Universidad
Carlos III de Madrid

Aplicaciones
Telematicas

Domain Name System (DNS)

Aplicaciones Telemáticas (Telematic Applications)
Grado en Ingeniería Tecnologías de las Telecomunicaciones

Based on Celeste Campo and Calos García slides.
Modified and new content by Daniel Díaz ,Andres Marín, Florina Almenarez.

Outlook

Outlook

1. Introduction and context
   - Objectives
   - Bibliography
   - DNS history
2. Name spaces in DNS
   - Operation
   - Relation with IP
   - Delegation
3. DNS Use cases
4. DNS Protocol
5. Query types in DNS
   - Critical resources
6. DNS extensions

Bibliography

- RFCs are the best source of information
  - The "history of DNS" section mentions several key RFCs
  - Some of them may be discussed later
    - Some changes has been added with time in other RFCs
- Basic bibliography
  - Kevin R. Fall; W. Richard Stevens. TCP/IP Illustrated, Volume 1: The Protocols, 2/E. Addison-Wesley Professional. 2012
    - Chapter 11 - DNS
  - Forouzan, Behrouz A. TCP/IP protocol suite. 4th ed. 2010
    - Chapter 19 - DNS

Introduction and context

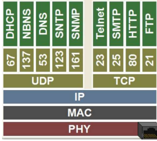
1. Introduction and context
   A. Objectives
   B. DNS history

Lesson outlook

1. Introduction and context
2. Namespaces in DNS
3. DNS Use cases
4. DNS Protocol
5. Query types in DNS
6. DNS extensions

Introduction to DNS and context

- TCP – an **IP and a port** required to open TCP connection
  - Humans do not remember many numbers
    - Despite Lu Chao was able to remember 67890 digits of PI
  - IP addressing is huge:
    - IPv4: 32-bit addresses, around 4.294.967.296 (2^{32})
    - IPv6: 128-bit addresses, around 3.4×10^{38} (1)
      - 2001:0db8:0000:0042:0000:8a2e:0370:7334
  - IP addresses may change dynamically for a service
    - *The name www.amazon.es* **do no change,** but does its IP
- **Domain Name System (DNS)**
  - Solution to the name-IP translation and email
  - It has many other uses today



(1) Many reserved segments reduces this number

Introdution to DNS and context >> Objectives

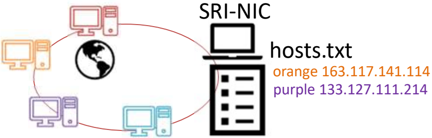
- Theory
  - Know DNS use cases
    - Name to IP translation and more
    - Mail exchange assistance
    - Aliases and load balancing
    - Security assistance
  - Discover DNS is a critic service nowadays
    - Current Internet size requires DNS
    - Huge dynamicity
  - Solve problems regarding scalability and extensibility

Introduction to DNS and context >> Objectives

- Lab
  - Learn to query a DNS server
  - Find out available services using DNS queries
  - Configure a DNS server

Introdution to DNS and context >> History of DNS (I)

- 1970 - ARPAnet several hundreds of hosts
  - hosts.txt file: contained IP to name associations
  - was handled by the Stanford Research Institute's Network Information Center (SRI-NIC) (updated daily)



- **1983 - Domain Name System (DNS)** was created as a solution (RFC 882 and RFC 883)
  - Initial versión of DNS
- **1987** – RFC 1034 and RCF 1035
  - Modern DNS moderno, master-slave (AXFR)

DNS Motivation

Early versions

Introduction to DNS and context >> History of DNS (II)

- **1996** - RFC 1995
  - NOTIFY so changes in primary DNS are notified to secondary DNS servers
  - IXFR transferencia incremental
- **1997** – RFC 2136
  - UPDATE, Dynamic DNS registry changes
- **1999** – RFC 2671
  - Extension mechanisms for DNS DNS (EDNS0)
  - TCP enabled (before only UDP) for long responses
  - Defines DNSSEC (RFC 4035)

Distribution improvement

Extensions

DNS name spaces

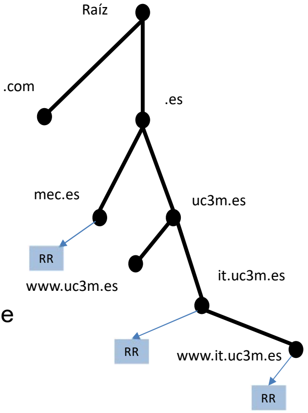
2. DNS name spaces
   - A. Levels
   - B. Nodes
   - C. Delegation

Lesson outlook

1. Introduction and context
2. Namespaces in DNS
3. DNS Use cases
4. DNS Protocol
5. Query types in DNS
6. Performance aspects in DNS
7. DNS extensions

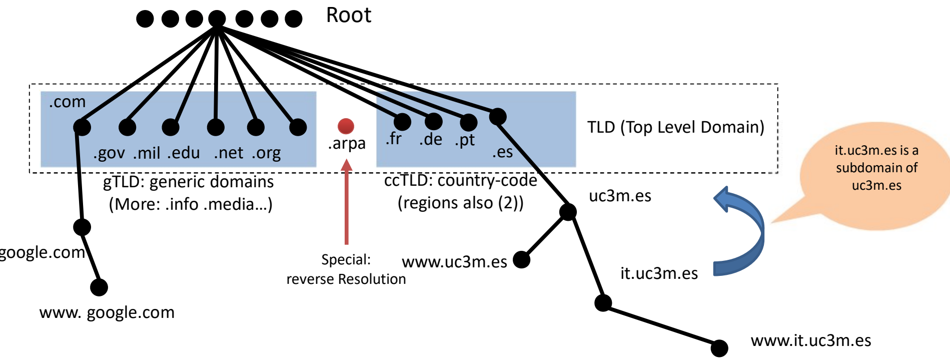
DNS name spaces >> At a glance

- DNS …
  - Is distributed for efficiency (thousands of names)
  - It is **hierarchical**
  - Conceived for humans
  - **Originally for**
    - Name to IP translation (A)
      - www.it.uc3m.es -> 163.117.139.115
    - Mail recipients (MD)
    - Mail forwarding servers (MF)
    - Alias (www.marca.es -> www.marca.com)
  - Each node stores information (RR)
    - The tree can be consulted by node and type
    - Today it's the "glue" of the Internet



DNS name spaces >> Levels

- Namespace organization
  - Tree with single logical root
    - many servers (several servers for redundancy)(1)
  - Several levels



(1) letter.root-servers.net where letter from A to M. They have a website to view metrics http://letter.root-servers.org

(2) Geographic country, regulated by ISO 3166-1

(3)

Based on Celeste Campo and Calos García slides. Modified by Daniel Díaz , Florina Almenarez, and Andrés Marín.

DNS name spaces >> Levels >> Upper levels

- The DNS tree
  - Multiple root servers ("Geographically distributed")
    - Their addresses are known beforehand
    - letter.root-servers.net where "letter" from A to M
  - TLD: Top Level Domain, there are four groups
    - **gTLD**: Generic TLDs as “**.com**”, “**.net**”, “**.info**”…
      - » Managed by ICANN (1)
      - » **ccTLD**: regions (according to ISO 3166)
      - » Delegates to local corporations (2)
    - .**arpa**: used for reverse resolution (3)
    - Internationalized domains (non-Latin characters)(4)
  - **Curious cases ".tv" (Tuvalu island now TV), ".ws" (west Samoa now web service)**

(1) ICANN (Internet Corporation for Assigned Names and Numbers) http://www.icann.org

(2) .es is managed by the Public Business Entity Red.Es of the Ministry of Industry, Energy and Tourism http://www.red.es/

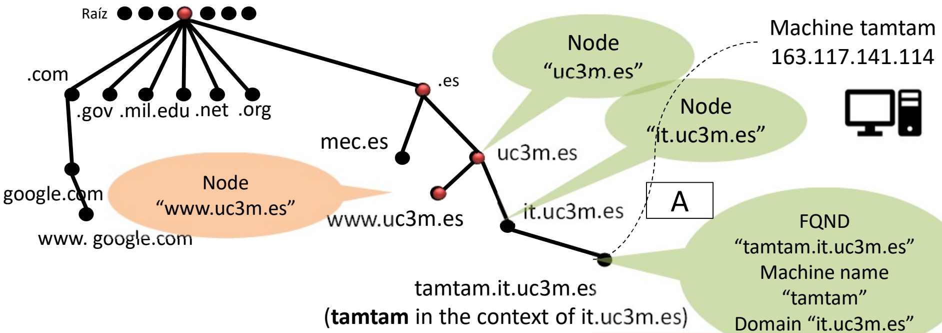
(3) Resolve an IP to a name instead of a name to an IP. The relationship is not always biunivocal.

(4) RFC 5890 y RFC 5891

DNS name spaces >> Nodes

- Domain names: A node in the tree
  - Label sequences separated by "."“
    - 63 characters maximum per tag
    - 255 characters in total (all tags)
    - Fully qualified domain name (FQDN): name of the machine and the domain to which it belongs

www . uc3m . es .

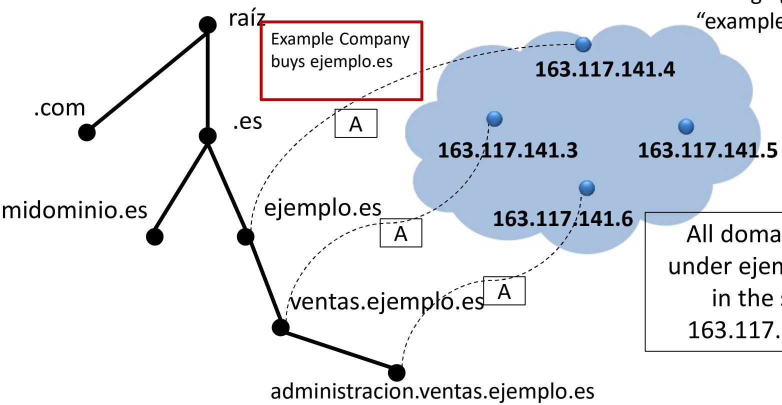


tamtam.it.uc3m.es
(**tamtam** in the context of it.uc3m.es)

Based on Celeste Campo and Calos García slides. Modified by Daniel Díaz , Florina Almenarez, and Andres Marin.

DNS name spaces >> Relation to IP (I)

- This hierarchy is independent of the IP addressing
  - Considering the record "Address" (A) (1)



Example Company buys ejemplo.es

segment 163.117.141.0/24 (2) belonging to company “example“

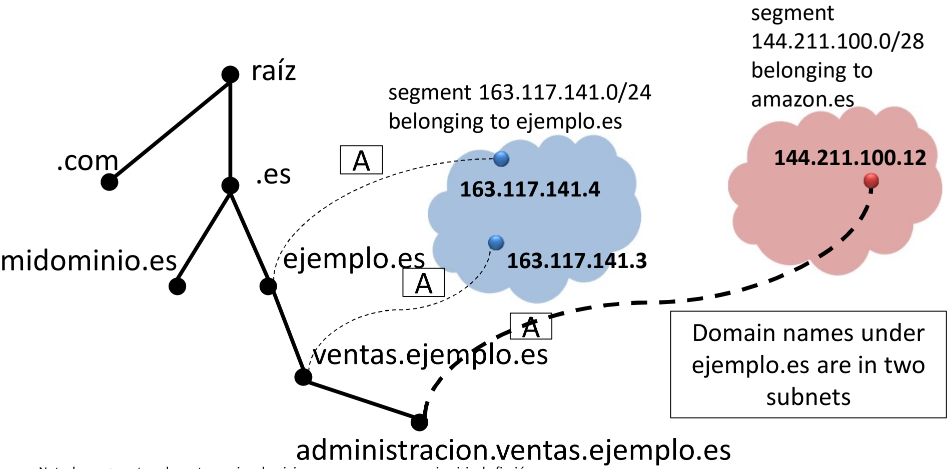
All domain names under ejemplo.es are in the subnet 163.117.141.0/24

(1) We'll see later, associate an FQDN with an IP address

(2) Notation CIDR (Classless Inter Domain Routing)

DNS name spaces >> Relation to IP (II)

- This hierarchy is independent of the IP addressing
  - Considering the record "Address" (A) (1)

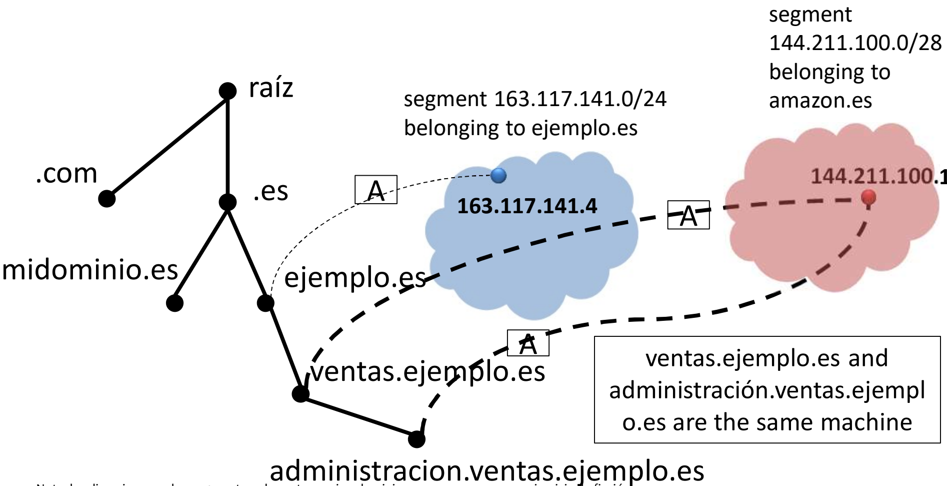


Domain names under ejemplo.es are in two subnets

Nota: los segmentos y la pertenencia a dominio.es o amazon.es es un ejercicio de ficción

DNS name spaces >> Relation to IP (III)

- This hierarchy is independent of the IP addressing
  - Considering the record "Address" (A) (1)



segment 144.211.100.0/28 belonging to amazon.es

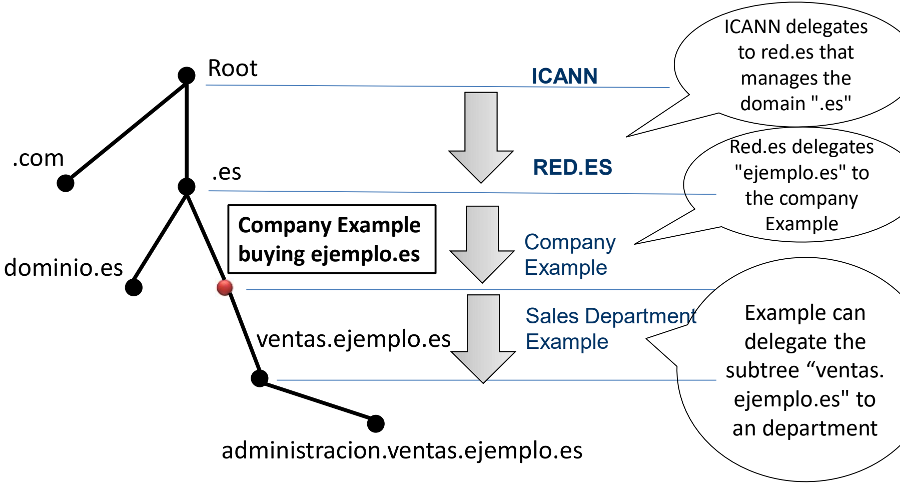
segment 163.117.141.0/24 belonging to ejemplo.es

ventas.ejemplo.es and administración.ventas.ejemplo.es are the same machine

Nota: las direcciones en los segmentos y la pertenencia a dominio.es o amazon.es es un ejercicio de ficción

DNS name spaces >> Delegation

- Reflects organizational boundaries
  - ICANN (1) delegates to RED.ES (2) the domain ".es“
  - Red.es manages it without ICANN intervention



Root

.com

.es

dominio.es

Company Example buying ejemplo.es

ventas.ejemplo.es

administracion.ventas.ejemplo.es

ICANN

RED.ES

Company Example

Sales Department Example

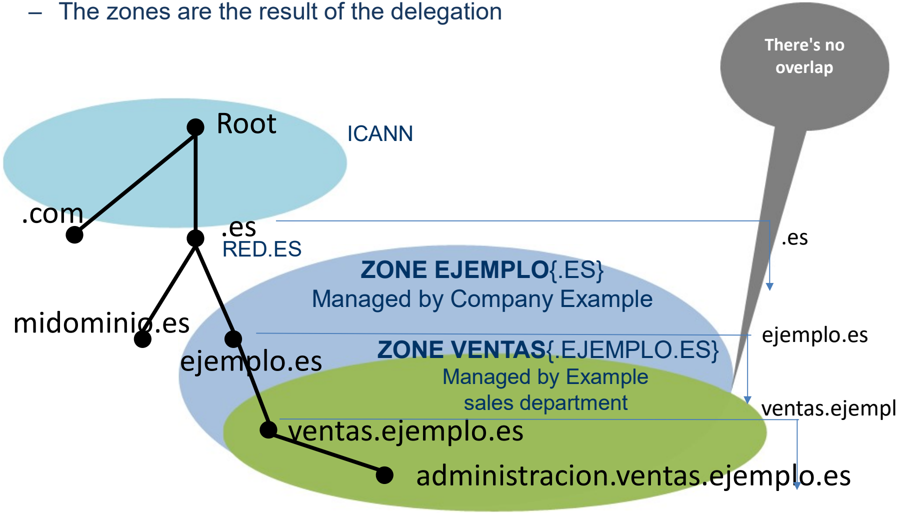
ICANN delegates to red.es that manages the domain ".es"

Red.es delegates "ejemplo.es" to the company Example

Example can delegate the subtree “ventas. ejemplo.es" to an department

DNS name spaces >> Delegation >> Zone

- Delegation allows you to distribute the database
  - Zones are defined: parts of the tree managed by an authority
  - The zones are the result of the delegation



DNS name spaces >> Delegation >> Obligations

- The delegation allows
  - The delegate freely assigning records within their zone
    - Names, addresses and other records
  - To the entity that delegates to decrease its load -> scalability
- The delegation requires
  - Creation of a SOA record indicating such delegation
  - The receiver of the delegation must have DNS servers
    - **Primary: Collects organization record assignment**
    - **Secondary(s) (copy of the primary) there may be one or more**

DNS Use cases

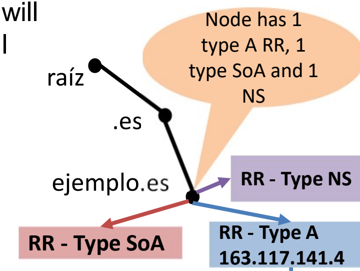
3. DNS Use cases
   - A. Fundamentals
   - B. Start of authority - SoA
   - C. Determine DNS server – NS
   - D. Translation – A/AAAA
   - E. Mail Exchange – MX
   - F. Canonical Name – CNAME
   - G. Reverse resolution

Lesson outlook

1. Introduction and context
2. Namespaces in DNS
3. DNS Use cases
4. DNS Protocol
5. Query types in DNS
6. Performance aspects in DNS
7. DNS extensions

DNS use cases >> Fundamentals (I)

- Let's look at the DNS use cases, for this we will see fundamental aspects of DNS that we will explain later
- What information does DNS store?
  - Resource Records (RR)
  - Each node in the tree can have 0, 1 or more
- What is the format of RRs?



	NAME	TYPE	CLASS	TTL	RDLEN	RDATA
LENGTH BITS	Var.	16	16	32	16	Variable
USE	Node name	Record type	IN(1)	Cache time	RDATA length	Record data
EJ.	`ejemplo.es`	`Address (A)`	`IN`	`3600`	`32`	`163.117.141.4`

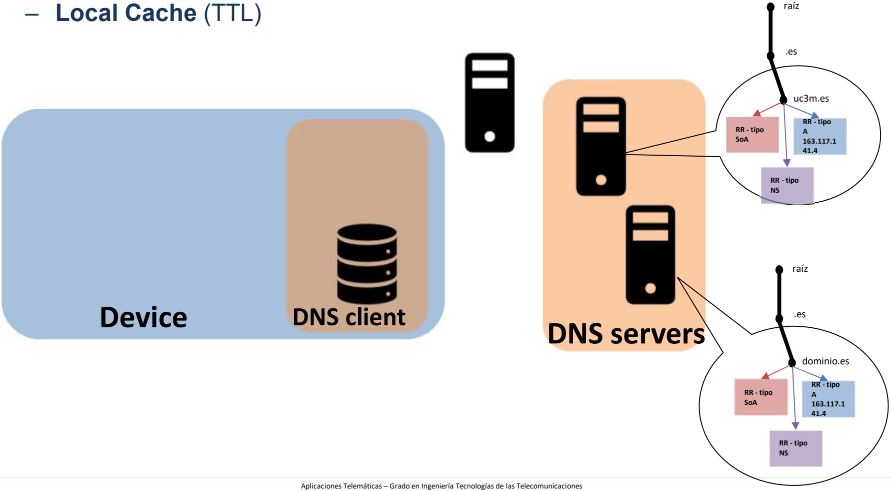
(1) Domain Name System (DNS) IANA Considerations defines values for Class of which only IN (internet) has general use today

(2) RFC2929/RFC5395 - Other CLASS values: Computer Science Network (CSNET), Chaos Net (Chaos), Hesiod

DNS use cases >> Fundamentals (II)

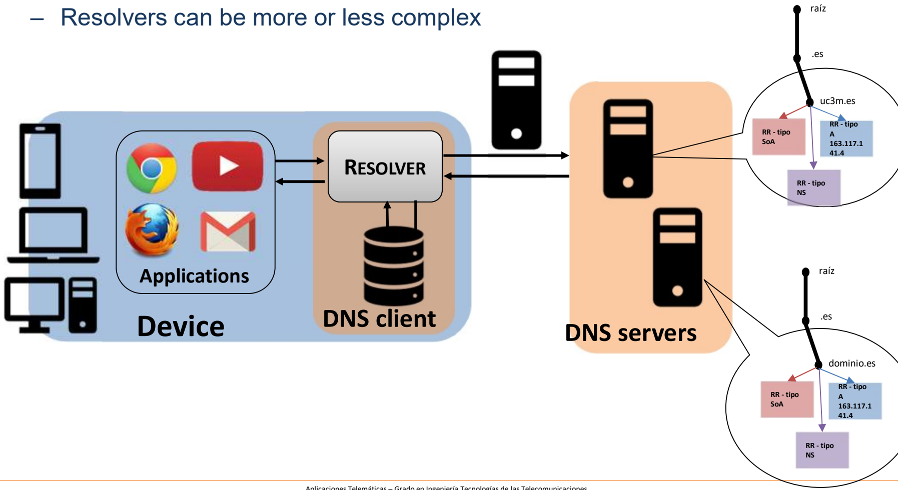
- Who provides that information?
  - Servers from the target domain (Authorized)
  - Intermediate servers (from their cache, TTL)
  - **Local Cache** (TTL)

DNS servers



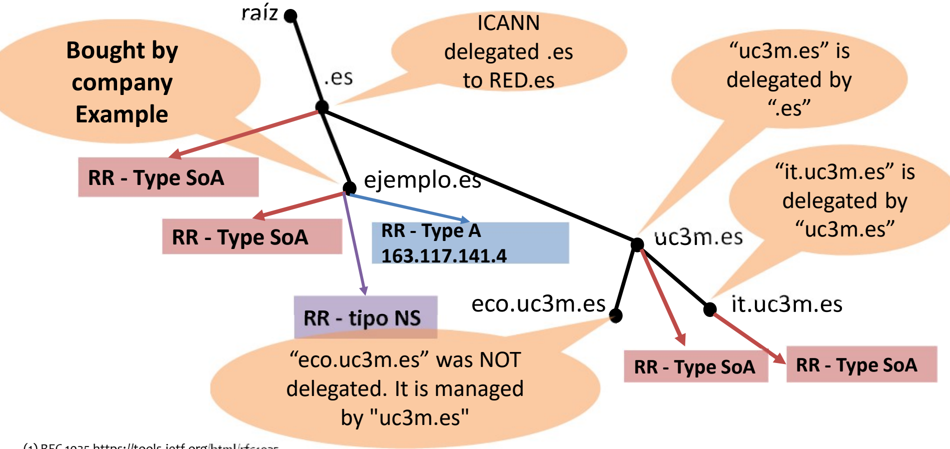
DNS use cases >> Fundamentals (II)

- Who requests that DNS information?
  - Any application that needs DNS information.
- How? With the RESOLVER
  - Resolvers can be more or less complex



DNS use cases >> Authority – SoA (I)

- Start of Authority (SoA)
  - Every piece of the tree that is delegated is a Zone
  - SoA record is used to indicate whether a particular node is delegated


raíz
.es
ejemplo.es
uc3m.es
eco.uc3m.es
it.uc3m.es
Bought by company Example
ICANN delegated .es to RED.es
“uc3m.es” is delegated by “.es”
“it.uc3m.es” is delegated by “uc3m.es”
“eco.uc3m.es” was NOT delegated. It is managed by "uc3m.es"
RR - Type SoA
RR - Type SoA
RR - Type A 163.117.141.4
RR - tipo NS
RR - Type SoA
RR - Type SoA

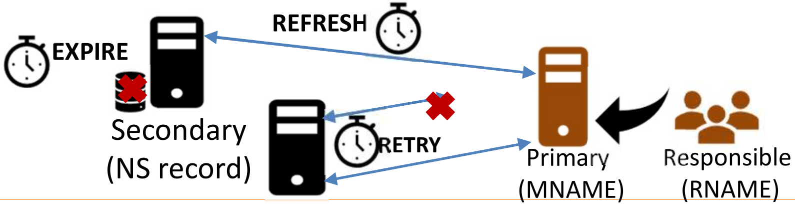
(1) RFC 1035 https://tools.ietf.org/html/rfc1035

DNS use cases >> Authority – SoA(II)

- A SOA type RR (1) stores in RDATA:
  - MNAME: domain name of the zone's primary DNS server
  - RNAME: mailing address of the person responsible for the zone
    - Change first point with "@", e.g.: dds.it.uc3m.es -> dds@it.uc3m.es
  - SERIAL: **serial number of the information version** (32 bits)
  - REFRESH: time period secondary copies primary (32 bits)
  - RETRY: **time after a refresh failure to retry** (32 bits)
  - EXPIRE: **maximum unupdated time to consider unauthorized** (if the secondary has not been able to update it will not be authorized) (32 bits)
  - MINIMUM: **Minimum TTL of any RR in the zone** (32bits)

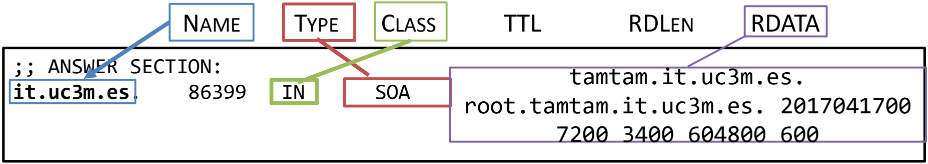
Delegation

Synchronization Primary-Secondary



DNS use cases >> Authority – SoA (III)

- Start of Authority Example (SoA)
  - We query the it.uc3m.es SoA RR (dig command)
  - The answer (in text mode) is an RR:



NAME TYPE CLASS TTL RDLEN RDATA

```
;; ANSWER SECTION:
it.uc3m.es.     86399   IN    SOA     tamtam.it.uc3m.es.
                                 root.tamtam.it.uc3m.es. 2017041700
                                      7200 3400 604800 600
```

  - a SoA type RR that is located in the it.uc3m.es tree node with TTL 86399
  - from its content:

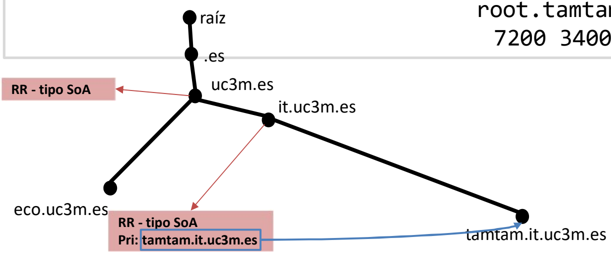
  - **tamtam.it.uc3m.es** is the primary server of the zone
  - The zone administrator has the email **root@tamtam.it.uc3m.es**
  - Serial number 2017041700, refresh time 7200, retry 3400, expires in 604800s and the minimum TTL is 600

(1) The commando dig will be studied in practices – available in https://gitlab.pervasive.it.uc3m.es/aptel/dns

DNS use cases >> Authority – SoA (IV)

- Start of Authority Example (SoA)
  - We deduced information from the tree with the response
    - it.uc3m.es has been delegated by uc3m.es
    - the primary DNS server is tamtam
    - There must be a node in the tree called tamtam

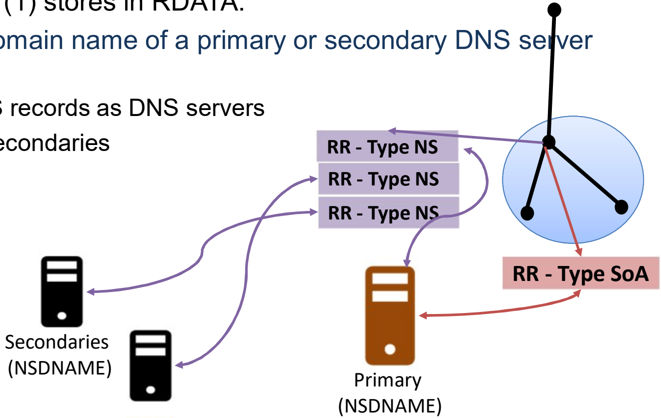
```
;; ANSWER SECTION:
it.uc3m.es.    86399   IN      SOA  tamtam.it.uc3m.es.
                                    root.tamtam.it.uc3m.es. 2017041700
                                     7200 3400 604800 600
```



(1) The command dig will be studied in practices – available in https://gitlab.pervasive.it.uc3m.es/aptel/dns

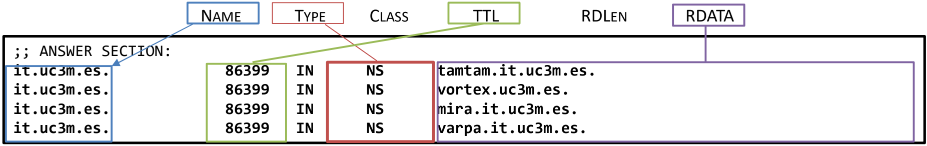
DNS use cases >> Determine DNS Server – NS (I)

- Name Server (NS)
  - Every piece of the tree that is delegated is an zone
  - Each zone has its own DNS servers
  - A primary and 1 or more secondary
- An RR of type NS (1) stores in RDATA:
  - NSDNAME: domain name of a primary or secondary DNS server in the zone
    - As many NS records as DNS servers
    - Primary + secondaries



DNS use cases >> Determine DNS Server – NS (II)

- Name Server Example (NS)
  - We query the NS type RR of it.uc3m.es (dig command (1))
  - The answer (in text mode) are several RRs



```
;; ANSWER SECTION:
it.uc3m.es.            86399   IN     NS    tamtam.it.uc3m.es.
it.uc3m.es.            86399   IN     NS    vortex.uc3m.es.
it.uc3m.es.            86399   IN     NS    mira.it.uc3m.es.
it.uc3m.es.            86399   IN     NS    varpa.it.uc3m.es.
```

  - NS RRs found in the tree node it.uc3m.es, received with TTL 86399
  - From their content

- **tamtam.it.uc3m.es, vortex.uc3m.es, mira.it.uc3m.es and varpa.it.uc3m.es** are DNS servers in the zone
- From the SoA query we made before we know that among all NS, tamtam is the primary

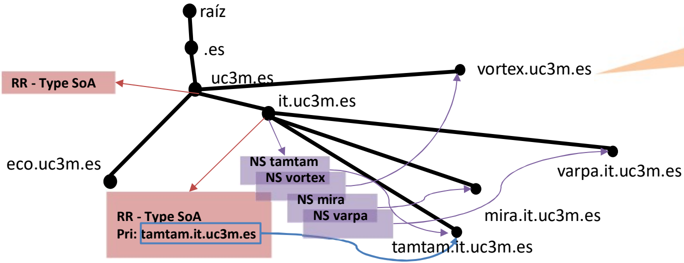
(1) The commando dig will be studied in practices – available in https://gitlab.pervasive.it.uc3m.es/aptel/dns

(2) At least two, one primary and one secondary

DNS use cases >> Determine DNS Server – NS (III)

- Name Server Example (NS)
  - We deduced from the answer
    - There must be nodes in the tree called tamtam.it.uc3m.es, vortex.uc3m.es, mira.it.uc3m.es, and varpa.it.uc3m.es
    - Each is a DNS server

```
;; ANSWER SECTION:
it.uc3m.es.             86399   IN      NS      tamtam.it.uc3m.es.
it.uc3m.es.             86399   IN      NS      vorteX.uc3m.es.
it.uc3m.es.             86399   IN      NS      mira.it.uc3m.es.
it.uc3m.es.             86399   IN      NS      varpa.it.uc3m.es.
```



It is recommended a secondary to be out of the Zone

DNS use cases >> Translation – A (I)

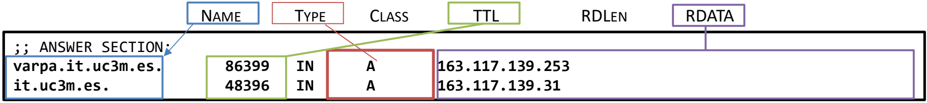
- Address (A and AAAA)
  - Some nodes in the tree will have an Address record
    - To indicate the IP address associated with a domain name
- An RR of type A (1) stores in RDATA:
  - Address: IPv4 address (32bits)
- A AAAA type RR (2) stores in RDATA
  - Address: IPv6 address (128bits)

(1) RFC 1035 https://tools.ietf.org/html/rfc1035

(2) RFC 3596 https://tools.ietf.org/html/rfc3596

DNS use cases >> Translation – A (II)

- Address Example (A)
  - We query the it.uc3m.es for A RR (dig command (1))
  - We check the type A RR of varpa.it.uc3m.es
  - The answer (in text mode) :



```
;; ANSWER SECTION:
varpa.it.uc3m.es.        86399   IN       A       163.117.139.253
it.uc3m.es.              48396   IN       A       163.117.139.31
```

- the Type A RRs we've consulted (there are more) are located in the tree nodes with it.uc3m.es domain names and varpa.it.uc3m.es
- From the content we find out:

> - **it.uc3m.es** has an Address record (you wouldn't have to)
> - **varpa.it.uc3m.es,** that is a DNS server (as we deduced earlier) has an Address record

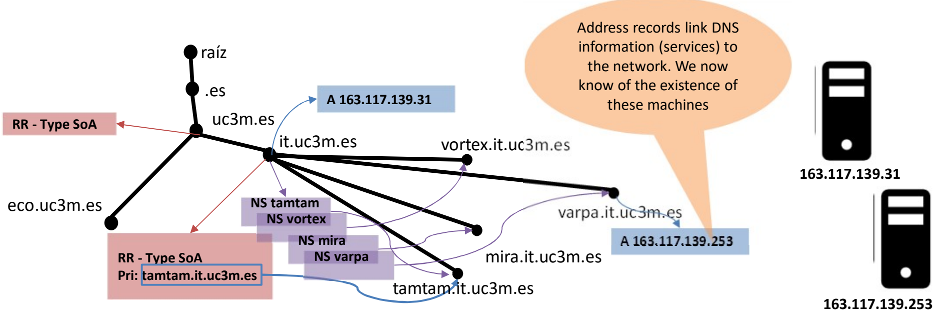
eco

(1) The commando dig will be studied in practices – available in https://gitlab.pervasive.it.uc3m.es/aptel/dns

DNS use cases >> Translation – A (III)

- Address Example (A)
  - We infer from the response that certain nodes have IP address
    - varpa.it.uc3m.es has IP address (unexpected)
    - it.uc3m.es has an IP address
  - We deduce the existence of certain servers

```
;; ANSWER SECTION:
varpa.it.uc3m.es.       86399   IN      A       163.117.139.253
it.uc3m.es.             48396   IN      A       163.117.139.31
```



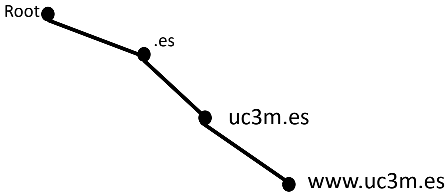
Address records link DNS information (services) to the network. We now know of the existence of these machines

Practical exercise I >> Approach

- Find out information related to www.uc3m.es
  - We'll ask ourselves questions
  - We'll make queries about known RR
- With the answers we will compose a tree
- Questions:
  - Is www.uc3m.es a zone?
    - If it is a zone get the data (primary and admin email)
    - If it's not a zone, what zone does it belong to? Get the data
  - Does the domain name www.uc3m.es have an address record?
    - One or more
    - If in the browser, instead of www.uc3m.es we use uc3m.es what happens?

Practical exercise I >> Development (I)

- Contextualize the domain name
  - We go up to the root

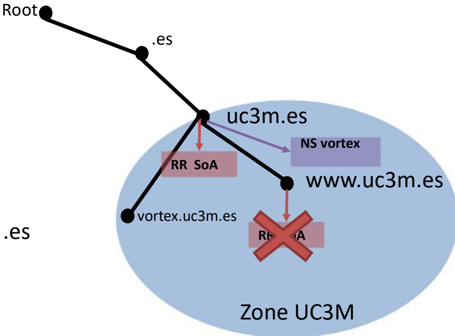


Practical exercise I >> Development (II)

- Is www.uc3m.es a zone?
  - To find out if it’s a zone I ask for the SoA record

```
dig SoA www.uc3m.es
;; ANSWER SECTION:
(no answer)
```

- What zone does it belong to?
  - Two options
    - that www.uc3m.es manages it
    - that www.uc3m.es is managed by .es



```
dig SoA uc3m.es
;; ANSWER SECTION:
uc3m.es.    86399   IN      SOA     vorteX.uc3m.es.
        netmaster.uc3m.es. 2017053101 86400 7200 2592000 172800
```

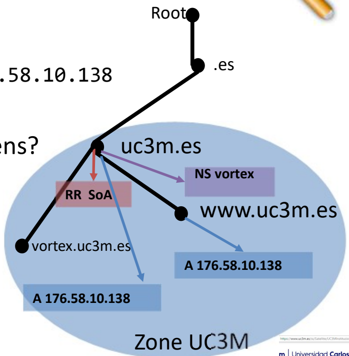
netmaster@uc3m.es

Practical exercise I >> Development (III)

- www.uc3m.es has an address record?
  - To find out if it has an A record

```
dig A www.uc3m.es
;; ANSWER SECTION:
www.uc3m.es.    85       IN       A        176.58.10.138
```

- If I remove "www" to www.uc3m.es what happens?
  - The browser requires the A record
    - Not uc3m.es www.uc3m.es



```
dig A uc3m.es
;; ANSWER SECTION:
uc3m.es.          299      IN       A        176.58.10.138
```

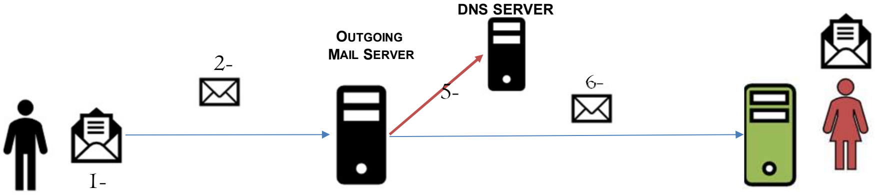
176.58.10.138

Practical exercise I >> Conclusions

- DNS allows you to find out what "services" are in a domain
  - Know where there is a change of responsibility (SoA)
  - Know the DNS servers that store information (NS)
    - Primary with SoA
  - Know which nodes have associated addresses (A)
  - Know if a machine exists or not

DNS use cases >> Mail Exchange – MX (I)

- Mail Exchange (MX)
  - Domains indicate where to send mail to them
- Brief explanation (we'll see it in mail)



1- Bob (bob@uc3m.es) writes an email to alice@mec.es

2- Bob taps send and mail travels to outgoing mail server

3- The server reads the recipient: alice@mec.es

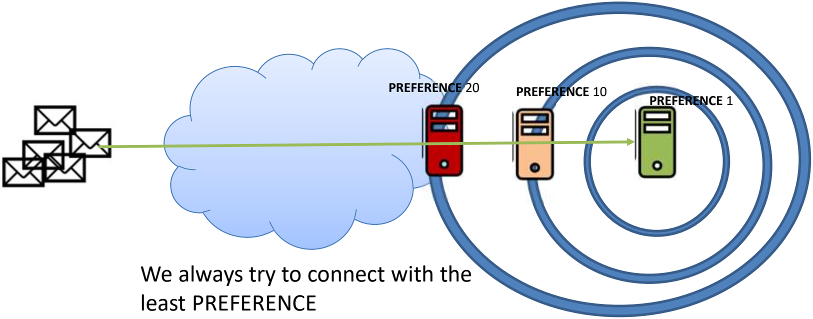
4- The server does not know who alice is, but knows the domain in which alice receives mail (mec.es)

5- asks the DNS server for the incoming mail server (MX) of domain mec.es

6- Send the mail to the mail server indicated in the DNS response

DNS use cases >> Mail Exchange – MX (II)

- An MX type RR (1) stores in RDATA
  - PREFERENCE: indicate the preference with a number of 16bits (the lower the higher the priority)
  - EXCHANGE: Mail server domain name

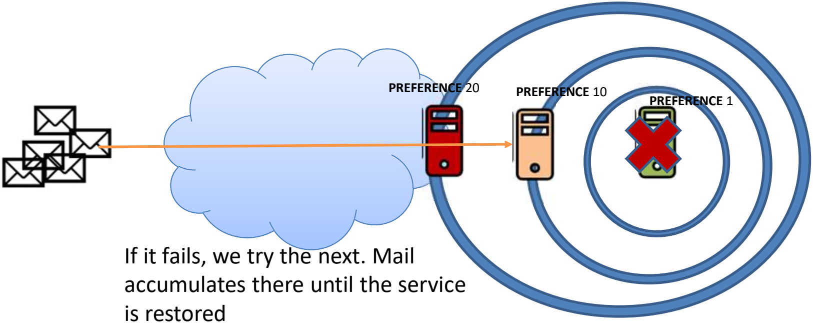


We always try to connect with the least PREFERENCE

(1) RFC 1035 https://tools.ietf.org/html/rfc1035

DNS use cases >> Mail Exchange – MX (II)

- An MX type RR (1) stores in RDATA
  - PREFERENCE: indicate the preference with a number of 16bits (the lower the higher the priority)
  - EXCHANGE: Mail server domain name

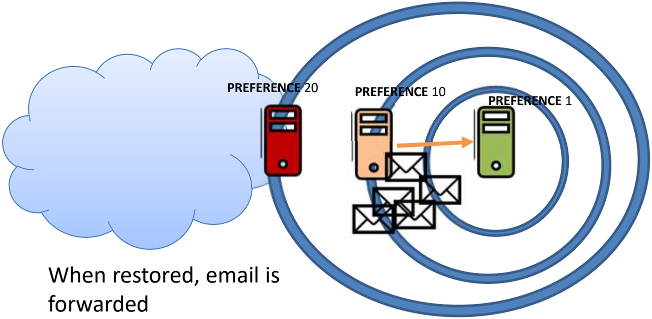


If it fails, we try the next. Mail accumulates there until the service is restored

(1) RFC 1035 https://tools.ietf.org/html/rfc1035

DNS use cases >> Mail Exchange – MX (II)

- An MX type RR (1) stores in RDATA
  - PREFERENCE: indicate the preference with a number of 16bits (the lower the higher the priority)
  - EXCHANGE: Mail server domain name

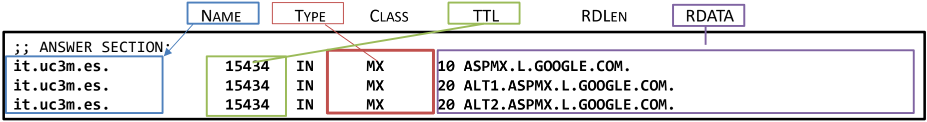


When restored, email is forwarded

(1) RFC 1035 https://tools.ietf.org/html/rfc1035

DNS use cases >> Mail Exchange – MX (III)

- Mail Exchange Example (MX)
  - We query the RR type MX of it.uc3m.es (command dig (1))
  - The answer (in text mode) :



```
;; ANSWER SECTION:
it.uc3m.es.          15434  IN      MX    10 ASPMX.L.GOOGLE.COM.
it.uc3m.es.          15434  IN      MX    20 ALT1.ASPMX.L.GOOGLE.COM.
it.uc3m.es.          15434  IN      MX    20 ALT2.ASPMX.L.GOOGLE.COM.
```

- RRs of type MX we received (there are more) are at it.uc3m.es node
- From the response, we find out:

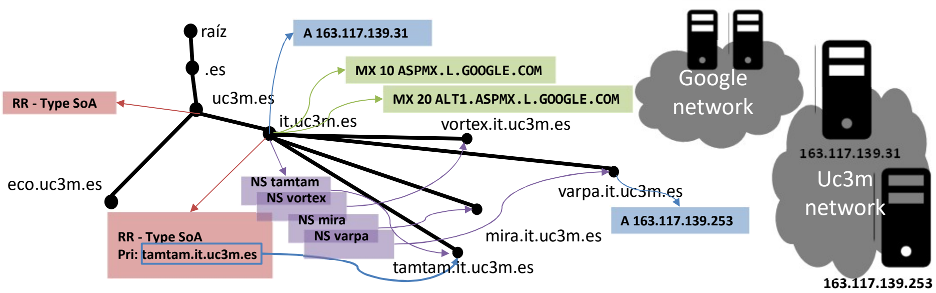
- **The university manages your mail with Gmail (hence pointing to Google)**
- **There are several servers, each with a preference of 10, 20...**
- **The mail server will try the 10 first, then the one with 20...**

(1) The commando dig will be studied in practices – available in https://gitlab.pervasive.it.uc3m.es/aptel/dns

DNS use cases >> Mail Exchange – MX (IV)

- Mail Exchange example (MX)
  - We infer that there are several servers that accept mail
  - We deduce the existence of certain servers

```
;; ANSWER SECTION:
it.uc3m.es.             15434   IN      MX      10 ASPMX.L.GOOGLE.COM.
it.uc3m.es.             15434   IN      MX      20 ALT1.ASPMX.L.GOOGLE.COM.
it.uc3m.es.             15434   IN      MX      20 ALT2.ASPMX.L.GOOGLE.COM.
```



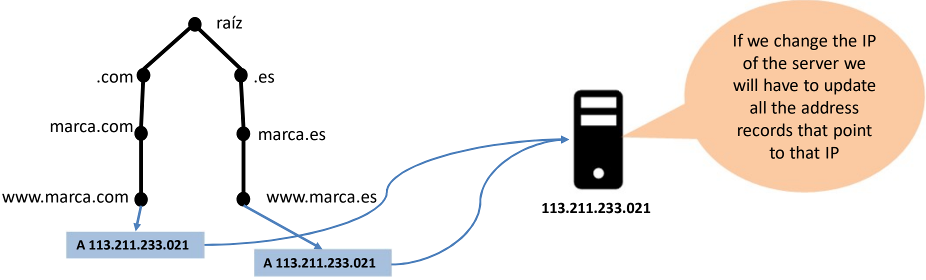
DNS use cases >> Canonical Name - CNAME (I)

- Cannonical Name (CNAME)
  - Indicates the canonical name of an alias
    - indicates that a domain name, such www.it.uc3m.es **is an alias of another** contrabajo.it.uc3m.es (which would be the canonical name)
    - The CNAME value must always be another domain name
      - never an IP
  - The domain name corresponding to the alias (www.it.uc3m.es) must not contain other RR as A (1)
    - The only exception is DNSSEC
- What changes to using multiple A records instead of CNAME?

DNS use cases >> Canonical Name - CNAME (II)

- What's the difference with multiple A records?
  - Let's say www.marca.es and www.marca.com want it to be served by the same web server

- First option: both www.marca.es and www.marca.com point to the same web server using address (A)
  - Both have the same importance

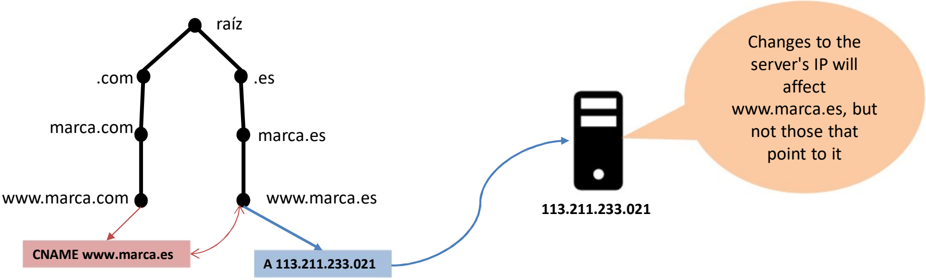


If we change the IP of the server we will have to update all the address records that point to that IP

DNS use cases >> Canonical Name - CNAME (III)

- What's the difference with multiple A records?
  - Let's say www.marca.es and www.marca.com want it to be served by the same web server

- Second option: www.marca.es is the main brand. www.marca.com used to collect more traffic or coporative image
- www.marca.com [.net, .info…] is an alias of www.marca.es



Changes to the server's IP will affect www.marca.es, but not those that point to it

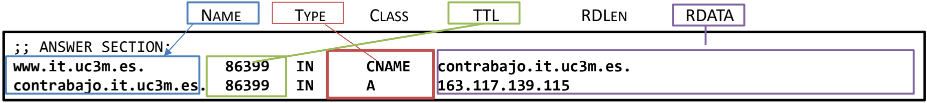
DNS use cases >> Canonical Name - CNAME (IV)

- An RR of type CNAME (1) stores in RDATA
  - CNAME: Canonical name referred to the alias (domain name) consulted

(1) RFC 1035 https://tools.ietf.org/html/rfc1035

DNS use cases >> Canonical Name - CNAME (V)

- Canonical Name Example (CNAME)
  - We check the RR type CNAME of www.it.uc3m.es
  - The answer (in text mode)
    - Provides not only CNAME but also canonical record A (additional processing according to RFC)



```
;; ANSWER SECTION:
www.it.uc3m.es.          86399   IN      CNAME   contrabajo.it.uc3m.es.
contrabajo.it.uc3m.es.   86399   IN      A       163.117.139.115
```

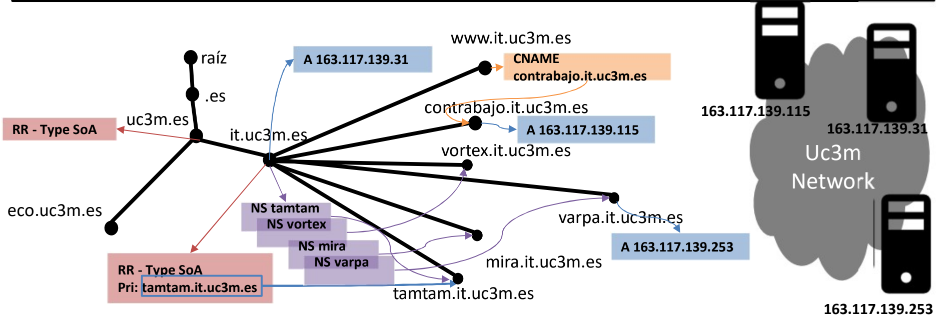
- The CNAME RR is in the node with name www.it.uc3m.es
- From the response, we find out:

- **The www.it.uc3m.es alias points to its canonical name contrabajo.it.uc3m.es**
- **The domain name contrabajo.it.uc3m.es has an address (A) record of value 163.117.139.115**

DNS use cases >> Canonical Name - CNAME (V)

- Canonical Name Example (CNAME)
  - We deduce that there is another node of the tree called contrabajo
    - **www.it.uc3m.es points to contrabajo.it.uc3m.es**
    - **contrabajo.it.uc3m.es has an A record**

```
;; ANSWER SECTION:
www.it.uc3m.es.          86399   IN      CNAME   contrabajo.it.uc3m.es.
contrabajo.it.uc3m.es.   86399   IN      A       163.117.139.115
```

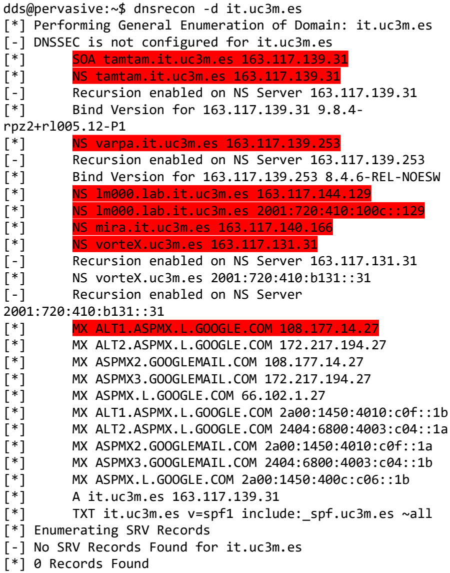


Practical Exercise II >> Approach

- Inspect a domain
  - Find out the distribution of services for a domain
  - Through various sources of information
  - Using the dns-recon script
- Instructions at
  - https://gitlab.gast.it.uc3m.es/aptel/dns-recon

Practical Exercise II >> Introduction

- Standard
  - Find out the most important records
  - Some of us already know them



```
dds@pervasive:~$ dnsrecon -d it.uc3m.es
[*] Performing General Enumeration of Domain: it.uc3m.es
[-] DNSSEC is not configured for it.uc3m.es
[*]      SOA tamtam.it.uc3m.es 163.117.139.31
[*]      NS tamtam.it.uc3m.es 163.117.139.31
[-]      Recursion enabled on NS Server 163.117.139.31
[*]      Bind Version for 163.117.139.31 9.8.4-
rpz2+rl005.12-P1
[*]      NS varpa.it.uc3m.es 163.117.139.253
[-]      Recursion enabled on NS Server 163.117.139.253
[*]      Bind Version for 163.117.139.253 8.4.6-REL-NOESW
[*]      NS lm000.lab.it.uc3m.es 163.117.144.129
[*]      NS lm000.lab.it.uc3m.es 2001:720:410:100c::129
[*]      NS mira.it.uc3m.es 163.117.140.166
[*]      NS vorteX.uc3m.es 163.117.131.31
[-]      Recursion enabled on NS Server 163.117.131.31
[*]      NS vorteX.uc3m.es 2001:720:410:b131::31
[-]      Recursion enabled on NS Server
2001:720:410:b131::31
[*]      MX ALT1.ASPMX.L.GOOGLE.COM 108.177.14.27
[*]      MX ALT2.ASPMX.L.GOOGLE.COM 172.217.194.27
[*]      MX ASPMX2.GOOGLEMAIL.COM 108.177.14.27
[*]      MX ASPMX3.GOOGLEMAIL.COM 172.217.194.27
[*]      MX ASPMX.L.GOOGLE.COM 66.102.1.27
[*]      MX ALT1.ASPMX.L.GOOGLE.COM 2a00:1450:4010:c0f::1b
[*]      MX ALT2.ASPMX.L.GOOGLE.COM 2404:6800:4003:c04::1a
[*]      MX ASPMX2.GOOGLEMAIL.COM 2a00:1450:4010:c0f::1a
[*]      MX ASPMX3.GOOGLEMAIL.COM 2404:6800:4003:c04::1b
[*]      MX ASPMX.L.GOOGLE.COM 2a00:1450:400c:c06::1b
[*]      A it.uc3m.es 163.117.139.31
[*]      TXT it.uc3m.es v=spf1 include:_spf.uc3m.es ~all
[*] Enumerating SRV Records
[-] No SRV Records Found for it.uc3m.es
[*] 0 Records Found
```

Practical Exercise II >> Introduction

- Brute force
  - Find out a lot of records
  - We can build a map of the network

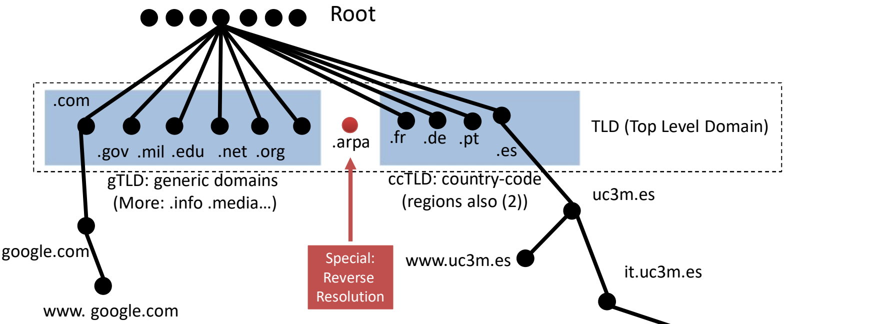
```
dds@pervasive:~$ sudo dnsrecon -d it.uc3m.es  -t brt
[*] No file was specified with domains to check.
[*] Using file provided with tool:
/usr/share/dnsrecon/namelist.txt
[*]      A amarillo.it.uc3m.es 10.116.101.240
[*]      CNAME apache.it.uc3m.es arpa.it.uc3m.es
[*]      A arpa.it.uc3m.es 163.117.139.120
[*]      CNAME backup.it.uc3m.es backup02.lab.it.uc3m.es
[*]      A backup02.lab.it.uc3m.es 163.117.144.194
[*]      A blogs.it.uc3m.es 163.117.140.145
[*]      CNAME bsd1.it.uc3m.es arpa.it.uc3m.es
[*]      A arpa.it.uc3m.es 163.117.139.120
[*]      CNAME cache.it.uc3m.es guitarra.it.uc3m.es
[*]      A guitarra.it.uc3m.es 163.117.139.106
[*]      A dns.it.uc3m.es 163.117.139.253
[*]      A dns.it.uc3m.es 163.117.139.120
[*]      CNAME dns3.it.uc3m.es arpa.it.uc3m.es
[*]      A arpa.it.uc3m.es 163.117.139.120
[*]      CNAME dns1.it.uc3m.es varpa.it.uc3m.es
[*]      A varpa.it.uc3m.es 163.117.139.253
[*]      CNAME dns2.it.uc3m.es tamtam.it.uc3m.es
[*]      A tamtam.it.uc3m.es 163.117.139.31
[*]      CNAME foros.it.uc3m.es contrabajo.it.uc3m.es
[*]      A contrabajo.it.uc3m.es 163.117.139.115
[*]      CNAME ftp.it.uc3m.es cuerno.it.uc3m.es
[*]      A cuerno.it.uc3m.es 163.117.139.105
…. continua
```

Practical Exercise II >> what to do

- Perform two domain surveys
  - subdomain of uc3m.es
    - From within the network
    - At home
  - Any other domain of your choice
    - Highlight known records and their use

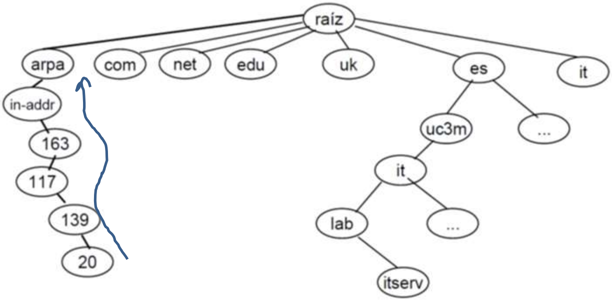
DNS use cases >> Reverse Resolution

- Reverse resolution



DNS use cases >> Reverse Resolution

- Records of type PTR are used “point queries”
- Tuples:
  - RR PTR for reverse resolution
    - (20.139.117.163.in-addr.arpa, TTL, IN, PTR, itserv.lab.it.uc3m.es)
  - RR Address
    - (itserv.lab.it.uc3m.es, TTL, IN, A, 163.117.139.20)



DNS use cases >> Reverse Resolution

- Reverse resolution
  - Consider a domain called “midominio.com”
    - They will publish their name tree
    - They will also publish the reverse resolution tree
  - There is no one-to-one relation between names and IPs
    - So, reverse resolution cannot be one-to-one always

Conclusions so far

- The DNS namespace has been presented
  - Designed for humans
  - Hierarchical
  - Distributed on different DNS servers
- RRs store information for use cases beyond translation
  - Authority Start (SoA)
  - Name Servers (NS)
  - Mail (MX)
  - Alias... (CNAME)
- Reverse resolution (.arpa tree and PTR record)
  - Find out information about a domain

DNS Protocol

4. DNS Protocol
    - A. Introduction
    - B. Queries
    - C. Message format

Lesson outlook

1. Introduction and context
2. Namespaces in DNS
3. DNS Use cases
4. DNS Protocol
5. DNS extensions

DNS Protocol

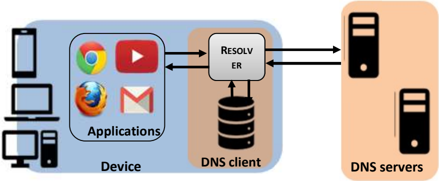
- We've discussed
  - Record format
  - Use cases
  - Primary and secondary DNS existence per domain
- We are going to discuss now,
  - How to exchange information
  - Types of queries
  - Format of DNS messages

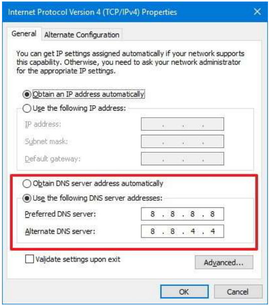
DNS Protocol >> Introduction to DNS Protocol (I)

- Uses port 53 UDP and 53 TCP
  - Usually UDP
    - But UDP has a máximum size of 512 bytes (conservative)
  - TCP when responses goes over 512 byte
    - Zone transfer
    - Response of any kind does not fit into an UDP datagram
    - DNS messages uses a 2 byte field to indicate lenght

DNS Protocol >> Queries (I)

- Overall
  - Client (resolver) requests information from a DNS server
  - the server is designated by your ISP (or obtained by zeronconf)
- Recursive Queries:
  - The server asks the next server and the server takes care of it and so on
- Iterative Queries
  - The server asks the next server and the server only tells who should ask
- Mixed Queries




Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: 8 . 8 . 4 . 4

□ Validate settings upon exit

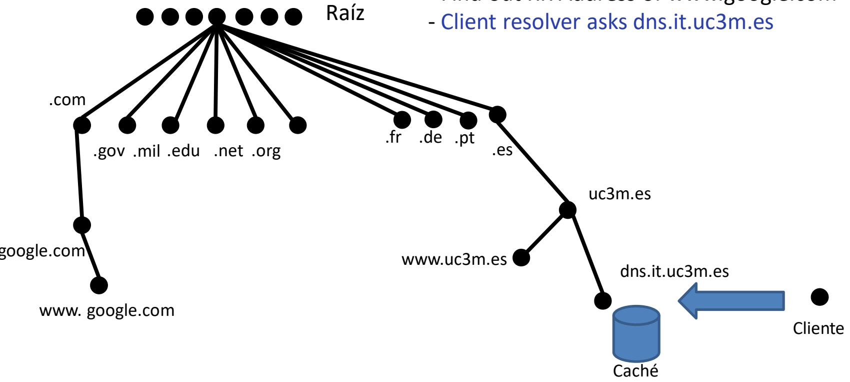
DNS Protocol >> Queries (II)

- Cache
  - Usefull to reduce traffic. Intermediate DNS servers store results during TTL time to accelerate others queries
    - Prevents continuous queries to remote servers
  - The Time to live (TTL) indicates per RR how long can be a RR stored in a chache
    - Once TTL is over, the record is deleted
- If a resolver obtains a RR from a cache, the response will be flagged as a non authorized record
  - Indicates the information is not fresh. Does not mean is not valid
  - There are DNS servers that acts just as a cache (not authorized for any zone).
    - They are use to reduce the DNS traffic (as in the labs)

DNS Protocol >> Queries (IV)

- How a query works

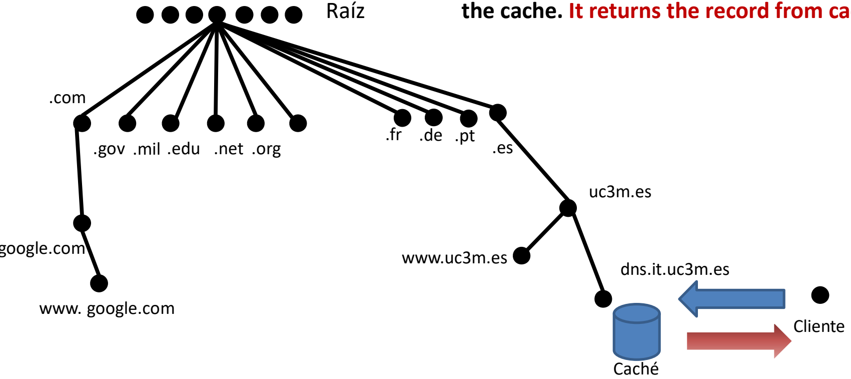
- The client has as DNS assigned dns.it.uc3m.es
- Find out RR Address of www.google.com
- Client resolver asks dns.it.uc3m.es



DNS Protocol >> Queries (V)

- The “trees” reside in the primary and secondary of each zone, you have to know who to ask

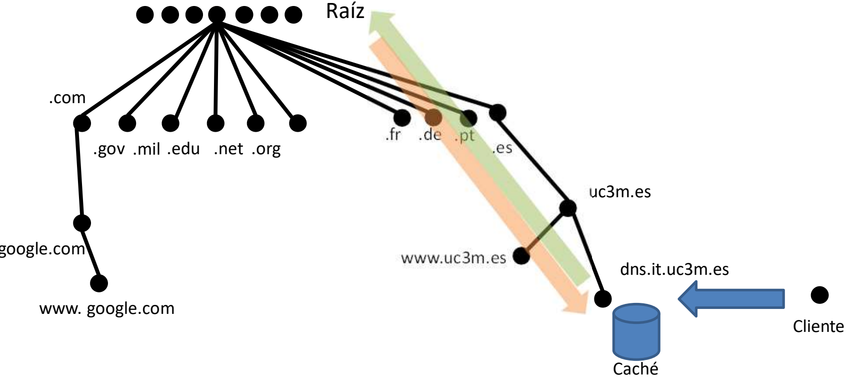
- The client has as DNS assigned dns.it.uc3m.es
- Find out RR Address of www.google.com
- Client solving asks dns.it.uc3m.es
- **Someone recently asked for it (<TTL) so it is in the cache. It returns the record from cache**



DNS Protocol >> Queries (VI)

- What happens if it is **not already in the cache**

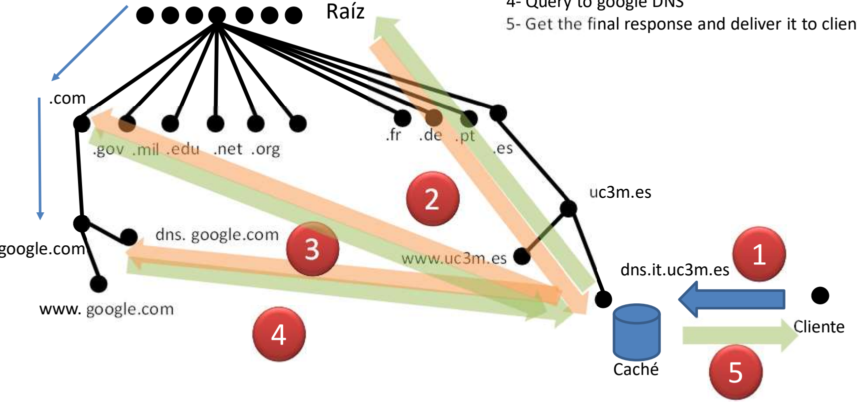
- Customer solving asks dns.it.uc3m.es
- dns.it.uc3m.es doesn't have it in the cache
- Query to root DNS (or other intermediate DNS)
- The root DNS tells you the NS records of .com



DNS Protocol >> Queries (VII)

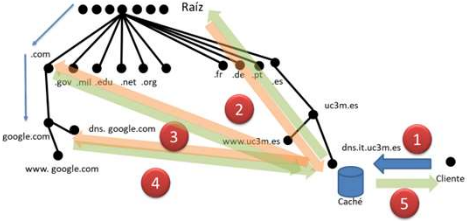
- We start from the root and go up in the tree

1- Find out RR Address of www.google.com
2- dns.it.uc3m.es doesn't have it in the cache
so it requests information to root servers, the root servers
answer with .com NS servers (in authority section)
3- dns.it.uc3m.es requests the record to .com DNS servers
and get the NS records of google.com (in authority section)
4- Query to google DNS
5- Get the final response and deliver it to client



DNS Protocol >> Queries >> Mixed Query

- Explain what kind of query/response is the one mentioned in slide Queries (VII)



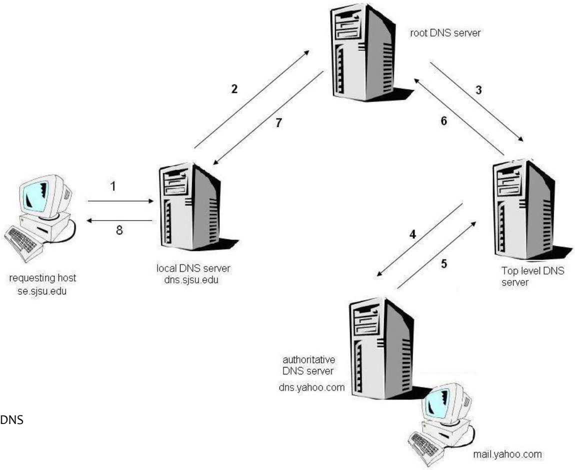
- Identify the RRs returned in every case

DNS Protocol >> Queries (VIII)

- Resolving queries a local name server.
  - Does the domain consulted fall under his jurisdiction?
  - YES: Returns records for the resource.
    - Authorized records.
  - NO: Do you have it in the cache?
    - YES: Returns records from the resource (unauthorized)
    - NO: two possibilities
      - Recursive query.
        - » Sends a query message to another server (which can in turn ask another server, etc.).
        - » Returns the obtained response
        - » Caches a copy during the "lifetime" of the log.
      - Iterative query.
        - » Returns the address of the next server to contact.

DNS Protocol >> Queries >> Recursive Query

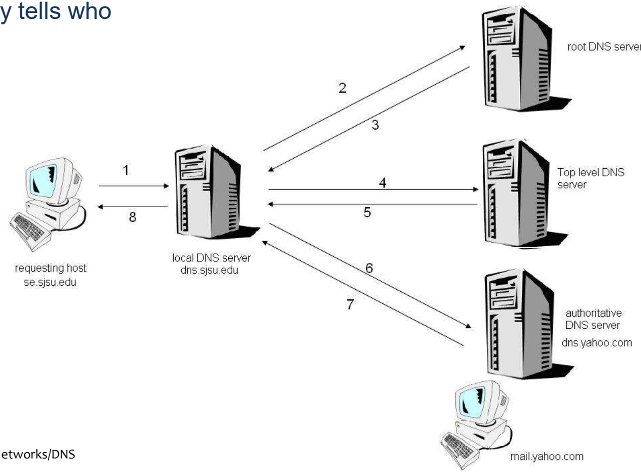
- Recursive Queries:
  - The server asks the next server and the server takes care of it, so on



https://en.wikibooks.org/wiki/Communication_Networks/DNS

DNS Protocol >> Queries >> Iterative Query

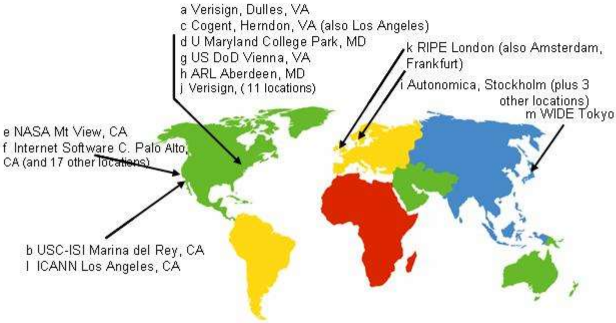
- Iterative queries
  - The server asks the next server and the server only tells who should ask



https://en.wikibooks.org/wiki/Communication_Networks/DNS

DNS Protocol >> Queries >> Mixed Query

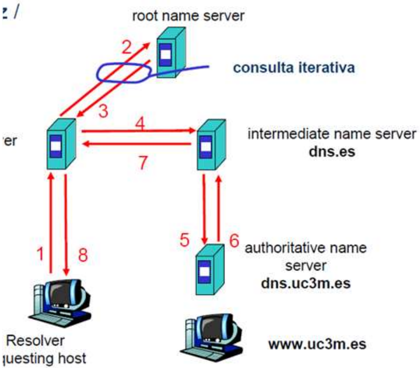
- Mixed queries
  - ROOT servers are a scarce resource


a Verisign, Dulles, VA
c Cogent, Herndon, VA (also Los Angeles)
d U Maryland College Park, MD
g US DoD Vienna, VA
h ARL Aberdeen, MD
j Verisign, (11 locations)
k RIPE London (also Amsterdam, Frankfurt)
i Autonomica, Stockholm (plus 3 other locations)
m WIDE Tokyo
e NASA Mt View, CA
f Internet Software C. Palo Alto, CA (and 17 other locations)
b USC-ISI Marina del Rey, CA
l ICANN Los Angeles, CA

https://en.wikibooks.org/wiki/Communication_Networks/DNS

DNS Protocol >> Queries >> Mixed Query

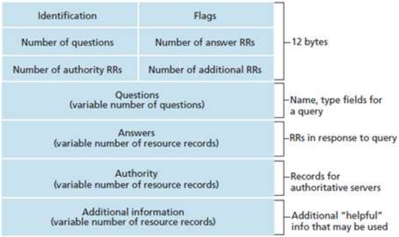
- Mixed queries
  - ROOT servers are a scarce resource



https://en.wikibooks.org/wiki/Communication_Networks/DNS

DNS Protocol >> Message format (I)

- The format of a message is (same for query/response)

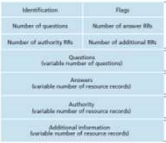


Identification	Flags	12 bytes
Number of questions	Number of answer RRs	
Number of authority RRs	Number of additional RRs	
Questions (variable number of questions)		Name, type fields for a query
Answers (variable number of resource records)		RRs in response to query
Authority (variable number of resource records)		Records for authoritative servers
Additional information (variable number of resource records)		Additional "helpful" info that may be used

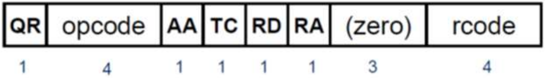
- The client only sends requests.
- The server returns:
  - Requests
  - Response resource logs to the request made.
  - Authorization information: RR of the zone's authorized name servers.
  - Additional information: prefetching responses to other possible requests.

DNS Protocol >> Message format (II)

- Identifies: unique name to match responses with queries
- Parameters:
  - bit 0: 0=request, 1=response.
  - bits 1-4: 0=standar, 1=reverse, 2=server state
  - bit 5: 1 is authoritative (aa-authoritative answer).
  - bit 6: 1 if truncated (tc-message truncated).
  - bit 7: 1 if recursión desired (rd-recursion desired).
  - bit 8: 1 if recursión available (ra-recursion available).
  - bits 9-11: reserved
  - bits 12-15: 0=no error, 1=bad request, 2=server fail, 3=name does not exist



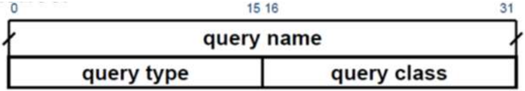
Identification	Flags
Number of questions	Number of answer RRs
Number of authority RRs	Number of additional RRs
Questions (variable number of questions)	
Answers (variable number of resource records)	
Authority (variable number of resource records)	
Additional information (variable number of resource records)	

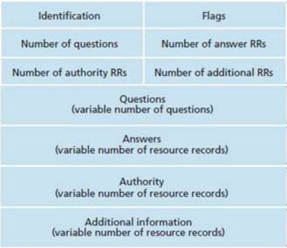


QR	opcode	AA	TC	RD	RA	(zero)	rcode
1	4	1	1	1	1	3	4

DNS Protocol >> Message format (III)

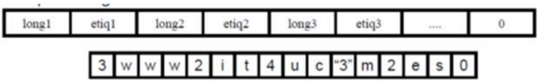
- Request:





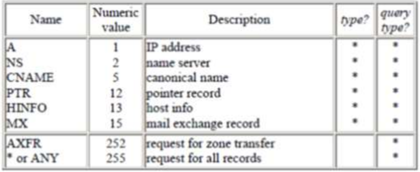
Identification	Flags
Number of questions	Number of answer RRs
Number of authority RRs	Number of additional RRs
Questions (variable number of questions)	
Answers (variable number of resource records)	
Authority (variable number of resource records)	
Additional information (variable number of resource records)	

- Domain name (any number of octects).
  - Sequence of labels
  - Every label=lenth (8bits)+ label
  - Last label lenght 0
  - Type of request (16 bits): A, MX, NS...
  - Type of request (16 bits): IN (1).



DNS Protocol >> Message format (IV)

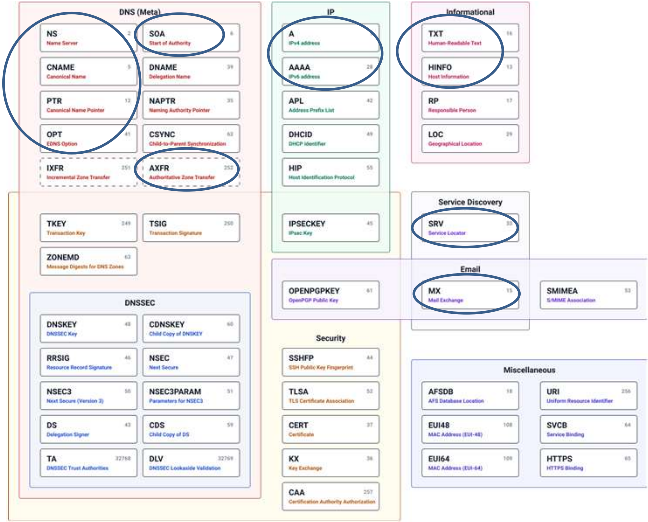
- Responses:
  - May contain 0, 1 or several RR
  - Every record contains
    - Domain name
    - Type (16 bits): A, MX, NS...
    - Class (16 bits): IN (1).
    - TTL (32 bits): second to be persisted in chache
    - Data length (16bits) in octects.
    - Data



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		•

DNS Protocol >> Message format (IV-bis)

- Responses: all the records that can be found in DNS request/response



DNS (Meta)

NS	Name Server	2
SOA	Start of Authority	6
CNAME	Canonical Name	5
DNAME	Delegation Name	39
PTR	Canonical Name Pointer	12
NAPTR	Naming Authority Pointer	35
OPT	EDNS Option	41
CSYNC	Child-to-Parent Synchronization	62
IXFR	Incremental Zone Transfer	251
AXFR	Authoritative Zone Transfer	252
TKEY	Transaction Key	249
TSIG	Transaction Signature	250
ZONEMD	Message Digests for DNS Zones	63

DNSSEC

DNSKEY	DNSSEC Key	48
CDNSKEY	Child Copy of DNSKEY	60
RRSIG	Resource Record Signature	46
NSEC	Next Secure	47
NSEC3	Next Secure (Version 3)	50
NSEC3PARAM	Parameters for NSEC3	51
DS	Delegation Signer	43
CDS	Child Copy of DS	59
TA	DNSSEC Trust Authorities	32768
DLV	DNSSEC Lookaside Validation	32769

IP

A	IPv4 address	1
AAAA	IPv6 address	28
APL	Address Prefix List	42
DHCID	DHCP Identifier	49
HIP	Host Identification Protocol	55
IPSECKEY	IPsec Key	45

Informational

TXT	Human-Readable Text	16
HINFO	Host Information	13
RP	Responsible Person	17
LOC	Geographical Location	29

Service Discovery

SRV	Service Locator	33

Email

OPENPGPKEY	OpenPGP Public Key	61
MX	Mail Exchange	15
SMIMEA	S/MIME Association	53

Security

SSHFP	SSH Public Key Fingerprint	44
TLSA	TLS Certificate Association	52
CERT	Certificate	37
KX	Key Exchange	36
CAA	Certification Authority Authorization	257

Miscellaneous

AFSDB	AFS Database Location	18
URI	Uniform Resource Identifier	256
EUI48	MAC Address (EUI-48)	108
SVCB	Service Binding	64
EUI64	MAC Address (EUI-64)	109
HTTPS	HTTPS Binding	65

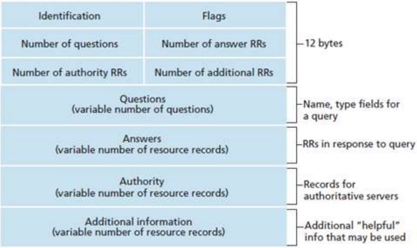
○ Discussed in class

DNS Protocol >> Message format (V)

- Responses:
  - Servers may return more information tan it was requested trying to anticípate client's future requests
  - For instance, CNAME/MX/NS requests retunrn a name but not an IP address
    - So, the response will also contain the IP address in “additional section”

DNS Protocol >> Message format (VI)

```
~> dig www.ietf.org
; <<>> DiG 9.2.1 <<>> www.ietf.org
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52261
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 4

;; QUESTION SECTION:
;www.ietf.org. IN A

;; ANSWER SECTION:
www.ietf.org. 3600 IN A 132.151.6.75
www.ietf.org. 3600 IN A 65.246.255.51

;; AUTHORITY SECTION:
ietf.org. 3600 IN NS ns.ietf.org.
ietf.org. 3600 IN NS ns.handle.net.
ietf.org. 3600 IN NS ns2.cw.net.
ietf.org. 3600 IN NS ns01.savvis.net.
ietf.org. 3600 IN NS ns.CNRI.Reston.VA.US.

;; ADDITIONAL SECTION:
ns.ietf.org. 48704 IN A 132.151.1.19
ns.handle.net. 105514 IN A 209.225.25.20
ns2.cw.net. 36532 IN A 204.70.57.242
ns01.savvis.net. 160628 IN A 204.70.128.1

;; Query time: 156 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Oct 13 20:27:42 2004
;; MSG SIZE rcvd: 263
```



Identification	Flags
Number of questions	Number of answer RRs
Number of authority RRs	Number of additional RRs

12 bytes

Questions (variable number of questions) — Name, type fields for a query

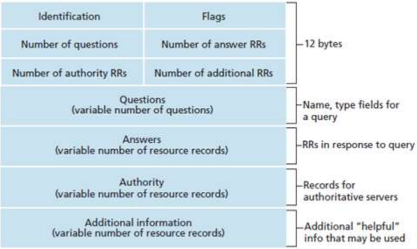
Answers (variable number of resource records) — RRs in response to query

Authority (variable number of resource records) — Records for authoritative servers

Additional information (variable number of resource records) — Additional "helpful" info that may be used

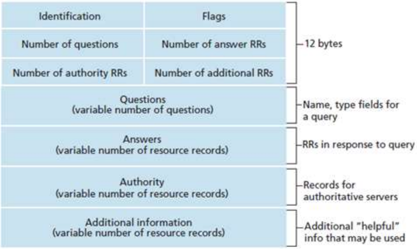
DNS Protocol >> Message format (VII)

```
dig -t MX it.uc3m.es @tamtam.it.uc3m.es
; <<>> DiG 9.2.1 <<>> -t MX it.uc3m.es @tamtam.it.uc3m.es
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10381
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 6, ADDITIONAL: 13

;; QUESTION SECTION:
;it.uc3m.es. IN MX

;; ANSWER SECTION:
it.uc3m.es. 120 IN MX 9 mail.rediris.es.
it.uc3m.es. 120 IN MX 5 smtp.uc3m.es.
it.uc3m.es. 120 IN MX 6 smtp01.uc3m.es.
it.uc3m.es. 120 IN MX 6 smtp02.uc3m.es.
it.uc3m.es. 120 IN MX 6 smtp03.uc3m.es.

;; AUTHORITY SECTION:
it.uc3m.es. 120 IN NS varpa.it.uc3m.es.
it.uc3m.es. 120 IN NS tamtam.it.uc3m.es.
it.uc3m.es. 120 IN NS vorteX.uc3m.es.
it.uc3m.es. 120 IN NS ns1.granitecanyon.com.
it.uc3m.es. 120 IN NS mira.it.uc3m.es.
it.uc3m.es. 120 IN NS lm000.lab.it.uc3m.es.
[...]
```


Identification
Flags
Number of questions
Number of answer RRs
Number of authority RRs
Number of additional RRs
12 bytes
Questions (variable number of questions)
Name, type fields for a query
Answers (variable number of resource records)
RRs in response to query
Authority (variable number of resource records)
Records for authoritative servers
Additional information (variable number of resource records)
Additional "helpful" info that may be used

DNS Protocol >> Message format (VII-cont)

```
[...]

;; ADDITIONAL SECTION:
mail.rediris.es. 26283 IN A 130.206.1.11
smtp.uc3m.es. 79228 IN A 163.117.136.121
smtp.uc3m.es. 79228 IN A 163.117.136.122
smtp.uc3m.es. 79228 IN A 163.117.136.123
smtp01.uc3m.es. 80210 IN A 163.117.136.121
smtp02.uc3m.es. 80210 IN A 163.117.136.122
smtp03.uc3m.es. 79539 IN A 163.117.136.123
varpa.it.uc3m.es. 120 IN A 163.117.139.253
tamtam.it.uc3m.es. 120 IN A 163.117.139.31
vorteX.uc3m.es. 159712 IN A 163.117.131.31
ns1.granitecanyon.com. 79512 IN A 205.166.226.38
mira.it.uc3m.es. 120 IN A 163.117.140.166
lm000.lab.it.uc3m.es. 60 IN A 163.117.144.129

;; Query time: 4 msec
;; SERVER: 163.117.139.31#53(tamtam.it.uc3m.es)
;; WHEN: Wed Oct 13 20:30:14 2004
;; MSG SIZE rcvd: 495
```



Identification	Flags
Number of questions	Number of answer RRs
Number of authority RRs	Number of additional RRs

12 bytes

Questions (variable number of questions) — Name, type fields for a query

Answers (variable number of resource records) — RRs in response to query

Authority (variable number of resource records) — Records for authoritative servers

Additional information (variable number of resource records) — Additional "helpful" info that may be used

Work

- Read and study DNS session
  - Have a look to RFC 1034 and RCF 1035
- Prepare the mandatory assigment as instructed by Lab professors
  - This page may have some information
  - https://gitlab.gast.it.uc3m.es/aptel/dns
- Find out the way to make queries to
  - Find out flags that signal a RR has been obtained from an authorized server
  - Find out the TTL of a RR
    - Careful with cache memory

DNS Extensions and other records

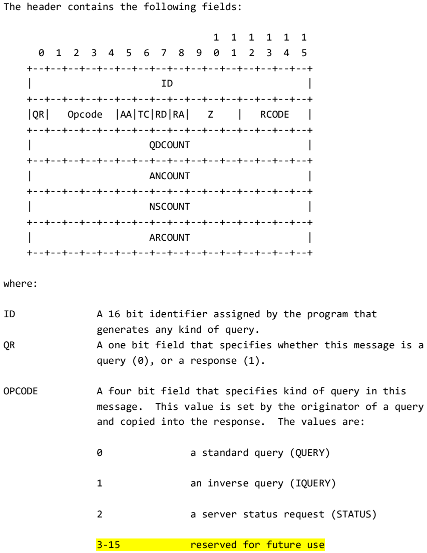
5. DNS extensions

Lesson outlook

1. Introduction and context
2. Namespaces in DNS
3. DNS Use cases
4. DNS Protocol
5. DNS extensions

DNS Extensions and other records >> DNS Extensions

- DNS was limited in functionality
  - No new parameters can be added to the DNS protocol header
- New records called OPT were added
  - OPT records are not included in the zone
  - OTR records are dynamically generated
  - Includes 16 new options and new response codes
- The header changes
  - Using the reserved bits of the header
- OPT RR uses RR type 41



```
The header contains the following fields:

                                    1  1  1  1  1  1
      0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                      ID                       |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    QDCOUNT                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    ANCOUNT                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    NSCOUNT                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
    |                    ARCOUNT                    |
    +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

where:

ID              A 16 bit identifier assigned by the program that
                generates any kind of query.
QR              A one bit field that specifies whether this message is a
                query (0), or a response (1).

OPCODE          A four bit field that specifies kind of query in this
                message.  This value is set by the originator of a query
                and copied into the response.  The values are:

                0               a standard query (QUERY)

                1               an inverse query (IQUERY)

                2               a server status request (STATUS)

                3-15            reserved for future use
```

DNS Extensions and other records >> SRV records

- Allow specifying a server and port for a given service
- Example
  - Service XMPP (protocol for messaging)
  - For domain example.com
  - Uses TCP at server.example.com port 5223

```
_xmpp._tcp.example.com. 86400 IN SRV 10 5 5223 server.example.com.
```

- Can be used for many protocols
  - LDAP, DANE, Puppet, XMPP, SIP, STUN, MineCraft…

DNS Extensions and other records >> TXT records

- Arbitrary text for many purposes
  - Domain verification
  - Domain ownership verification
  - Security…

```
example.com.   IN   TXT   "This domain name is reserved for use in documentation"
```