Management and Operations of Networks, Services, and Systems

Domain Name System

Ricardo Morla

FEUP – GORS/M.EEC, GRS/M.EIC

Domain names

- While browsing the Internet, people are better with names than with IP addresses
  - Easier to remember
  - They can have meaning
- Organizations can choose names that make sense to people…
  - vpn.org1.pt
  - simulator.engineering.org1.pt
- But they don’t have to make sense…
  - I39rsrutuwef39ru4cg3.virtualmachines.org1.pt

Importance of DNS

- Domain names are what people use to access web sites
  - Applications also use them to access other applications
- IP adddresses is how information gets routed on the Internet
- DNS does mapping between domain names and IP addresses

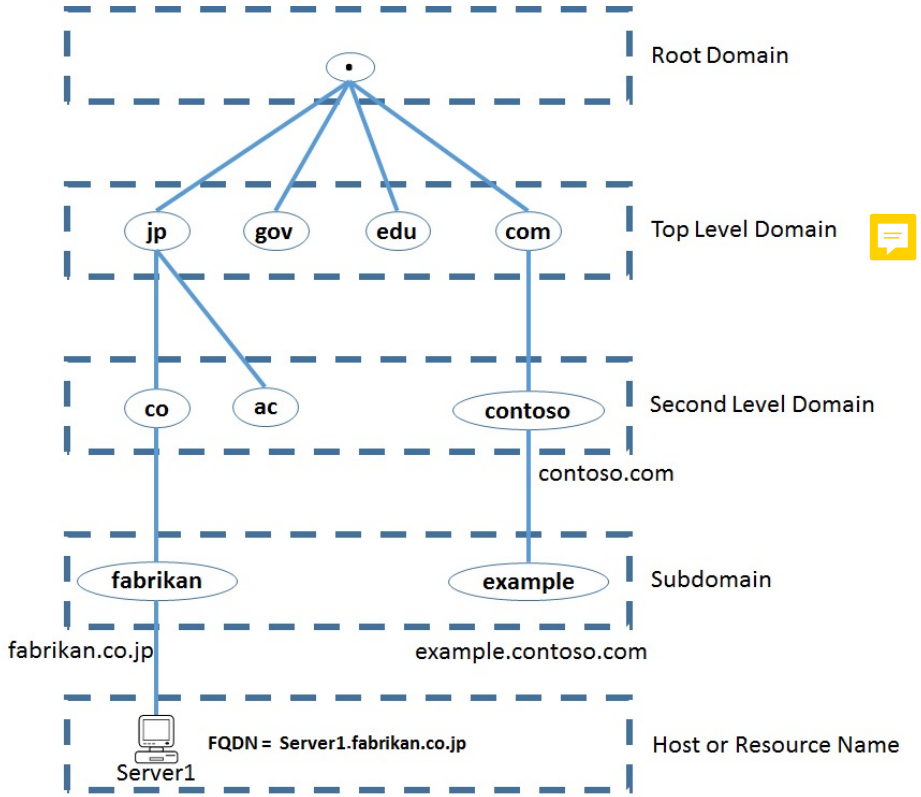
There are two parts to DNS

- Establish the map between domain names and IPs
  - Owners of names and IPs do this
  - Using ‘authoritative’ domain name servers
- Answer queries from users
  - Users can issues queries directly to the authoritative name servers

  OR
  - Users group together so that responses can be cached and the burden can be eased on authoritative servers
  - This is done via ‘cache’, ‘proxy’, ‘resolver’ domain name servers

Domain name hierarchy

- Root domain
- Top level domain
- Second level
- Subdomains (possibly)



https://gitlearning.wordpress.com/2015/06/23/dns-server/

Domain names specifications

- Internet Corporation for Assigned Names and Numbers (ICANN)
- Internet Assigned Numbers Authority (IANA)

- ASCII (original)
- Internationalized Domain Names
  - Multibyte unicode, encoded in ASCII (punycode)
  - Converted per level, xn--Mnchen-3ya

Root Authoritative Servers

- A DNS zone is a portion of the DNS namespace that is managed by a specific organization or administrator
- The DNS root zone contains all domain names
- Root servers respond to TLD requests

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

Non-root Authoritative Servers

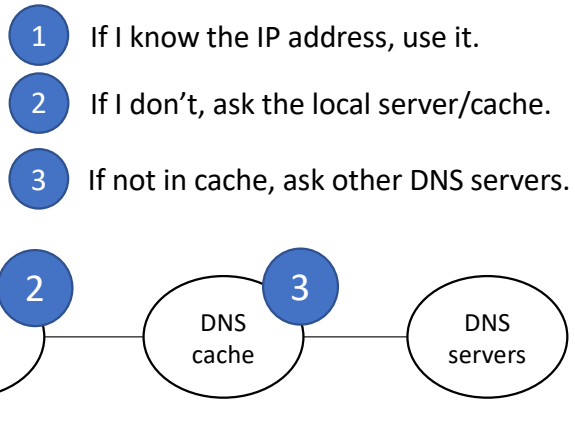
- Top Level Domains
  - gTLD – Generic Top-Level Domains
    - Original: .com, .org, .net, .int, .edu, .gov, .mil, .arpa
    - 1502 new TLDs as of April 2021, internacionalized
    - https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains
  - ccTLD – Country Code Top-Level Domains
    - 316 ccTLDs as of June 2020, including internationalized
    - https://en.wikipedia.org/wiki/Country_code_top-level_domain

Non-root Authoritative Servers

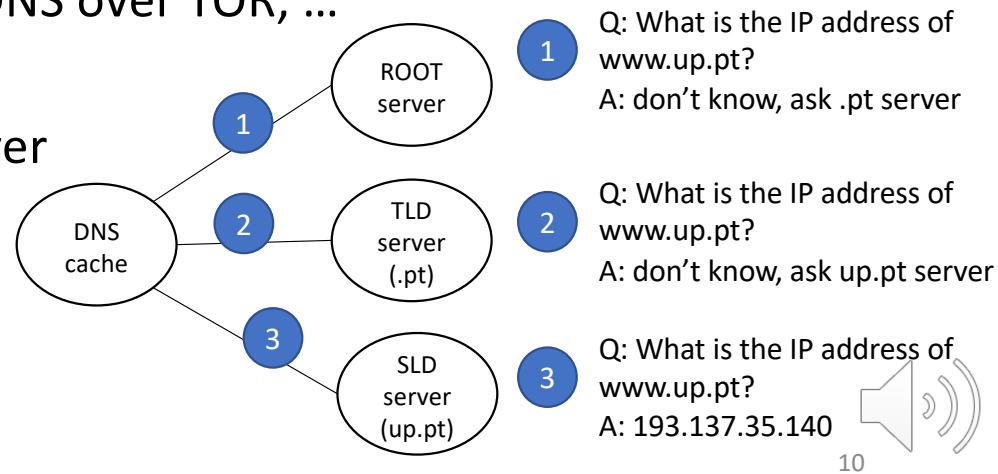
https://en.wikipedia.org/wiki/Name_server

- Second-level domains
  - Each TLD has a TLD manager organization, responsible for assigning SLDs under that TLD
  - The same happens down the hierarchy until the final host or resource name
- Masters
  - stores the definitive versions of all records
  - identified in start-of-authority (SOA) resource record
- Slaves
  - automatic updating mechanism to maintain an identical copy of the primary server's database for a zone
  - DNS zone transfer, AXFR, https://en.wikipedia.org/wiki/DNS_zone_transfer

Architecture and Protocol



- Local
  - /etc/hosts, resolv.conf, DHCP
  - Non-recursive, recursive, iterative
- DNS Request and reply messages
  - QR, AA, NAME, TYPE
  - Over TCP or UDP ports 53; DoT, DoH, DNS over TOR, …
- Servers
  - Local/remote DNS server/cache/resolver
  - Root name server, TLD, SLD
  - Caching
  - Split server



https://en.wikipedia.org/wiki/Domain_Name_System

DNS tool: dig

```
$ dig sigarra.up.pt

;; QUESTION SECTION:
;sigarra.up.pt.                 IN      A

;; ANSWER SECTION:
sigarra.up.pt.          49      IN      A       193.137.35.140

;; AUTHORITY SECTION:
up.pt.                  4904    IN      NS      ns4.up.pt.
up.pt.                  4904    IN      NS      ns2.up.pt.
up.pt.                  4904    IN      NS      ns3.up.pt.
up.pt.                  4904    IN      NS      ns1.up.pt.

;; ADDITIONAL SECTION:
ns1.up.pt.              10275   IN      A       193.137.55.30
ns2.up.pt.              2204    IN      A       193.137.55.31
ns3.up.pt.              74589   IN      A       193.137.55.32
ns4.up.pt.              26925   IN      A       193.137.55.33
ns1.up.pt.              11393   IN      AAAA    2001:690:2200:a10::30
ns2.up.pt.              2204    IN      AAAA    2001:690:2200:a10::31
ns3.up.pt.              74589   IN      AAAA    2001:690:2200:a10::32
ns4.up.pt.              26925   IN      AAAA    2001:690:2200:a10::33
```

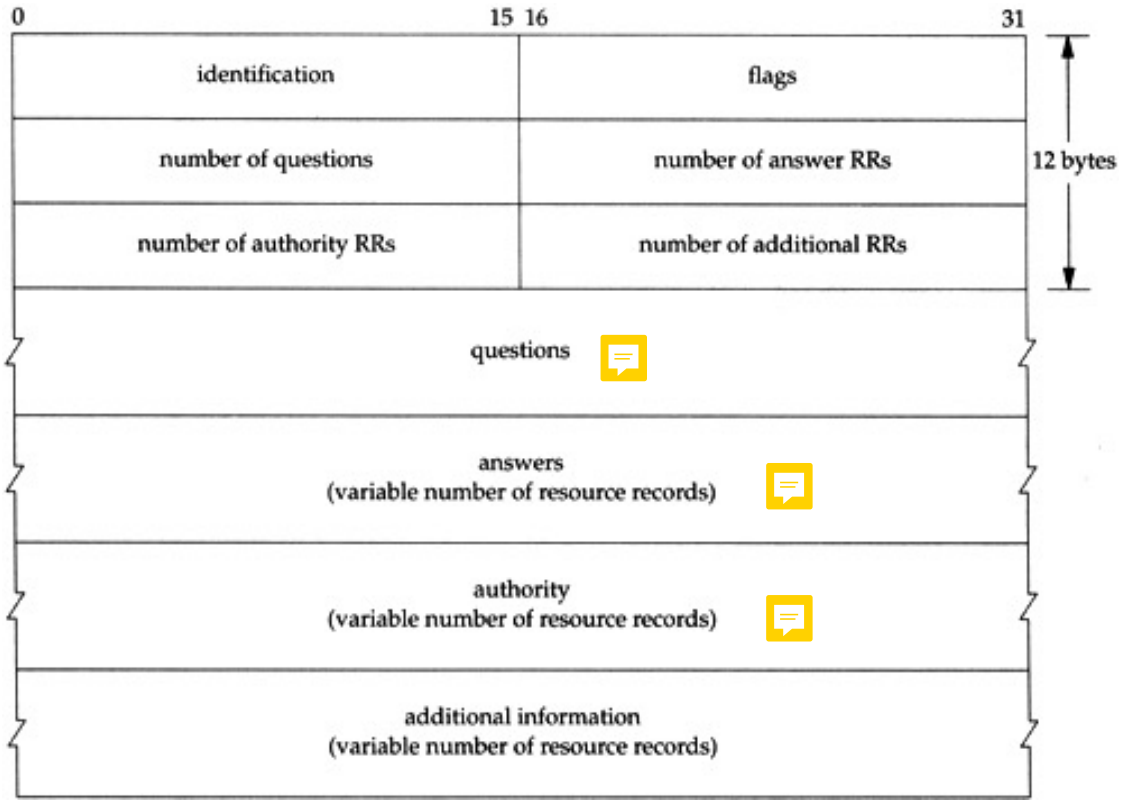
```
$ dig cloudflare.com
(...)
;; QUESTION SECTION:
;cloudflare.com.                IN      A

;; ANSWER SECTION:
cloudflare.com.         300     IN      A       104.16.132.229
cloudflare.com.         300     IN      A       104.16.133.229

;; AUTHORITY SECTION:
cloudflare.com.         6256    IN      NS      ns4.cloudflare.com.
cloudflare.com.         6256    IN      NS      ns7.cloudflare.com.
cloudflare.com.         6256    IN      NS      ns5.cloudflare.com.
cloudflare.com.         6256    IN      NS      ns6.cloudflare.com.
cloudflare.com.         6256    IN      NS      ns3.cloudflare.com.

;; ADDITIONAL SECTION:
ns3.cloudflare.com.     64      IN      A       162.159.0.33
ns3.cloudflare.com.     64      IN      A       162.159.7.226
ns4.cloudflare.com.     64      IN      A       162.159.1.33
ns4.cloudflare.com.     64      IN      A       162.159.8.55
ns5.cloudflare.com.     64      IN      A       162.159.2.9
ns5.cloudflare.com.     64      IN      A       162.159.9.55
ns6.cloudflare.com.     64      IN      A       162.159.3.11
ns6.cloudflare.com.     64      IN      A       162.159.5.6
ns7.cloudflare.com.     64      IN      A       162.159.4.8
ns7.cloudflare.com.     64      IN      A       162.159.6.6
ns3.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:21
ns3.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:7e2
ns4.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:121
ns4.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:837
ns5.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:209
ns5.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:937
ns6.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:30b
ns6.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:506
ns7.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:408
ns7.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:606
```

DNS message format



https://flylib.com/books/en/3.223.1.151/1/

Flags

QR: 0 query, 1 response

opcode: 0 standard query, 1 inverse query

RD: recursive query

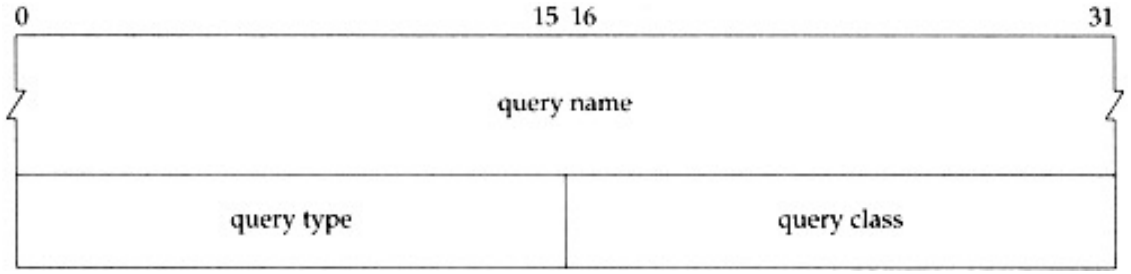
rcode: 0 no error, 3 NXDOMAIN, 5 UPDATE, …

Resource records

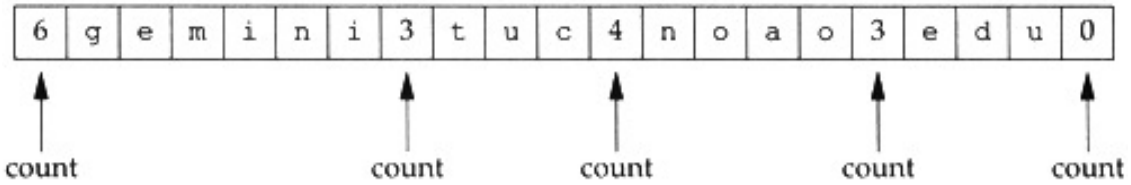
Different types

Questions, queries

- Domain name to query
  - Per level, length-value encoding
  - 1 byte: number of characters in level, range **0-63**
  - No limit to total size of domain name, only to levels
  - Query ends with **0**
- Query types
  - ‘type’ is for answer
  - Record resource type requested
- Query class
  - 1, query for IP addresses

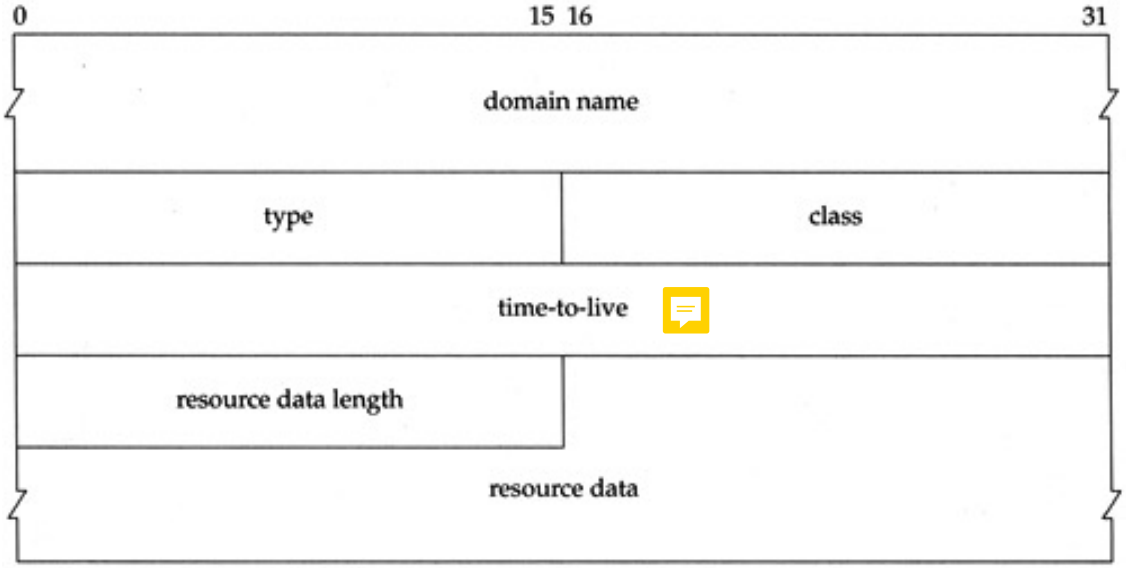


`gemini.tuc.noao.edu`



Name	Numeric value	Description	*type?*	*query type?*
A	1	IP address	•	•
NS	2	name server	•	•
CNAME	5	canonical name	•	•
PTR	12	pointer record	•	•
HINFO	13	host info	•	•
MX	15	mail exchange record	•	•
AXFR	252	request for zone transfer		•
* or ANY	255	request for all records		•

Resource records



- Assigns resources to names
- Common format for:
  - Answers
  - Authority
  - Additional Information
- Domain name, type, class – similar to question
- Resource data – depends on resource record type

RR examples

https://datatracker.ietf.org/doc/html/rfc1035#section-3.3.11

https://en.wikipedia.org/wiki/SOA_record

```
$ dig ns up.pt
;; QUESTION SECTION:
;up.pt.                         IN      NS
;; ANSWER SECTION:
up.pt.                  66217   IN      NS      ns4.up.pt.
up.pt.                  66217   IN      NS      ns1.up.pt.
up.pt.                  66217   IN      NS      ns3.up.pt.
up.pt.                  66217   IN      NS      ns2.up.pt.
```

```
$ dig soa up.pt
;; QUESTION SECTION:
;up.pt.                         IN      SOA
;; ANSWER SECTION:
up.pt.                  86400   IN      SOA     ns1.up.pt. it.up.pt. 1636712510 28800 7200 72000 86400
```

```
$ dig ns ns1.up.pt
;; QUESTION SECTION:
;ns1.up.pt.                     IN      NS
;; AUTHORITY SECTION:
up.pt.                  806     IN      SOA     ns1.up.pt. it.up.pt. 1636712510 28800 7200 72000 86400
```

RR examples

https://en.wikipedia.org/wiki/CNAME_record
https://en.wikipedia.org/wiki/MX_record
https://datatracker.ietf.org/doc/html/rfc1035#section-3.3.12

```
$ dig mx up.pt
;; QUESTION SECTION:
;up.pt.                         IN      MX
;; ANSWER SECTION:
up.pt.                  300     IN      MX      10 mx05.up.pt.
up.pt.                  300     IN      MX      10 mx03.up.pt.
up.pt.                  300     IN      MX      10 mx02.up.pt.
```

```
$ dig A up.pt
;; QUESTION SECTION:
;up.pt.                         IN      A
;; ADDITIONAL SECTION:
up.pt.                  1845    IN      A       193.137.55.13
```

```
$ dig A www.up.pt
;; QUESTION SECTION:
;www.up.pt.                     IN      A
;; ANSWER SECTION:
www.up.pt.              3528    IN      CNAME   www.up.pt.cdn.cloudflare.net.
www.up.pt.cdn.cloudflare.net. 228 IN    A       104.18.7.105
www.up.pt.cdn.cloudflare.net. 228 IN    A       104.18.6.105
```

```
$ dig -x 193.137.55.13
;; QUESTION SECTION:
;13.55.137.193.in-addr.arpa.    IN      PTR
;; ADDITIONAL SECTION:
13.55.137.193.in-addr.arpa. 3592 IN     PTR     up.pt.
```

Timeouts – Example with SOA and slaves (secondary NS)

- Expire: Number of seconds after which secondary name servers should stop answering request for this zone if the master does not respond. This value must be bigger than the sum of *Refresh* and *Retry*.

```
@   IN  SOA     ns.icann.org. noc.dns.icann.org. (
        2020080302  ;Serial
        7200        ;Refresh
        3600        ;Retry
        1209600     ;Expire
        3600        ;Negative response caching TTL
)
```

https://en.wikipedia.org/wiki/SOA_record

Resolvers and caches

- Recursive

vs.

- Iterative

- Referral
  - NS: ”can’t find this name, try this NS”
  - (2) and (4) in red in the figure

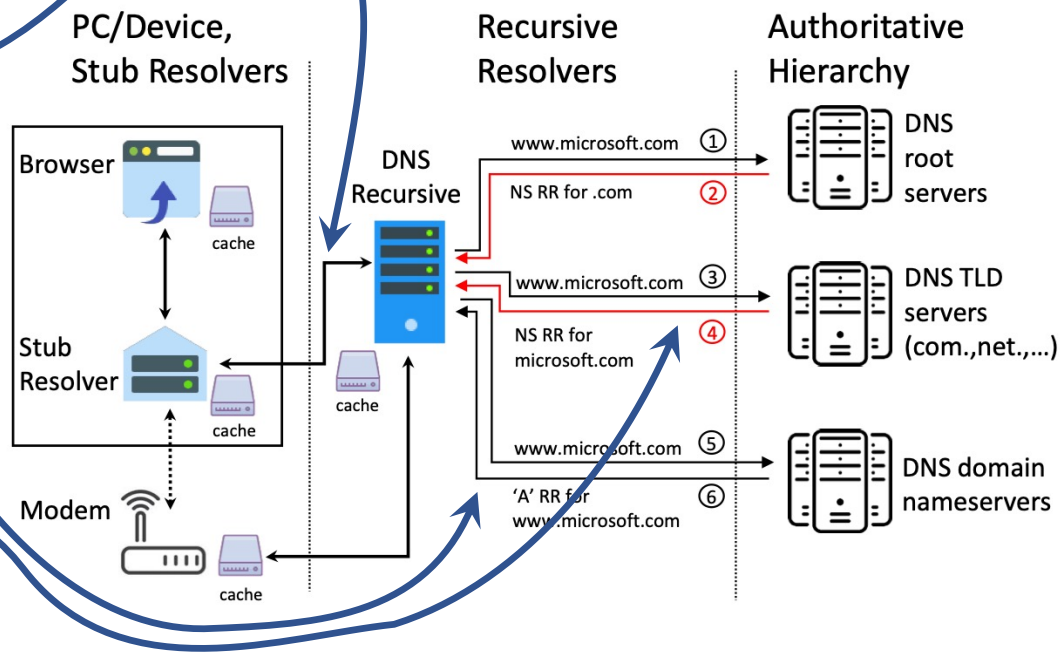
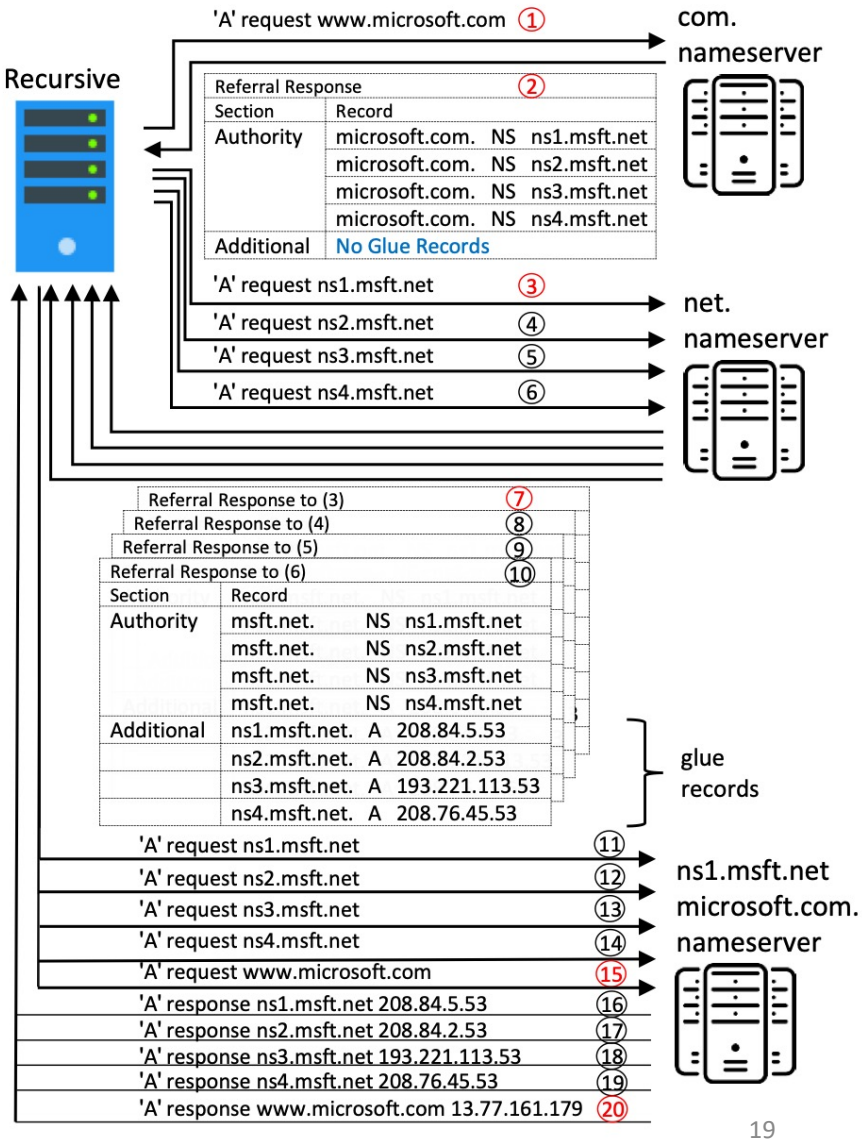


Figure 1: The resolution process, in theory, for the domain www.microsoft.com. The red steps represent NS referral responses.

https://www.usenix.org/conference/usenixsecurity20/presentation/afek

Redundancy overhead

- Multiple name servers for redundancy
- Results in multiple queries to multiple nameservers



https://www.usenix.org/conference/usenixsecurity20/presentation/afek

NXDOMAIN: performance issues with caching

- Caching tries to save resources on the authoritative server
  - First query for a given name -> goes for the authoritative server
  - Subsequent queries are replied by the cache without using the auth. Server
- This works ok assuming queried domain names are somehow repeated
  - Each client may lookup the same domain name multiple times
  - Multiple clients may lookup the same domain name
- What if the queried domain names are not repeated?
  - Most queries go to the authoritative server
  - Authoritative server gets more queries than designed for

Security Extensions

- DNSSEC: Domain Name System Security Extensions
- Provide integrity in the query answers
  - RRSIG resource record provides the signature to authenticate another RR
- DNSKEY of the server, for the resolver to verify the signature
  - Chain of trust from root servers
- Does not provide confidentiality
  - Eavesdroppers can still know what you're querying

Dynamic DNS

- Dynamic updating
  - Motivation: update traditional records without manual editing
  - RFC 2136: UPDATE, opcode 5 in DNS message
- Client updates
  - Motivation: client IP addresses change, name-IP mapping must be updated
  - Service to update IP address, often HTTP based

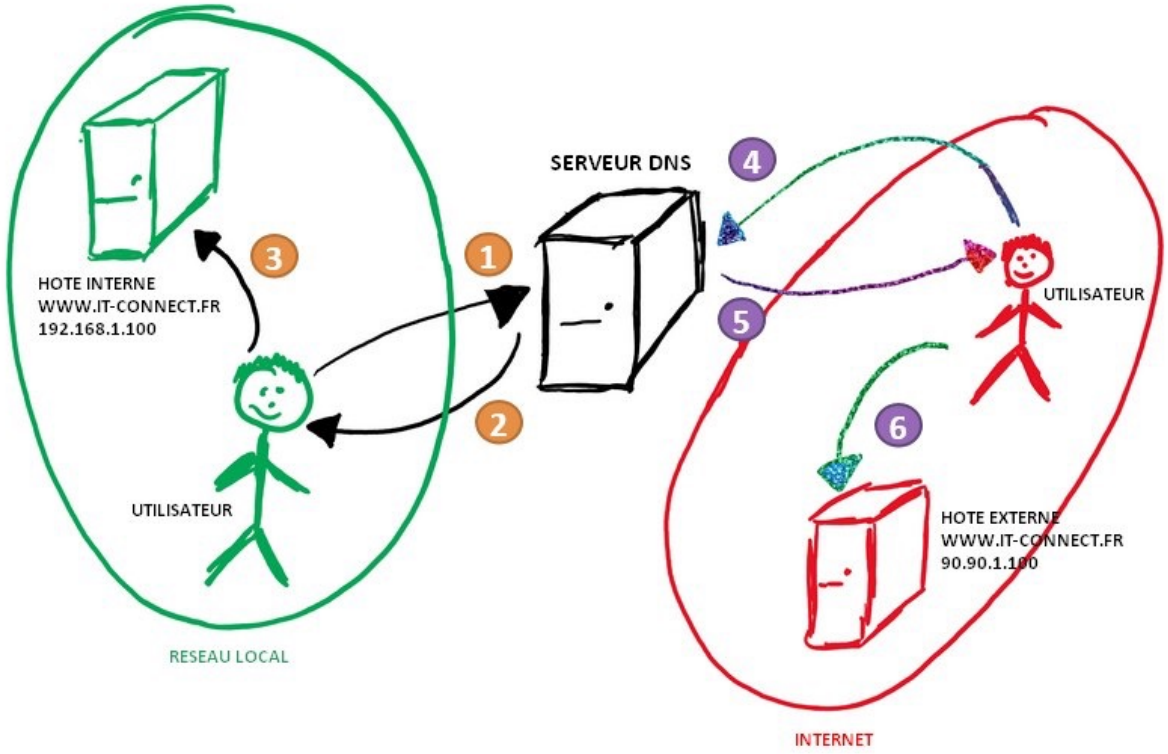
Transport Protocols for DNS

- DNS typically runs on UDP port 53
- Can be used over TCP (also on port 53)
  - When expecting large replies (UDP max 512 bytes)
  - Or for zone transfers to slave servers (AXFR)
- Motivation for using other (encrypted) transport protocols
  - Privacy concerns between the client and the resolver
  - Easy to recover domain name of HTTP request from DNS query
  - Even if HTTP connection is encrypted and Server Name Indicator (TLS) is encrypted
  - Can’t we use DNSSEC? Yes you can/should, but it “only” gives you integrity of query answers

Transport Protocols for DNS

- DoT
  - Establish a TLS connection, send DNS messages over the TLS connection
  - Based on the TCP version of DNS
  - https://datatracker.ietf.org/doc/html/rfc7858
  - https://developers.cloudflare.com/1.1.1.1/encrypted-dns/dns-over-tls
- DoH
  - DNS messages sent as HTTP's MIME type: application/dns-message
  - HTTP/2
  - https://developers.cloudflare.com/1.1.1.1/encrypted-dns/dns-over-https/make-api-requests/dns-wireformat
- Integrity about query answers? DNSSec

Deployment – split DNS



Management and Operations of Networks, Services, and Systems

Domain Name System

Ricardo Morla

FEUP – GORS/M.EEC, GRS/M.EIC