# Network Services 1

2019-2020

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática

Licenciatura em Engenharia Informática

Ramo de Redes e Administração de Sistemas

# *DNS*

**School Year 2019-2020**

**© - Pedro Geirinhas**

# Introduction

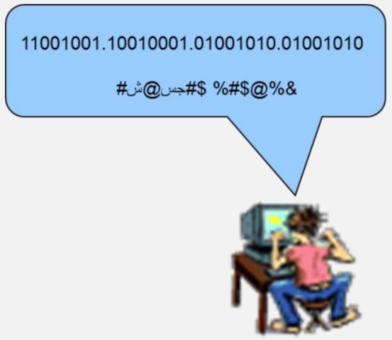
We have already studied that addressing / identifying computers on a network is done with IP and physical MAC addresses that they have to be unique. So, why when we surf the Internet do we use names and not these identifiers?

# Introduction

- Communication between systems is currently a relatively simple process as long as there is knowledge about the IP addresses involved.
- Man more easily memorizes names than numbers. Usually we more easily decorate the name of an acquaintance than your telephone number.
- One solution is to associate IPs with easily memorizable names:
  - 193.137.78.20 => webmail.isec.pt
  - 213.13.146.140 => www.sapo.pt
- This solution implies the existence of a system that does the translation / mapping between the names and their IP addresses:
  - System for Name Resolution (DNS)
  - Systems that do the opposite to translate IPs into names (reverse DNS)

# Introduction

- DNS allows you to:
  - The possibility for the human being to abstract from network addresses (IP addresses) whose memory is complex.
  - Allows changes to addresses to be made without the user having to know this change to continue to use a service;
  - The guarantee that machines and their names are managed in a hierarchical and distributed way, thus allowing greater availability of information.



# History

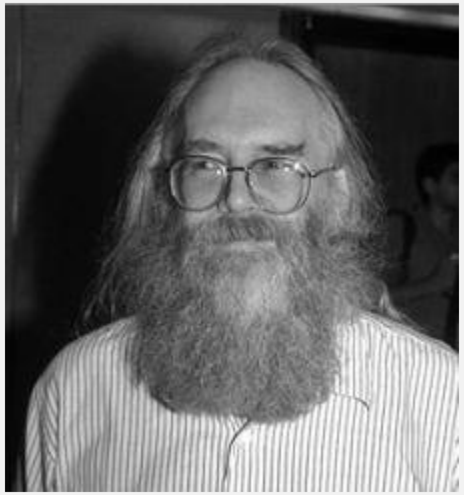
- Early 70s
  - Only IPs were used to identify the ARPANET network systems.
  - As the number of systems connected to the network grew, it became impracticable to access the machines by their IP addresses as they started to be in large numbers.
  - In search of a simplified memorization process, the idea of “naming” machines with names came up.
  - In each system there was a global “database” (hosts.txt) with the mappings used.

# History

- Esta foi a primeira solução e encontra-se ainda ativa nos sistemas atuais.
  - Ainda existe atualmente nas maquinas em Windows\System32\drivers\etc.
  - Assim, se desejar fazer um mapeamento IP-Nome não dependente do servidor DNS que utiliza, pode fazer essa alteração neste ficheiro já que este é o local onde primeiro a sua máquina vai procurar.
- A solução passava por ter um ficheiro (hosts.txt) por máquina:
  - Implicava uma gestão individual do ficheiro em cada sistema.
  - Os nomes guardados eram nomes simples (só o nome da maquina).
- A "evolução" foi ter um ficheiro que era atualizado centralmente e distribuído depois por todas as máquinas ligadas na rede.

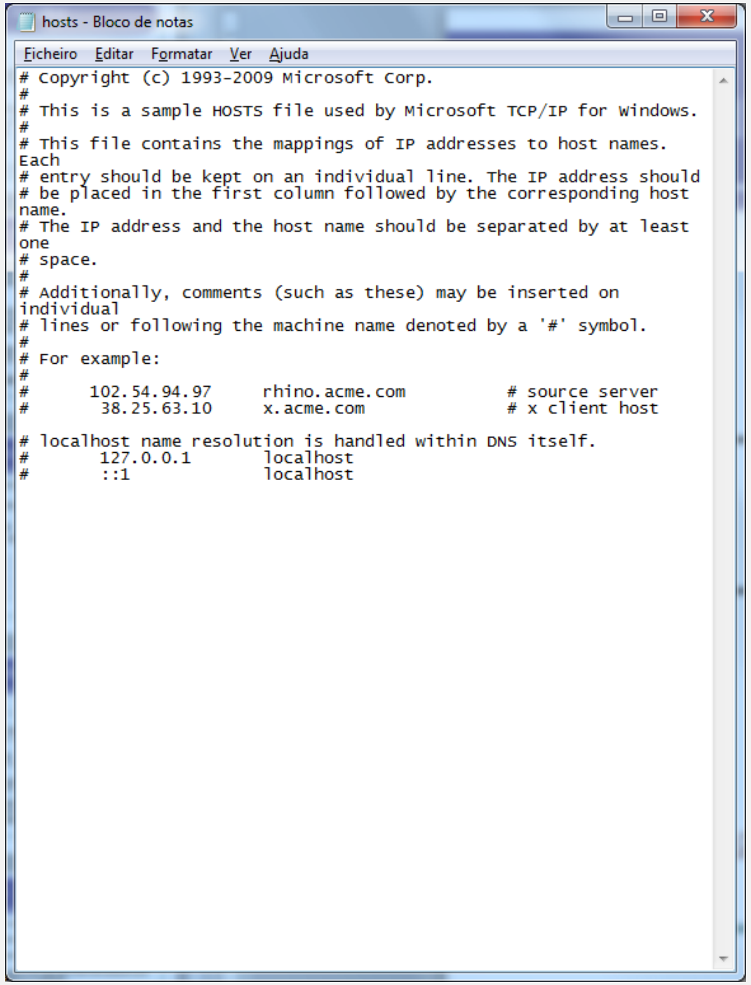
# History

- The hosts.txt file was centrally maintained (initially at the University of California, Los Angeles, UCLA) and distributed via FTP to all systems that wanted to have name resolution in mind.
- The central management of that file was initially entrusted to Jon (athan) B. Postel, a graduate student at UCLA at the time under an agreement with the Department of Defense (DoD). Postel is considered one of the pioneers of the Internet and one of its greatest thinkers.

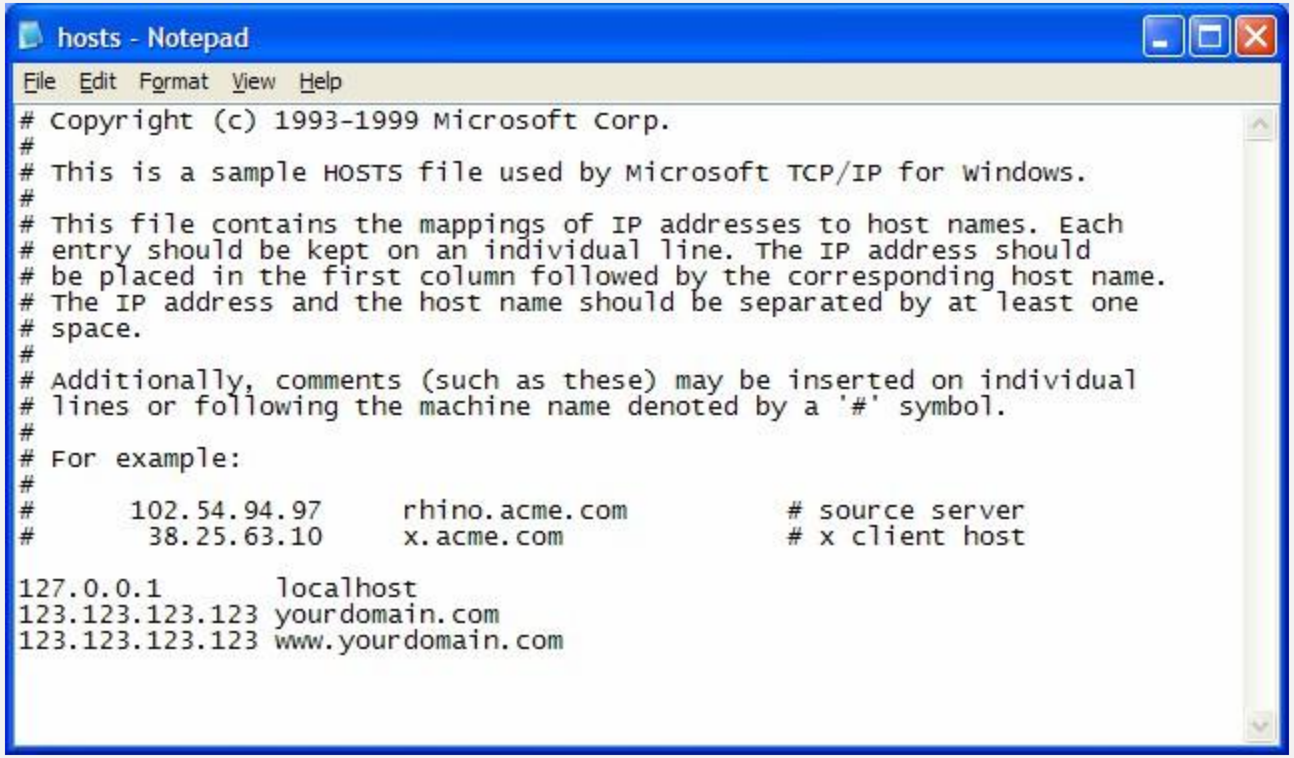


https://www.internethalloffame.org//inductees/jon-postel?gclid=Cj0KCQjwm9D0BRCMARIsAIfvfIaVlkisWaj7DBVVbGfvWHjOgoUFqe18bm_L7YBGNF3YUN8RXqR05b4aAp5WEALw_wcB

# História



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names.
Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host
name.
# The IP address and the host name should be separated by at least
one
# space.
#
# Additionally, comments (such as these) may be inserted on
individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
123.123.123.123 yourdomain.com
123.123.123.123 www.yourdomain.com
```

Note: There is always the address 127.0.0.1 that identifies the localhost ...

# History

- So why not put all the IPs on the Internet in the file?
  - We would spend a good part of our lives writing IPs and we would never have the table updated!
  - Any change in a name or IP, or any addition or removal from the table, would require all users to download the file again;
  - And who was responsible for this update and management of names and IPs?

# History

- In parallel, Jon Postel started organizing the archive of technical documents written by the researchers at ARPANET, called Request For Comments (RFC), remaining until he died as its editor.
- In 1971 (September 27) J. Postel published RFC 229 proposing a list of names (host mnemonics) and standard 8-character nicknames, thus identifying all ARPANet systems differently.
- During 1972, J. Postel published two RFCs (RFC 229 in May and RFC 433 in December) where a list of standardized port numbers to be used by each network service is proposed.

# History

- Due to the expansion in the interconnection of systems through data networks, the need arose to organize the names assigned to the machines.
- A simple name ("alpha", "omega", ...) did not respond to the needs and sometimes caused conflicts between systems
- In 1982 came the format host.domain for the names of computer systems:

| After | Before |
|---|---|
| **alpha** | apha.xxx.yyy |
| **omega** | omega.aaa.bbb |

- In August 1982, RFC 819 Z. Su, J. Postel, "Domain naming convention for Internet user applications" was published, where the machine name structure is defined. Domain.

# History

- However, there was still the difficulty introduced by the variety / multiplicity of name resolution files.
- Each system had to have its file and that was a problem since:
  - The tasks of updating / managing the file were not performed equally in all systems.
  - There was a need to liberalize the naming of systems in one organization without increasing the complexity of maintenance in another organization's systems.
  - There was a greater likelihood of errors.

# History

- In 1983, the first experiments and implementations of a distributed system for domain name resolution (DNS) appeared.
- Architecture was developed by Paul Mockapetris.
- In November, several fundamental RFCs for DNS are published:
  - RFC 881 J. Postel, "Domain names plan and schedule" where the DNS introduction calendar is presented.
  - RFC 882 P. Mockapetris, "Domain names - concepts and facilities“ where key DNS concepts are specified.
  - RFC 883 P. Mockapetris, "Domain names - implementation and specification“ where DNS implementation is detailed.

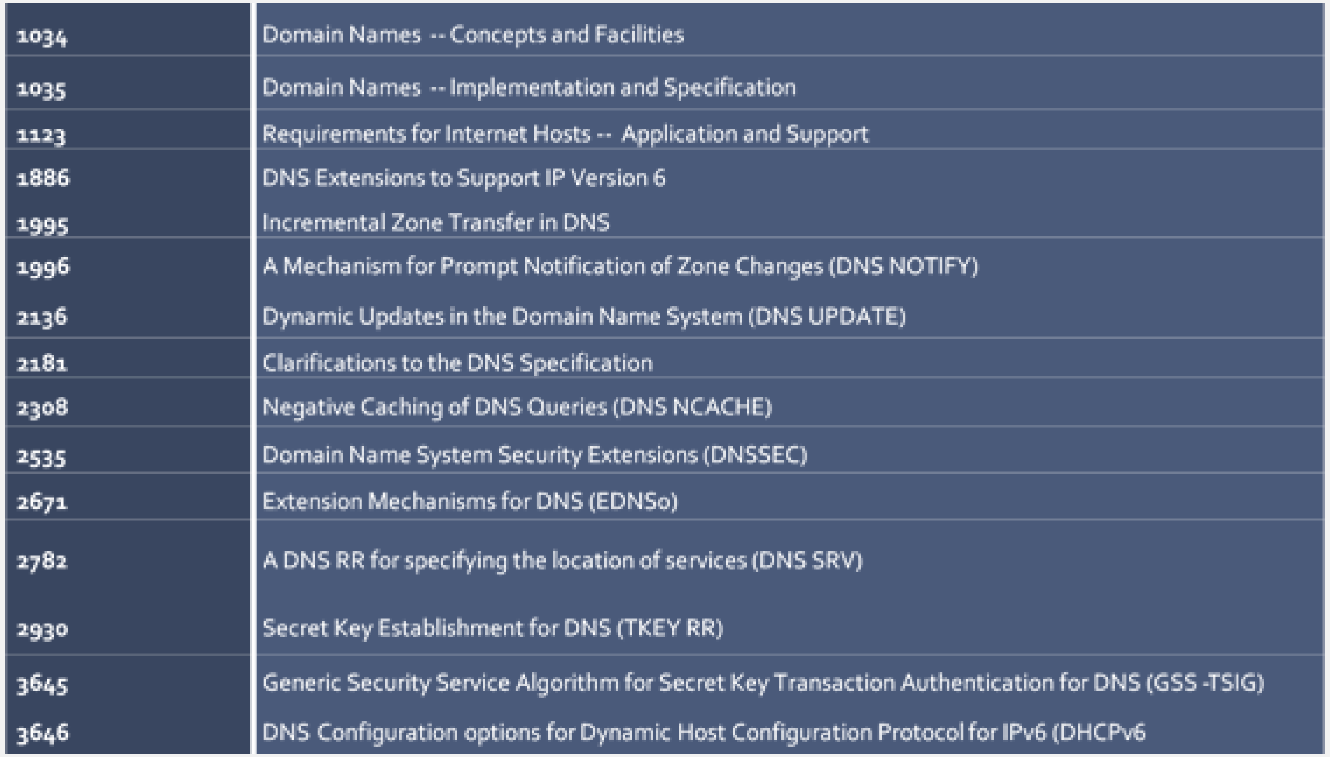
https://internethalloffame.org/inductees/paul-mockapetris

# History

- In 1984, DNS was put into operation, replacing the hosts.txt file with DNS servers.
- In March 1985 the first DNS domain (Symbolics.com) is registered
- In 1986, the National Science Foundation (NSF) was assigned the development of NSFNET, which today constitutes the main backbone of the Internet.
- The exponential growth of the Internet started…
- In November 1987 Paul Mockapetris publishes two RFCs that are a revision of the initial specification and on which the DNS is still based today:
  - RFC 1034 P.V. Mockapetris, “Domain names - concepts and facilities”
  - RFC 1035 P.V. Mockapetris, ”Domain names - implementation and specification”

# History

- Most important RFCs for DNS are:
  - RFCs 882 and 883 - Basic Operation
  - RFCs 1034, 1035 - Current Model
  - RFCs 1535, 1536, 1537 - Security, Implementation, Adm



| | |
|---|---|
| 1034 | Domain Names -- Concepts and Facilities |
| 1035 | Domain Names -- Implementation and Specification |
| 1123 | Requirements for Internet Hosts -- Application and Support |
| 1886 | DNS Extensions to Support IP Version 6 |
| 1995 | Incremental Zone Transfer in DNS |
| 1996 | A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY) |
| 2136 | Dynamic Updates in the Domain Name System (DNS UPDATE) |
| 2181 | Clarifications to the DNS Specification |
| 2308 | Negative Caching of DNS Queries (DNS NCACHE) |
| 2535 | Domain Name System Security Extensions (DNSSEC) |
| 2671 | Extension Mechanisms for DNS (EDNS0) |
| 2782 | A DNS RR for specifying the location of services (DNS SRV) |
| 2930 | Secret Key Establishment for DNS (TKEY RR) |
| 3645 | Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS -TSIG) |
| 3646 | DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6 |

# History

- One of the great advantages of this new system is that no entity is solely responsible for the entire updating of the system.
- It is based on the concept of a distributed database, existing on many different name servers around the world, but none of these servers have all the information. This allows a virtually unlimited growth of the DNS.
- In Microsoft systems, DNS has become the standard name resolution service since Windows 2000 Server, replacing WINS.

# Organizations

- The DNS service is directly dependent on the assignment of IPs and domain names to organizations.
- This function is the responsibility of the IANA (Internet Assigned Numbers Authority) or to whom it delegates this function.
- In Portugal, competence was delegated on June 30, 1988 to the Foundation for National Scientific Computing (FCCN), which is responsible for managing the '.pt' domain.
- The DNS.PT Association, was formally created on May 9, 2013 and succeeded, FCCN in the rights and obligations in the responsibility for the management, registration and maintenance of domains under the '.pt' (Top Level Domain) TLD.
- Its members are the Foundation for Science and Technology, FCT - IP, the Digital Economy Association (ACEPI) and the Portuguese Association for Consumer Protection (DECO).

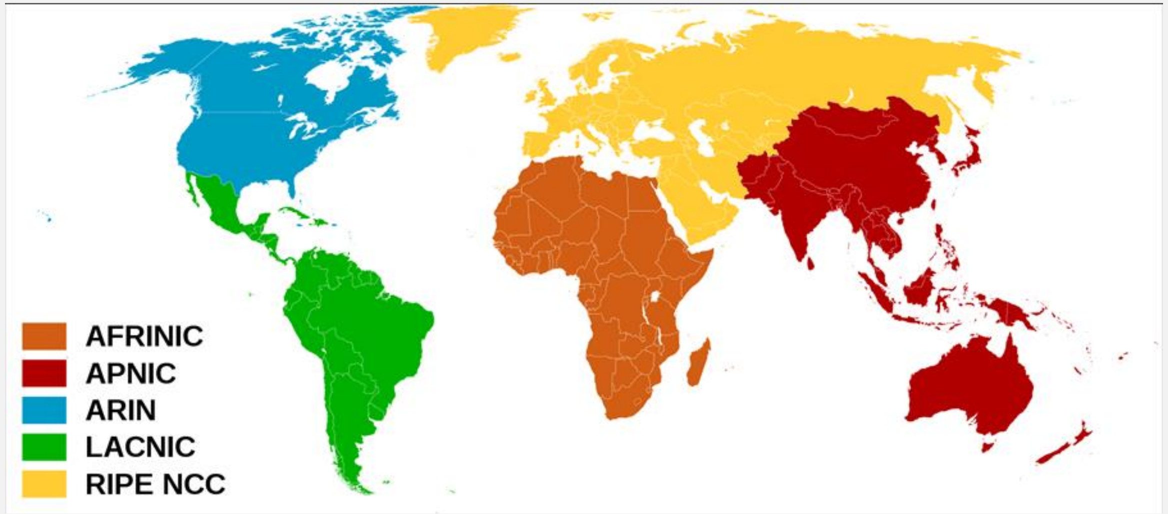
iana
Internet Assigned Numbers Authority

FCT Fundação para a Ciência e a Tecnologia
Computação Científica Nacional
FCCN

.pt

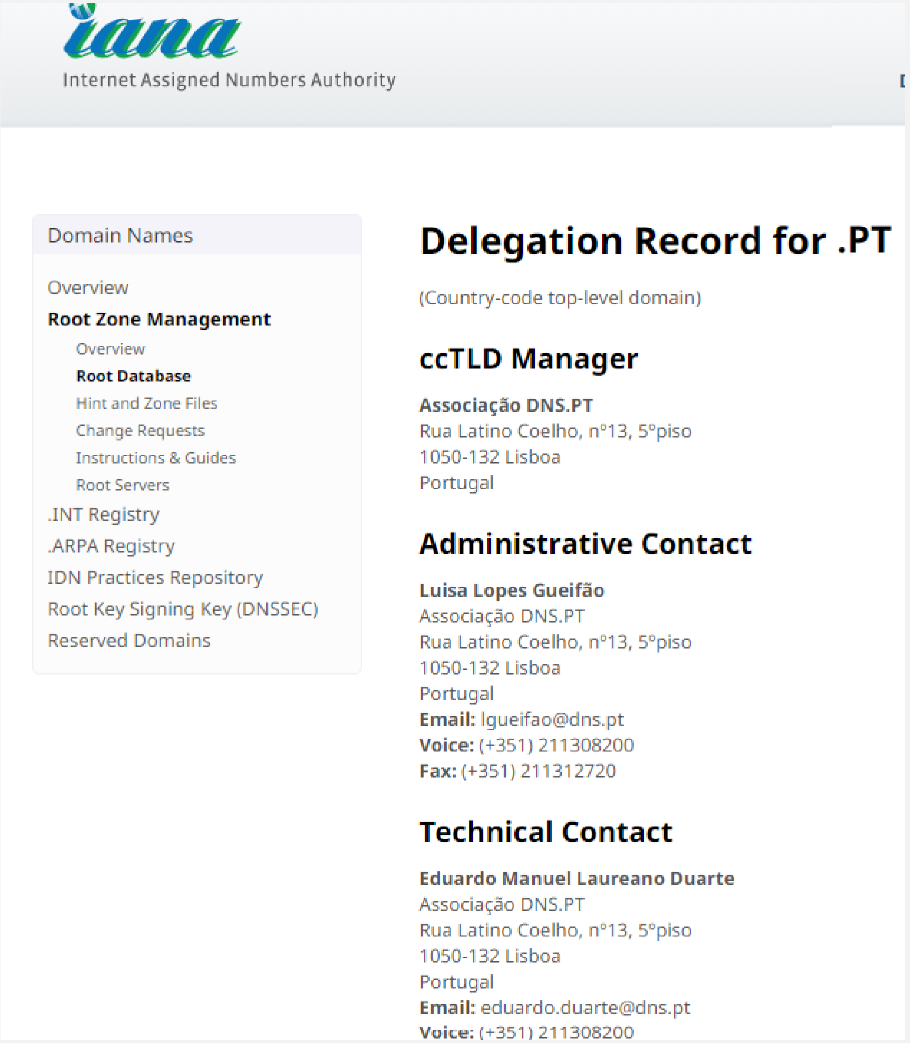
# Organizations

At the top of the hierarchy is the IANA (Internet Assigned Numbers Authority), linked to ICANN (Internet Corporation for Assigned Names and Numbers), which coordinates activities globally.
The IANA delegates part of these activities to authorities with a smaller scope, usually from the area of continents that are called RIR (Regional Internet Registry).
There are currently 5 regional entities which are: ARIN, RIPE NCC, APNIC, LACNIC and AfriNIC



**Fonte:**
https://pt.wikipedia.org/wiki/Registro_Regional_da_Internet#/media/Ficheiro:Regional_Internet_Registries_world_map.svg

# Organizations



## Delegation Record for .PT

(Country-code top-level domain)

### ccTLD Manager

**Associação DNS.PT**
Rua Latino Coelho, nº13, 5ºpiso
1050-132 Lisboa
Portugal

### Administrative Contact

**Luisa Lopes Gueifão**
Associação DNS.PT
Rua Latino Coelho, nº13, 5ºpiso
1050-132 Lisboa
Portugal
**Email:** lgueifao@dns.pt
**Voice:** (+351) 211308200
**Fax:** (+351) 211312720

### Technical Contact

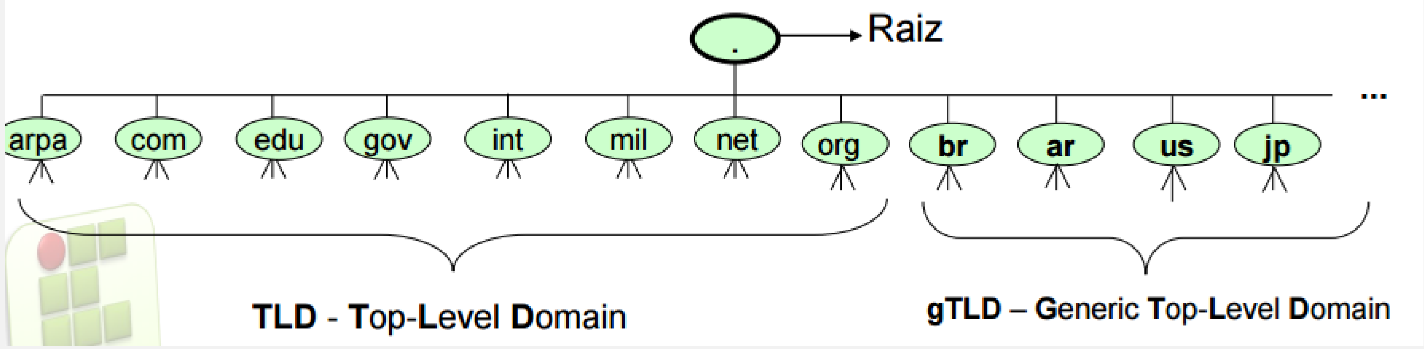
**Eduardo Manuel Laureano Duarte**
Associação DNS.PT
Rua Latino Coelho, nº13, 5ºpiso
1050-132 Lisboa
Portugal
**Email:** eduardo.duarte@dns.pt
**Voice:** (+351) 211308200

# Domains

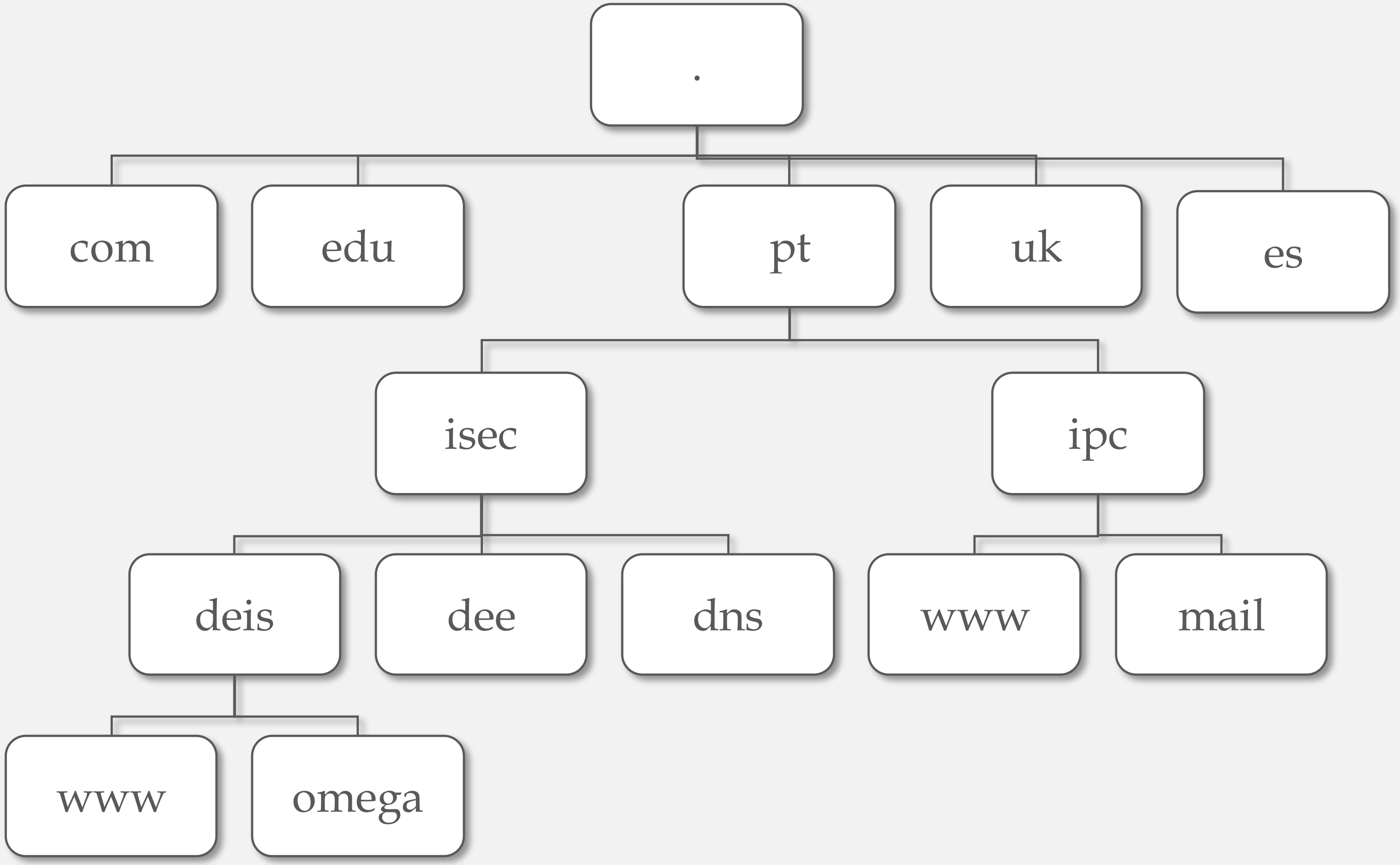
- Domain names are built hierarchically, with the highest level of the hierarchy being the last identifier.
- Because DNS was originally introduced in the United States and the final component of an address was intended to indicate the type of organization where the computer was located. Thus, some top-level domains (.edu, .gov and .mil) are still only used by US-based organizations.
- The two-letter codes indicating the country of origin are defined in ISO 3166 with the exception of UK used by the UK (United Kingdom) instead of gb, although there are some websites that use it (https://www.iso.org/obp/ui/#search).

# Domains

- You can now register names under several top domains:
  - com, aero, biz, cat, coop, edu, gov, info, int, jobs, mil, mobi, museum, name, net, org, pro, travel, tv
  - Domains for countries or regions: pt, eu, es, fr, uk, …
  - See the list at https://www.iana.org/domains/root/db
- The name of each node / identifier (except for the root node) must be a maximum of 63 characters, and case-insensitive. Identifiers must begin with a letter and may consist only of letters, digits and dashes (-).
- As a whole, a fully qualified domain name can not exceed 255 characters.

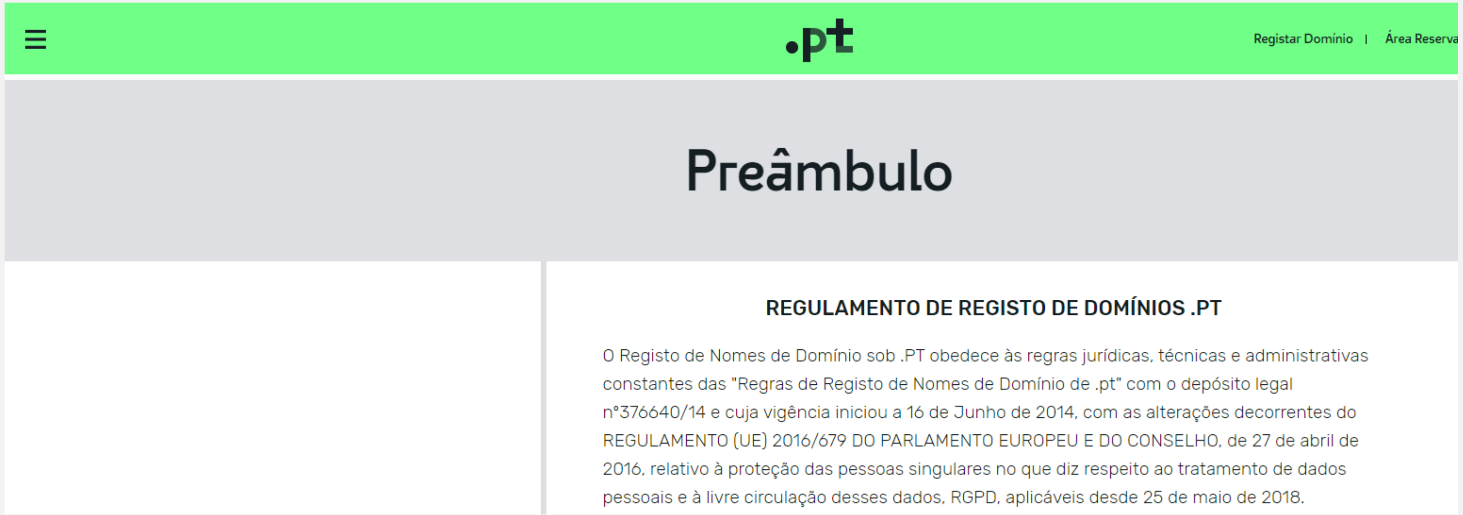


# Domains



# Domains

- In Portugal, FCCN also offers second level domains for the ‘pt’ domains: com, edu, gov, int, net, name, org, publ.
- The rules for registering a domain in Portugal are defined in:
  - https://www.dns.pt/pt/dominio/regras-de-dominios/preambulo/



## Preâmbulo

**REGULAMENTO DE REGISTO DE DOMÍNIOS .PT**

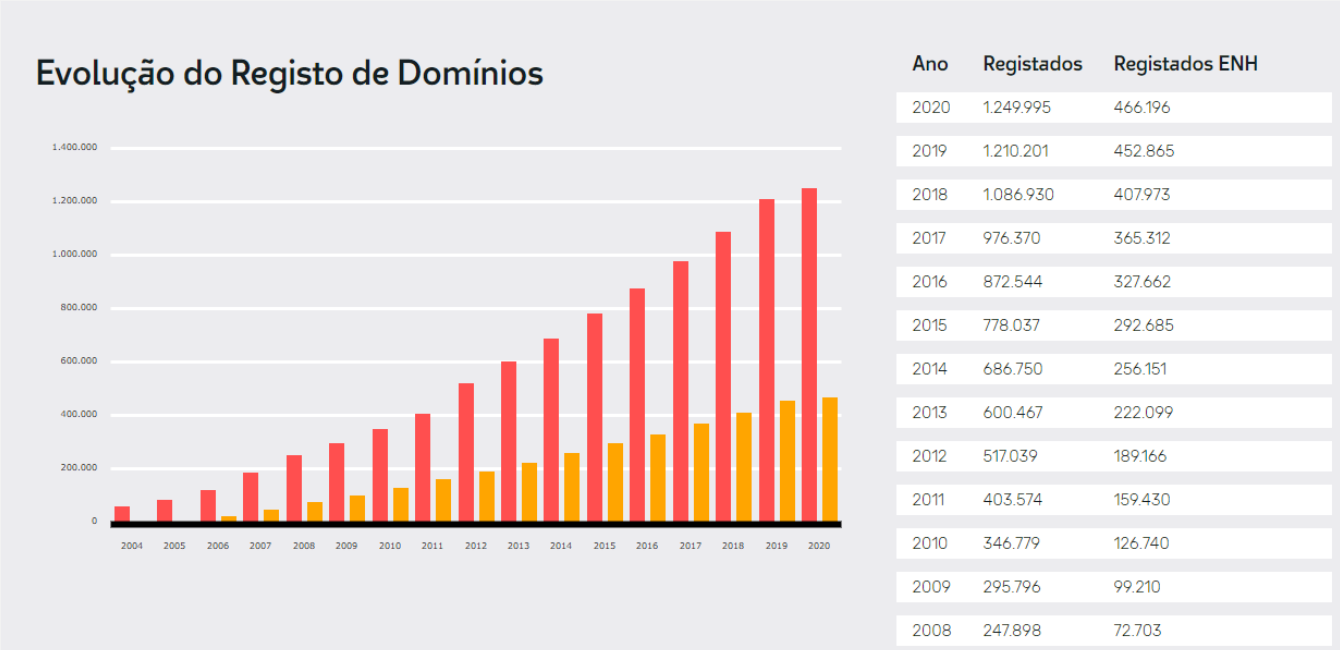
O Registo de Nomes de Domínio sob .PT obedece às regras jurídicas, técnicas e administrativas constantes das "Regras de Registo de Nomes de Domínio de .pt" com o depósito legal n°376640/14 e cuja vigência iniciou a 16 de Junho de 2014, com as alterações decorrentes do REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, RGPD, aplicáveis desde 25 de maio de 2018.

# Domains

- Entities that accept registration of names are called Registrars.
- They are entities specialized in the registration and management of domain names.
- In Portugal, they are accredited by the FCCN through a protocol that recognizes reciprocal rights and obligations, allowing greater flexibility and agility in the management of domain names by these entities.
- To apply for an accredited FCCN Registrar, you must guarantee a set of requirements that you can consult at:
  - **https://www.dns.pt/pt/registrar/ser-registrar-pt/**
- You can consult the list at (101 companies are currently registered):
  - **http://www.dns.pt/en/registrars/**

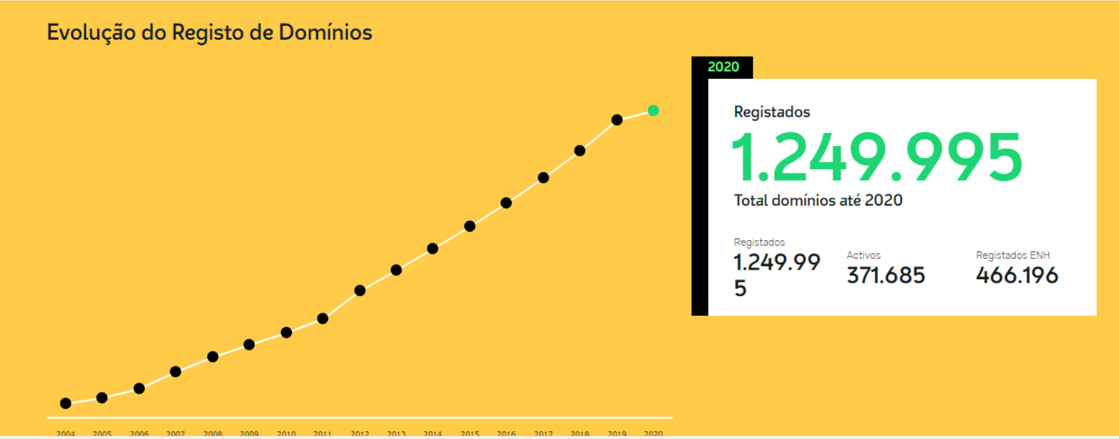
# Domains

- Evolution of registration and active domains



Evolução do Registo de Domínios

| Ano | Registados | Registados ENH |
|---|---|---|
| 2020 | 1.249.995 | 466.196 |
| 2019 | 1.210.201 | 452.865 |
| 2018 | 1.086.930 | 407.973 |
| 2017 | 976.370 | 365.312 |
| 2016 | 872.544 | 327.662 |
| 2015 | 778.037 | 292.685 |
| 2014 | 686.750 | 256.151 |
| 2013 | 600.467 | 222.099 |
| 2012 | 517.039 | 189.166 |
| 2011 | 403.574 | 159.430 |
| 2010 | 346.779 | 126.740 |
| 2009 | 295.796 | 99.210 |
| 2008 | 247.898 | 72.703 |



Evolução do Registo de Domínios

2020

Registados

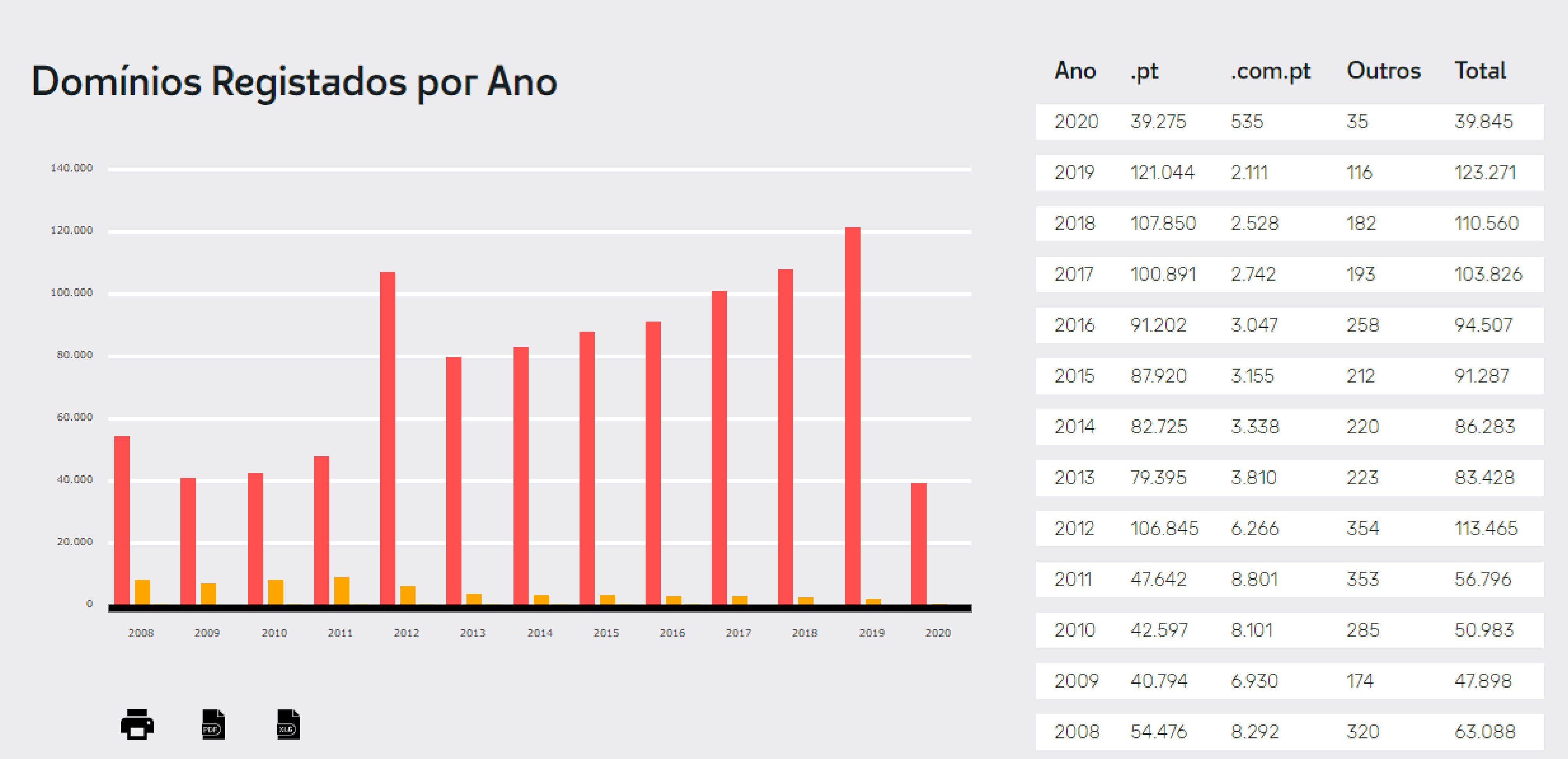
1.249.995

Total domínios até 2020

| Registados | Activos | Registados ENH |
|---|---|---|
| 1.249.99<br>5 | 371.685 | 466.196 |

Fonte: https://www.dns.pt

# Números

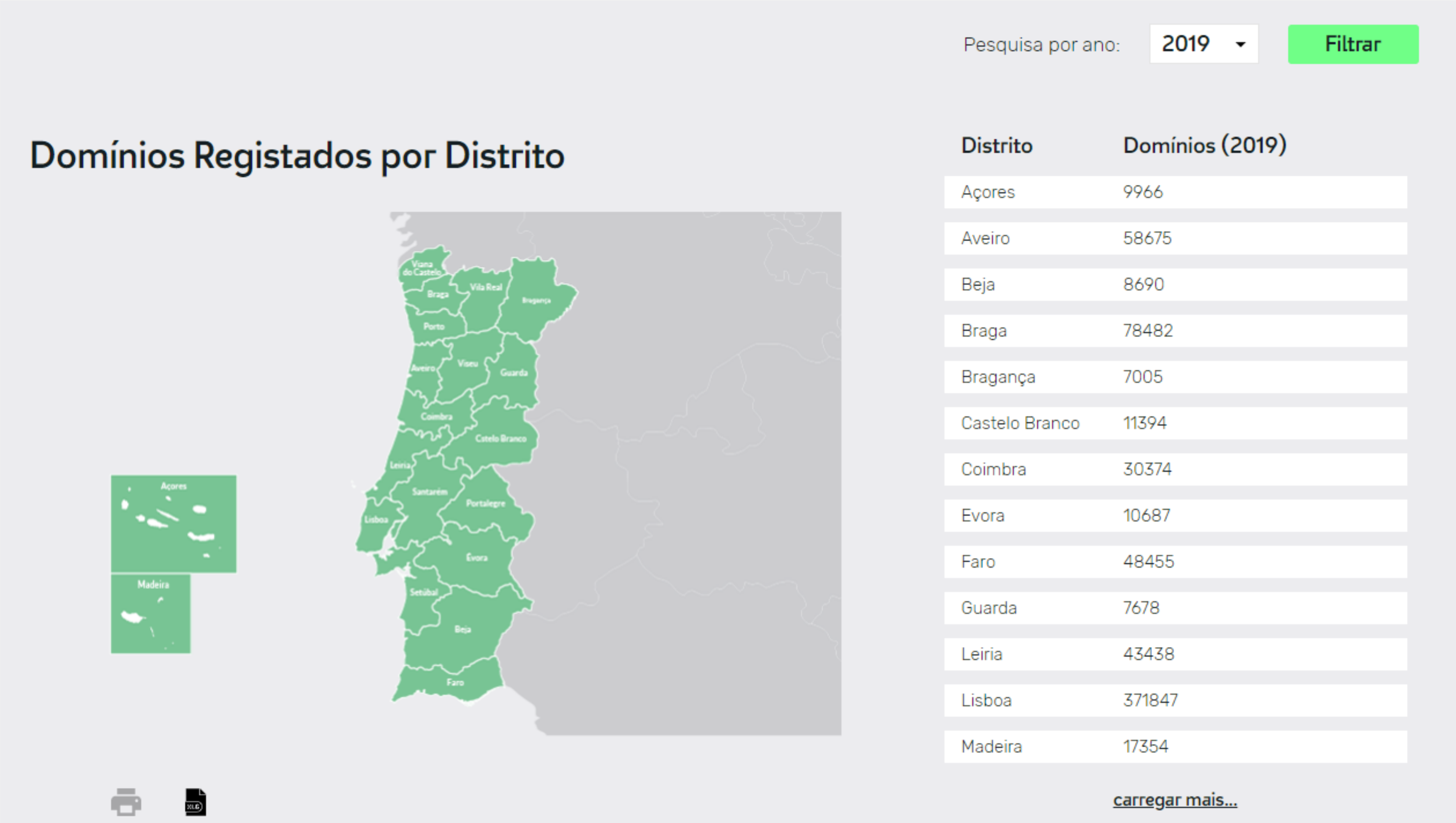


## Domínios Registados por Ano

| Ano | .pt | .com.pt | Outros | Total |
|---|---|---|---|---|
| 2020 | 39.275 | 535 | 35 | 39.845 |
| 2019 | 121.044 | 2.111 | 116 | 123.271 |
| 2018 | 107.850 | 2.528 | 182 | 110.560 |
| 2017 | 100.891 | 2.742 | 193 | 103.826 |
| 2016 | 91.202 | 3.047 | 258 | 94.507 |
| 2015 | 87.920 | 3.155 | 212 | 91.287 |
| 2014 | 82.725 | 3.338 | 220 | 86.283 |
| 2013 | 79.395 | 3.810 | 223 | 83.428 |
| 2012 | 106.845 | 6.266 | 354 | 113.465 |
| 2011 | 47.642 | 8.801 | 353 | 56.796 |
| 2010 | 42.597 | 8.101 | 285 | 50.983 |
| 2009 | 40.794 | 6.930 | 174 | 47.898 |
| 2008 | 54.476 | 8.292 | 320 | 63.088 |

Fonte: https://www.dns.pt

# Números



Pesquisa por ano: 2019 Filtrar

## Domínios Registados por Distrito

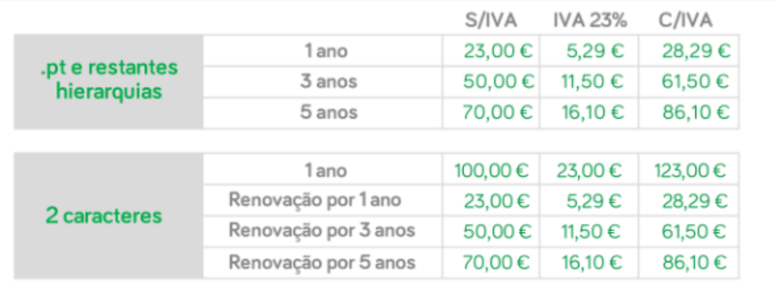
| Distrito | Domínios (2019) |
|---|---|
| Açores | 9966 |
| Aveiro | 58675 |
| Beja | 8690 |
| Braga | 78482 |
| Bragança | 7005 |
| Castelo Branco | 11394 |
| Coimbra | 30374 |
| Evora | 10687 |
| Faro | 48455 |
| Guarda | 7678 |
| Leiria | 43438 |
| Lisboa | 371847 |
| Madeira | 17354 |

carregar mais...

Fonte: https://www.dns.pt

# Custos

- Domain registration is usually paid for.
- Prices may vary depending on the domain type
- Between € 10 and € 60 per year (sometimes there is an initial submission fee)
- For Portugal these are the costs:



| | | S/IVA | IVA 23% | C/IVA |
|---|---|---|---|---|
| .pt e restantes hierarquias | 1 ano | 23,00 € | 5,29 € | 28,29 € |
| | 3 anos | 50,00 € | 11,50 € | 61,50 € |
| | 5 anos | 70,00 € | 16,10 € | 86,10 € |
| 2 caracteres | 1 ano | 100,00 € | 23,00 € | 123,00 € |
| | Renovação por 1 ano | 23,00 € | 5,29 € | 28,29 € |
| | Renovação por 3 anos | 50,00 € | 11,50 € | 61,50 € |
| | Renovação por 5 anos | 70,00 € | 16,10 € | 86,10 € |

- Source: https://www.dns.pt/pt/dominio/precos/
- Whoever registers a name can make it available to another entity (read ... sell it ;-))

# Domains and Zones

- **Domain / Sub-domain**
  - Sub-tree of the namespace defined by DNS.
  - Examples:
    - isec.pt.
    - deis.isec.pt.
  - The domain deis.isec.pt. is a subdomain of isec.pt.
- **Zone**
  - Contents of a contiguous section of the namespace normally delimited by administrative boundaries that may or may not coincide with a domain or subdomain.

# Zones

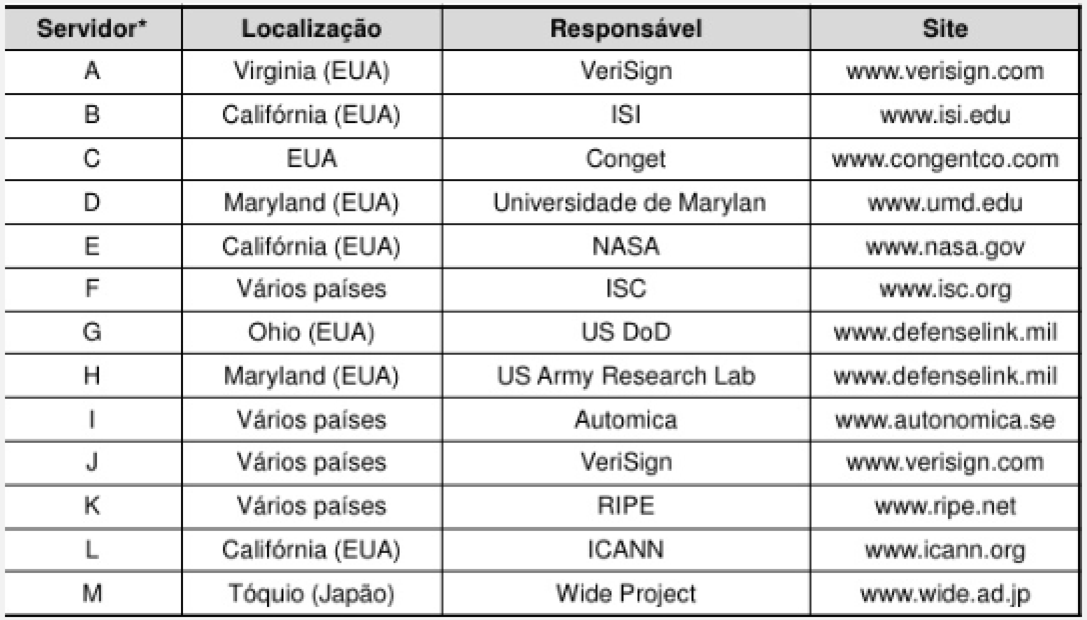
- Computers and organizations hanging on the same node as the DNS tree share a portion of the name of their domains.
- For example, all existing computers and departments in ISEC use the isec.pt domain. You can then define a zone for this DNS subtree that can be a Top Level National Domain (TLND) or department / organization level.
- Within a zone the DNS service for subsidiary zones can be delegated together with a subsidiary domain.
- Thus, although there is an entity responsible for the administration of the pt domain, which is the FCCN, the responsibility of the administration of the domain isec.pt has been delegated to the ISEC.

# Domain Names

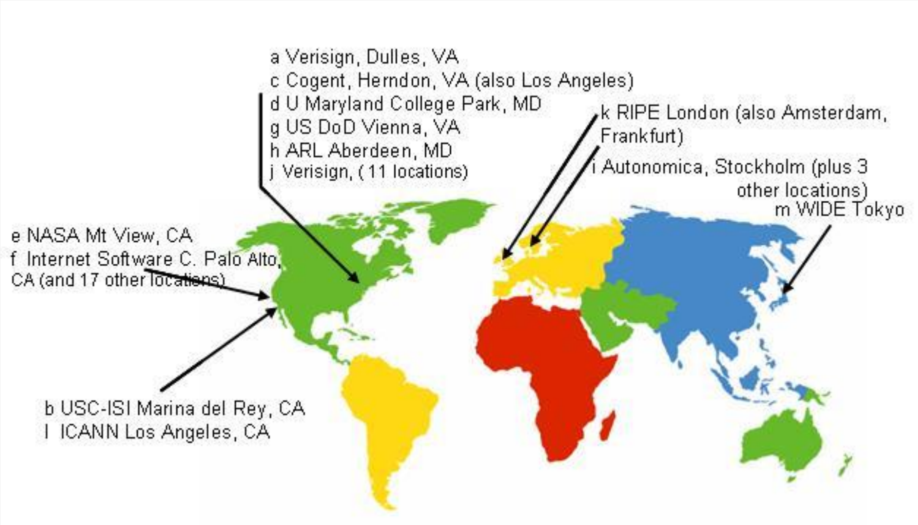
- **Fully Qualified Domain Name (FQDN)**
  - It is structured as follows: "host.3rd-level-domain.2nd-level-domain.top-leveldomain"
  - The number of levels is not fixed.
  - If no domain is defined, the localdomain default domain is used.
  - Example: www.isec.pt
- **Relative name**
  - Sequence not terminated by "."
  - Example: www

# ROOT Servers

- They are authoritative servers with special roles, without them the Internet does not work.
- There are 13 servers (10 in the United States, 2 in Europe and 1 in Asia). The content of each is replicated 2 times a day automatically. There are replicas of these servers scattered around the world.
- It has a table that indicates which DNS server is responsible for solving each of the Top Level Domanis



| Servidor* | Localização | Responsável | Site |
|---|---|---|---|
| A | Virginia (EUA) | VeriSign | www.verisign.com |
| B | Califórnia (EUA) | ISI | www.isi.edu |
| C | EUA | Conget | www.congentco.com |
| D | Maryland (EUA) | Universidade de Marylan | www.umd.edu |
| E | Califórnia (EUA) | NASA | www.nasa.gov |
| F | Vários países | ISC | www.isc.org |
| G | Ohio (EUA) | US DoD | www.defenselink.mil |
| H | Maryland (EUA) | US Army Research Lab | www.defenselink.mil |
| I | Vários países | Automica | www.autonomica.se |
| J | Vários países | VeriSign | www.verisign.com |
| K | Vários países | RIPE | www.ripe.net |
| L | Califórnia (EUA) | ICANN | www.icann.org |
| M | Tóquio (Japão) | Wide Project | www.wide.ad.jp |

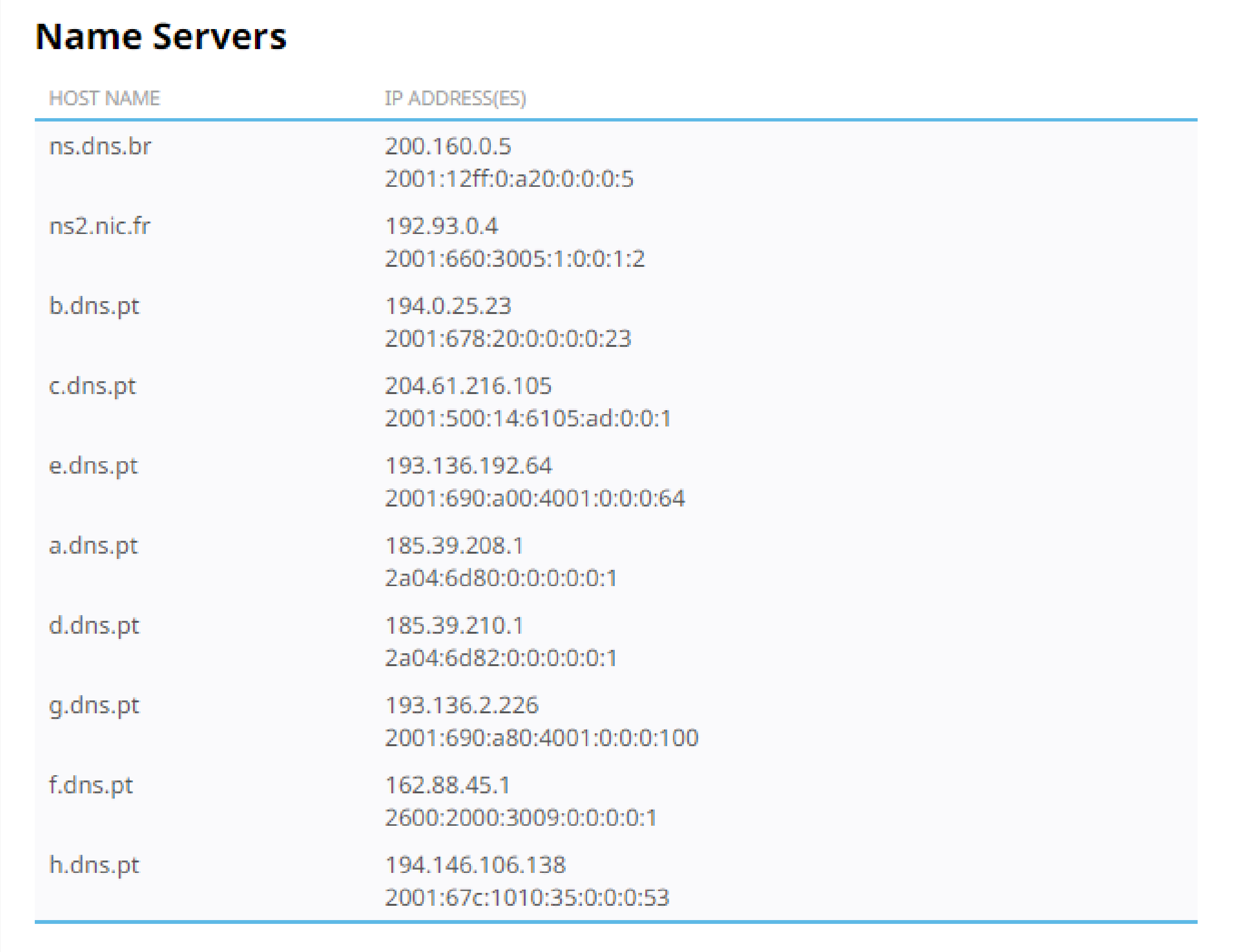

a Verisign, Dulles, VA
c Cogent, Herndon, VA (also Los Angeles)
d U Maryland College Park, MD
g US DoD Vienna, VA
h ARL Aberdeen, MD
j Verisign, ( 11 locations)
k RIPE London (also Amsterdam, Frankfurt)
i Autonomica, Stockholm (plus 3 other locations)
m WIDE Tokyo
e NASA Mt View, CA
f Internet Software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

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

# *Top Level Domains Servers*

- The top-level domain is one of the components of addresses. Each domain name consists of a few names separated by periods, the last of which is the top domain.
- There are two types:
  - **Generic Top level domains** - related to the roles of organizations
    - Generic - used for generic organizations (.com, .info, .net, .org)
    - Generic restricted - used for certain functions (.biz, .name, .pro)
    - Infrastructure - used only in the DNS infrastructure (.arpa)
    - Sponsored domains - can only be used by companies or entities linked to these sectors (.edu, .gov, .mil,. Travel etc)
  - **Country Code Top Level Domain** - related to the location of organizations (.pt, .br, .fr, etc.)

# Servidores *Top Level Domains .pt*



## Name Servers

| HOST NAME | IP ADDRESS(ES) |
|---|---|
| ns.dns.br | 200.160.0.5<br>2001:12ff:0:a20:0:0:0:5 |
| ns2.nic.fr | 192.93.0.4<br>2001:660:3005:1:0:0:1:2 |
| b.dns.pt | 194.0.25.23<br>2001:678:20:0:0:0:0:23 |
| c.dns.pt | 204.61.216.105<br>2001:500:14:6105:ad:0:0:1 |
| e.dns.pt | 193.136.192.64<br>2001:690:a00:4001:0:0:0:64 |
| a.dns.pt | 185.39.208.1<br>2a04:6d80:0:0:0:0:0:1 |
| d.dns.pt | 185.39.210.1<br>2a04:6d82:0:0:0:0:0:1 |
| g.dns.pt | 193.136.2.226<br>2001:690:a80:4001:0:0:0:100 |
| f.dns.pt | 162.88.45.1<br>2600:2000:3009:0:0:0:0:1 |
| h.dns.pt | 194.146.106.138<br>2001:67c:1010:35:0:0:0:53 |

# Local Servers

- The entity responsible for the zone must have a single primary server and preferably one or more secondary servers.
- The big difference between these two types of servers is that a primary server loads all the information from the zone concerned from existing (database) files to disk, while the secondary servers get all the information from the primary server.
- When a secondary server obtains its primary information, this operation is called zone transfer.
- When a new computer is added to the zone, the administrator adds the appropriate information (name and IP address) to an existing disk file on the primary server (which is the local DNS database). The primary name server is then notified that it must reread the configuration files.
- Secondary servers contact the primary on a regular basis (usually every 3 hours), and if the primary has new data, the secondary ones obtain this data through the zone transfer mechanism (TCP port 53).
- A particular server can be primary or secondary from several zones.

# Primary Servers

- It is a DNS server responsible for at least one zone, obtaining the data for that zone from local files (Zone files).
- It is said that it is Authoritarian for that Zone, and the alteration of the information related to it (addition of domains or machines) can only be done locally.
- In general, the Master Name Server is the primary server in the zone.
- You do not need to run on the network (physical and logical) of the authority responsible for the Zone:
  - may be running on a different network.
  - Zone files can be imported via FTP or email when there is a need to update the zone information.

# Secondary server

- Server that obtains zone data from another DNS server (Master Zone Server - primary or secondary server)
- Periodically or whenever the server starts up, the need to update the zone data is verified (Zone Transfer)
- Each ISP, institution, etc. has several local servers that are used directly by users the users' DNS queries are directed to these servers
- Advantages of having secondary servers:
  - **Redundancy** - If one of the servers fails, the others can be contacted alternatively (timeout mechanism).
  - **Remote location** - To avoid latency of WAN connections, it is a good policy for subdomains to have a secondary server in their parent domain.
  - **Distribution of the processing load** - To avoid congestion of a single server, queries to a domain must be distributed among several servers.

# Other Servers

- ***Forward***
  - It is the server of an organization elected to interact with the servers outside it when there is a need to resolve non-local names. It is a configuration made per server, not per zone.
- ***Stub Server***
  - It maintains only a shorthand copy of the zone (stub zone), containing the list of 'authoritative' servers for that zone
- ***Caching-only server***
  - They are characterized by only having information that they obtained through previous requests for resolution

# *Resolvers*

- These are servers used by client applications to query the DNS.
- They need to know at least the location of a name server.
- They use the information provided by the known name server to answer queries from clients.
- The answer can be directly provided by the known name server or by successive contact with other referred servers.
- They are all the more efficient the greater the scope of your cache.

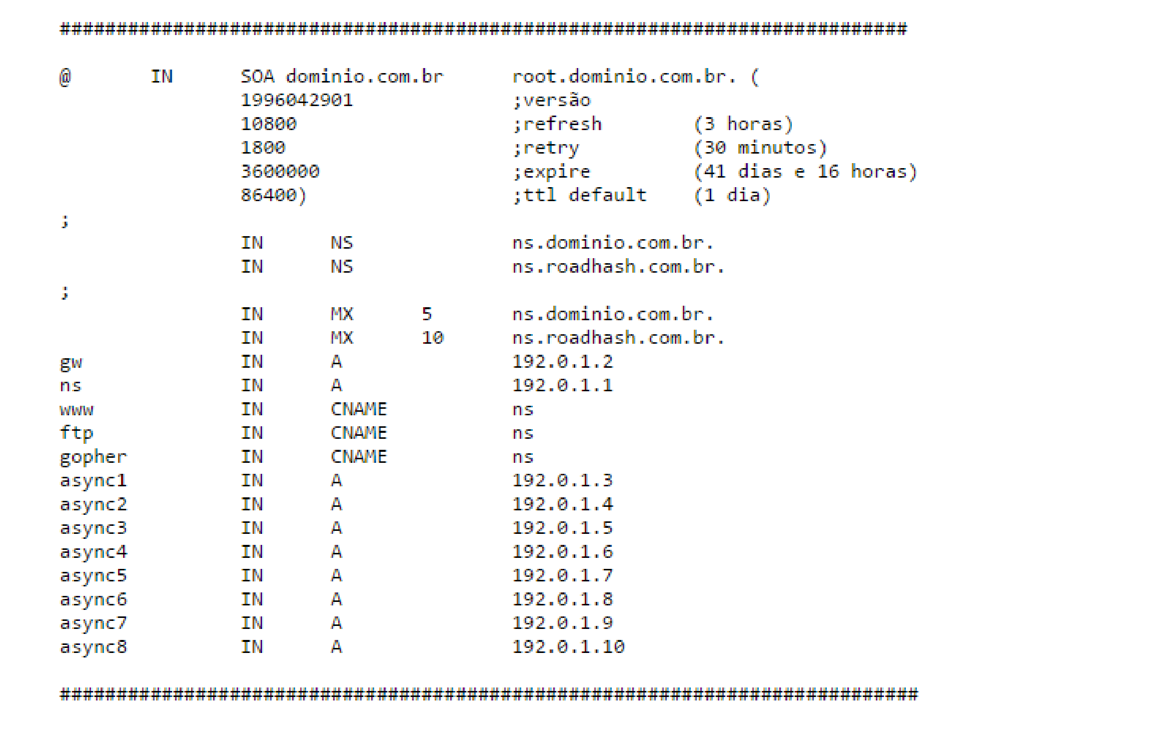
# DNS records (SOA)

- **SOA - Start of Authority -** defines the general characteristics of the zone
  - **NAMESERVER**: indicates the authoritative DNS server for that zone;
  - **MNAME -** domain name of the nameserver (eg isec.pt);
  - **RNAME -** email address of the zone administrator (domain);
  - **SERIAL -** version of the zone file. This value must be increased whenever any part of the zone file information is changed. The tacit commonly used is to write a number with the date format (year / month / day / version - 0..99): 2001053000.
  - **REFRESH -** periodicity (in seconds) with which the secondary servers consult the primary to check the current version of the zone. Typical value: 3600 = 1h
  - **RETRY -** Periodicity (in seconds) with which the secondary servers repeat the attempt to verify the serial number of the master file after a contact has failed. Typical value: 600 = 10m
  - **EXPIRE -** Maximum limit (in seconds) for replica retention of the zone without being able to ascertain the serial number. After this value expires, the secondary can no longer answer for the zone. Typical value: 3600000 -> 42d;
  - **MINIMUM TTL -** defines how long the record for this zone should remain in the cache of a DNS server before an update is made. Typical value: 864000 -> 10d

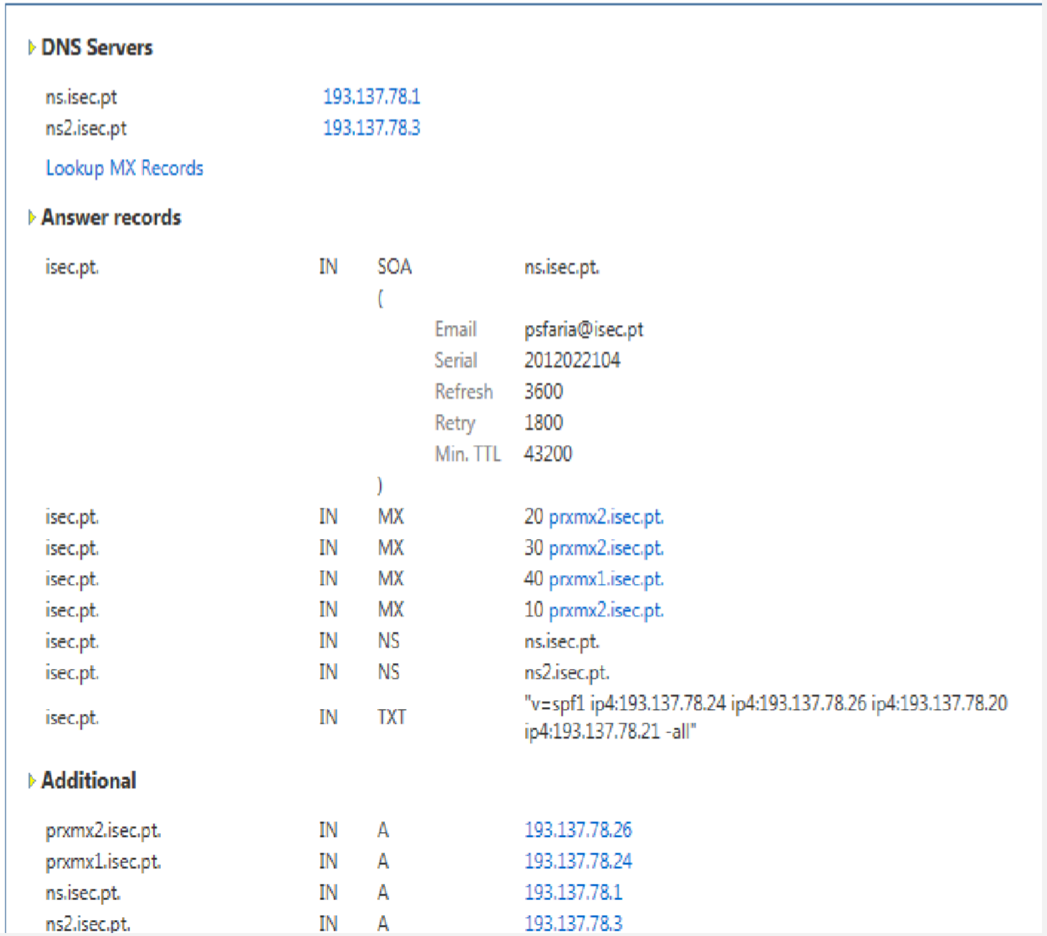
# DNS records

- **A** - host address - this is the basic type that matches a canonical name to an IP address (For IP V4)
- **AAAA** - same as above but for IP V6.
- **CNAME** - alias - maps an alias name to a true or canonical domain name. It is particularly useful for providing alternative names that correspond to the different services of the same machine
- **MX** - Mail Exchanger - Informs the IPs of the SMTP servers of a domain. This type of record has as its particularity one more field, which informs the priority of the SMTP server. The lower the value, the higher the priority ..
- **PTR** - Pointer (IP => name) - Associates an IP address with a hostname for reverse DNS resolution.
- **SRV** - Service Location - used to identify computers hosting specific services
- **NS** - domain name - Informs the IPs of the authoritative DNS servers in a domain.
- **TXT -** You can store any information in text format. Initially created to store comments or information about the domain, today it is widely used by anti-spam tools.

# Example



```
###########################################################################

@       IN      SOA dominio.com.br      root.dominio.com.br. (
                1996042901              ;versão
                10800                   ;refresh        (3 horas)
                1800                    ;retry          (30 minutos)
                3600000                 ;expire         (41 dias e 16 horas)
                86400)                  ;ttl default    (1 dia)
;
                IN      NS              ns.dominio.com.br.
                IN      NS              ns.roadhash.com.br.
;
                IN      MX      5       ns.dominio.com.br.
                IN      MX      10      ns.roadhash.com.br.
gw              IN      A               192.0.1.2
ns              IN      A               192.0.1.1
www             IN      CNAME           ns
ftp             IN      CNAME           ns
gopher          IN      CNAME           ns
async1          IN      A               192.0.1.3
async2          IN      A               192.0.1.4
async3          IN      A               192.0.1.5
async4          IN      A               192.0.1.6
async5          IN      A               192.0.1.7
async6          IN      A               192.0.1.8
async7          IN      A               192.0.1.9
async8          IN      A               192.0.1.10

############################################################################
```

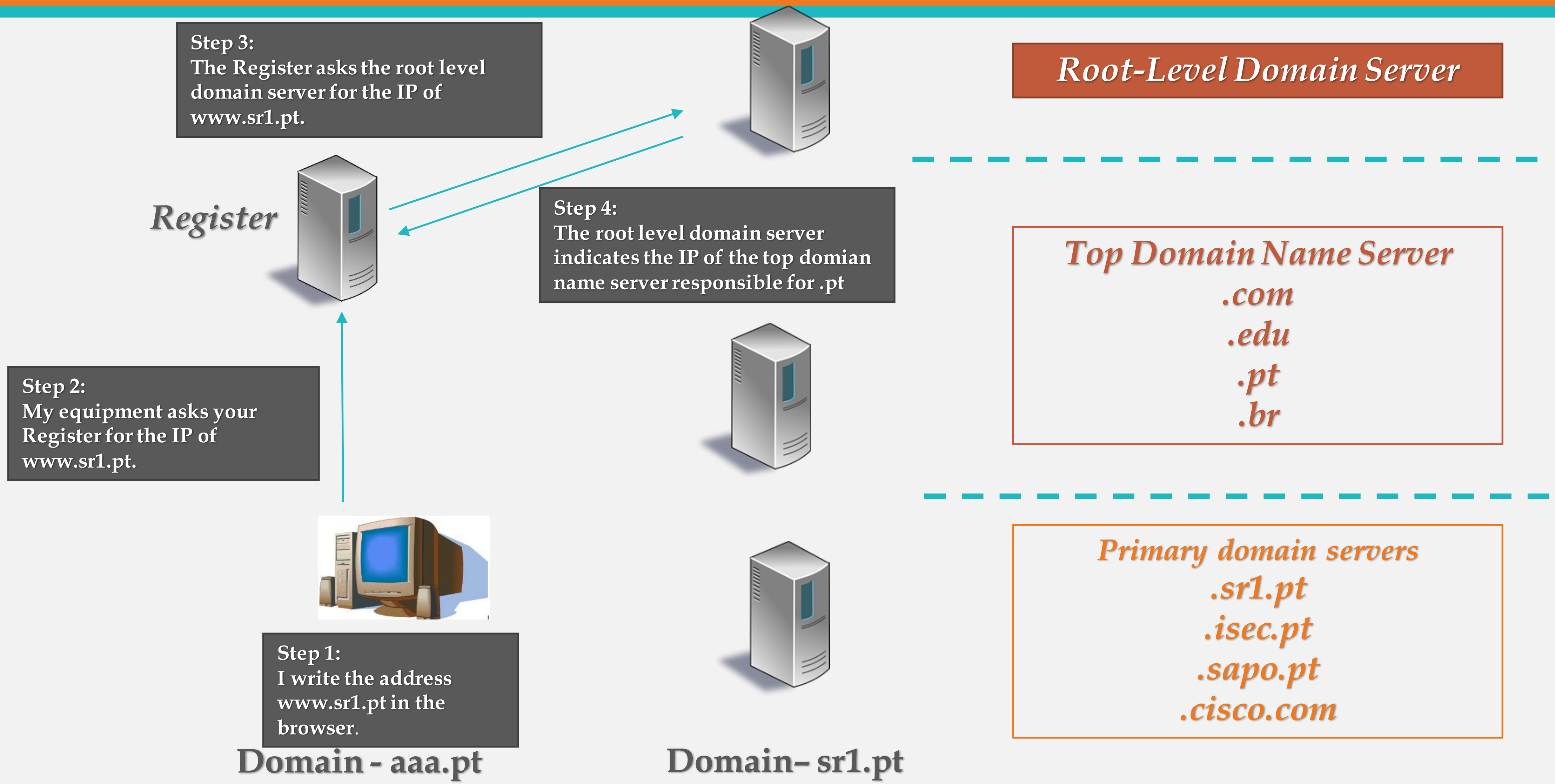


```
▸ DNS Servers

  ns.isec.pt                193.137.78.1
  ns2.isec.pt               193.137.78.3

  Lookup MX Records

▸ Answer records

  isec.pt.            IN    SOA              ns.isec.pt.
                            (
                                 Email       psfaria@isec.pt
                                 Serial      2012022104
                                 Refresh     3600
                                 Retry       1800
                                 Min. TTL    43200
                            )
  isec.pt.            IN    MX               20 prxmx2.isec.pt.
  isec.pt.            IN    MX               30 prxmx2.isec.pt.
  isec.pt.            IN    MX               40 prxmx1.isec.pt.
  isec.pt.            IN    MX               10 prxmx2.isec.pt.
  isec.pt.            IN    NS               ns.isec.pt.
  isec.pt.            IN    NS               ns2.isec.pt.
                                             "v=spf1 ip4:193.137.78.24 ip4:193.137.78.26 ip4:193.137.78.20
  isec.pt.            IN    TXT              ip4:193.137.78.21 -all"

▸ Additional

  prxmx2.isec.pt.     IN    A                193.137.78.26
  prxmx1.isec.pt.     IN    A                193.137.78.24
  ns.isec.pt.         IN    A                193.137.78.1
  ns2.isec.pt.        IN    A                193.137.78.3
```

# Operation

- We have already seen in other classes, that the connection between two machines is only possible with the knowledge of two fundamental information:
  - IP adress.
  - Physical address (MAC).
- So for machine A to connect to machine B it is necessary to know the IP address and then the MAC of that machine.
- But if in the browser I write the name of the target machine, how does my machine know the IP of the target machine?
- Yes, I know this is the role of DNS, but how does it work?

# Operation



Step 3:
The Register asks the root level domain server for the IP of www.sr1.pt.

*Register*

Step 4:
The root level domain server indicates the IP of the top domian name server responsible for .pt

Step 2:
My equipment asks your Register for the IP of www.sr1.pt.

Step 1:
I write the address www.sr1.pt in the browser.

**Domain - aaa.pt**

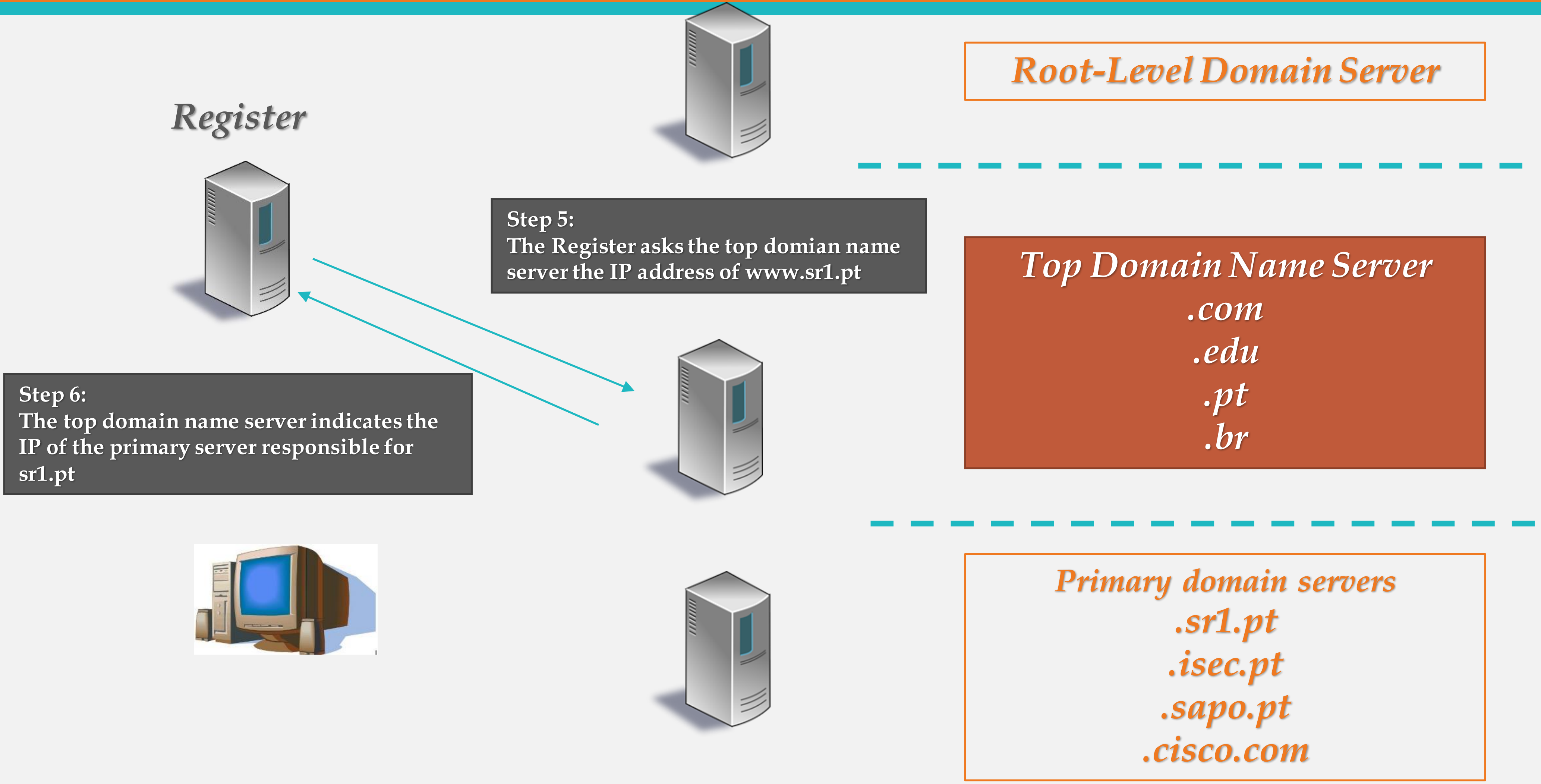
**Domain– sr1.pt**

*Root-Level Domain Server*

*Top Domain Name Server*
*.com*
*.edu*
*.pt*
*.br*

*Primary domain servers*
*.sr1.pt*
*.isec.pt*
*.sapo.pt*
*.cisco.com*

# Operation



*Register*

*Root-Level Domain Server*

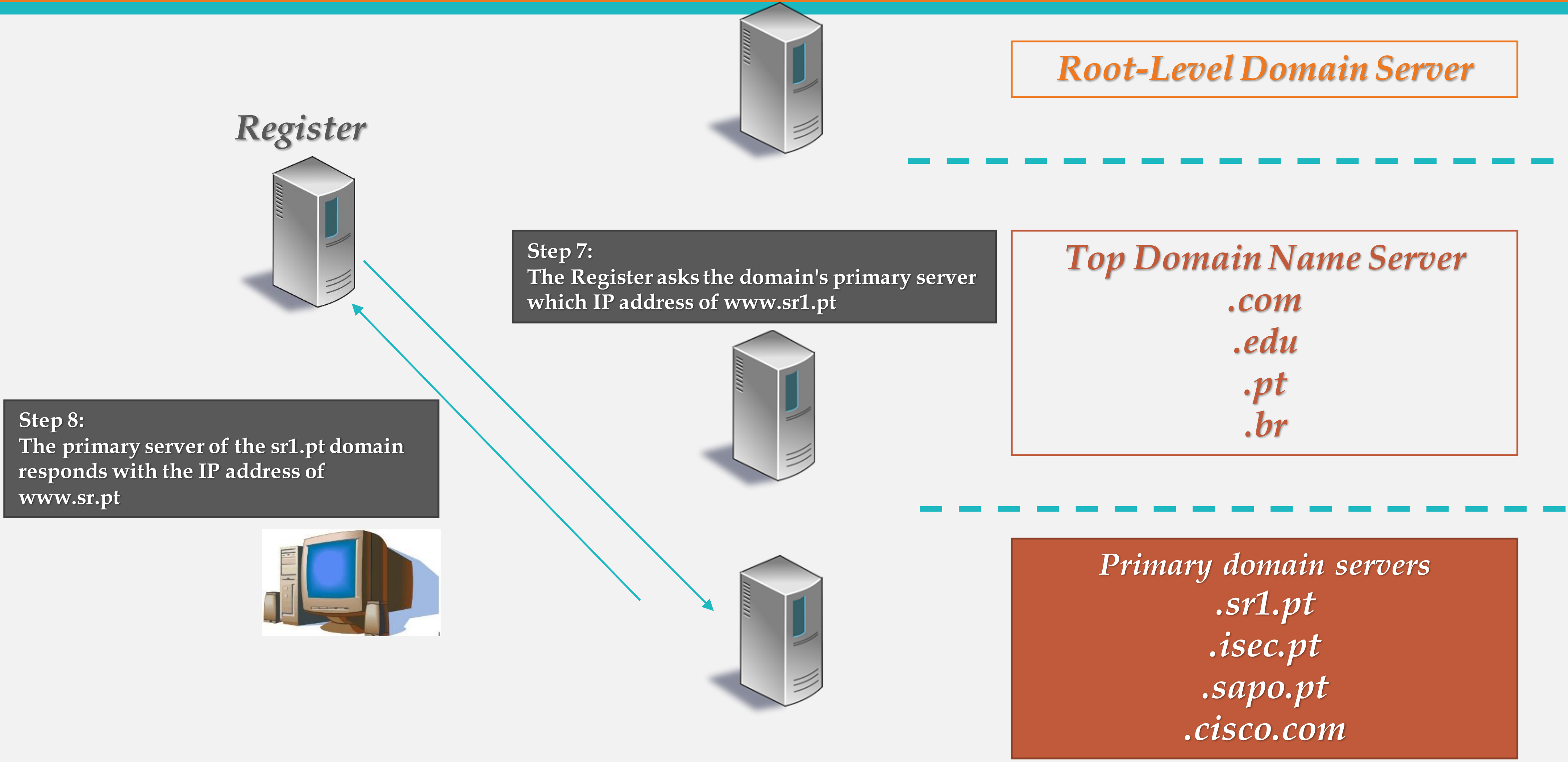
Step 5:
The Register asks the top domian name server the IP address of www.sr1.pt

*Top Domain Name Server*
*.com*
*.edu*
*.pt*
*.br*

Step 6:
The top domain name server indicates the IP of the primary server responsible for sr1.pt

*Primary domain servers*
*.sr1.pt*
*.isec.pt*
*.sapo.pt*
*.cisco.com*

# Operation



*Root-Level Domain Server*

*Register*

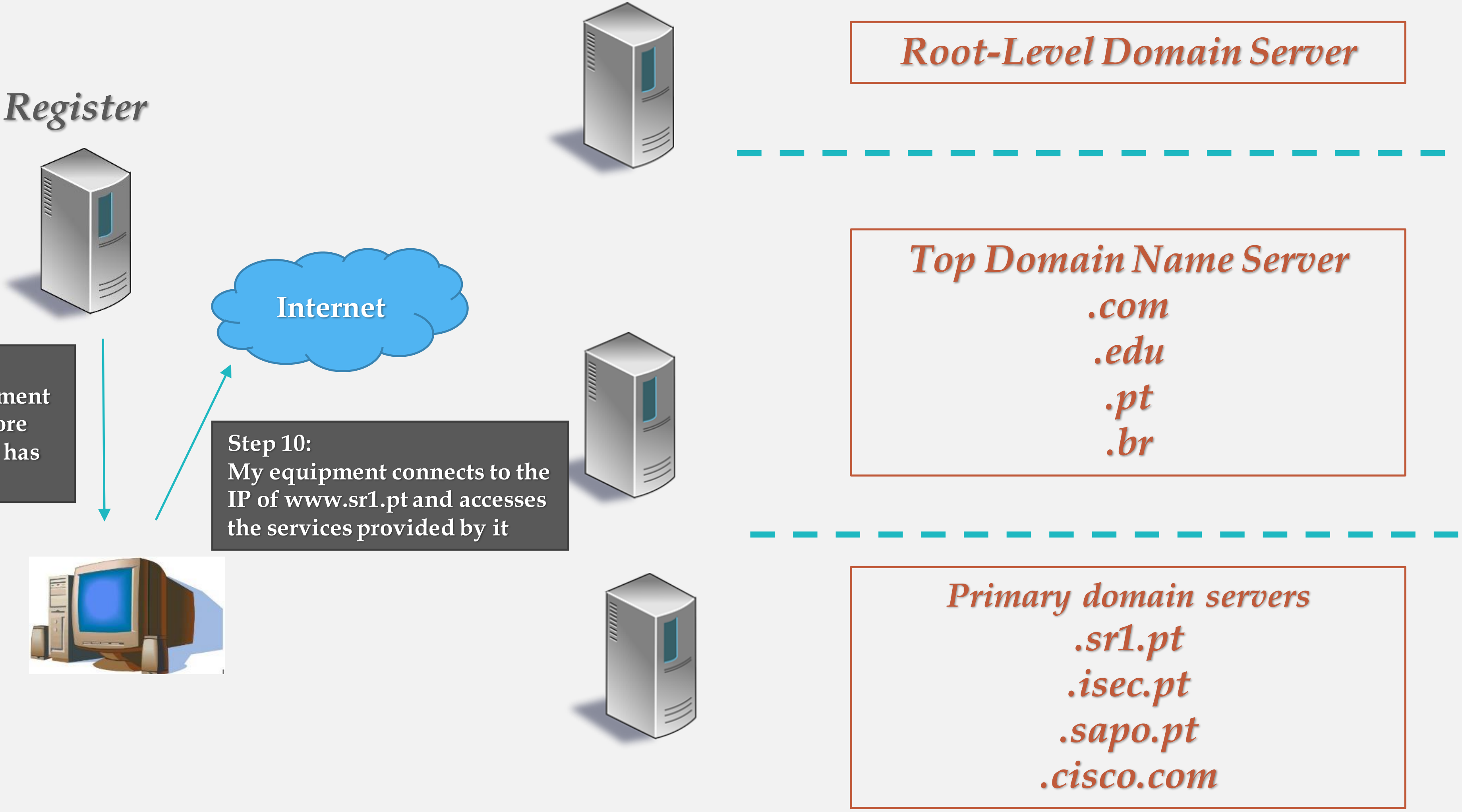
Step 7:
The Register asks the domain's primary server which IP address of www.sr1.pt

*Top Domain Name Server*
*.com*
*.edu*
*.pt*
*.br*

Step 8:
The primary server of the sr1.pt domain responds with the IP address of www.sr.pt

*Primary domain servers*
*.sr1.pt*
*.isec.pt*
*.sapo.pt*
*.cisco.com*

# Operation



Root-Level Domain Server

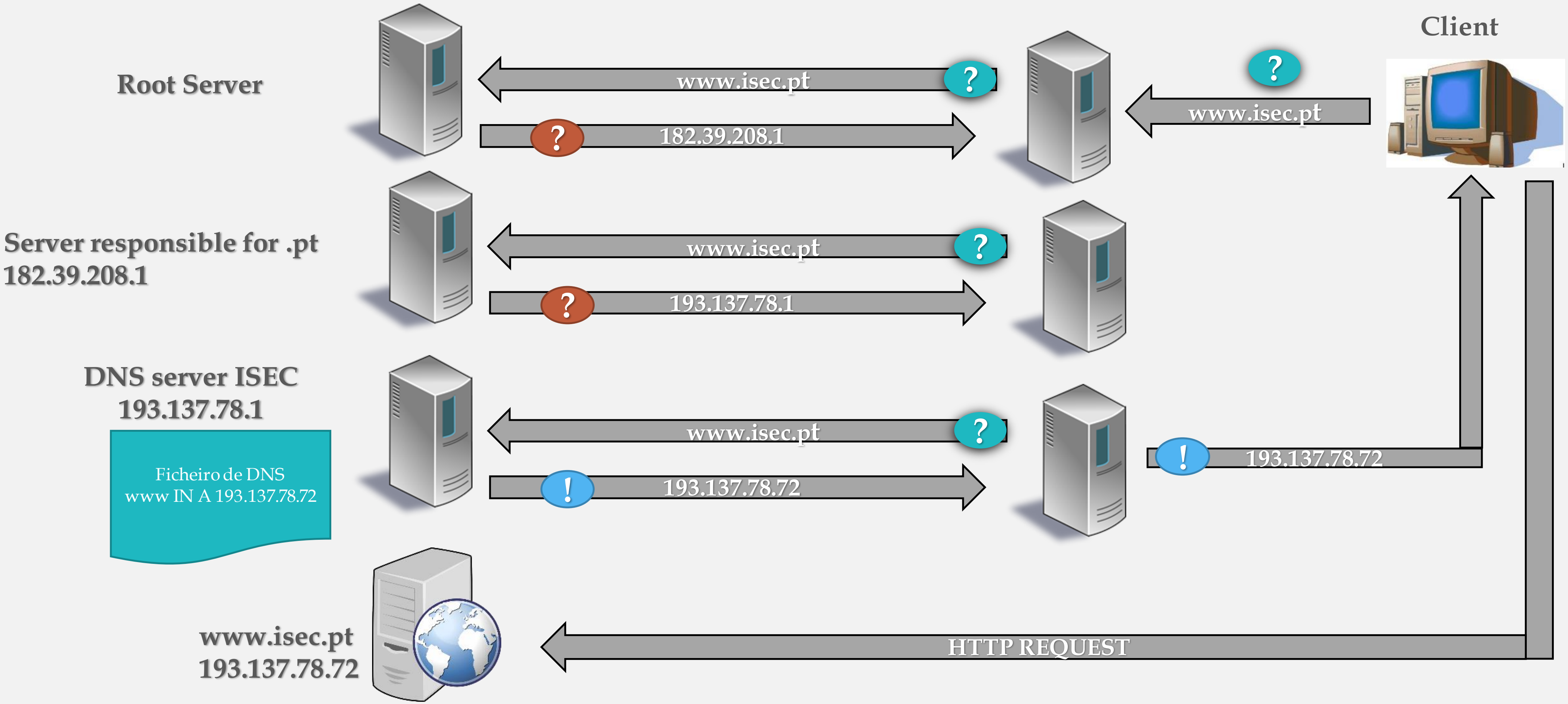
Top Domain Name Server
.com
.edu
.pt
.br

Primary domain servers
.sr1.pt
.isec.pt
.sapo.pt
.cisco.com

Step 9:
The Register informs my equipment the IP of www.sr1.pt and can store this information in its table if it has active caching.

Step 10:
My equipment connects to the IP of www.sr1.pt and accesses the services provided by it

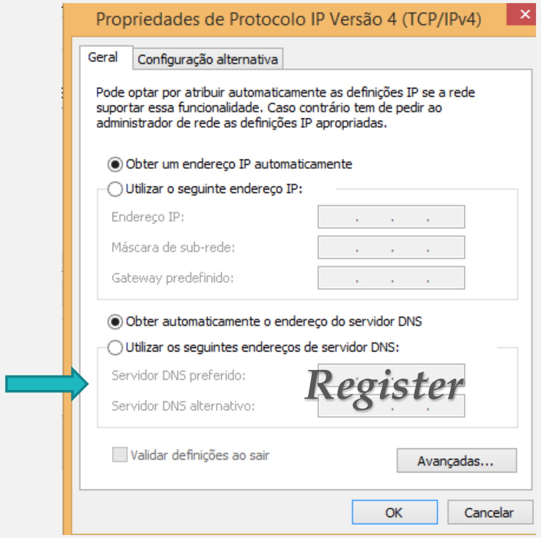
# Operation



Client
Root Server
Server responsible for .pt
182.39.208.1
DNS server ISEC
193.137.78.1
Ficheiro de DNS
www IN A 193.137.78.72
www.isec.pt
193.137.78.72
www.isec.pt
?
www.isec.pt
?
182.39.208.1
?
www.isec.pt
?
193.137.78.1
?
www.isec.pt
?
193.137.78.72
!
193.137.78.72
!
HTTP REQUEST

# Operation

- **Is the Register the first place my machine uses to try to obtain the IP?**
- No. On your machine, the first action you take is to consult the hosts file and only if this correspondence is not in this file, do you ask your register.
- **What is the IP address of the Register that the local machine uses?**
- The IP you put on your equipment's network card in the DNS field or which is defined in your DHCP service as your DNS server.
- **What is the IP address that a domain's primary server returns when asked?**
- Whatever is configured in your table. Thus, in the previous example, if in the table of the server responsible for the sr1.pt domain a type A record with the IP 203.100.2001.1 was created for the www machine, that would be the value that it answered.
- **Does the Register that I have defined on my PC have to be a machine on my local network?**
- No, it could be a machine outside my network.
- **Can the Register be the primary server for my DNS domain?**
- It can. The server for a given domain can also be the Register of machines in that domain.



Pode optar por atribuir automaticamente as definições IP se a rede suportar essa funcionalidade. Caso contrário tem de pedir ao administrador de rede as definições IP apropriadas.

● Obter um endereço IP automaticamente
○ Utilizar o seguinte endereço IP:
Endereço IP: . . .
Máscara de sub-rede: . . .
Gateway predefinido: . . .

● Obter automaticamente o endereço do servidor DNS
○ Utilizar os seguintes endereços de servidor DNS:
Servidor DNS preferido:
Servidor DNS alternativo:

□ Validar definições ao sair

Register

# *Caching*

- A fundamental feature of DNS is caching. That is, when a name server receives information about a mapping from a computer, it caches that information for future use in equal questions.
- Then, a later query regarding this mapping can use the cached result, thus avoiding additional inquiries to other servers.
- DNS uses caching to optimize the search cost.
- In this way, the addresses of the TLD (Top Level Domin) servers are always cached.
- An entry is kept in the cache up to a time limit controlled by the server administrator responsible for the cached name through the TTL (Time To Live) attribute.
- Entry is automatically removed from the cache when your TTL expires.

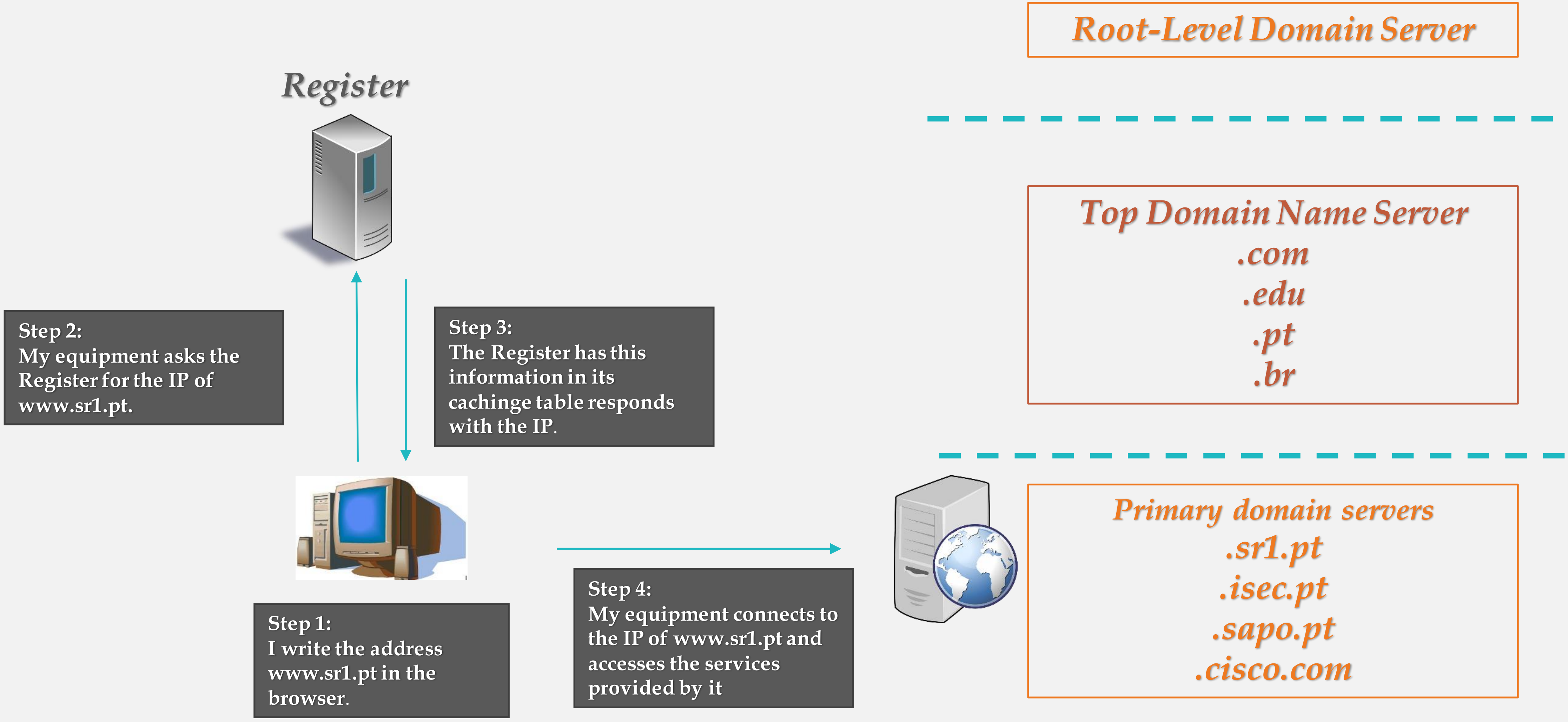
# *Caching*

- Since information about a given name can be changed, a server may have incorrect information in its caching table.
- Then the TTL value is used to decide when the information can no longer be considered as valid.
- If a server responds to a query with cached information it must:
  - update the RR TTL provided in the response
  - indicate that this is non-authoritative bit AA (authoritative answer) information set to 0 (false).

# *Caching*

- DNS optionally supports caching of negative responses.
  - Example: a server can distribute a TTL with an indication of “name error”.
- The customer who receives this information can assume that the name in question does not exist during TTL without consulting authoritative data.
- In the same way, a query can be made with a QTYPE that represents multiple types and cache a response with the indication that part of the types are not present.
- Servers that provide recursive service must be well stocked with memory!

# Operation - Caching and if the Register already has information on the IP of www.sr1.pt



*Root-Level Domain Server*

*Top Domain Name Server*
*.com*
*.edu*
*.pt*
*.br*

*Primary domain servers*
*.sr1.pt*
*.isec.pt*
*.sapo.pt*
*.cisco.com*

*Register*

Step 1:
I write the address www.sr1.pt in the browser.

Step 2:
My equipment asks the Register for the IP of www.sr1.pt.

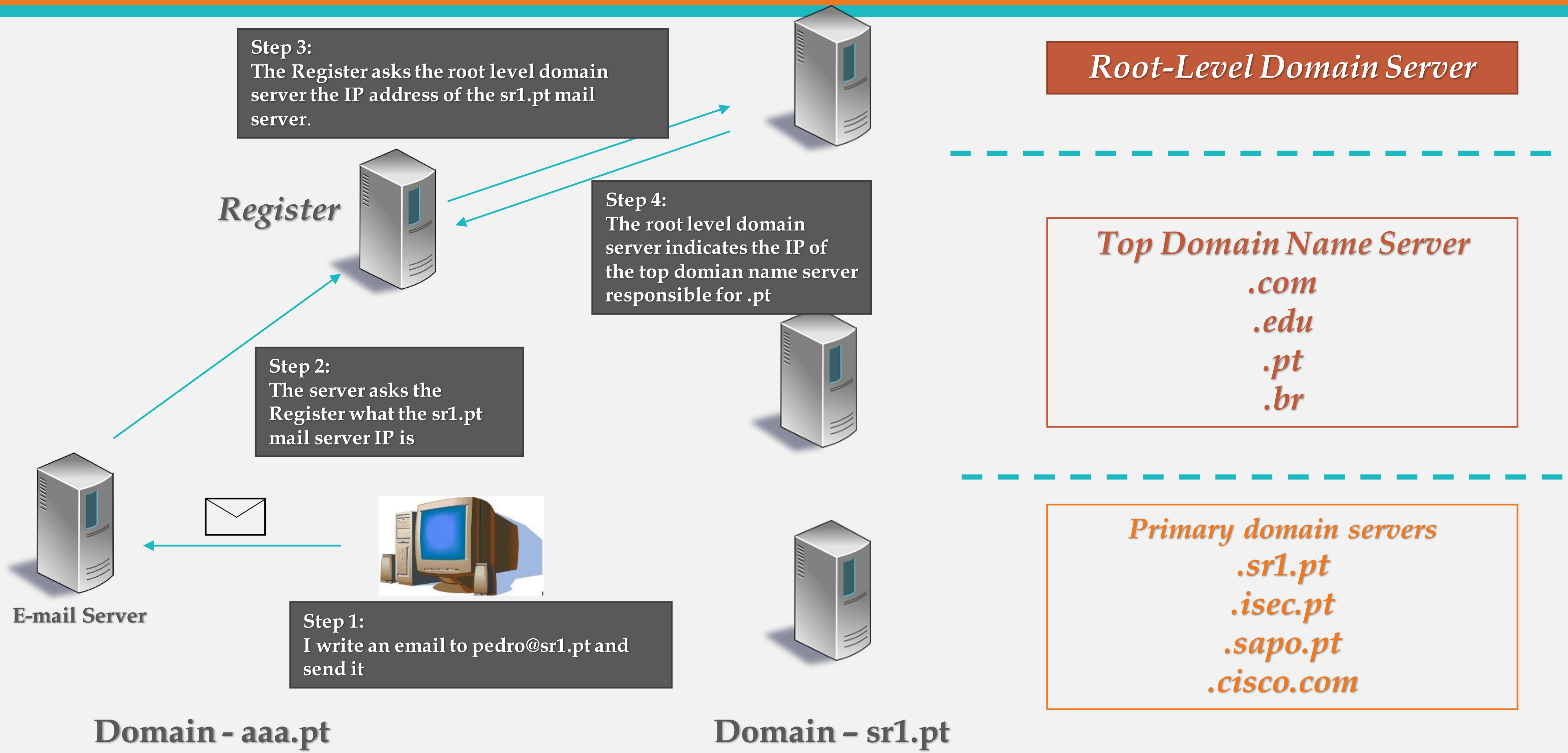
Step 3:
The Register has this information in its cachinge table responds with the IP.

Step 4:
My equipment connects to the IP of www.sr1.pt and accesses the services provided by it

# Operation - E-mail (MX)

- In case you want to send an email, your server does not know the name of the machine where you have to deliver the message. You only know the recipient's email address and therefore the domain.
- The operation will be identical to the one described for knowing the IP of a machine name, but now the question will not be answered by the IP of a name, but of the MX record of the destination domain.

# Operation - E-mail (MX)



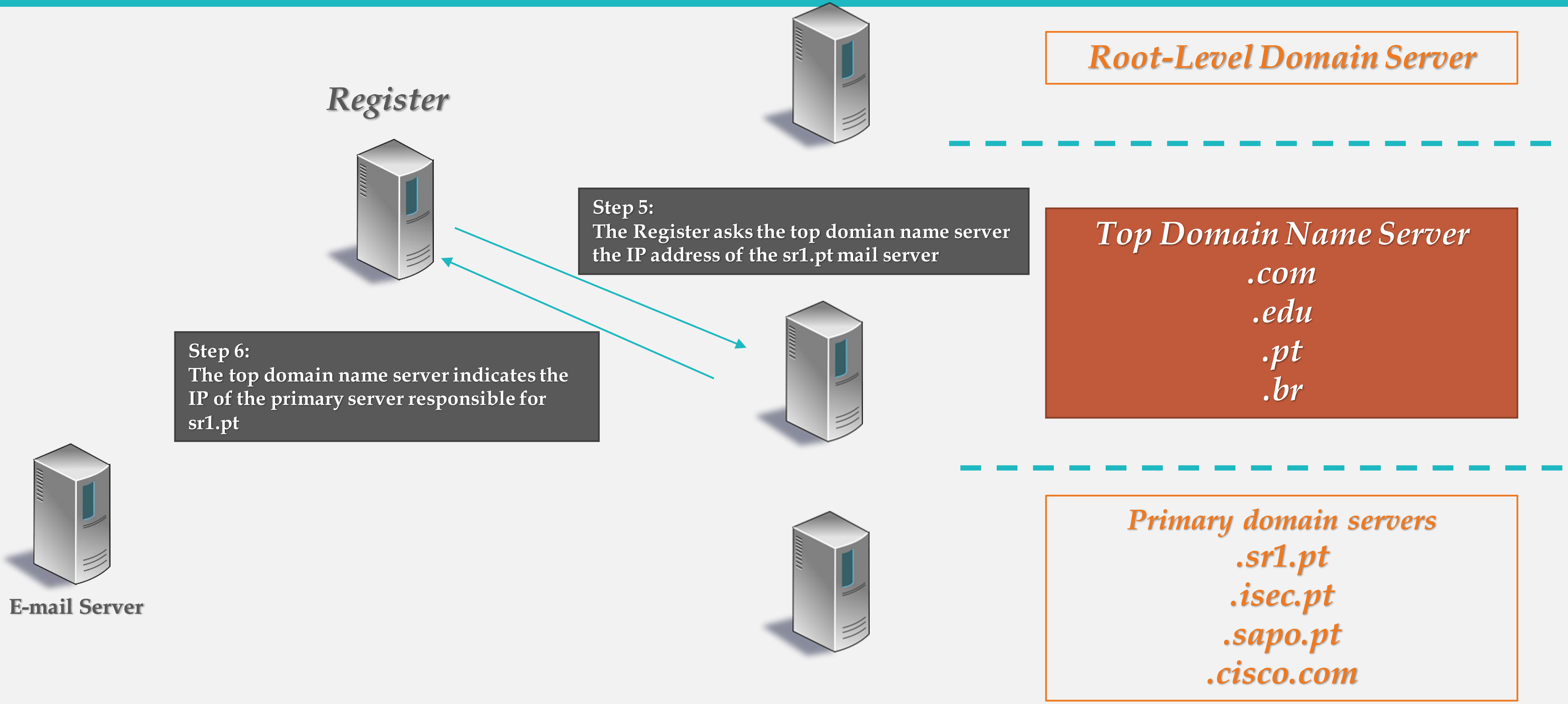
Step 3:
The Register asks the root level domain server the IP address of the sr1.pt mail server.

Step 4:
The root level domain server indicates the IP of the top domian name server responsible for .pt

Step 2:
The server asks the Register what the sr1.pt mail server IP is

Step 1:
I write an email to pedro@sr1.pt and send it

# Operation - E-mail (MX)



*Register*

Step 5:
The Register asks the top domian name server the IP address of the sr1.pt mail server

Step 6:
The top domain name server indicates the IP of the primary server responsible for sr1.pt

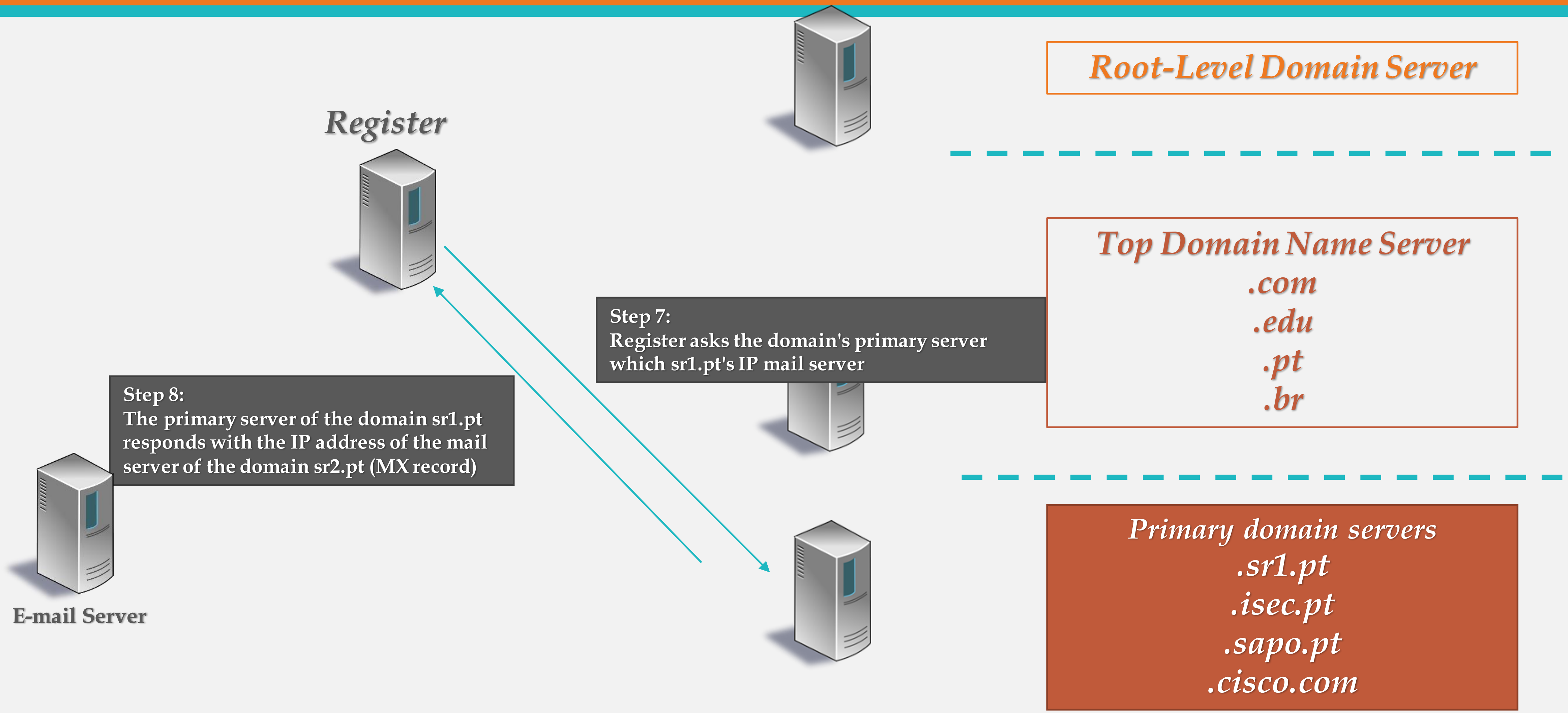
E-mail Server

*Root-Level Domain Server*

*Top Domain Name Server*
*.com*
*.edu*
*.pt*
*.br*

*Primary domain servers*
*.sr1.pt*
*.isec.pt*
*.sapo.pt*
*.cisco.com*

# Operation - E-mail (MX)



*Root-Level Domain Server*

*Register*

*Top Domain Name Server*
*.com*
*.edu*
*.pt*
*.br*

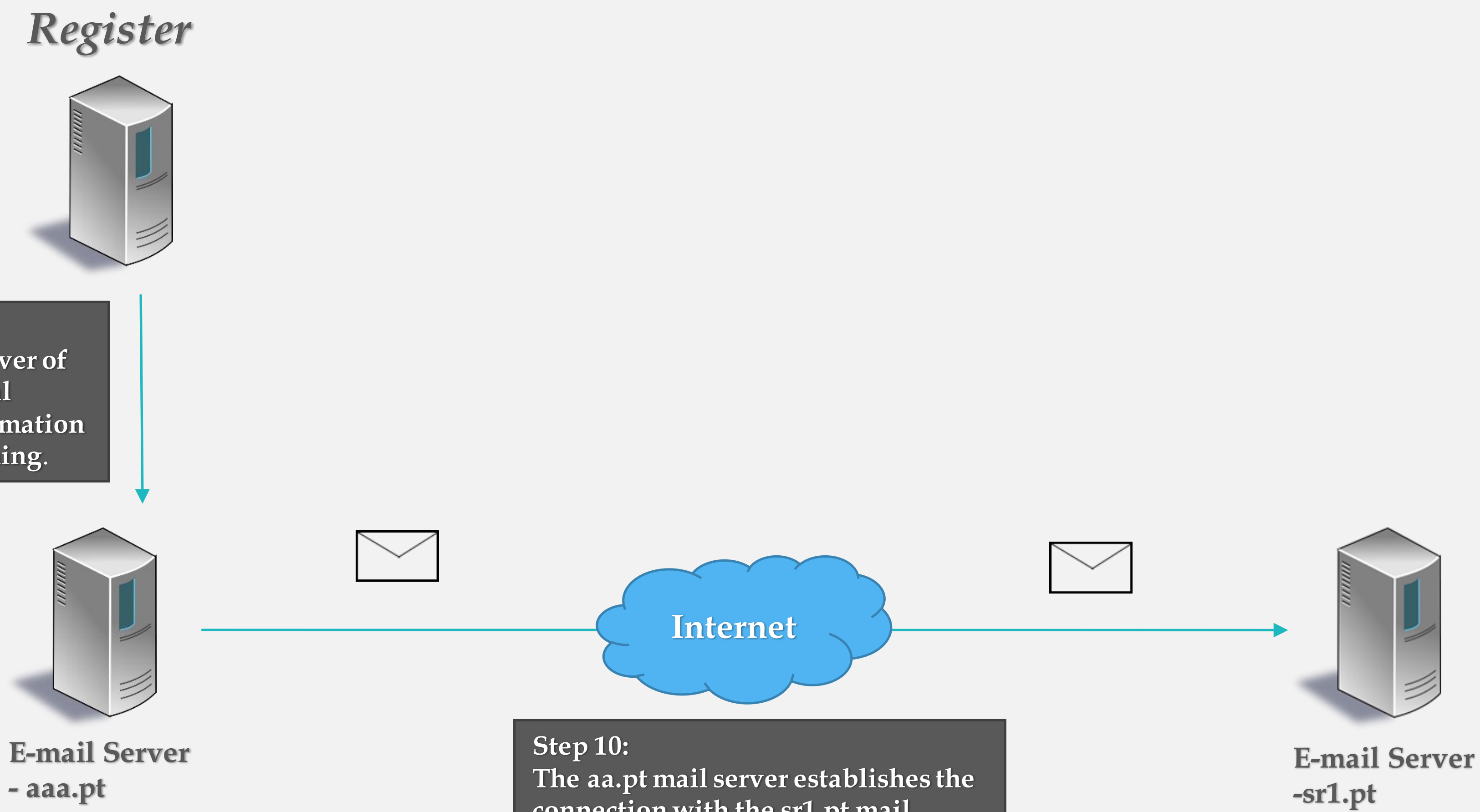
Step 7:
Register asks the domain's primary server which sr1.pt's IP mail server

Step 8:
The primary server of the domain sr1.pt responds with the IP address of the mail server of the domain sr2.pt (MX record)

*Primary domain servers*
*.sr1.pt*
*.isec.pt*
*.sapo.pt*
*.cisco.com*

E-mail Server

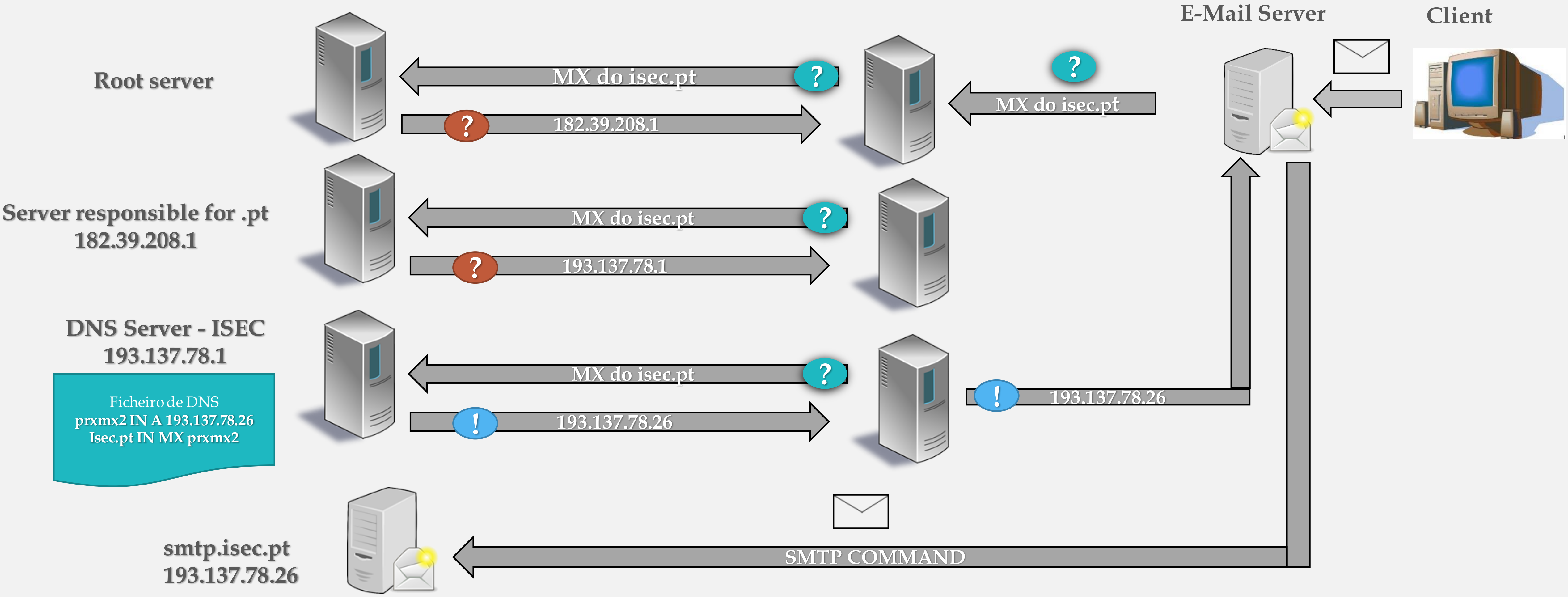
# Operation - E-mail (MX)



Step 9:
The Register informs mail server of the IP address of the sr2.pt mal server and can store this information in its table if it has active caching.

Step 10:
The aa.pt mail server establishes the connection with the sr1.pt mail server and delivers the mail message to pedro@sr1.pt

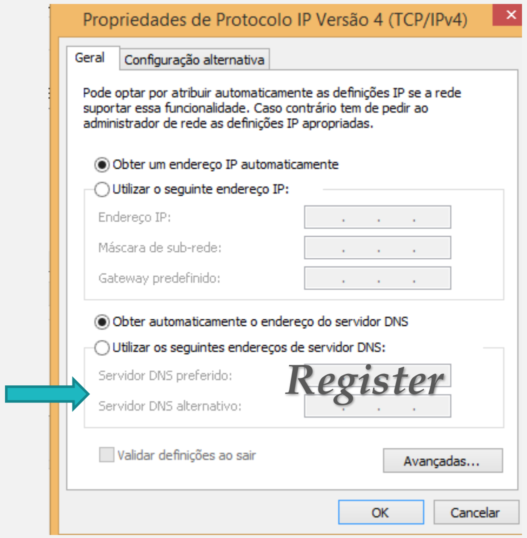
# Operation - E-mail (MX)



Ficheiro de DNS
prxmx2 IN A 193.137.78.26
Isec.pt IN MX prxmx2

# Operation - E-mail (MX)

- **What is the IP address of the Register for the aa.pt mail server?**
- The IP you put on your server's network card in the DNS field. On servers we should not use addresses assigned by DHCP
- **What is the IP address that a domain's primary server returns when asked if it does not know the name of the machine?**
- When the mail server starts the process, it does not know the name of the destination machine, but only the name of the address of the recipient of the message (the message is to be delivered in user @ domain). Then the response from the DNS server of the destination domain will not be from a machine (type A record), but from the machine with the MX record.



Propriedades de Protocolo IP Versão 4 (TCP/IPv4)

Pode optar por atribuir automaticamente as definições IP se a rede suportar essa funcionalidade. Caso contrário tem de pedir ao administrador de rede as definições IP apropriadas.

● Obter um endereço IP automaticamente

○ Utilizar o seguinte endereço IP:

Endereço IP: . . .

Máscara de sub-rede: . . .

Gateway predefinido: . . .

● Obter automaticamente o endereço do servidor DNS

○ Utilizar os seguintes endereços de servidor DNS:

Servidor DNS preferido:

Servidor DNS alternativo: . . .

□ Validar definições ao sair

# Type of queries

- **Interactive**
  - This is a query to which the contacted server responds with information available locally.
  - The answer may consist of:
    - In IP address - if it is authoritative information or is cached.
    - In a reference to a server "closer" to the answer.
    - In error - in case of poorly formulated queries.
  - Who conducts these consultations?
    - DNS servers that attempt to respond to a recursive query.
    - resolvers (rarely).
  - Servers are required to accept this mode.

# Type of queries

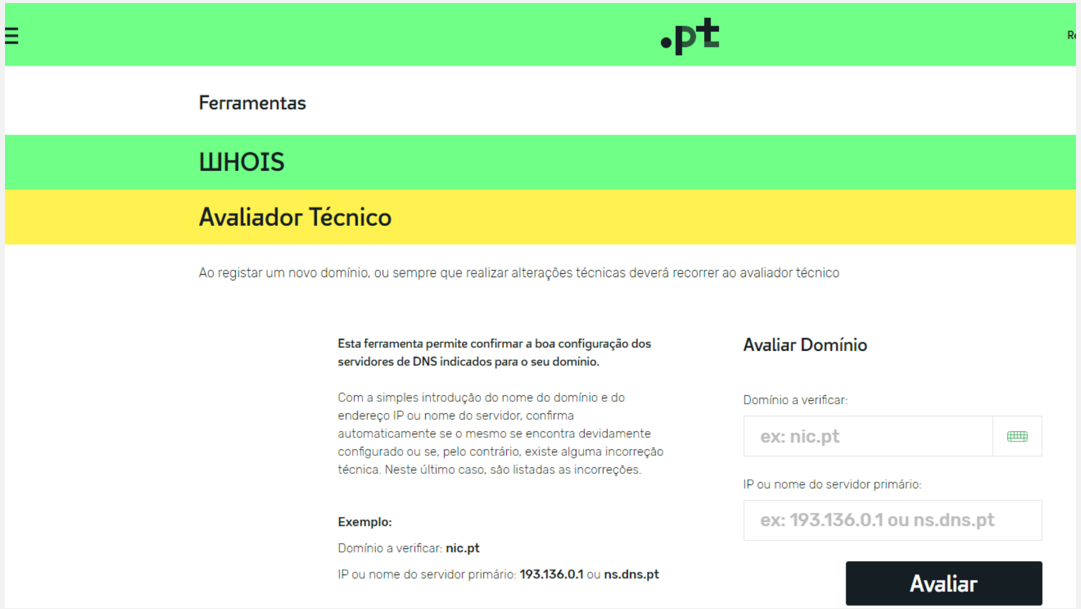
- **Recursive**
  - It is a query to which the contacted server always responds with the requested resolution or with an error indication (i.e. provides the final answer!)
  - Who conducts these consultations?
    - resolvers (typically)
    - DNS servers configured to use a forwarder
  - No DNS server is required to accept this type of query (e.g., root servers do not!)
  - There must be a DNS server, per local network, capable of accepting recursive queries.
  - Centralizing the interaction with the outside improves the caching effect!

# Answer

- **Authoritative -** Generated by servers that have authority in the domain of the resolved name. Very reliable answer, but may be incorrect (if provided by a secondary server and not the primary)
- **Non-authoritative -** Generated by servers that do not have authority in the domain of the resolved name. The answer is not so reliable, as the information may have been modified.

# Tools

- There are websites on the Internet that allow you to validate the correct configuration of your DNS server.
- One that you can use is provided by the FCCN:
  - http://www.dns.pt/en/tools/avaliador-tecnico/



Ferramentas

WHOIS

Avaliador Técnico

Ao registar um novo domínio, ou sempre que realizar alterações técnicas deverá recorrer ao avaliador técnico

**Esta ferramenta permite confirmar a boa configuração dos servidores de DNS indicados para o seu domínio.**

Com a simples introdução do nome do domínio e do endereço IP ou nome do servidor, confirma automaticamente se o mesmo se encontra devidamente configurado ou se, pelo contrário, existe alguma incorreção técnica. Neste último caso, são listadas as incorreções.

**Exemplo:**

Domínio a verificar: **nic.pt**

IP ou nome do servidor primário: **193.136.0.1** ou **ns.dns.pt**

Avaliar Domínio

Domínio a verificar: ex: nic.pt

IP ou nome do servidor primário: ex: 193.136.0.1 ou ns.dns.pt

# nslookup

- It is a tool, common to Windows and Linux, used to obtain information about DNS records of a given domain, host or IP.
- In a default query, the access provider's DNS server is queried, and returns information about the searched domain or host.
- The information "Non-authoritative answer" means that the DNS server used does not answer for this domain, in other words, this means that an external query was made to the DNS servers. Imagine that you are at your home making a query about an ISEC machine, if your server is to answer that question the answer will be Non-authoritative answer if it is the ISEC server it will be Authoritative answer.

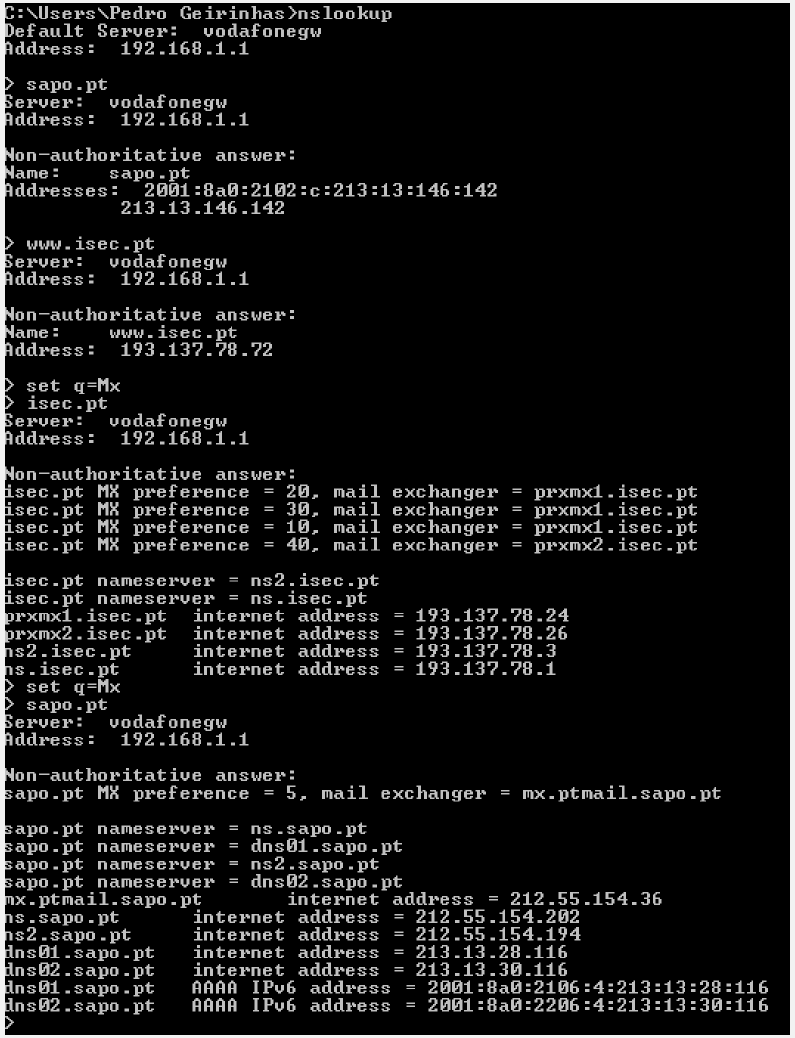
# nslookup - Mode

- **Non-interactive mode**
  - This mode is used to display the name and associated information related to a computer (host) or domain.
  - The name or Internet address is provided as the first parameter. The second parameter is optional and corresponds to the name or address of a domain name server.
- **Interactive mode**
  - With interactive mode, the user can query domain name servers in order to obtain information about several computers and domains or to print the list of computers in a domain.
  - This mode is invoked when specifying the nslookup command without parameters, using the default domain name server.
  - You can also invoke this interactive mode if the first parameter used is one - and the second parameter is the name of a computer or Internet address of a domain name server.

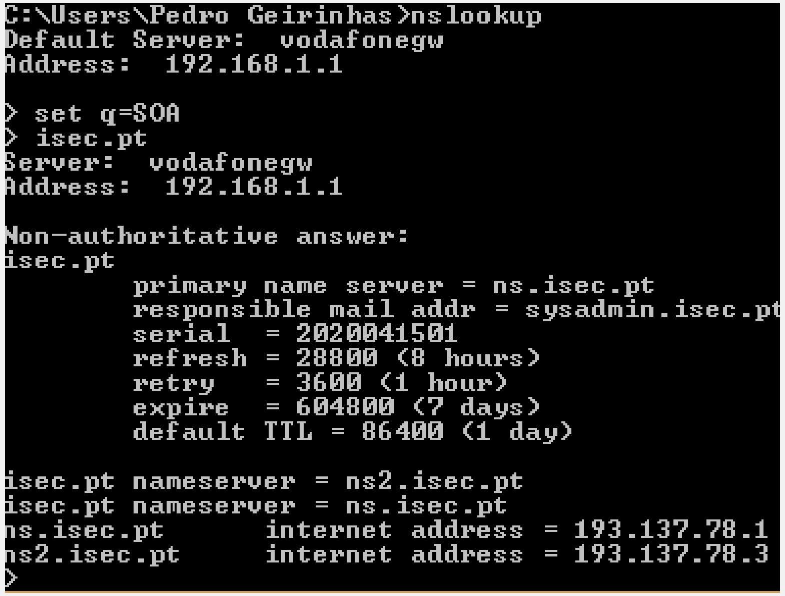
# nslookup

- The type of inquiry you want is defined by the command set q =
  - **A**
    - A simple inquiry requesting the IP address corresponding to a computer
  - **CNAME**
    - A given computer may have several DNS names. One of these is the canonical name (or canonical name).
  - **MX**
    - An inquiry concerning the mail exchanger.
  - **SOA**
    - A query to the Start of Authority for a given domain.
  - **PTR**
    - A PTR survey, which demonstrates reverse resolution (inverse or reverse). Notice the somewhat odd way in which the survey was introduced, which is partly because IP addresses have the most significant part on the left side while DNS addresses have it on the right side of the address.

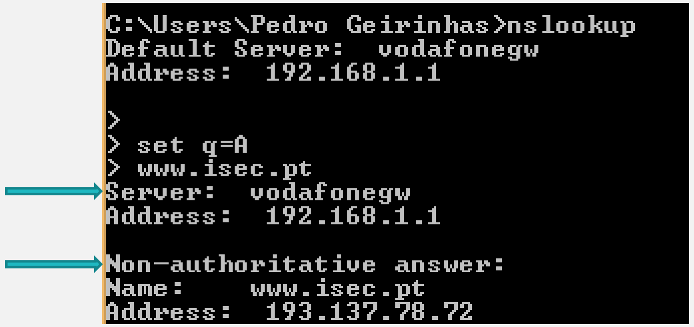
# nslookup



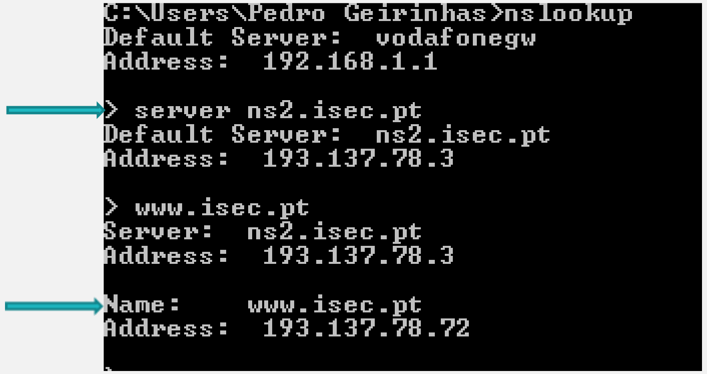
```
C:\Users\Pedro Geirinhas>nslookup
Default Server:  vodafonegw
Address:  192.168.1.1

> sapo.pt
Server:  vodafonegw
Address:  192.168.1.1

Non-authoritative answer:
Name:    sapo.pt
Addresses:  2001:8a0:2102:c:213:13:146:142
          213.13.146.142

> www.isec.pt
Server:  vodafonegw
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.isec.pt
Address:  193.137.78.72

> set q=Mx
> isec.pt
Server:  vodafonegw
Address:  192.168.1.1

Non-authoritative answer:
isec.pt MX preference = 20, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 30, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 10, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 40, mail exchanger = prxmx2.isec.pt

isec.pt nameserver = ns2.isec.pt
isec.pt nameserver = ns.isec.pt
prxmx1.isec.pt  internet address = 193.137.78.24
prxmx2.isec.pt  internet address = 193.137.78.26
ns2.isec.pt     internet address = 193.137.78.3
ns.isec.pt      internet address = 193.137.78.1
> set q=Mx
> sapo.pt
Server:  vodafonegw
Address:  192.168.1.1

Non-authoritative answer:
sapo.pt MX preference = 5, mail exchanger = mx.ptmail.sapo.pt

sapo.pt nameserver = ns.sapo.pt
sapo.pt nameserver = dns01.sapo.pt
sapo.pt nameserver = ns2.sapo.pt
sapo.pt nameserver = dns02.sapo.pt
mx.ptmail.sapo.pt       internet address = 212.55.154.36
ns.sapo.pt      internet address = 212.55.154.202
ns2.sapo.pt     internet address = 212.55.154.194
dns01.sapo.pt   internet address = 213.13.28.116
dns02.sapo.pt   internet address = 213.13.30.116
dns01.sapo.pt   AAAA IPv6 address = 2001:8a0:2106:4:213:13:28:116
dns02.sapo.pt   AAAA IPv6 address = 2001:8a0:2206:4:213:13:30:116
>
```



```
C:\Users\Pedro Geirinhas>nslookup
Default Server:  vodafonegw
Address:  192.168.1.1

> set q=SOA
> isec.pt
Server:  vodafonegw
Address:  192.168.1.1

Non-authoritative answer:
isec.pt
        primary name server = ns.isec.pt
        responsible mail addr = sysadmin.isec.pt
        serial  = 2020041501
        refresh = 28800 (8 hours)
        retry   = 3600 (1 hour)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)

isec.pt nameserver = ns2.isec.pt
isec.pt nameserver = ns.isec.pt
ns.isec.pt      internet address = 193.137.78.1
ns2.isec.pt     internet address = 193.137.78.3
>
```



```
C:\Users\Pedro Geirinhas>nslookup
Default Server:  vodafonegw
Address:  192.168.1.1

>
> set q=A
> www.isec.pt
Server:  vodafonegw
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.isec.pt
Address:  193.137.78.72
```

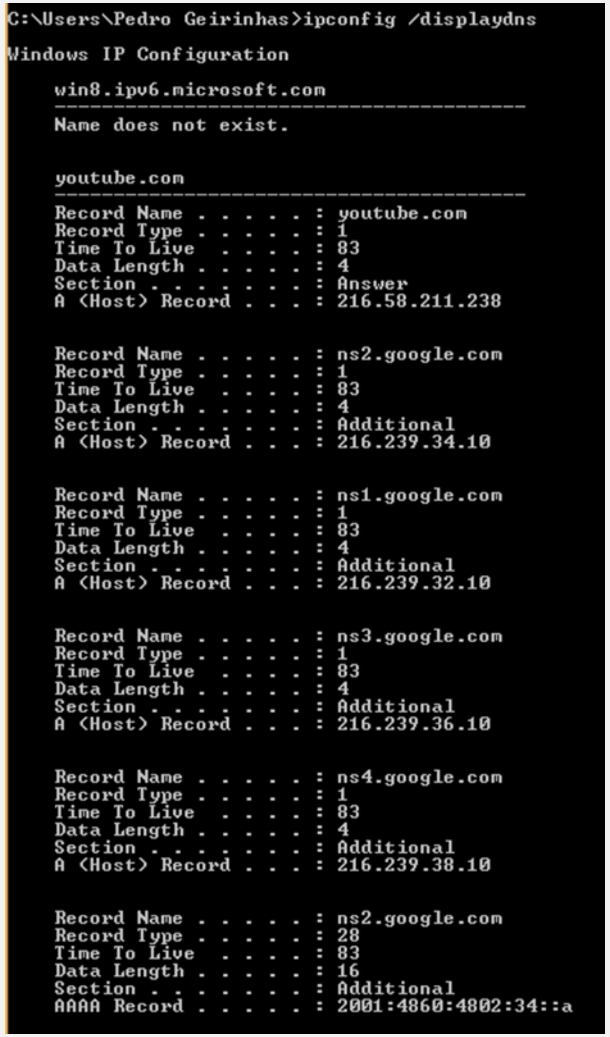


```
C:\Users\Pedro Geirinhas>nslookup
Default Server:  vodafonegw
Address:  192.168.1.1

> server ns2.isec.pt
Default Server:  ns2.isec.pt
Address:  193.137.78.3

> www.isec.pt
Server:  ns2.isec.pt
Address:  193.137.78.3

Name:    www.isec.pt
Address:  193.137.78.72
```

# ipconfig

- To view the name resolution cache on a client you can do the following:
  - ipconfig /displaydns

  - To empty and reset a client resolver cache:
    - ipconfig / flushdns



```
C:\Users\Pedro Geirinhas>ipconfig /displaydns

Windows IP Configuration

    win8.ipv6.microsoft.com
    ----------------------------------------
    Name does not exist.


    youtube.com
    ----------------------------------------
    Record Name . . . . . : youtube.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 83
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 216.58.211.238


    Record Name . . . . . : ns2.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 83
    Data Length . . . . . : 4
    Section . . . . . . . : Additional
    A (Host) Record . . . : 216.239.34.10


    Record Name . . . . . : ns1.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 83
    Data Length . . . . . : 4
    Section . . . . . . . : Additional
    A (Host) Record . . . : 216.239.32.10


    Record Name . . . . . : ns3.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 83
    Data Length . . . . . : 4
    Section . . . . . . . : Additional
    A (Host) Record . . . : 216.239.36.10


    Record Name . . . . . : ns4.google.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 83
    Data Length . . . . . : 4
    Section . . . . . . . : Additional
    A (Host) Record . . . : 216.239.38.10


    Record Name . . . . . : ns2.google.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 83
    Data Length . . . . . : 16
    Section . . . . . . . : Additional
    AAAA Record . . . . . : 2001:4860:4802:34::a
```

# DNS propagation

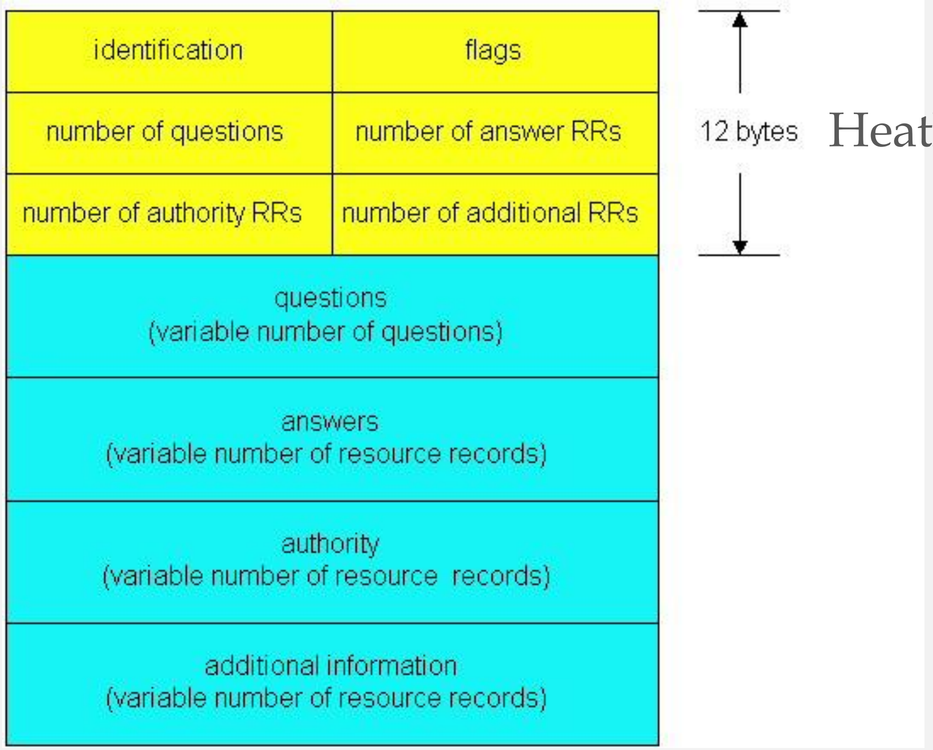
- It is the time required for a domain to be published and disseminated on all existing DNS servers. Thus, between the activation of the domain and the DNS servers receiving the newly created domain, it takes a time interval, which is then the time of DNS propagation.
- This time also happens when you change your DNS configuration for example with the addition or change of a new record.
- Propagation takes 8 to 48 hours. During this time, the service is unstable, being able to work at certain times and depending on the Register that customers use.
- There are several reasons, but what makes the operation slow is precisely the need to inform other DNS servers of the new domain or the change made as there are a few million servers takes your time ...
- The publication process is done by the bodies responsible for registering domains. These entities update their servers and publish a "list" of new domain registrations and changes to DNS servers, for domains already registered.
- Then there is what we call propagation, during which the databases of the ISP's DNS servers (Internet Service Providers) are updated. After this process, the domains start to point to the IP address of the server where the site information is.
- Usually, the publication does not exceed 48 hours, but situations can occur, mainly in the case of international domains, in which this period may be longer. This depends exclusively on the policy of the entity that carries out the records. In addition, the propagation of this information to the ISP's DNS servers can also take some time and delay the entire process.

# Transport Protocols

- **UDP**
  - DNS requests and responses are typically carried in a UDP datagram (initially and as long as the response is <512 bytes)
  - In case the information to be carried is larger than the size of that datagram, the response is sent incomplete and the Truncated flag is activated.
- **TCP**
  - When the volume of information to be transferred does not fit in a UDP datagram, the DNS client establishes a TCP connection with the server to carry out the transfer.
    - when a response is received with the Truncated flag enabled
    - for transferring zone information from the primary server to the secondary ones

# The Protocol

The question and answer messages both have the same format:



| | |
|---|---|
| identification | flags |
| number of questions | number of answer RRs |
| number of authority RRs | number of additional RRs |
| questions<br>(variable number of questions) | |
| answers<br>(variable number of resource records) | |
| authority<br>(variable number of resource  records) | |
| additional information<br>(variable number of resource records) | |

Heather

# Message fields

**Header -** let you know if it is a request or a response, if the response is authoritative, whether recursion is desired and whether it is available, error codes, etc.
The ID field is put by the client and saved by the server so that the client can bind the request to the response.

**Questions -** a question to ask or ask

**Answers -** What the server can know in response to this question (can be cached information)

**Authority -** data about name servers with authority over the data listed in the response

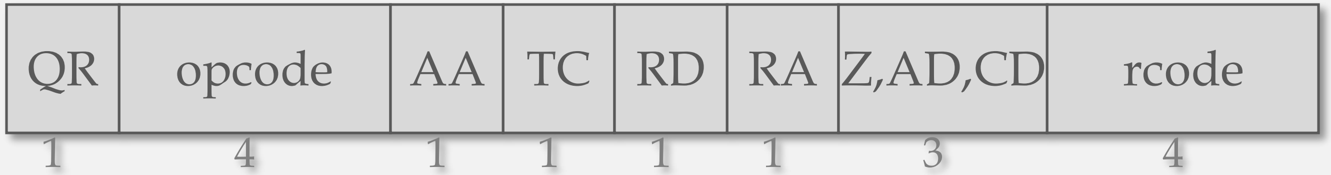
**Additional information -** which may be useful (supplementary information which may avoid further questions).

# The Protocol

- ***Identification***

It is a value established by the client and returned by the server so that those who consult know that the message is the answer to a certain question

- ***Flags***

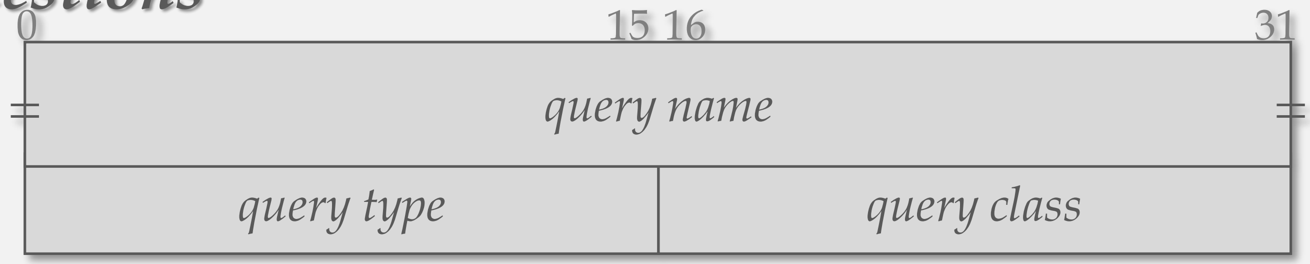


| QR | opcode | AA | TC | RD | RA | Z,AD,CD | rcode |
|---|---|---|---|---|---|---|---|
| 1 | 4 | 1 | 1 | 1 | 1 | 3 | 4 |

- QR = { 0 - query | 1- response }
- opcode = { 0 - standard query | 1- inverse query | 2 - server status | … }
- AA = { 1 - authoritative answer | 0 }
- TC = { 1- truncated (UDP máx = 512 bytes) | 0 }
- RD = { 1- recursion desired | 0 }
- RA = { 1- recursion available | 0 }
- rcode = { 0 - no error | 3 - name error (domínio inexistente) | …}

# The Protocol

- ***questions***



- query name: the domain that is questioned

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | w | w | w | 4 | i | s | e | c | 2 | p | t | 0 |

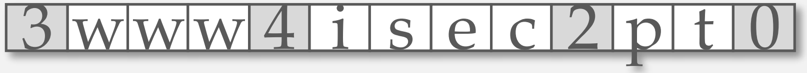
- query type: type of information requested

| Códig | Nome | Descrição |
|---|---|---|
| 1 | A | IP address |
| 2 | NS | name server |
| 5 | CNA<br>ME | canonical name |
| 252 | AXFR | req. zone transfer |

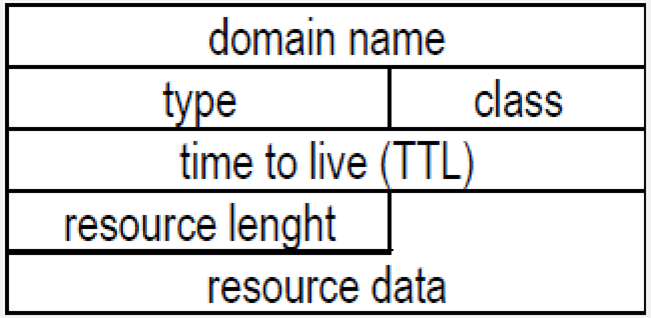
| Códig | Nome | Descrição |
|---|---|---|
| 12 | PTR | pointer records |
| 13 | HINF<br>O | host info |
| 15 | MX | mail exchange |
| 255 | *ANY | req. all records |

# Protocol

- ***Answers***
  - Domain Name
    - Search key (Ex .: Machine name)
    - Type
      - (see next slide table)
  - Class
    - Tip. 1 - Internet
  - Time To Live
    - Validity of information (*cache*)
  - Resource Data Domain Name
    - Additional information



| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | w | w | w | 4 | i | s | e | c | 2 | p | t | 0 |



domain name

type

class

time to live (TTL)

resource lenght

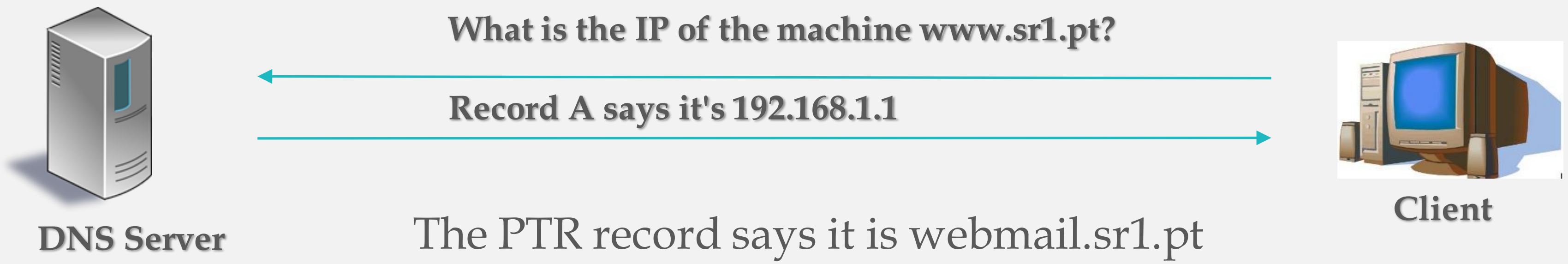
resource data

# Reverse resolution

- Resource used to resolve a name using an IP address, ie reverse DNS operation
- Used to ensure the reliability of the name to be displayed, by checking the name with the IP address.
- Benefits
  - Security (for example: filtering by name or geographical area).
  - Easy reading of log files.
  - Reduction of SPAM (destination server can ask if the MX of the domain that is trying to deliver the message has the IP of the machine that is connecting to it).

# Reverse resolution

## Direct resolation

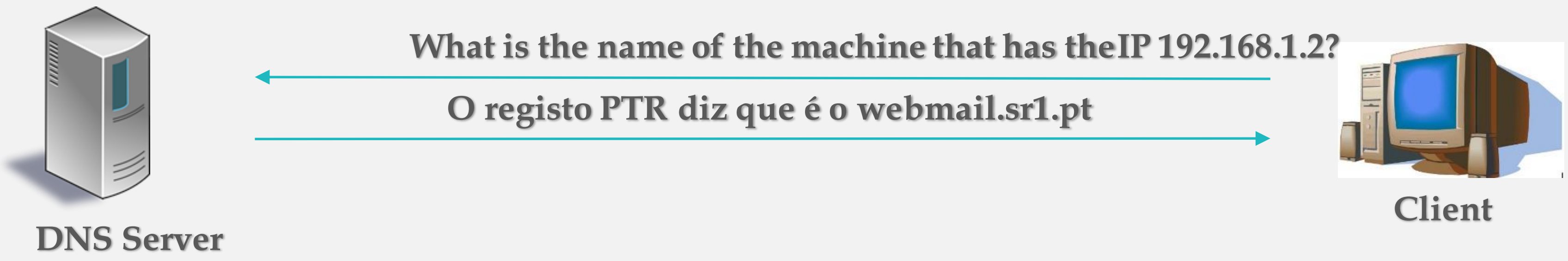


What is the IP of the machine www.sr1.pt?

Record A says it's 192.168.1.1

The PTR record says it is webmail.sr1.pt

## Reverse resolution



What is the name of the machine that has theIP 192.168.1.2?

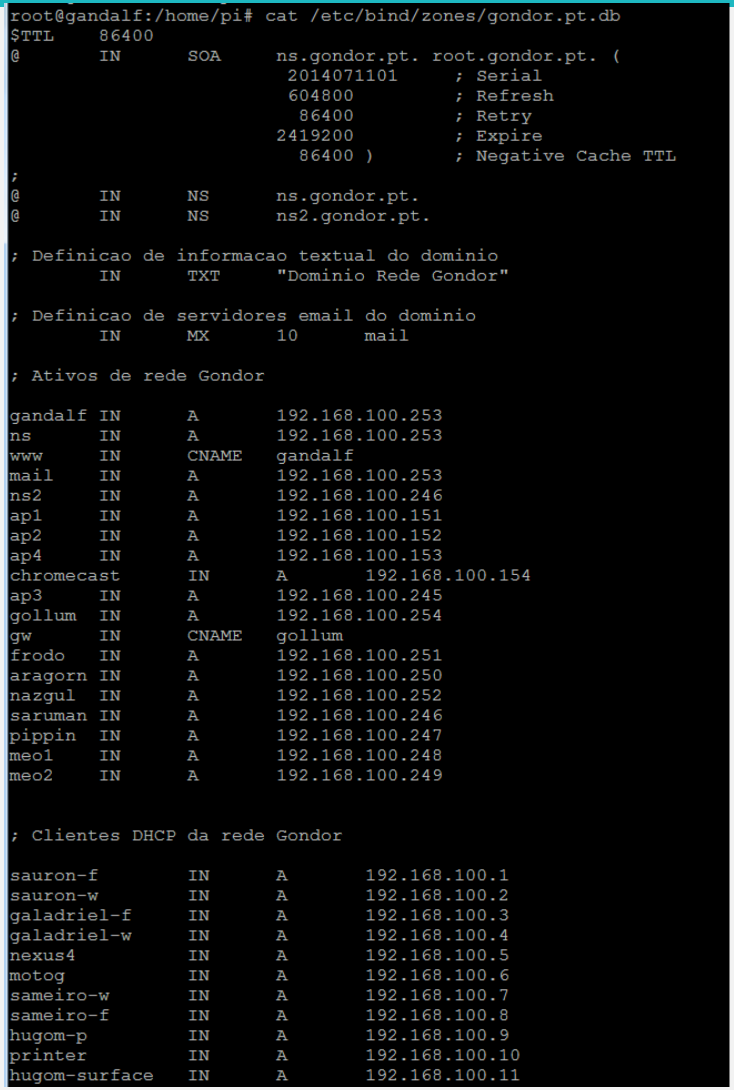
O registo PTR diz que é o webmail.sr1.pt

# Reverse resolution

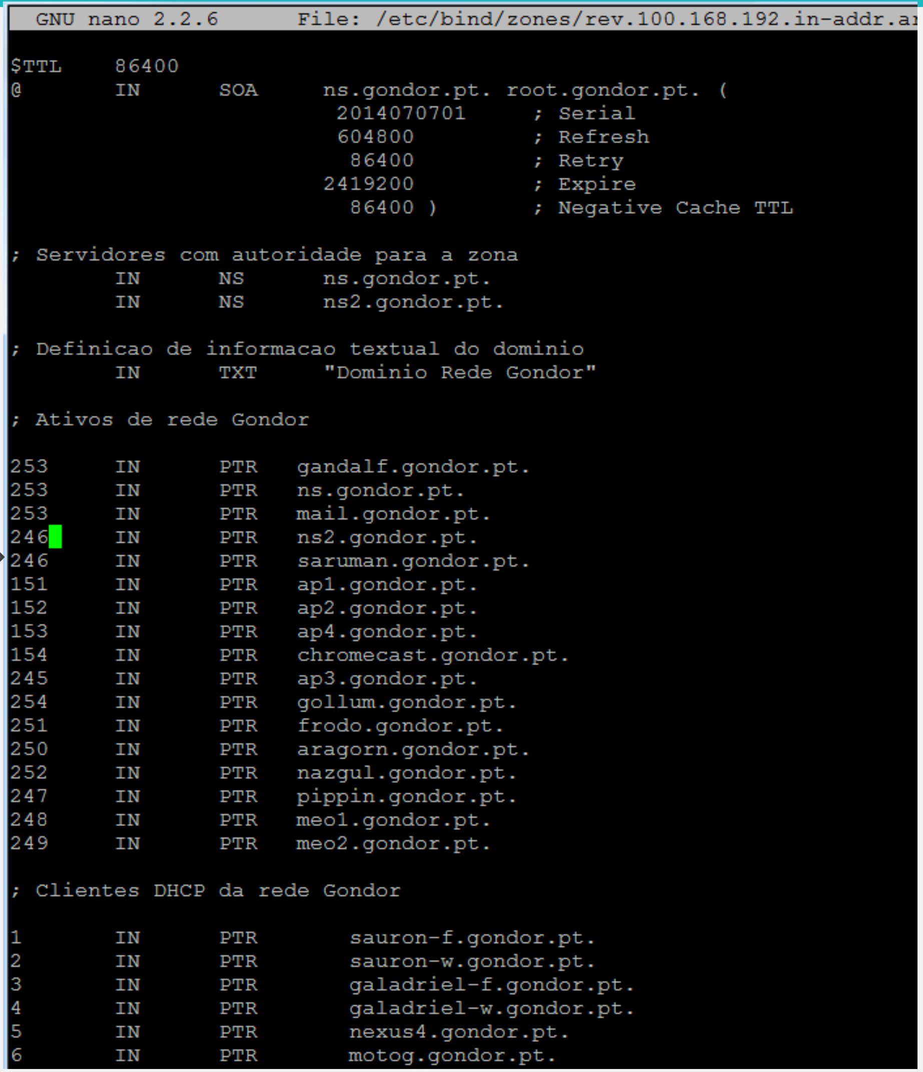
- The configuration of the inverse resolution is done through domains defined for the purpose, belonging to the 'in-addr.arpa' domain.
  - Subdomains are defined by entering the octets of the network address, in reverse order
    - Example (ISEC): 78.137.193.in-addr.arpa
- The management of an'inaddr.arpa. 'Domain can only be delegated if the class addresses (class C, class B, ...) have all been assigned to a single entity:
  - Example (ISEC): ISEC can manage the domain 78.137.193.in-addr.arpa because it has been delegated this management by who has delegated management of class B 193.137.0.0 (FCCN).
- The management of non-complete classes is possible but has a higher level of complexity, mainly in terms of its maintenance.
- In the case of IPv6 the reverse resolution is done through the IP6.ARPA domain
  - the existing initial domain for this purpose, IP6.INT, is being abandoned.

# Reverse resolution

Diret



```
root@gandalf:/home/pi# cat /etc/bind/zones/gondor.pt.db
$TTL    86400
@       IN      SOA     ns.gondor.pt. root.gondor.pt. (
                         2014071101     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      ns.gondor.pt.
@       IN      NS      ns2.gondor.pt.

; Definicao de informacao textual do dominio
        IN      TXT     "Dominio Rede Gondor"

; Definicao de servidores email do dominio
        IN      MX      10      mail

; Ativos de rede Gondor

gandalf IN      A       192.168.100.253
ns      IN      A       192.168.100.253
www     IN      CNAME   gandalf
mail    IN      A       192.168.100.253
ns2     IN      A       192.168.100.246
ap1     IN      A       192.168.100.151
ap2     IN      A       192.168.100.152
ap4     IN      A       192.168.100.153
chromecast      IN      A       192.168.100.154
ap3     IN      A       192.168.100.245
gollum  IN      A       192.168.100.254
gw      IN      CNAME   gollum
frodo   IN      A       192.168.100.251
aragorn IN      A       192.168.100.250
nazgul  IN      A       192.168.100.252
saruman IN      A       192.168.100.246
pippin  IN      A       192.168.100.247
meo1    IN      A       192.168.100.248
meo2    IN      A       192.168.100.249


; Clientes DHCP da rede Gondor

sauron-f        IN      A       192.168.100.1
sauron-w        IN      A       192.168.100.2
galadriel-f     IN      A       192.168.100.3
galadriel-w     IN      A       192.168.100.4
nexus4          IN      A       192.168.100.5
motog           IN      A       192.168.100.6
sameiro-w       IN      A       192.168.100.7
sameiro-f       IN      A       192.168.100.8
hugom-p         IN      A       192.168.100.9
printer         IN      A       192.168.100.10
hugom-surface   IN      A       192.168.100.11
```

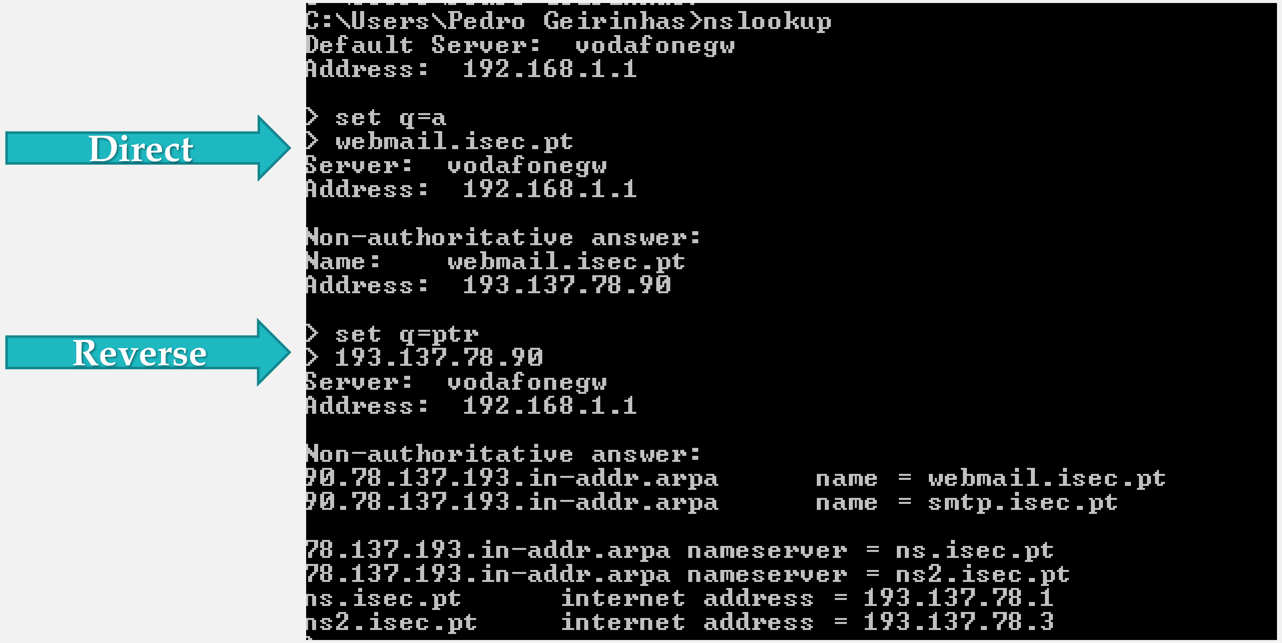


```
  GNU nano 2.2.6      File: /etc/bind/zones/rev.100.168.192.in-addr.ar

$TTL    86400
@       IN      SOA     ns.gondor.pt. root.gondor.pt. (
                         2014070701     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL

; Servidores com autoridade para a zona
        IN      NS      ns.gondor.pt.
        IN      NS      ns2.gondor.pt.

; Definicao de informacao textual do dominio
        IN      TXT     "Dominio Rede Gondor"

; Ativos de rede Gondor

253     IN      PTR   gandalf.gondor.pt.
253     IN      PTR   ns.gondor.pt.
253     IN      PTR   mail.gondor.pt.
246     IN      PTR   ns2.gondor.pt.
246     IN      PTR   saruman.gondor.pt.
151     IN      PTR   ap1.gondor.pt.
152     IN      PTR   ap2.gondor.pt.
153     IN      PTR   ap4.gondor.pt.
154     IN      PTR   chromecast.gondor.pt.
245     IN      PTR   ap3.gondor.pt.
254     IN      PTR   gollum.gondor.pt.
251     IN      PTR   frodo.gondor.pt.
250     IN      PTR   aragorn.gondor.pt.
252     IN      PTR   nazgul.gondor.pt.
247     IN      PTR   pippin.gondor.pt.
248     IN      PTR   meo1.gondor.pt.
249     IN      PTR   meo2.gondor.pt.

; Clientes DHCP da rede Gondor

1       IN      PTR       sauron-f.gondor.pt.
2       IN      PTR       sauron-w.gondor.pt.
3       IN      PTR       galadriel-f.gondor.pt.
4       IN      PTR       galadriel-w.gondor.pt.
5       IN      PTR       nexus4.gondor.pt.
6       IN      PTR       motog.gondor.pt.
```

Reverse

http://dicasdozefacadas.blogspot.pt/2014/07/instalar-e-configurar-um-servidor-dns.html

# Reverse resolution



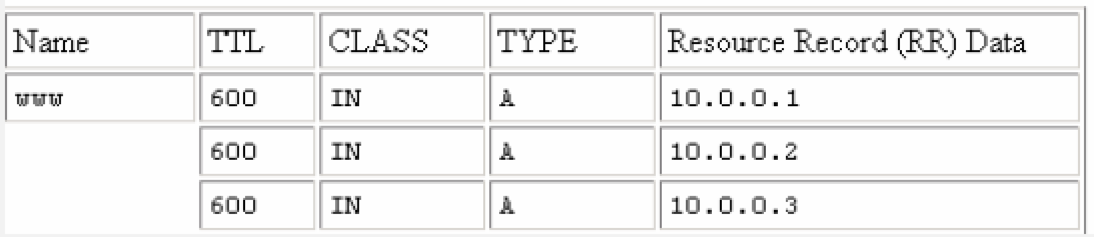
```
C:\Users\Pedro Geirinhas>nslookup
Default Server:  vodafonegw
Address:  192.168.1.1

> set q=a
> webmail.isec.pt
Server:  vodafonegw
Address:  192.168.1.1

Non-authoritative answer:
Name:    webmail.isec.pt
Address:  193.137.78.90

> set q=ptr
> 193.137.78.90
Server:  vodafonegw
Address:  192.168.1.1

Non-authoritative answer:
90.78.137.193.in-addr.arpa      name = webmail.isec.pt
90.78.137.193.in-addr.arpa      name = smtp.isec.pt

78.137.193.in-addr.arpa nameserver = ns.isec.pt
78.137.193.in-addr.arpa nameserver = ns2.isec.pt
ns.isec.pt      internet address = 193.137.78.1
ns2.isec.pt     internet address = 193.137.78.3
```

# *Load Balancing*

- Load balancing in this perspective consists of distributing the clients of a resource (ftp server, www, mail, ...) among the various suppliers of the resource.
- Therefore, it is assumed that the same resource will be replicated by several systems on the network.
- A common technique (RFC 1794), based on the DNS, to perform load balancing is to order in a different way (e.g. by round-robin) the registrations of the same domain, class and type in each response to a resolution request.
- In order to make this technique effective to such registers, reduced TTL values are generally associated.

# *Load Balancing*

- You can load balance your servers using DNS for this. You just have to have multiple A records for a name.
- For example, if there are three WWW servers with the addresses 10.0.0.1, 10.0.0.2 and 10.0.0.3, a set of records such as the following ones implies that clients will connect a third of the time to each machine:



| Name | TTL | CLASS | TYPE | Resource Record (RR) Data |
|---|---|---|---|---|
| www | 600 | IN | A | 10.0.0.1 |
|  | 600 | IN | A | 10.0.0.2 |
|  | 600 | IN | A | 10.0.0.3 |

- When one decides to ask for these records, the DNS will run them and answer the question with the records in a different order. In the example above, customers will randomly receive records in order 1, 2, 3; 2, 3, 1; and 3, 1, 2. Many customers will use the first registration and ignore the rest.

# Security

- The DNS has always been, and intends to remain, a repository of public information and therefore no mechanism is provided to support the confidentiality of the information it handles and exchanges.
- However, with the evolution and widespread use, it started to be vulnerable to attacks. So it was thought of a way to introduce some security.
- The first steps were taken with Secure DNS:
  - RFC 2065 - January 1997 “Domain Name System Security Extensions”
- Later, following the dynamic update proposal of the DNS (RFC 2136), and based on DNSSEC, the
  - RFC 2137 - April 1997 “Secure Domain Name System Dynamic Update”
- In 1999, DNS security extensions were redefined more comprehensively in four documents:
  - RFC 2535 - March 1999 “Domain Name System Security Extensions”
  - RFC 2536 - March 1999 “DSA KEYs and SIGs in the DNS”
  - RFC 2538 - March 1999 “Storing Certificates in the DNS”
  - RFC 2541 - March 1999 “DNS Operational Security Considerations”

# Security

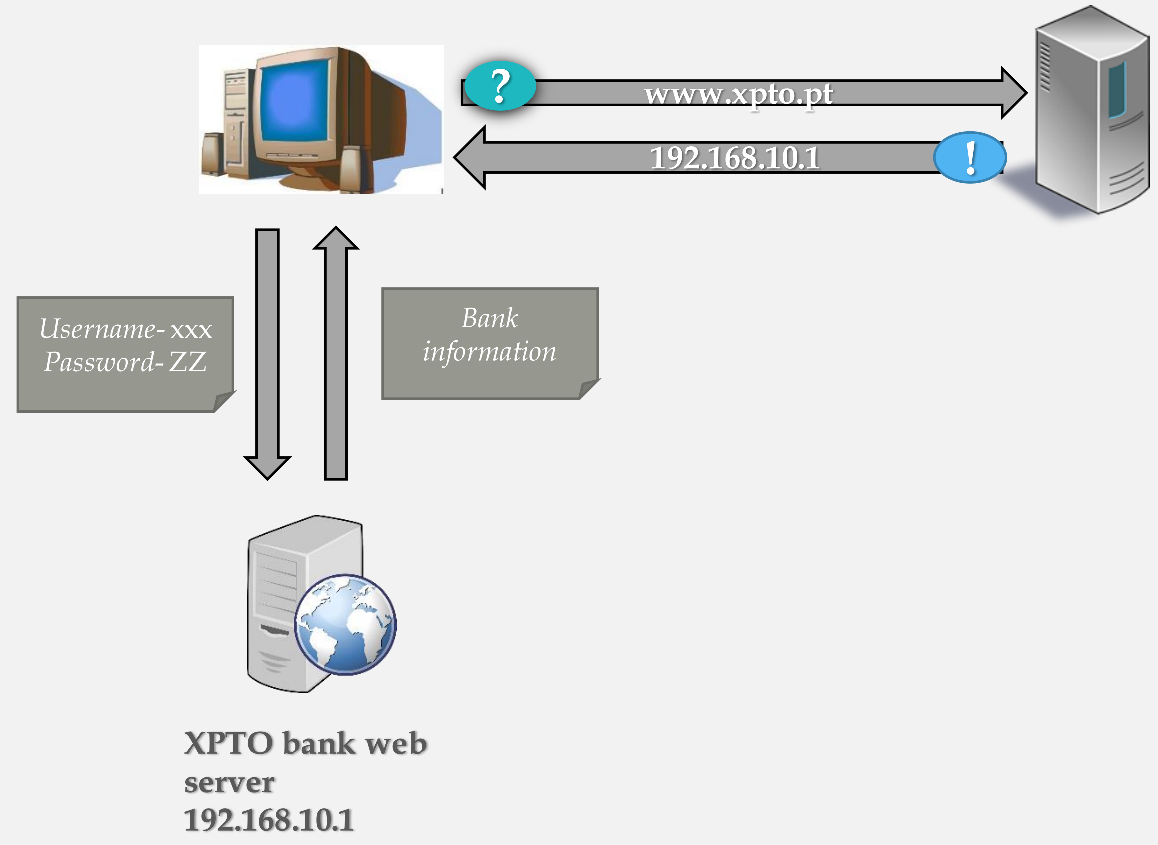
- DNSSEC (Domain Name System Security Extensions) is the name given to security extensions to the DNS protocol designed to protect and authenticate your traffic.
- The security mechanisms provided for in DNSSEC are complementary and transparent to the user, thus not interfering with the normal functioning of the DNS protocol.
- The extensions aim to improve the reliability of users in the services provided, namely:
  - Suppress weaknesses;
  - Prevent attacks;
  - Reduce the risk of manipulation;
  - Provide a secure service;
  - Strengthen security.
- In order to fully benefit from this service, it is necessary to have an implementation on the ISPs side so that this service reaches the final customer.

# Security

- Security extensions are essentially based on public key cryptography technologies and digital signatures based on public keys.
- The security extensions proposed in RFC 2535 consider three services:
  - Key Distribution.
  - Data Source Authentication and Integrity.
  - Authentication of DNS Orders and Transactions.

# Security–*man-in-the middle*

## Normal Situation



?

www.xpto.pt

192.168.10.1

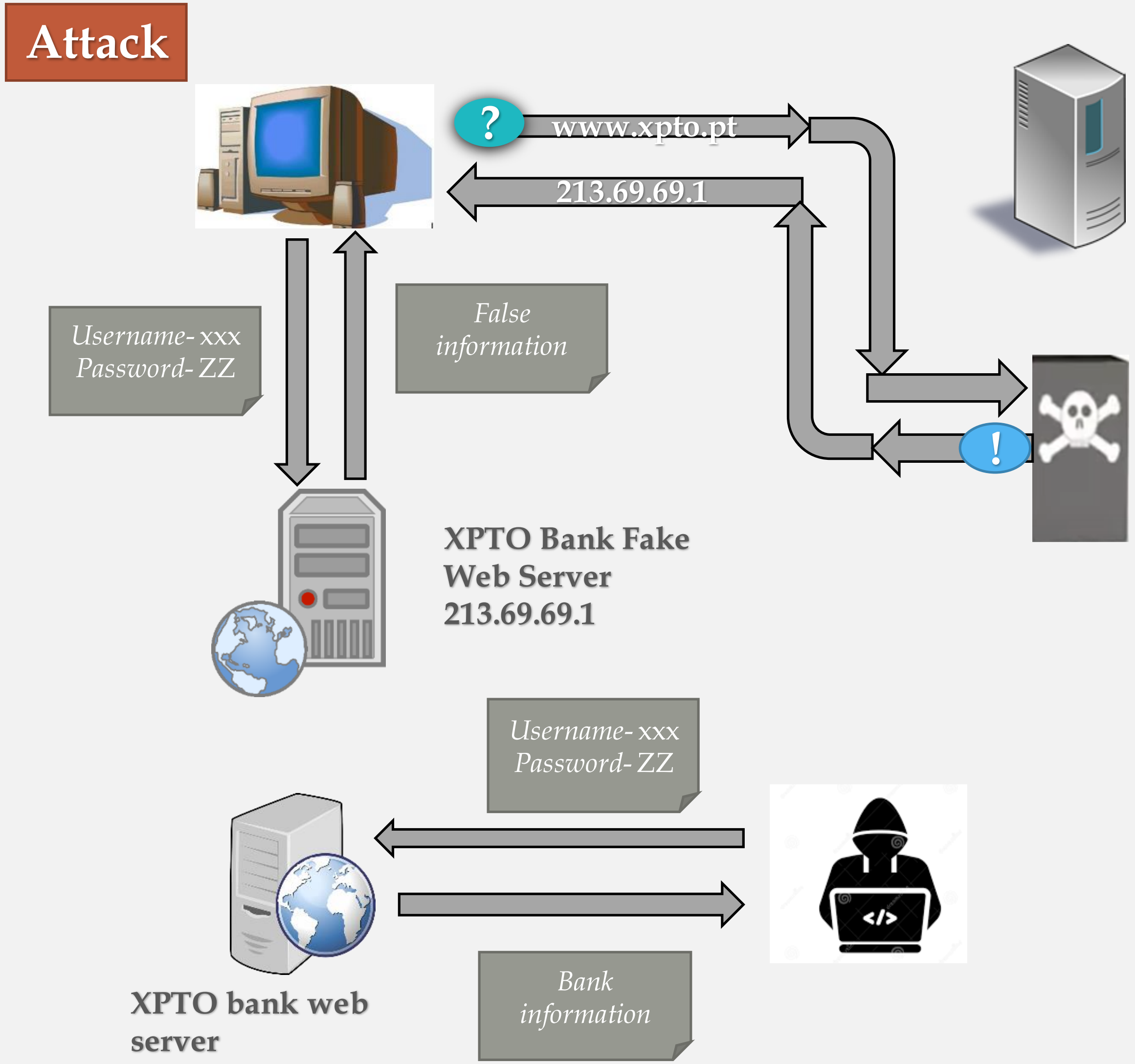
!

*Username- xxx*
*Password- ZZ*

*Bank information*

**XPTO bank web server 192.168.10.1**

## Attack



?

www.xpto.pt

213.69.69.1

!

*Username- xxx*
*Password- ZZ*

*False information*

**XPTO Bank Fake Web Server 213.69.69.1**

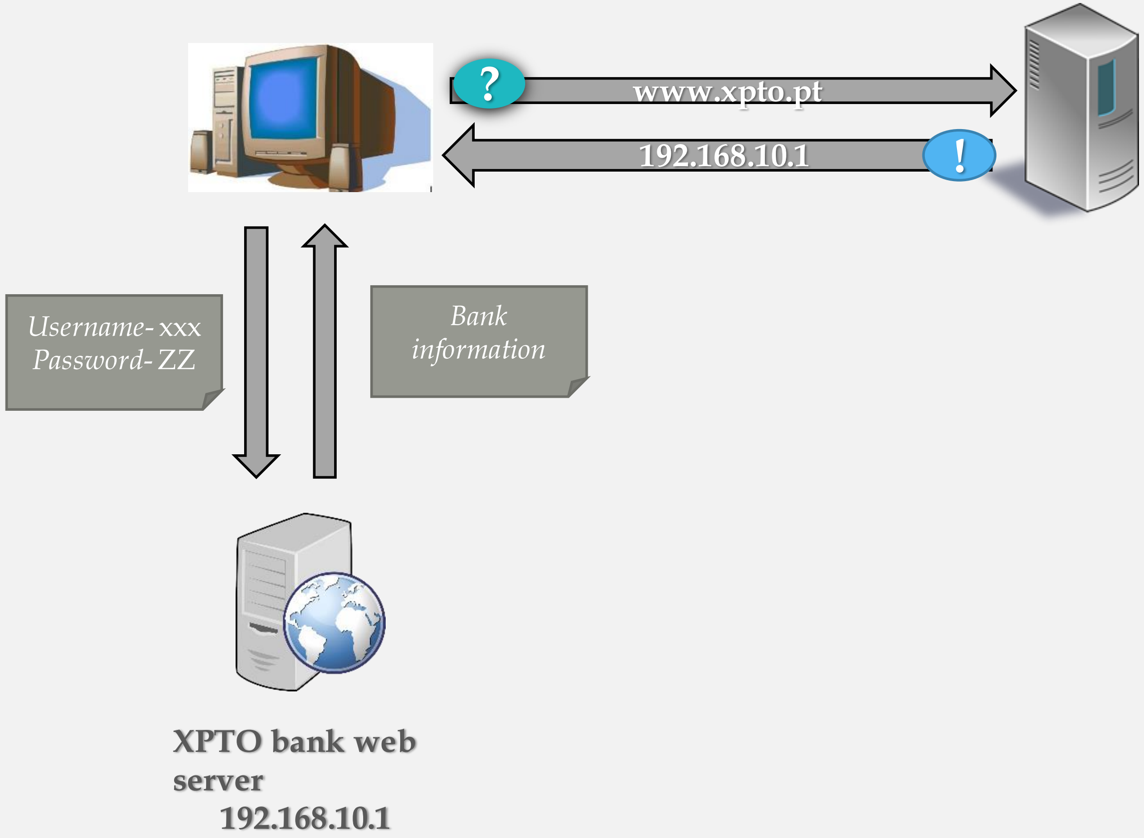
*Username- xxx*
*Password- ZZ*

*Bank information*

**XPTO bank web server**

# Security –*cache poisoning*

## Normal Situation



?

www.xpto.pt

192.168.10.1

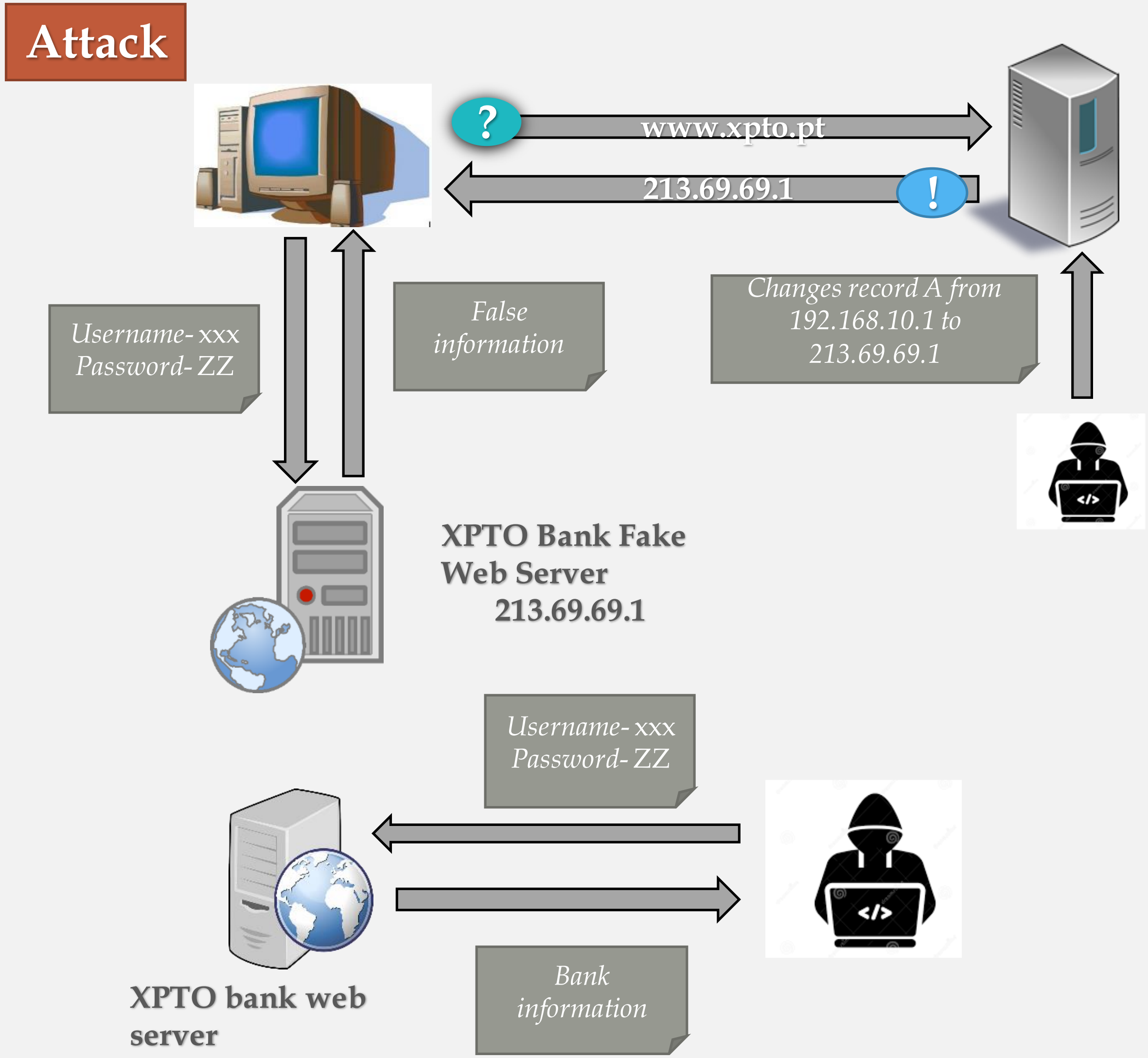
!

*Username- xxx*
*Password- ZZ*

*Bank information*

**XPTO bank web server**
**192.168.10.1**

## Attack



?

www.xpto.pt

213.69.69.1

!

*Username- xxx*
*Password- ZZ*

*False information*

*Changes record A from 192.168.10.1 to 213.69.69.1*

**XPTO Bank Fake Web Server**
**213.69.69.1**

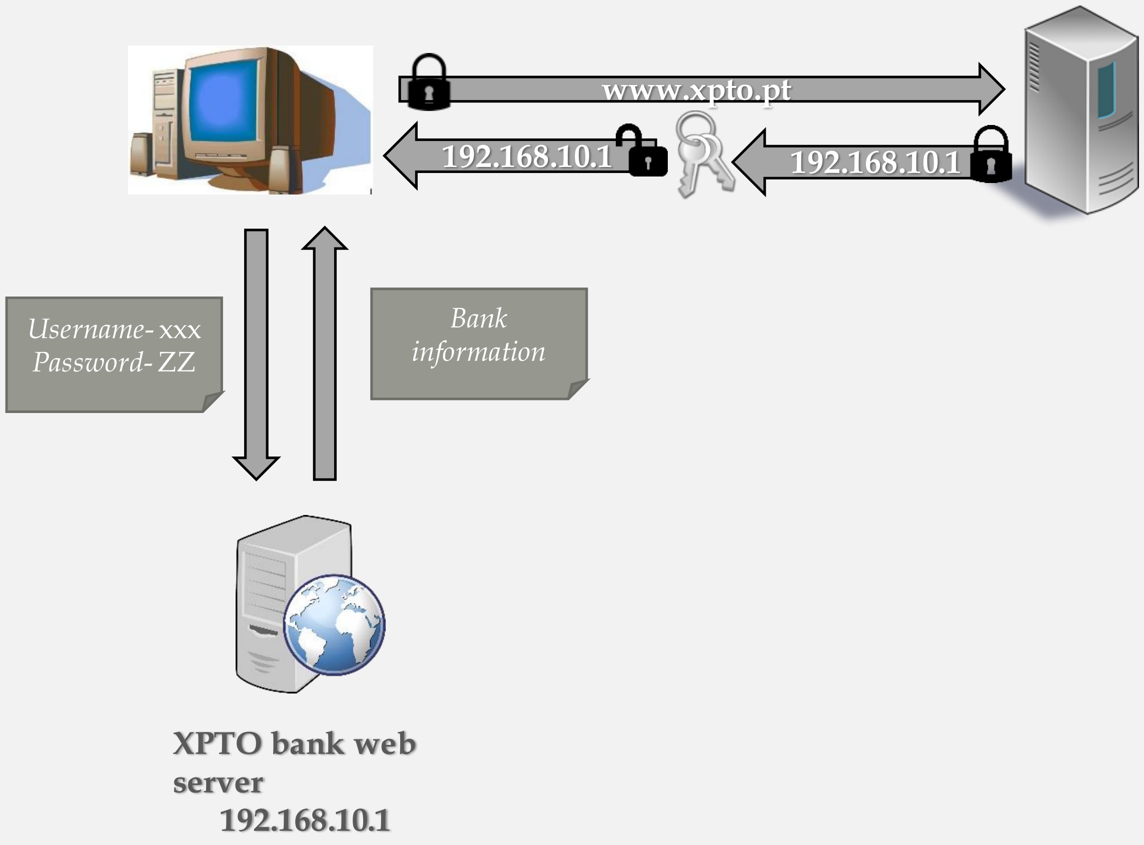
*Username- xxx*
*Password- ZZ*

*Bank information*

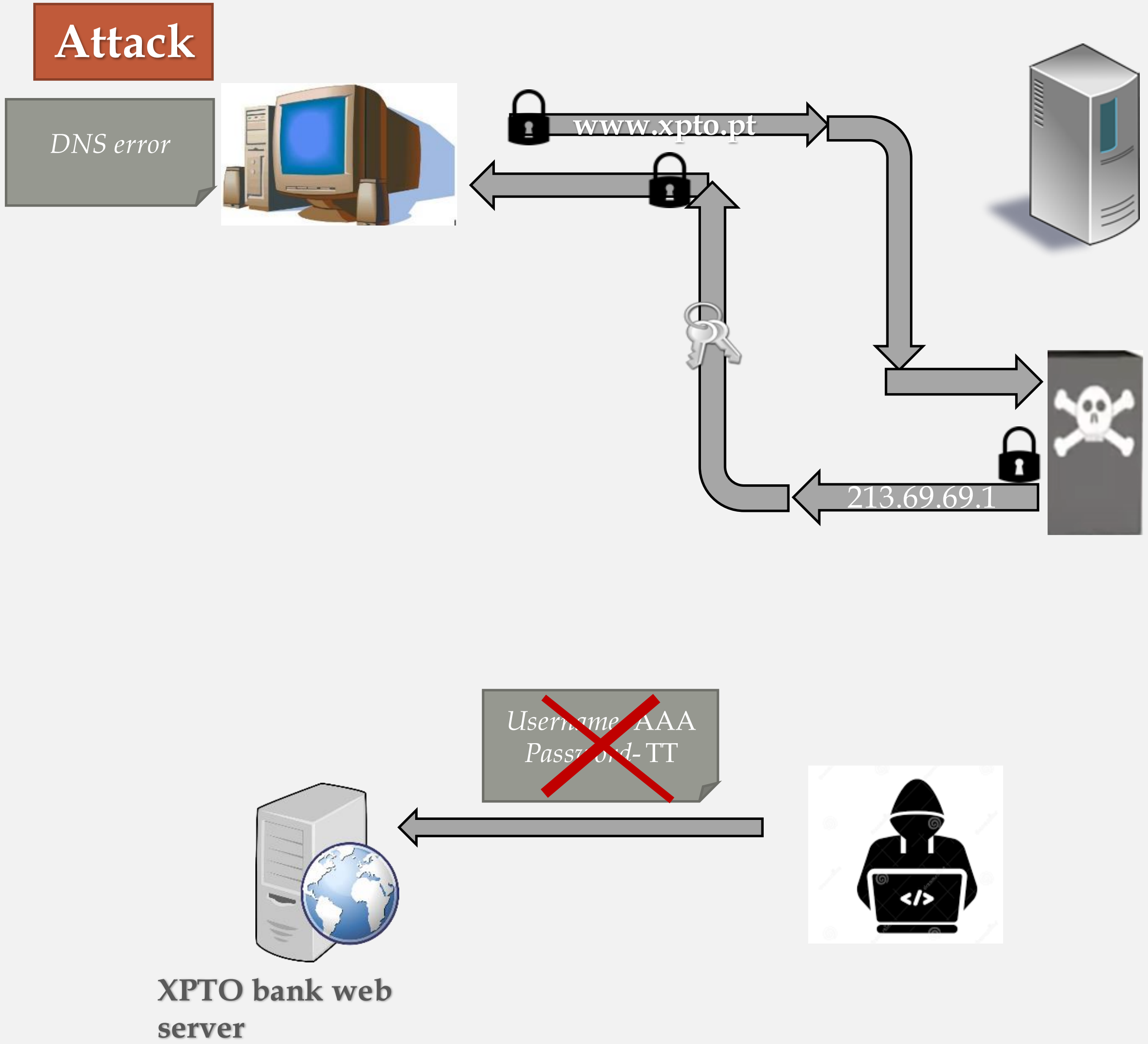
**XPTO bank web server**

# Security – DNSSEC

## Normal Situation



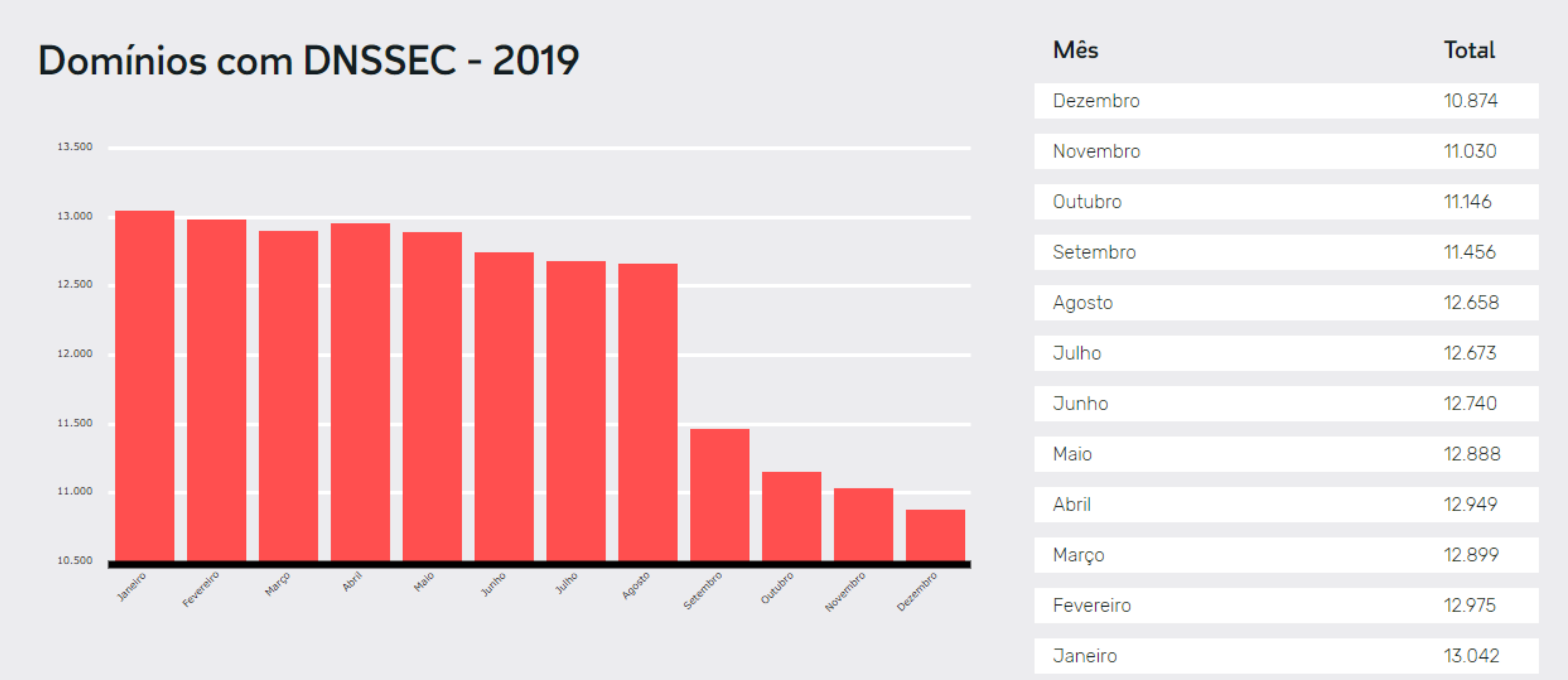
## Attack



# Security

- What guarantees?
  - Origin (Authenticity).
  - Integrity.
- What does not guarantee?
  - Confidentiality.
  - Protection against denial of service attacks.

# Security



## Domínios com DNSSEC - 2019

| Mês | Total |
|---|---|
| Dezembro | 10.874 |
| Novembro | 11.030 |
| Outubro | 11.146 |
| Setembro | 11.456 |
| Agosto | 12.658 |
| Julho | 12.673 |
| Junho | 12.740 |
| Maio | 12.888 |
| Abril | 12.949 |
| Março | 12.899 |
| Fevereiro | 12.975 |
| Janeiro | 13.042 |

https://www.dns.pt/pt/estatisticas/?graph=0&type=9&year=2019&subm=Filtrar

# Security

- DNSSEC introduces additional records that are divided into four different types:
  - DNSKEY - Public key;
  - RRSIG - RRset's Digital Signature;
  - NSEC / NSEC3 - Authenticated response to the non-existence of a domain or set of Resource Records associated with a domain;
  - DS - Synthesis of the public key that makes the connection between a domain and subdomain in order to build a chain of trust;

# *Public* DNS

- When Google released its public DNS service at the end of 2009, it promised to be the fastest, simplest and most robust to use.
- The idea of the company made the Internet even faster, using distributed DNS servers, but that all responded by the same IP addresses.
- This project has grown and is now a mature service. It is also the most used DNS service on the Internet, processing more than 70 billion requests per day.

Google™
DNS
8.8.8.8
8.8.4.4

# Public DNS

- What advantages:
  - Performance
  - Safety
  - Hit rate
- You can see more details of this service at
  - https://developers.google.com/speed/public-dns/docs/intro

# *Public* DNS

**GTEI DNS** (agora Verizon)
4.2.2.1

4.2.2.2

4.2.2.3

4.2.2.4

4.2.2.5

4.2.2.6

**Opennicproject**
151.236.6.156
118.88.20.195

**SafeDNS**
195.46.39.39
195.46.39.40

**OpenDNS**
208.67.222.222
208.67.220.220

**DynDNS**
216.146.35.35
216.146.36.36

**Comodo Secure DNS**
8.26.56.26
8.20.247.20

**Dnsadvantage**
156.154.70.1
156.154.71.1

# Dynamic Updates

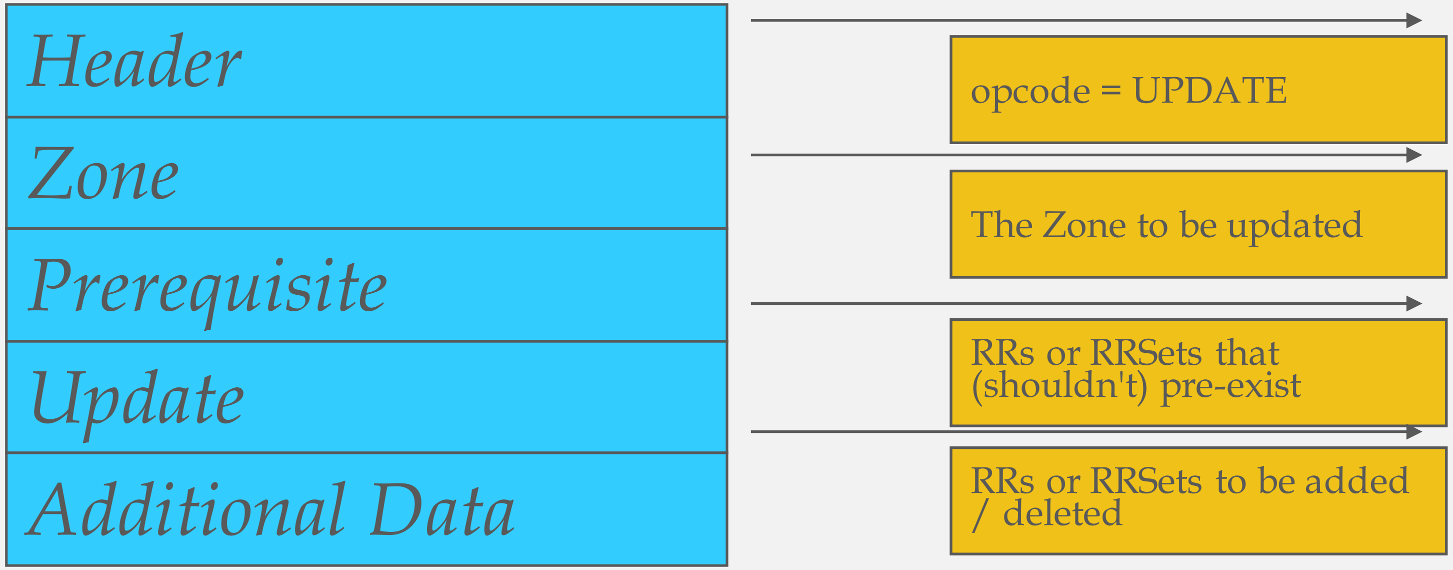
- DNS is a directory service that assumes that information in the Zones changes very rarely.
- It is therefore acceptable that the mechanism for updating Zone files is outside the protocol itself (usually by manually editing the files themselves).
- However, in environments with dynamic addresses (for example: DHCP) it becomes useful to have a name resolution system that is also updated dynamically.
- These updates may be required by clients or by DHCP servers.
- The DNS services present in the latest operating systems allow dynamic updates.

# Dynamic Updates

- RFC 2136 defines a new operation (opcode = UPDATE) that will allow:
  - add or delete RRs or RRSets to a specific zone
  - specify prerequisites to check to carry out such update operations:
  - the previous existence (or not) of an RRSet
  - the previous existence (or not) of a specific RR
- The UPDATE operation is only verified if all prerequisites are verified and never in parallel with another UPDATE operation.

# Dynamic Updates

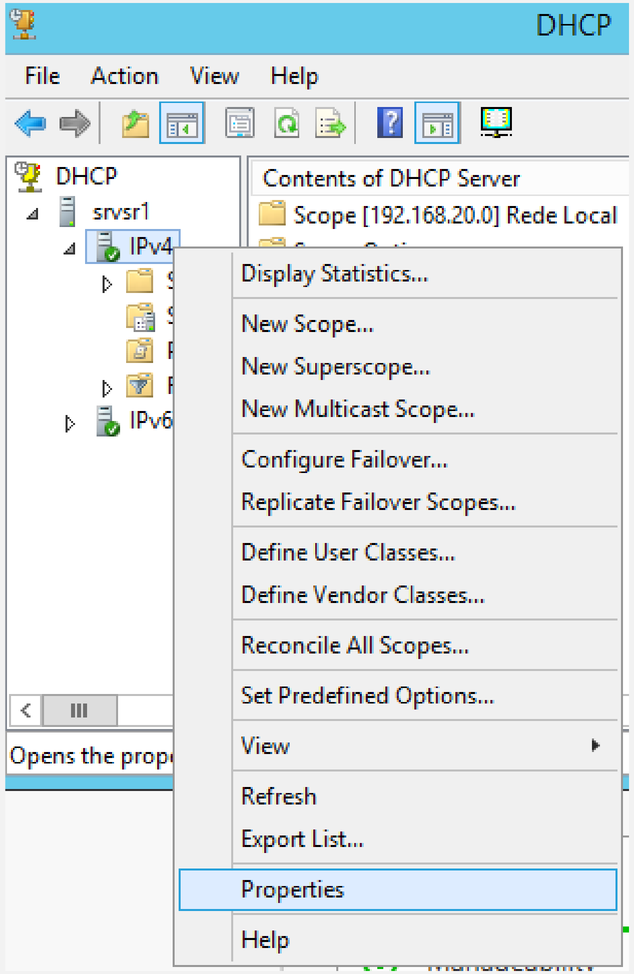
- UPDATE package format

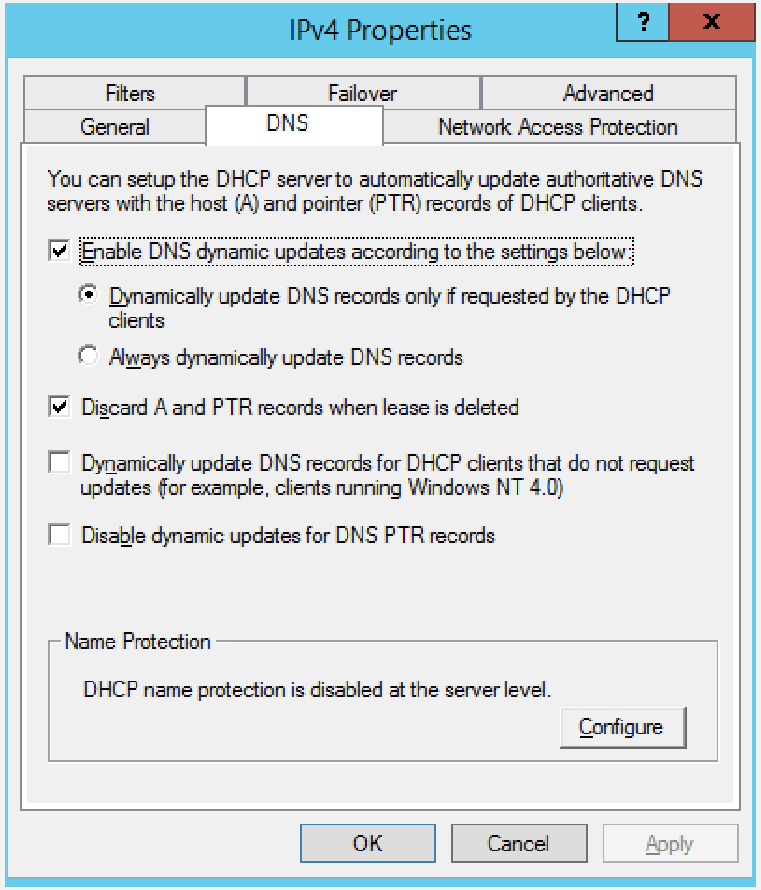


# Dynamic Updates

- O requisitante de uma operação de UPDATE (e.g. servidor DHCP) deve tentar dirigir o pedido directamente para o servidor primário da zona.
- Se por algum motivo tal for impossível deve contactar um dos restantes servidores autoritários da zona.
- Um servidor autoritário não primário ao receber um pedido de atualização deve reencaminhá-lo para o servidor primário assumindo o papel de requisitante da operação. Assim que receba a resposta deve retorná-la para o requisitante original.

# Dynamic Updates - DHCP - DNS





You can setup the DHCP server to automatically update authoritative DNS servers with the host (A) and pointer (PTR) records of DHCP clients.

☑ Enable DNS dynamic updates according to the settings below:

● Dynamically update DNS records only if requested by the DHCP clients

○ Always dynamically update DNS records

☑ Discard A and PTR records when lease is deleted

□ Dynamically update DNS records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0)

□ Disable dynamic updates for DNS PTR records

Name Protection

DHCP name protection is disabled at the server level.

# Questions

# Referências

- http://www.arctel-cplp.org/app/uploads/publicacoes/20680184405a47d5d66beb7.pdf - acedido em abril de 2020
- https://www.iana.org/reports/2013/pt-report-20130808.html - acedido em abril de 2020
- https://www.profissionaisti.com.br/2018/04/cloudflare-dns-1-1-1-1-velocidade-e-privacidade-parte-16-o-que-e-dns/ - - acedido em abril de 2020
- https://www.hostnet.com.br/info/dns/ - acedido em abril de 2020.
- http://paginas.fe.up.pt/~mgi97018/dns.html - acedido em abril de 2020
- http://www.dns.pt
- http://docente.ifrn.edu.br/diegopereira/disciplinas/2012/redes-de-computadores-e-aplicacoes/aula-47-protocolo-dns/view - acedido em abril de 2020
- "DNS" – Luís Santos - ISEC
- Material de suporte às aulas de Redes de Computadores de J. Legatheaux Martins DI - FCT/ UNL