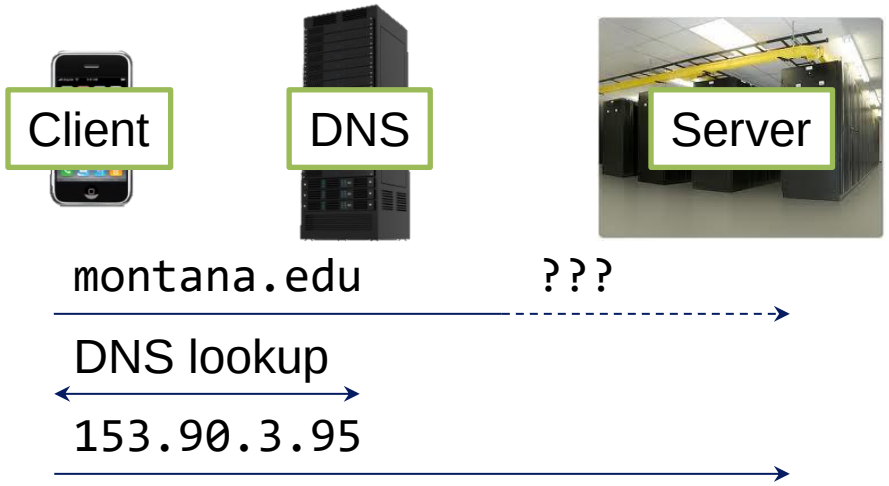
https://root-servers.org/

DNS

Application layer protocol

- Lookups over UDP on port 53

(handshake not needed)
(DNS requests are small)
(reliability can be added in the application layer)

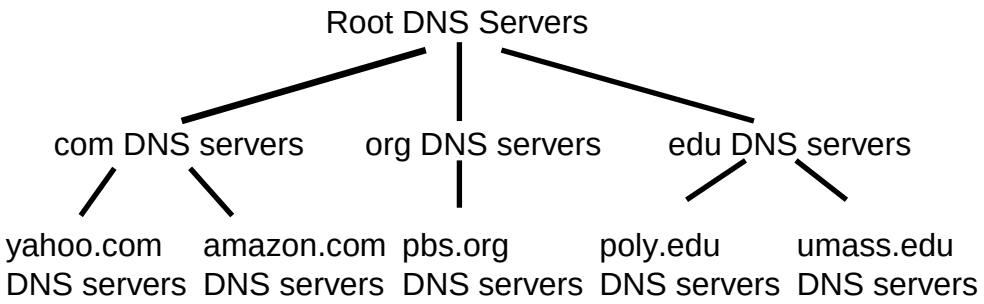


DNS provides hostname to IP mappings, host aliasing, mail server aliasing, and load distribution

Local DNS servers are also used

- Acts as a proxy
- Maintained by ISP
- Caches records

```
C:\Users\Reese Pearsall>ipconfig/displaydns

Windows IP Configuration

    www.gstatic.com
    ----------------------------------------
    Record Name . . . . . : www.gstatic.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 18
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 142.251.211.227
```



Some DNS records are also stored and maintained in your computer

- Any issues?? 👀

What if an IP address gets changed?

DNS Commands

```
[09/09/22]seed@VM:~$ host montana.edu
montana.edu has address 153.90.3.95
montana.edu has address 153.90.2.191
montana.edu mail is handled by 50 montana-edu.mail.protection.outlook.com.
[09/09/22]seed@VM:~$
```

153.90.3.95

- DNS services
  - Hostname to IP address translation

    `host montana.edu`
  - Hostname to IPv6 address translation
    - `host -t AAAA montana.edu`
  - Host aliasing

    `host -t CNAME img.huffingtonpost.com`
  - Mail server aliasing

    `host -t MX montana.edu`
  - Load distribution

    `host huffpost.com | grep "address" | sed -n -e 's/^.*address //p'`
  - Redirection
    - Look up same host from servers in different regions

    `host google.com 8.8.8.8`

(*nslookup* also works. This is what you will use in the lab)

DNS Commands

- DNS services
  - Hostname to IP address translation

    `host montana.edu`
  - Hostname to IPv6 address translation
    - `host -t AAAA montana.edu`
  - Host aliasing

    `host -t CNAME img.huffingtonpost.com`
  - Mail server aliasing

    `host -t MX montana.edu`
  - Load distribution

    `host huffpost.com | grep "address" | sed -n -e 's/^.*address //p'`
  - Redirection
    - Look up same host from servers in different regions

    `host google.com 8.8.8.8`

```
[09/09/22]seed@VM:~$ host -t AAAA montana.edu
montana.edu has no AAAA record
[09/09/22]seed@VM:~$
```

DNS Commands

- DNS services
  - Hostname to IP address translation

    `host montana.edu`
  - Hostname to IPv6 address translation
    - `host -t AAAA montana.edu`
  - Host aliasing

    `host -t CNAME img.huffingtonpost.com`
  - Mail server aliasing

    `host -t MX montana.edu`
  - Load distribution

    `host huffpost.com | grep "address" | sed -n -e 's/^.*address //p'`
  - Redirection
    - Look up same host from servers in different regions

    `host google.com 8.8.8.8`

```
[09/09/22]seed@VM:~$ host -t CNAME img.huffingtonpost.com
img.huffingtonpost.com is an alias for buzzfeed2.map.fastly.net.
[09/09/22]seed@VM:~$
```

DNS Commands

- DNS services
  - Hostname to IP address translation

    `host montana.edu`
  - Hostname to IPv6 address translation
    - `host -t AAAA montana.edu`
  - Host aliasing

    `host -t CNAME img.huffingtonpost.com`
  - Mail server aliasing

    `host -t MX montana.edu`

```
[09/09/22]seed@VM:~$ host -t MX montana.edu
montana.edu mail is handled by 50 montana-edu.mail.protection.outlook.com.
```

  - Load distribution

    `host huffpost.com | grep "address" | sed -n -e 's/^.*address //p'`
  - Redirection
    - Look up same host from servers in different regions

    `host google.com 8.8.8.8`

DNS Commands

- DNS services
  - Hostname to IP address translation

    `host montana.edu`
  - Hostname to IPv6 address translation
    - `host -t AAAA montana.edu`
  - Host aliasing

    `host -t CNAME img.huffingtonpost.com`
  - Mail server aliasing

    `host -t MX montana.edu`
  - Load distribution

    `host huffpost.com | grep "address" | sed -n -e 's/^.*address //p'`
  - Redirection
    - Look up same host from servers in different regions

    `host google.com 8.8.8.8`

```
[09/09/22]seed@VM:~$ host huffpost.com | grep "address" | sed -n -e 's/^.*addres
s //p'
108.138.94.40
108.138.94.73
108.138.94.78
108.138.94.30
[09/09/22]seed@VM:~$ host huffpost.com | grep "address" | sed -n -e 's/^.*addres
s //p'
108.138.94.30
108.138.94.78
108.138.94.73
108.138.94.40
```

Rotation!

DNS Commands

- DNS services
  - Hostname to IP address translation

    `host montana.edu`
  - Hostname to IPv6 address translation
    - `host -t AAAA montana.edu`
  - Host aliasing

    `host -t CNAME img.huffingtonpost.com`
  - Mail server aliasing

    `host -t MX montana.edu`
  - Load distribution

    `host huffpost.com | grep "address" | sed -n -e 's/^.*address //p'`
  - Redirection
    - Look up same host from servers in different regions

    `host google.com 8.8.8.8`

```
[09/09/22]seed@VM:~$ host google.com 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

google.com has address 172.217.14.206
google.com has IPv6 address 2607:f8b0:400a:80a::200e
google.com mail is handled by 10 smtp.google.com.
[09/09/22]seed@VM:~$ host google.com
google.com has address 142.251.211.238
google.com has IPv6 address 2607:f8b0:400a:804::200e
google.com mail is handled by 10 smtp.google.com.
```

!!!

DNS Commands

- DNS services
  - Hostname to IP address translation

    `host montana.edu`
  - Hostname to IPv6 address translation
    - `host -t AAAA montana.edu`
  - Host aliasing

    `host -t CNAME img.huffingtonpost.com`
  - Mail server aliasing

    `host -t MX montana.edu`
  - Load distribution

    `host huffpost.com | grep "address" | sed -n -e 's/^.*address //p'`
  - Redirection
    - Look up same host from servers in different regions

    `host google.com 8.8.8.8`

See cached DNS entries on computer

- `ipconfig/displaydns`

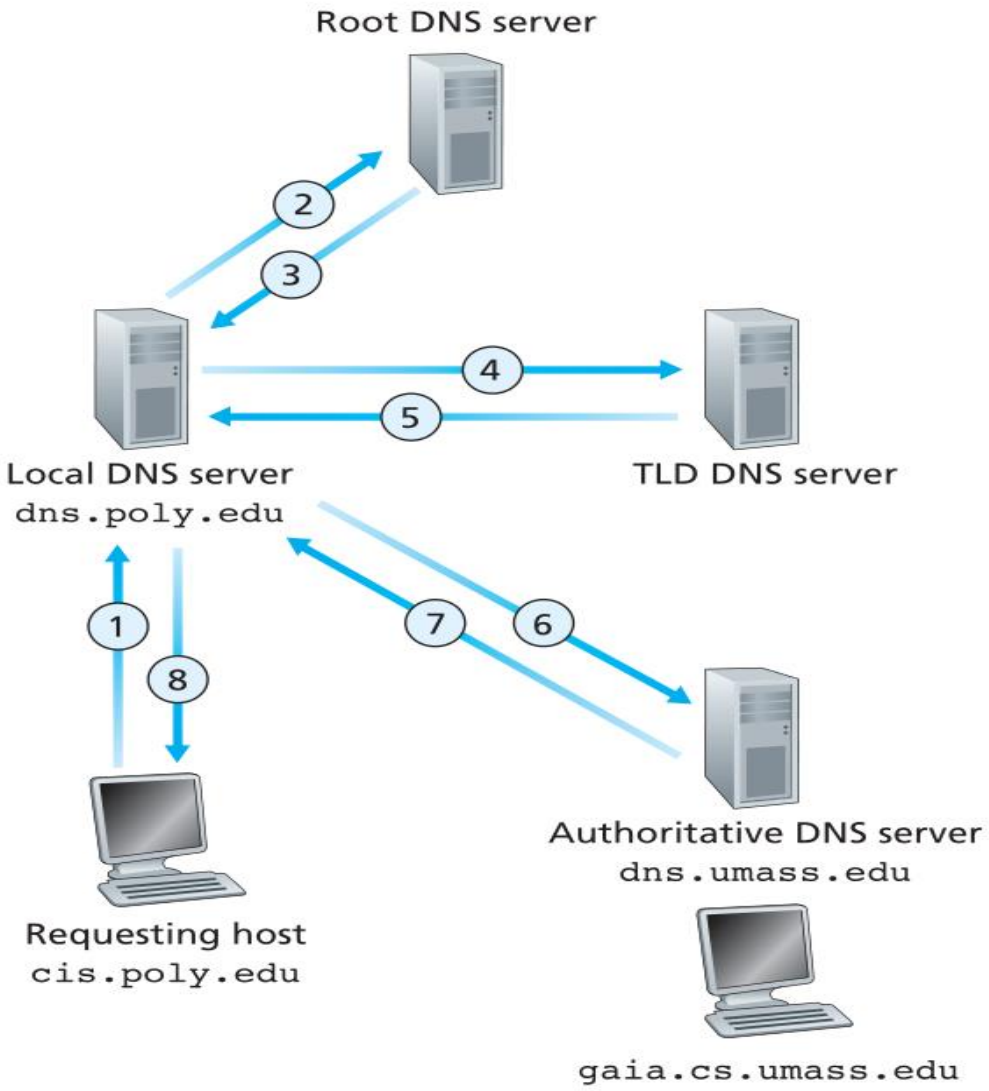
```
C:\Users\Reese Pearsall>ipconfig/displaydns

Windows IP Configuration

    safebrowsing.googleapis.com
    ----------------------------------------
    Record Name . . . . . : safebrowsing.googleapis.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 34
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 142.250.69.202
```

```
www.cs.montana.edu
----------------------------------------
Record Name . . . . . : www.cs.montana.edu
Record Type . . . . . : 5
Time To Live  . . . . : 3002
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : web1.cs.montana.edu


Record Name . . . . . : web1.cs.montana.edu
Record Type . . . . . : 1
Time To Live  . . . . : 3002
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 153.90.127.197
```

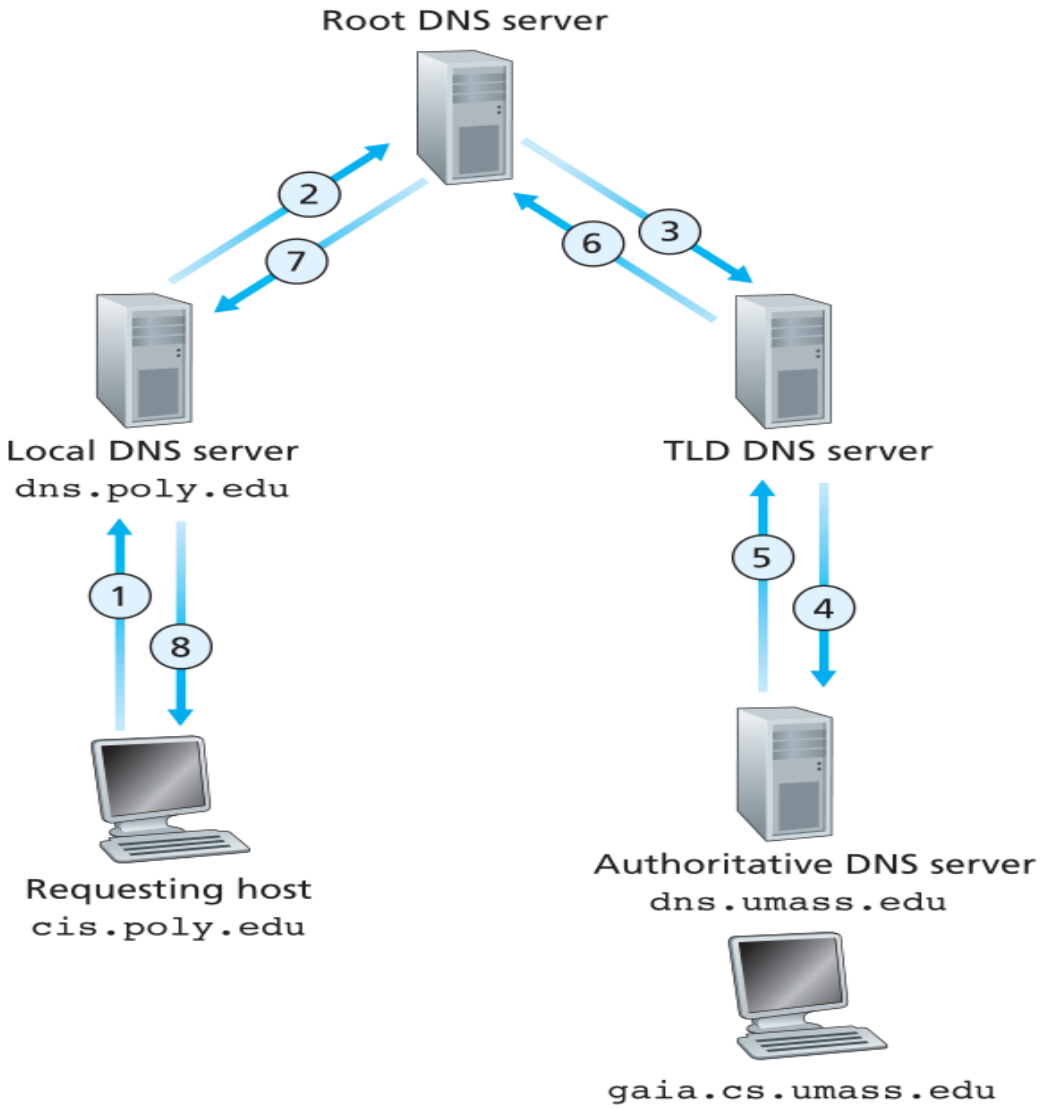
```
www.tcpipguide.com
----------------------------------------
Record Name . . . . . : www.tcpipguide.com
Record Type . . . . . : 5
Time To Live  . . . . : 1543
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record  . . . . : tcpipguide.com


Record Name . . . . . : tcpipguide.com
Record Type . . . . . : 1
Time To Live  . . . . : 1543
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 216.92.67.219
```

```
calendar.google.com
----------------------------------------
Record Name . . . . . : calendar.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 144
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 142.251.211.238
```

DNS Requests

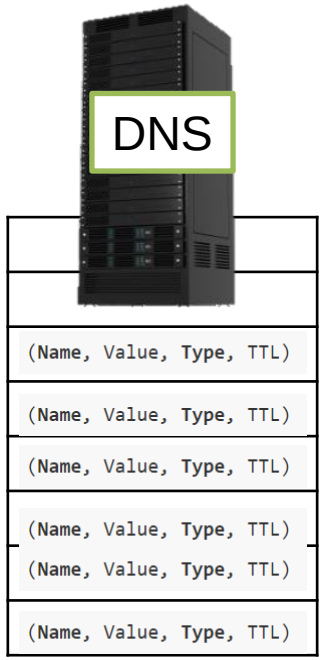


Iterative Lookup



Recursive Lookup

DNS Response Records

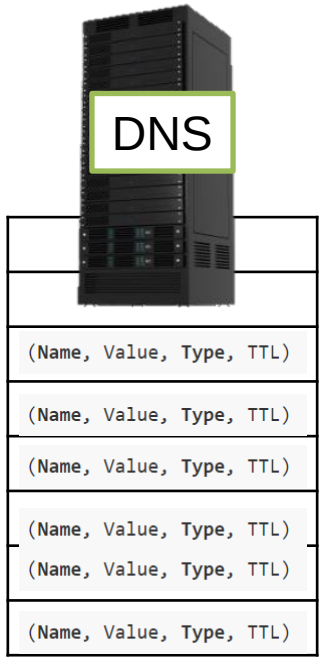


DNS servers store **resource records (RRs)**

RR is a four-tuple

```
(Name, Value, Type, TTL)
```

DNS Response Records



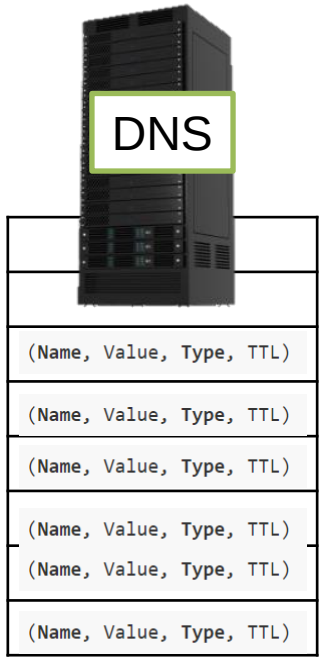
DNS servers store **resource records (RRs)**

RR is a four-tuple

```
(Name, Value, Type, TTL)
```

TTL – “Time to Live”. Determines when a resource should be removed from a cache

DNS Response Records



DNS servers store **resource records (RRs)**

RR is a four-tuple

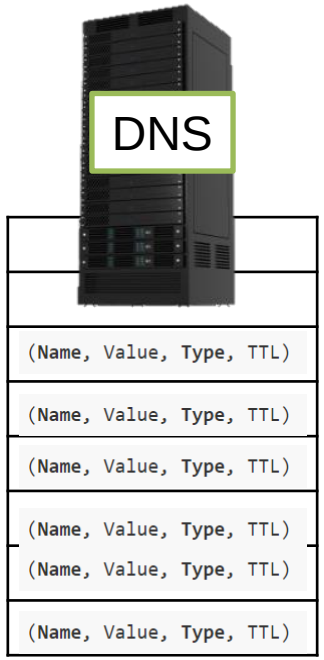
```
(Name, Value, Type, TTL)
```

TTL – "Time to Live". Determines when a resource should be removed from a cache

Type – type of record

- Type **A** – IPv4 address
- Type **AAAA** – IPv6 address
- Type **NS** – Authoritative DNS hostname
  (`foo.com`, `dns.foo.com`)
- Type **CNAME** – Canonical hostname for an alias
  (`foo.com`, `items.foo.com`)
- Type **MX-** Canonical name for a mail server
  (`foo.com`, `mail.foo.com`)

DNS Response Records



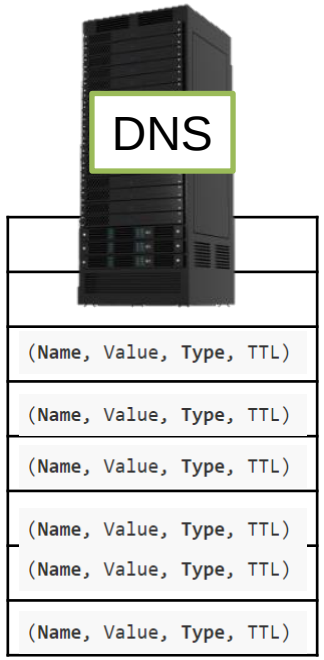
DNS servers store **resource records (RRs)**

RR is a four-tuple

```
(Name, Value, Type, TTL)
```

```
(foo.com, 145.37.93.126, A, 24)
(foo.com, 0913:cc84:9414:59e6:ae63:7299:dae5:b2f9, AAAA, 24)
(foo.com, mail.foo.com, MX, 24)
(foo.com, dns.foo.com, NS, 24)
(foo.com, items.foo.com, CNAME, 24)
```

DNS Response Records



DNS servers store **resource records (RRs)**

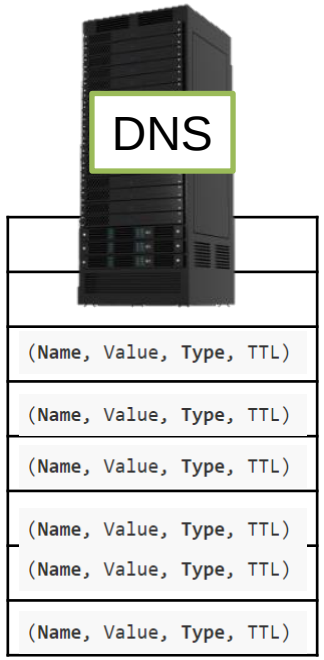
RR is a four-tuple

```
(Name, Value, Type, TTL)
```

```
(foo.com, 145.37.93.126, A, 24)
(foo.com, 0913:cc84:9414:59e6:ae63:7299:dae5:b2f9, AAAA, 24)
(foo.com, mail.foo.com, MX, 24)
(foo.com, dns.foo.com, NS, 24)
(foo.com, items.foo.com, CNAME, 24)
```

If a nameserver is authoritative for a particular domain, it will have type A record(s) for the hostname

DNS Response Records



DNS servers store **resource records (RRs)**

RR is a four-tuple

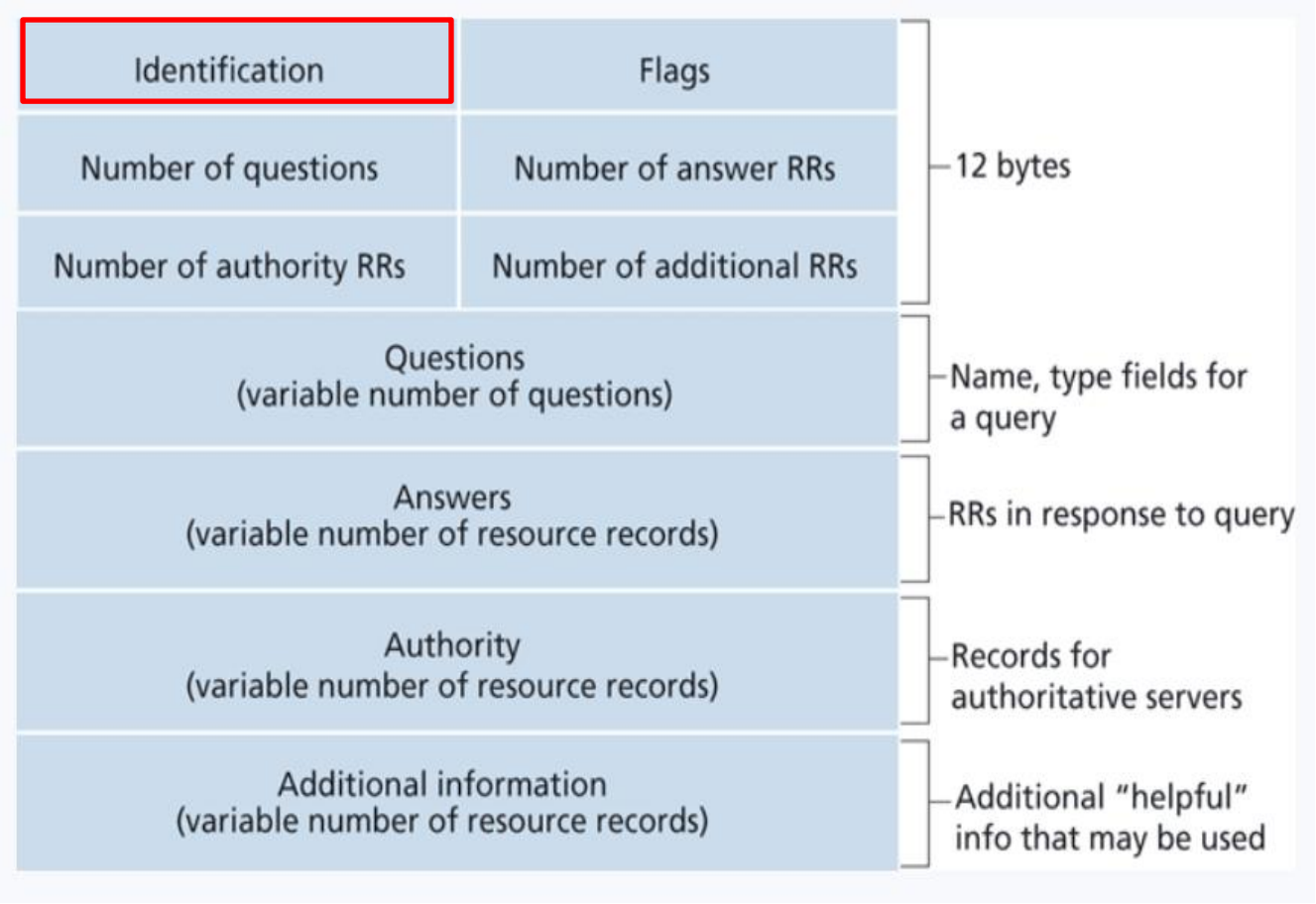
```
(Name, Value, Type, TTL)
```

```
(foo.com, 145.37.93.126, A, 24)
(foo.com, 0913:cc84:9414:59e6:ae63:7299:dae5:b2f9, AAAA, 24)
(foo.com, mail.foo.com, MX, 24)
(foo.com, dns.foo.com, NS, 24)
(foo.com, items.foo.com, CNAME, 24)
```

If a nameserver is authoritative for a particular domain, it will have type A record(s) for the hostname

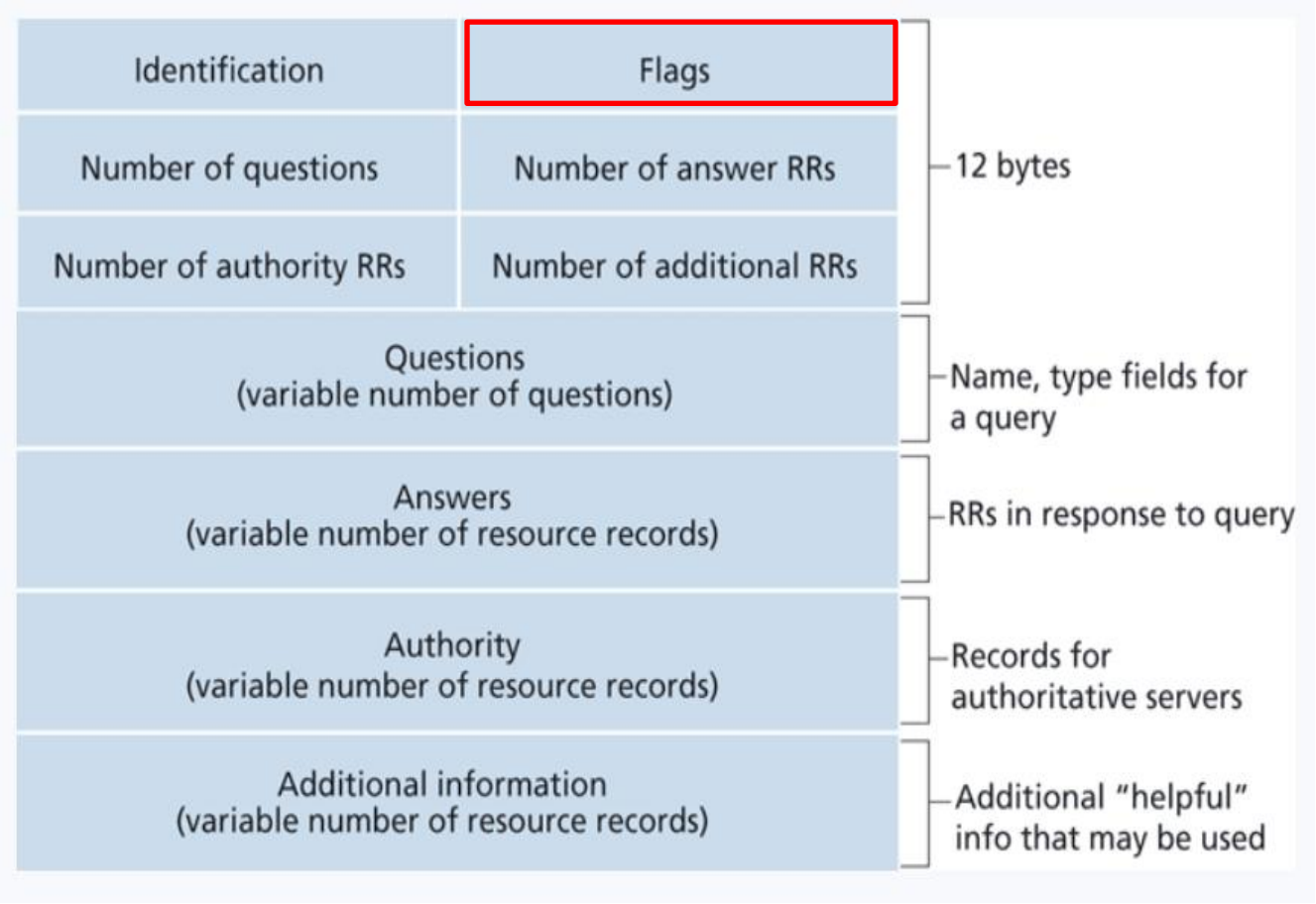
Otherwise, it will have NS records for the DNS server that does know the answer

DNS Requests *(The format of a DNS request packet)*



ID number for the query. Used to match a request to its response easily

DNS Requests *(The format of a DNS request packet)*

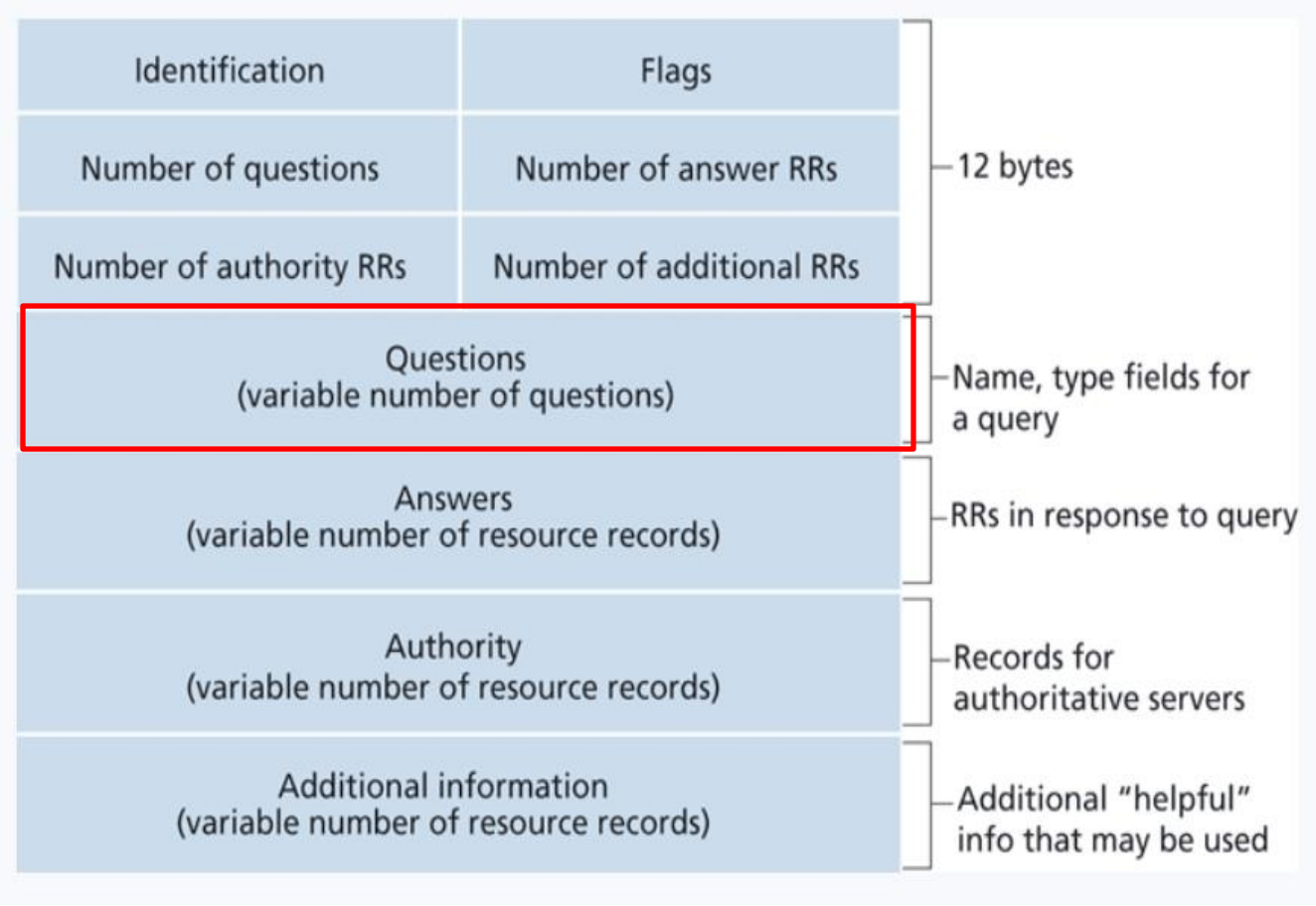


ID number for the query. Used to match a request to its response easily

A set of 0/1 that provide information about the query

- Is it authoritative?
- Is it a response or a query?
- Should it be done recursively?

DNS Requests *(The format of a DNS request packet)*



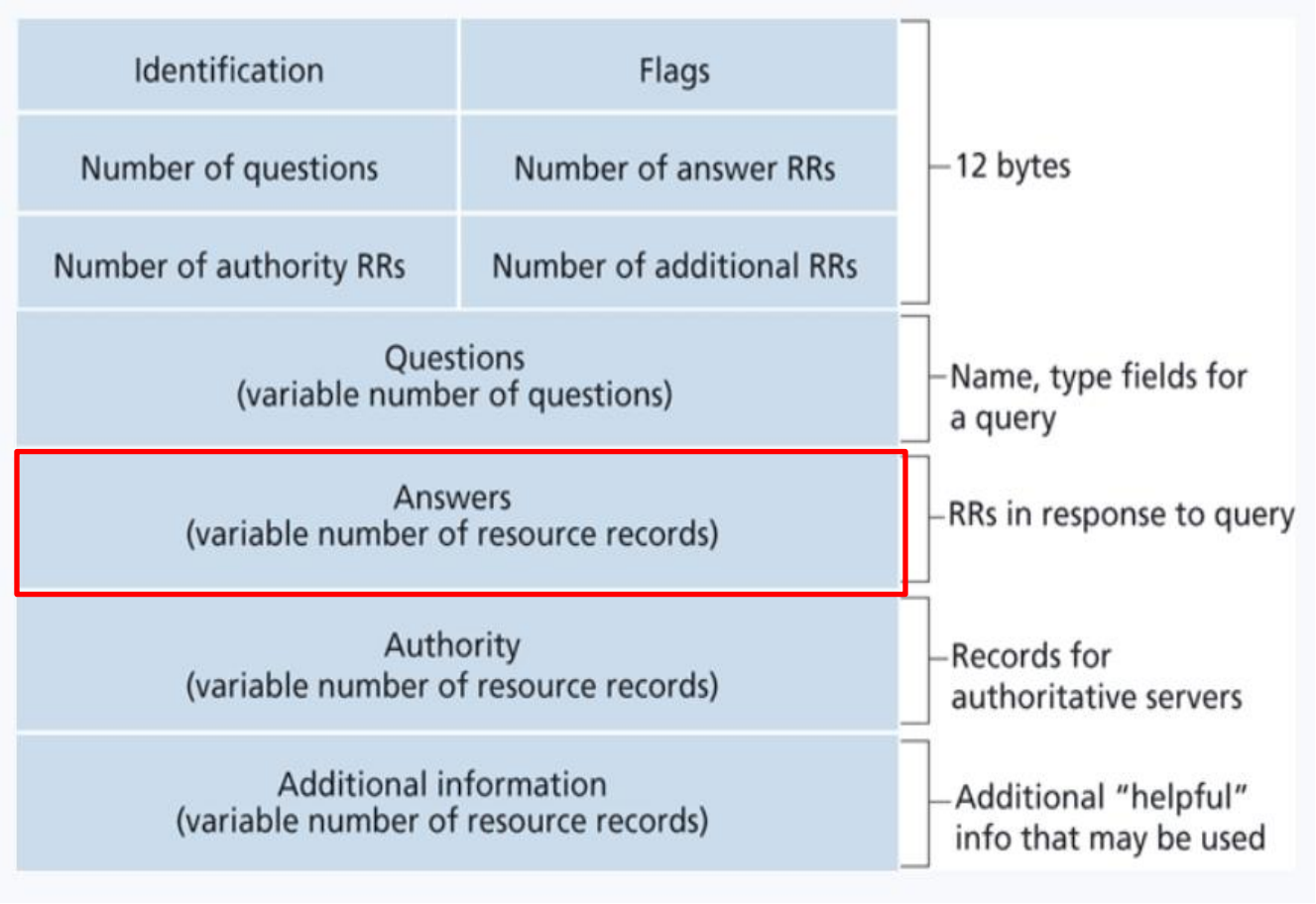
ID number for the query. Used to match a request to its response easily

A set of 0/1 that provide information about the query

- Is it authoritative?
- Is it a response or a query?
- Should it be done recursively?

What question is the query asking?
(ie. type `A` for wikipedia.com)

DNS Requests *(The format of a DNS request packet)*



ID number for the query. Used to match a request to its response easily

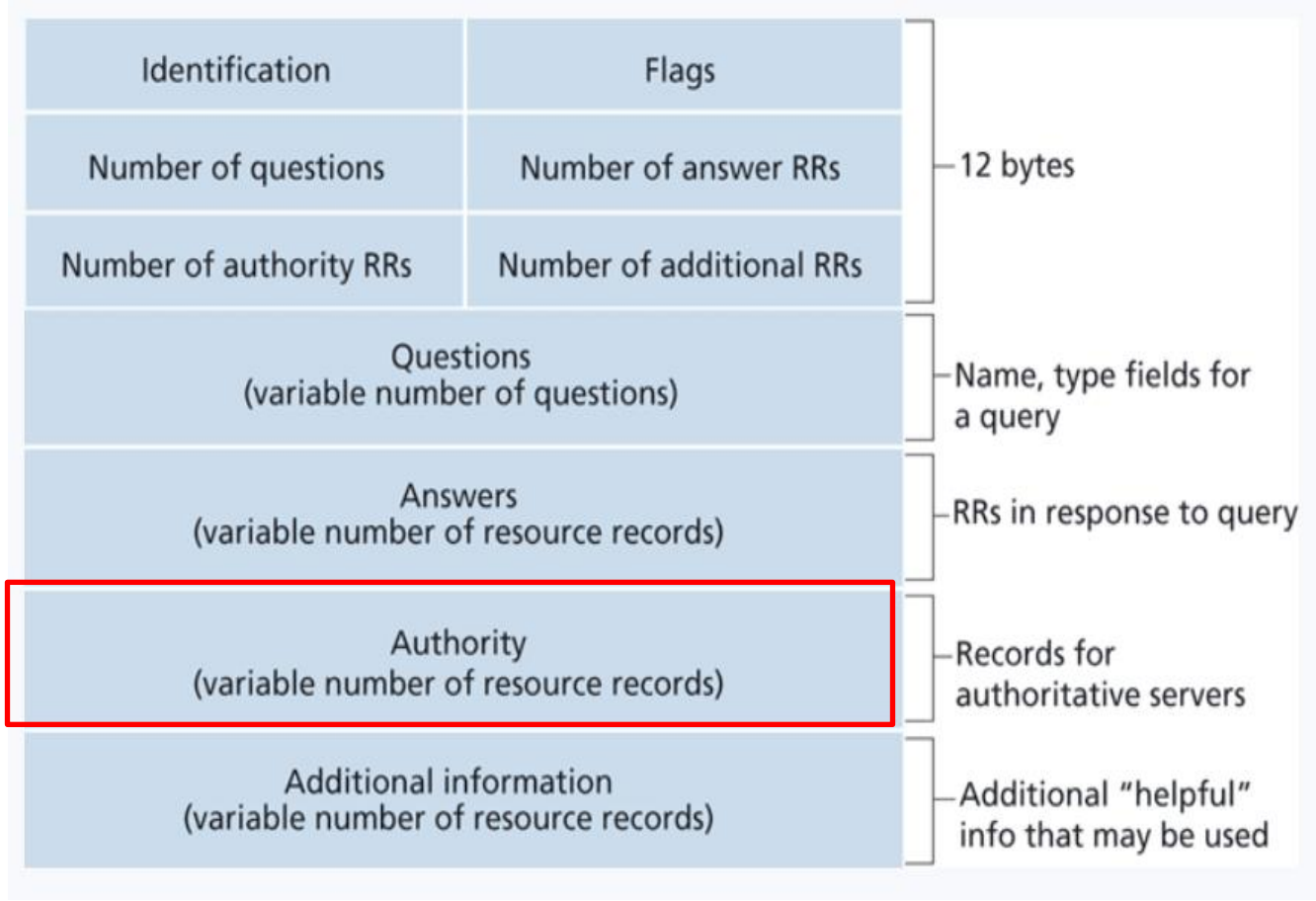
A set of 0/1 that provide information about the query

- Is it authoritative?
- Is it a response or a query?
- Should it be done recursively?

What question is the query asking?
(ie. type `A` for wikipedia.com)

If the packet is a response, the answer to the query will be located here

DNS Requests *(The format of a DNS request packet)*



ID number for the query. Used to match a request to its response easily

A set of 0/1 that provide information about the query

- Is it authoritative?
- Is it a response or a query?
- Should it be done recursively?

What question is the query asking?
(ie. type `A` for wikipedia.com)

If the packet is a response, the answer to the query will be located here

Information about other authoritative server

DNS Requests in Wireshark

dns

No.	Time	Source	Destination	Protocol	Length	Info
71	1.835642	192.168.1.4	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
82	1.867607	192.168.1.1	192.168.1.4	DNS	172	Standard query response 0x0001 No such name PTR 1.1.168.192.in-addr.arpa SOA p
83	1.869114	192.168.1.4	192.168.1.1	DNS	73	Standard query 0x0002 A wikipedia.org
85	1.909891	192.168.1.1	192.168.1.4	DNS	100	Standard query response 0x0002 A wikipedia.org A 208.80.154.224 OPT
86	1.912529	192.168.1.4	192.168.1.1	DNS	73	Standard query 0x0003 AAAA wikipedia.org
103	1.986902	192.168.1.1	192.168.1.4	DNS	112	Standard query response 0x0003 AAAA wikipedia.org AAAA 2620:0:861:ed1a::1 OPT

```
nslookup wikipedia.org
```

```
> Frame 83: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \
> Ethernet II, Src: Giga-Byt_ae:b1:0f (e0:d5:5e:ae:b1:0f), Dst: Netgear_2b:78:46 (9c
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 54515, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > wikipedia.org: type A, class IN
    [Response In: 85]
```

```
0000  9c 3d cf 2b 78 46 e0 d5  5e ae b1 0f 08 00 45 00   ·=·+xF·· ^·····E·
0010  00 3b e8 fe 00 00 80 11  00 00 c0 a8 01 04 c0 a8   ·;····· ********
0020  01 01 d4 f3 00 35 00 27  83 8e 00 02 01 00 00 01   ·····5·' ********
0030  00 00 00 00 00 00 09 77  69 6b 69 70 65 64 69 61   ·····w ikipedia
0040  03 6f 72 67 00 00 01 00  01                        ·org···· ·
```

DNS Requests in Wireshark

```
C:\Users\Reese Pearsall>nslookup wikipedia.org
Server:  dns2.msu.montana.edu
Address:  153.90.2.1

Non-authoritative answer:
Name:    wikipedia.org
Addresses:  2620:0:863:ed1a::1
          198.35.26.96


C:\Users\Reese Pearsall>
```

Information about the local DNS server that was contacted

DNS Response
(Wikipedia.org's IP address is 198.35.26.96 !)

DNS Requests in Wireshark

```
C:\Users\Reese Pearsall>nslookup wikipedia.org
Server:  dns2.msu.montana.edu
Address:  153.90.2.1

Non-authoritative answer:
Name:    wikipedia.org
Addresses:  2620:0:863:ed1a::1
          198.35.26.96


C:\Users\Reese Pearsall>
```

Information about the local DNS server that was contacted

DNS Response
(Wikipedia.org's IP address is 198.35.26.96 !)

"Non-authoritative answer" means that this answer came from a cache somewhere rather than the Authoritative DNS server for Wikipedia.com

DNS Requests in Wireshark

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

Filter for just DNS traffic

No.	Time	Source	Destination	Protocol	Length	Info
208	3.955746	153.90.2.1	153.90.118.6	DNS	123	Standard query response 0x523f HTTPS www.montana.edu CNAME www.montana.edu…
402	9.359296	153.90.118.85	153.90.2.1	DNS	83	Standard query 0x0001 PTR 1.2.90.153.in-addr.arpa
403	9.360125	153.90.2.1	153.90.118.85	DNS	117	Standard query response 0x0001 PTR 1.2.90.153.in-addr.arpa PTR dns2.msu.mo…
404	9.360592	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0002 A wikipedia.org.msu.montana.edu
405	9.361410	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0002 No such name A wikipedia.org.msu.montana.ed…
406	9.361540	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0003 AAAA wikipedia.org.msu.montana.edu
407	9.362236	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0003 No such name AAAA wikipedia.org.msu.montana…
408	9.362361	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0004 A wikipedia.org.montana.edu
409	9.362884	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0004 No such name A wikipedia.org.montana.edu SO…
410	9.363070	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0005 AAAA wikipedia.org.montana.edu
411	9.363874	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0005 No such name AAAA wikipedia.org.montana.edu…
412	9.364079	153.90.118.85	153.90.2.1	DNS	73	Standard query 0x0006 A wikipedia.org
413	9.364809	153.90.2.1	153.90.118.85	DNS	89	Standard query response 0x0006 A wikipedia.org A 198.35.26.96

This is the DNS Request and Response for the Type A record for `wikipedia.org`

DNS Requests in Wireshark

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

Filter for just DNS traffic

No.	Time	Source	Destination	Protocol	Length	Info
208	3.955746	153.90.2.1	153.90.118.6	DNS	123	Standard query response 0x523f HTTPS www.montana.edu CNAME www.montana.edu…
402	9.359296	153.90.118.85	153.90.2.1	DNS	83	Standard query 0x0001 PTR 1.2.90.153.in-addr.arpa
403	9.360125	153.90.2.1	153.90.118.85	DNS	117	Standard query response 0x0001 PTR 1.2.90.153.in-addr.arpa PTR dns2.msu.mo…
404	9.360592	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0002 A wikipedia.org.msu.montana.edu
405	9.361410	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0002 No such name A wikipedia.org.msu.montana.ed…
406	9.361540	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0003 AAAA wikipedia.org.msu.montana.edu
407	9.362236	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0003 No such name AAAA wikipedia.org.msu.montana…
408	9.362361	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0004 A wikipedia.org.montana.edu
409	9.362884	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0004 No such name A wikipedia.org.montana.edu SO…
410	9.363070	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0005 AAAA wikipedia.org.montana.edu
411	9.363874	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0005 No such name AAAA wikipedia.org.montana.edu…
412	9.364079	153.90.118.85	153.90.2.1	DNS	73	Standard query 0x0006 A wikipedia.org
413	9.364809	153.90.2.1	153.90.118.85	DNS	89	Standard query response 0x0006 A wikipedia.org A 198.35.26.96

The IP address of my machine (yours will probably be different)

The IP address of my local DNS server (dns2.msu.montana.edu) (yours will probably be different)

DNS Requests in Wireshark

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

Filter for just DNS traffic

No.	Time	Source	Destination	Protocol	Length	Info
208	3.955746	153.90.2.1	153.90.118.6	DNS	123	Standard query response 0x523f HTTPS www.montana.edu CNAME www.montana.edu…
402	9.359296	153.90.118.85	153.90.2.1	DNS	83	Standard query 0x0001 PTR 1.2.90.153.in-addr.arpa
403	9.360125	153.90.2.1	153.90.118.85	DNS	117	Standard query response 0x0001 PTR 1.2.90.153.in-addr.arpa PTR dns2.msu.mo…
404	9.360592	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0002 A wikipedia.org.msu.montana.edu
405	9.361410	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0002 No such name A wikipedia.org.msu.montana.ed…
406	9.361540	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0003 AAAA wikipedia.org.msu.montana.edu
407	9.362236	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0003 No such name AAAA wikipedia.org.msu.montana…
408	9.362361	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0004 A wikipedia.org.montana.edu
409	9.362884	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0004 No such name A wikipedia.org.montana.edu SO…
410	9.363070	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0005 AAAA wikipedia.org.montana.edu
411	9.363874	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0005 No such name AAAA wikipedia.org.montana.edu…
412	9.364079	153.90.118.85	153.90.2.1	DNS	73	Standard query 0x0006 A wikipedia.org
413	9.364809	153.90.2.1	153.90.118.85	DNS	89	Standard query response 0x0006 A wikipedia.org A 198.35.26.96

```
> Frame 412: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \De
> Ethernet II, Src: Dell_93:f1:78 (00:be:43:93:f1:78), Dst: Cisco_9f:f4:65 (00:00:0c:9f
> Internet Protocol Version 4, Src: 153.90.118.85, Dst: 153.90.2.1
> User Datagram Protocol, Src Port: 62939, Dst Port: 53
> Domain Name System (query)
```

← Expand this to see UDP information

← Expand this to DNS information

DNS Requests in Wireshark

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

Filter for just DNS traffic

No.	Time	Source	Destination	Protocol	Length	Info
208	3.955746	153.90.2.1	153.90.118.6	DNS	123	Standard query response 0x523f HTTPS www.montana.edu CNAME www.montana.edu…
402	9.359296	153.90.118.85	153.90.2.1	DNS	83	Standard query 0x0001 PTR 1.2.90.153.in-addr.arpa
403	9.360125	153.90.2.1	153.90.118.85	DNS	117	Standard query response 0x0001 PTR 1.2.90.153.in-addr.arpa PTR dns2.msu.mo…
404	9.360592	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0002 A wikipedia.org.msu.montana.edu
405	9.361410	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0002 No such name A wikipedia.org.msu.montana.ed…
406	9.361540	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0003 AAAA wikipedia.org.msu.montana.edu
407	9.362236	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0003 No such name AAAA wikipedia.org.msu.montana…
408	9.362361	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0004 A wikipedia.org.montana.edu
409	9.362884	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0004 No such name A wikipedia.org.montana.edu SO…
410	9.363070	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0005 AAAA wikipedia.org.montana.edu
411	9.363874	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0005 No such name AAAA wikipedia.org.montana.edu…
412	9.364079	153.90.118.85	153.90.2.1	DNS	73	Standard query 0x0006 A wikipedia.org
413	9.364809	153.90.2.1	153.90.118.85	DNS	89	Standard query response 0x0006 A wikipedia.org A 198.35.26.96

```
User Datagram Protocol, Src Port: 62939, Dst Port: 53
    Source Port: 62939
    Destination Port: 53
    Length: 39
```

It is sent to port 53 (the reserved port for DNS traffic)

```
Domain Name System (query)
    Transaction ID: 0x0006
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        wikipedia.org: type A, class IN
    [Response In: 413]
```

← This is the question. “What is the IPv4 Address for Wikipedia.org?”

← You can click on this to find the DNS response (the answer)

DNS Requests in Wireshark

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

Filter for just DNS traffic

No.	Time	Source	Destination	Protocol	Length	Info
208	3.955746	153.90.2.1	153.90.118.6	DNS	123	Standard query response 0x523f HTTPS www.montana.edu CNAME www.montana.edu…
402	9.359296	153.90.118.85	153.90.2.1	DNS	83	Standard query 0x0001 PTR 1.2.90.153.in-addr.arpa
403	9.360125	153.90.2.1	153.90.118.85	DNS	117	Standard query response 0x0001 PTR 1.2.90.153.in-addr.arpa PTR dns2.msu.mo…
404	9.360592	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0002 A wikipedia.org.msu.montana.edu
405	9.361410	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0002 No such name A wikipedia.org.msu.montana.ed…
406	9.361540	153.90.118.85	153.90.2.1	DNS	89	Standard query 0x0003 AAAA wikipedia.org.msu.montana.edu
407	9.362236	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0003 No such name AAAA wikipedia.org.msu.montana…
408	9.362361	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0004 A wikipedia.org.montana.edu
409	9.362884	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0004 No such name A wikipedia.org.montana.edu SO…
410	9.363070	153.90.118.85	153.90.2.1	DNS	85	Standard query 0x0005 AAAA wikipedia.org.montana.edu
411	9.363874	153.90.2.1	153.90.118.85	DNS	137	Standard query response 0x0005 No such name AAAA wikipedia.org.montana.edu…
412	9.364079	153.90.118.85	153.90.2.1	DNS	73	Standard query 0x0006 A wikipedia.org
413	9.364809	153.90.2.1	153.90.118.85	DNS	89	Standard query response 0x0006 A wikipedia.org A 198.35.26.96

```
Domain Name System (response)
  Transaction ID: 0x0006
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    wikipedia.org: type A, class IN
  Answers
    wikipedia.org: type A, class IN, addr 198.35.26.96
  [Request In: 412]
  [Time: 0.000730000 seconds]
```

To find the answer to our query, we find the DNS response and check the “Answers” section

IP Whois

```
NetRange:       198.35.26.0 - 198.35.27.255
CIDR:           198.35.26.0/23
NetName:        WIKIMEDIA
NetHandle:      NET-198-35-26-0-1
Parent:         NET198 (NET-198-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS14907
Organization:   Wikimedia Foundation Inc. (WIKIM)
RegDate:        2013-07-16
Updated:        2021-12-14
Ref:            https://rdap.arin.net/registry/ip/198.35.26.0
```

The IP address of `wikipedia.com` is 198.35.26.96