

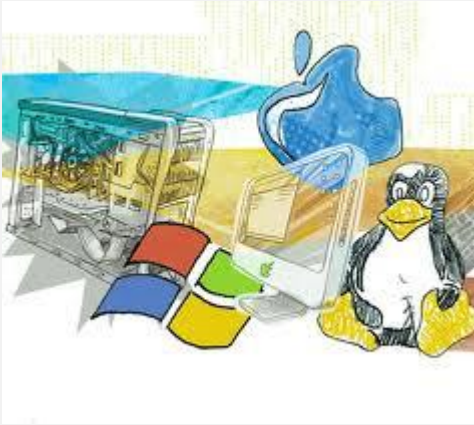
# Serviços de Rede 1

2019-2020

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática





# Serviços de Rede 1

*DNS – Domain Name System*

© - Pedro Geirinhas

# Introdução

---

Já estudamos que o endereçamento/identificação dos computadores numa rede é feito com endereços IP e físicos MAC que eles têm de ser únicos. Então, porque quando navegamos na Internet utilizamos nomes e não estes identificadores?

# Introdução

- O ser humano memoriza mais facilmente nomes do que números. Habitualmente, mais facilmente decoramos o nome de um conhecido que o seu número de telefone.
- Uma solução passa assim, por associar aos IPs nomes facilmente memorizáveis:
  - 193.137.78.20 => webmail.isec.pt
  - 213.13.146.140 => www.sapo.pt
- Esta solução implica a existência de um sistema que efetue a tradução/mapeamento entre os nomes e os respetivos endereços IP:
  - Sistema para resolução de nomes (Domain Name System – DNS)
  - Sistemas que permitam fazer o contrário traduzir IPs em nomes (reverse DNS)



# Introdução

- O DNS permite:
  - A possibilidade ao ser humano de se abstrair de endereços de rede (endereços IP) cuja memorização é complexa.
  - Permite que as alterações aos endereços se possam fazer sem que o utilizador tenha que conhecer essa alteração para continuar a usar um serviço. Ou seja pode mudar o IP de um determinado serviço e isso ser completamente transparente para o utilizador.
  - A garantia que as máquinas e os seus nomes são geridos de forma hierárquica e distribuída permitindo assim uma maior disponibilidade da informação.

11001001.10010001.01001010.01001010

#جس@ش %\$#@%&



# História

- Início dos anos 70
  - Usavam-se apenas IPs para identificar os sistemas da rede ARPANET.
  - À medida que o número de sistemas ligado à rede crescia tornava-se impraticável aceder às máquinas pelos seus endereços IP já que estes começavam a ser em grande número.
  - Em busca de um processo de memorização simplificada surgiu a ideia de “batizar” as máquina com nomes.
  - Em cada sistema estava presente uma “base de dados” (hosts.txt) global com os mapeamentos usados.

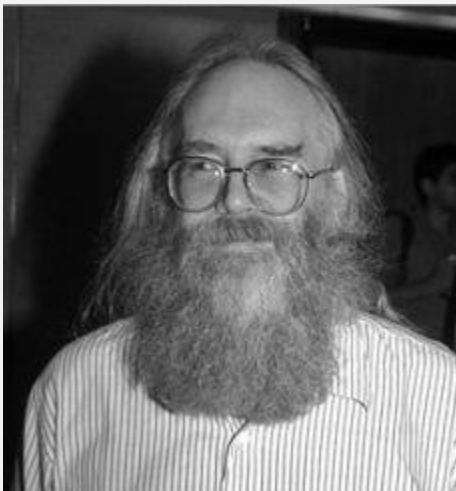
# História

- Esta foi a primeira solução e encontra-se ainda ativa nos sistemas atuais.
  - Ainda existe atualmente nas máquinas 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 máquina).
- A “evolução” foi ter um ficheiro que era atualizado centralmente e distribuído depois por todas as máquinas ligadas na rede.



# História

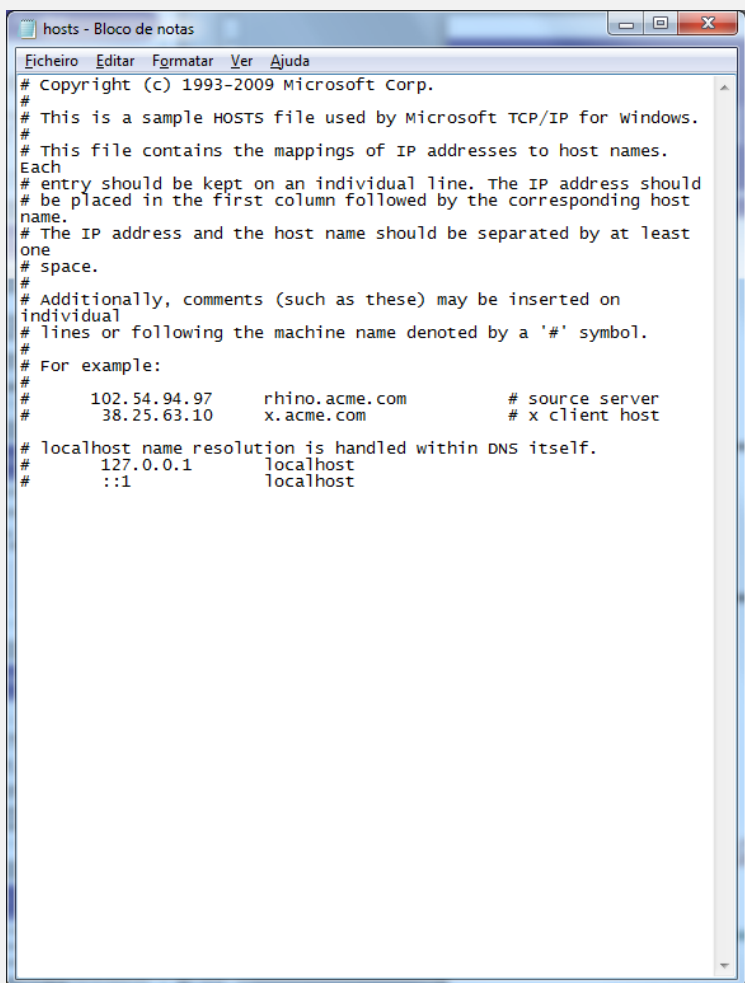
- O ficheiro hosts.txt era mantido centralmente (inicialmente na University of California, Los Angeles, UCLA) e distribuído por FTP para todos os sistemas que pretendiam ter presente a resolução de nomes.
- A gestão central desse ficheiro ficou inicialmente a cargo de Jon(athan) B. Postel, na altura um estudante graduado da UCLA ao abrigo de um acordo mantido com Department of Defense (DoD). Postel é considerado um dos pioneiros da Internet e um dos seus maiores pensadores.



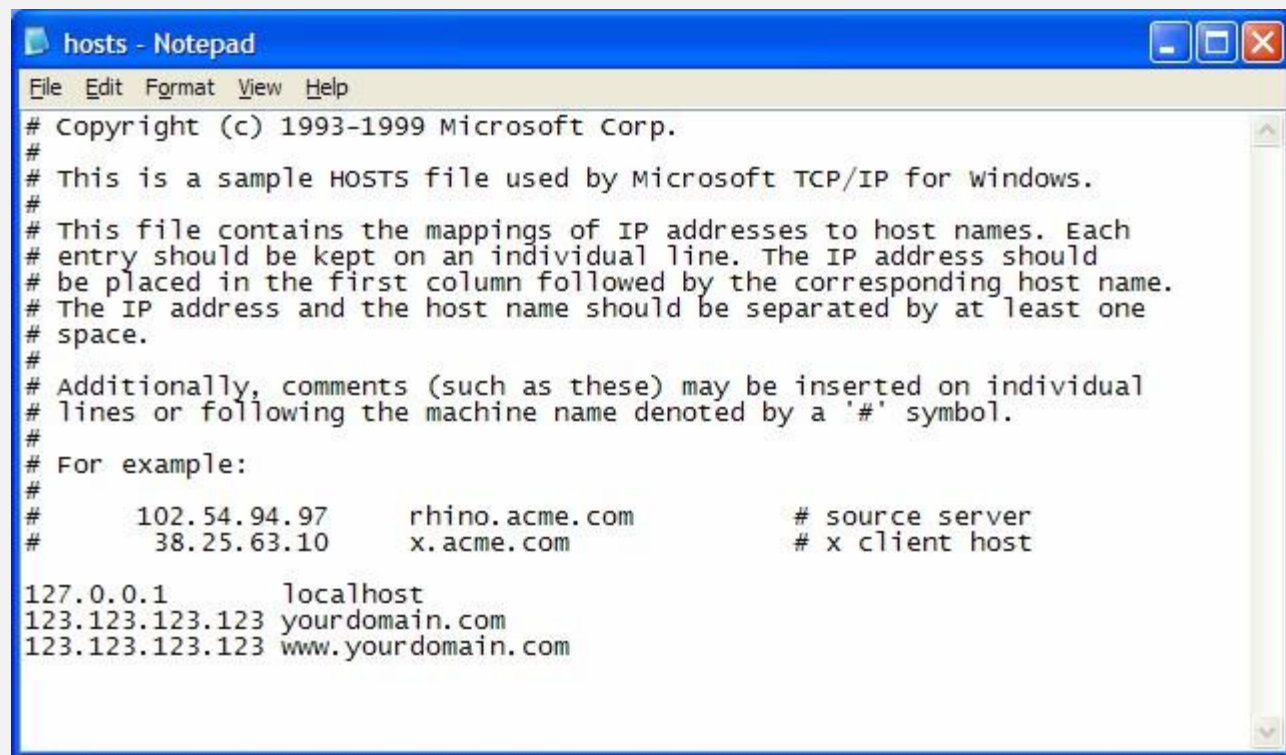
[https://www.internethalloffame.org//inductees/jon-postel?gclid=Cj0KCQjwm9D0BRCMARIsAIfvflaVlkisWaj7DBVVbGfvWHjOgoUFqe18bm\\_L7YBGNF3YUN8RXqR05b4aAp5WEALw\\_wcB](https://www.internethalloffame.org//inductees/jon-postel?gclid=Cj0KCQjwm9D0BRCMARIsAIfvflaVlkisWaj7DBVVbGfvWHjOgoUFqe18bm_L7YBGNF3YUN8RXqR05b4aAp5WEALw_wcB)



# 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
```

Nota: Existe sempre o endereço 127.0.0.1 que identifica o localhost...

# História

- Então porque não colocar no ficheiro todos os IPs existentes na Internet?
  - Passaríamos uma boa parte da nossa vida a escrever IPs e nunca teríamos a tabela atualizada!
  - Qualquer alteração num nome ou IP, ou qualquer adição ou remoção da tabela, exigiria que todos os utilizadores fizessem um novo download do ficheiro;
  - E quem se responsabilizava por esta atualização e gestão dos nomes e IPs?

# História

- Em paralelo, Jon Postel iniciou a organização do arquivo de documentos técnicos escritos pelos investigadores da ARPANET, denominados **Request For Comments** (RFC) mantendo-se até falecer como seu editor.
- Em 1971 (27 de Setembro) J. Postel publica o RFC 229 propondo uma lista de nomes (host mnemonics) e alcunhas normalizadas de 8 caracteres identificando assim todos sistemas da ARPANet de forma diferenciada.
- Durante 1972, J. Postel publica dois RFC (em maio o RFC 229 e em Dezembro o RFC 433) onde é proposta uma lista dos números normalizados das portas a serem utilizados por cada um dos serviços de rede.

# História

- Devido à expansão na interligação de sistemas através de redes de dados, surgiu a necessidade de organizar os nomes atribuídos às máquinas.
- Um nome simples (“alpha”, “omega”, ...) não respondia às necessidades e originava, por vezes, conflitos entre sistemas porque existiam máquinas diferentes com o mesmo nome.
- Em 1982 surgiu o formato host.domain para os nomes dos sistemas informáticos:

Antes	Depois
alpha	apha.xxx.yyy
omega	omega.aaa.bbb

- Em agosto de 1982 é publicado o RFC 819 Z. Su, J. Postel, "*Domain naming convention for Internet user applications*" onde é definido a estrutura nome da maquina. Domínio.

# História

- Contudo, existia ainda a dificuldade introduzida pela variedade/multiplicidade de ficheiros de resolução de nomes.
- Cada sistema tinha de ter o seu ficheiro e isso era um problema já que:
  - As tarefas de atualização/gestão do ficheiro não eram efetuadas de igual forma em todos os sistemas.
  - Existia a necessidade de liberalizar a atribuição de nomes aos sistemas de uma organização sem que isso implica-se aumento da complexidade da manutenção nos sistemas de outra organização.
  - Existia uma maior probabilidade de erros.

# História

- Em 1983 surgiram as primeiras experiências e implementações de um sistema distribuído para efetuar a resolução de nomes o **Domain Name System** (DNS).
- Arquitetura foi desenvolvida por Paul Mockapetris.
- Em Novembro são publicados vários RFC fundamentais para o DNS:
  - RFC 881 J. Postel, "*Domain names plan and schedule*" onde apresentado o calendário de introdução do DNS.
  - RFC 882 P. Mockapetris, "*Domain names – concepts and facilities*" onde são especificados os conceitos chave do DNS.
  - RFC 883 P. Mockapetris, "*Domain names – implementation and specification*" onde é detalhada a implementação do DNS.



# História

- Em 1984 é posto em funcionamento o DNS, substituindo o ficheiro hosts.txt por servidores DNS.
- Em março de 1985 é registado o primeiro domínio DNS (Symbolics.com)
- Em 1986 é atribuída à *National Science Foundation* (NSF) o desenvolvimento da NSFNET que constitui hoje o principal *backbone* da Internet.
- O crescimento exponencial da Internet iniciou-se...
- Em novembro 1987 Paul Mockapetris publica dois RFC que se tratam de uma revisão da especificação inicial e na qual assenta ainda hoje o DNS:
  - RFC 1034 P.V. Mockapetris, "*Domain names - concepts and facilities*"
  - RFC 1035 P.V. Mockapetris, "*Domain names - implementation and specification*"



# História

- Os RFCs mais importantes para o DNS são:
  - RFCs 882 e 883 – Funcionamento básico
  - RFCs 1034, 1035 – Modelo Vigente
  - RFCs 1535, 1536, 1537 – Segurança, Implementação, Administração.

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 (EDNSo)
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)

# História

---

- Uma das grandes vantagens deste novo sistema é que nenhuma entidade é a única responsável por toda a atualização do sistema.
- Baseia-se no conceito de base de dados distribuída, existindo em muitos servidores de nomes diferentes em todo o mundo, mas nenhum desses servidores possui toda a informação. Isto permite assim um crescimento praticamente ilimitado do DNS.
- Nos sistema da Microsoft o DNS passou a ser o serviço de resolução de nomes padrão a partir do Windows 2000 Server substituindo o WINS.

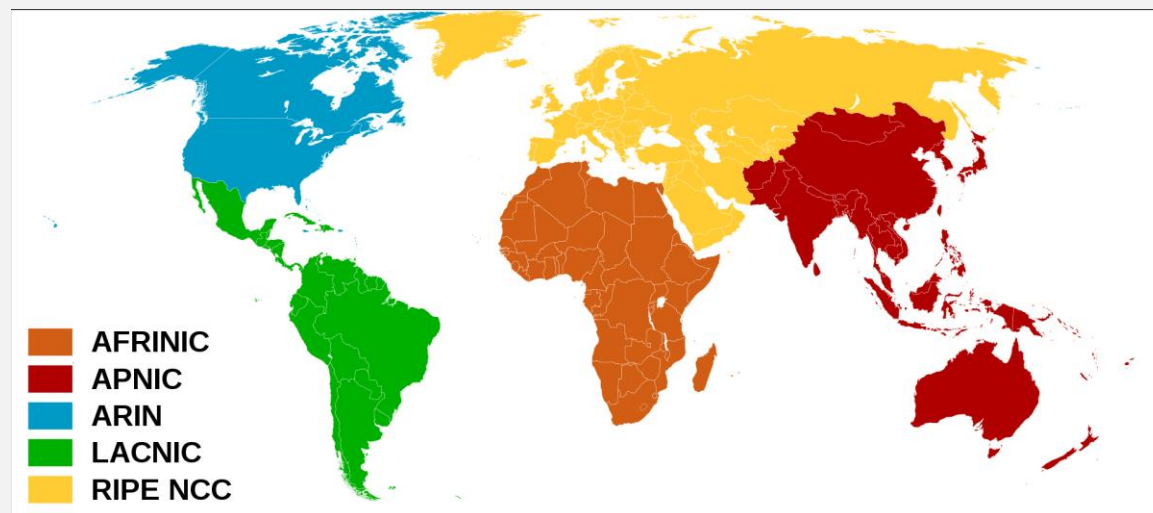
# Organizações

- O serviço de DNS está diretamente dependente da atribuição de IPs e nomes de domínios às organizações.
- Esta função é da competência da IANA (Internet Assigned Numbers Authority) ou a quem ela delegar essa função.
- Em Portugal a competência foi delegada em 30 de Junho de 1988 à Fundação para a Computação Científica Nacional (FCCN), cabendo a esta a responsabilidade de gerir o domínio '.pt'.
- A Associação DNS.PT, foi formalmente criada no dia 9 de maio de 2013 e sucedeu à, FCCN nos direitos e obrigações na responsabilidade pela gestão, registo e manutenção de domínios sob o TLD (Top Level Domain) '.pt'.
- Tem como associados a Fundação para a Ciência e a Tecnologia, FCT - IP, Associação da Economia Digital (ACEPI) e a Associação Portuguesa para a Defesa do Consumidor (DECO).



# Organizações


- No topo da hierarquia está a IANA (Internet Assigned Numbers Authority), vinculada à ICANN (Internet Corporation for Assigned Names and Numbers), que coordena as atividades globalmente.
- A IANA delega parte dessas atividades para autoridades com abrangência menor, normalmente da área de continentes que são denominadas RIR (Regional Internet Registry).
- Atualmente existem 5 entidades regionais que são: ARIN, RIPE NCC, APNIC, LACNIC e AfriNIC



**Fonte:**

[https://pt.wikipedia.org/wiki/Registro\\_Regional\\_da\\_Internet#/media/Ficheiro:Regional\\_Internet\\_Registries\\_world\\_map.svg](https://pt.wikipedia.org/wiki/Registro_Regional_da_Internet#/media/Ficheiro:Regional_Internet_Registries_world_map.svg)

# Organizações



Internet Assigned Numbers Authority

Domain Names

Overview

**Root Zone Management**

Overview

**Root Database**

Hint and Zone Files

Change Requests

Instructions & Guides

Root Servers

.INT Registry

.ARPA Registry

IDN Practices Repository

Root Key Signing Key (DNSSEC)

Reserved Domains

## Delegation Record for .PT

(Country-code top-level domain)

### ccTLD Manager

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

### Administrative Contact

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

### Technical Contact

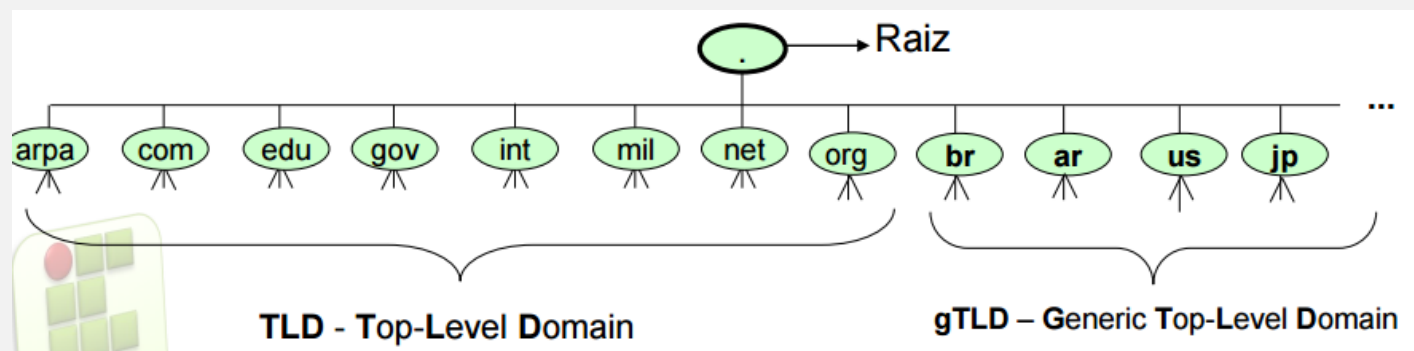
**Eduardo Manuel Laureano Duarte**  
Associação DNS.PT  
Rua Latino Coelho, nº13, 5º piso  
1050-132 Lisboa  
Portugal  
**Email:** eduardo.duarte@dns.pt  
**Voice:** (+351) 211308200

# Domínios

- Os nomes de domínios são construídos hierarquicamente, sendo o nível mais alto da hierarquia o último identificador.
- Como o DNS foi introduzido originalmente nos Estados Unidos, a parte final de um endereço destinava-se a indicar o tipo de organização onde estava localizado o computador. Dessa forma, alguns dos domínios de topo (.edu, .gov e .mil) ainda só são utilizados por organizações localizadas nos Estados Unidos.
- Os códigos de duas letras que indicam o país de origem estão definidos no **ISO 3166** com a exceção do uk utilizado pelo Reino Unido (United Kingdom) em vez de gb, embora existam alguns sites que o utilizem (<https://www.iso.org/obp/ui/#search>).

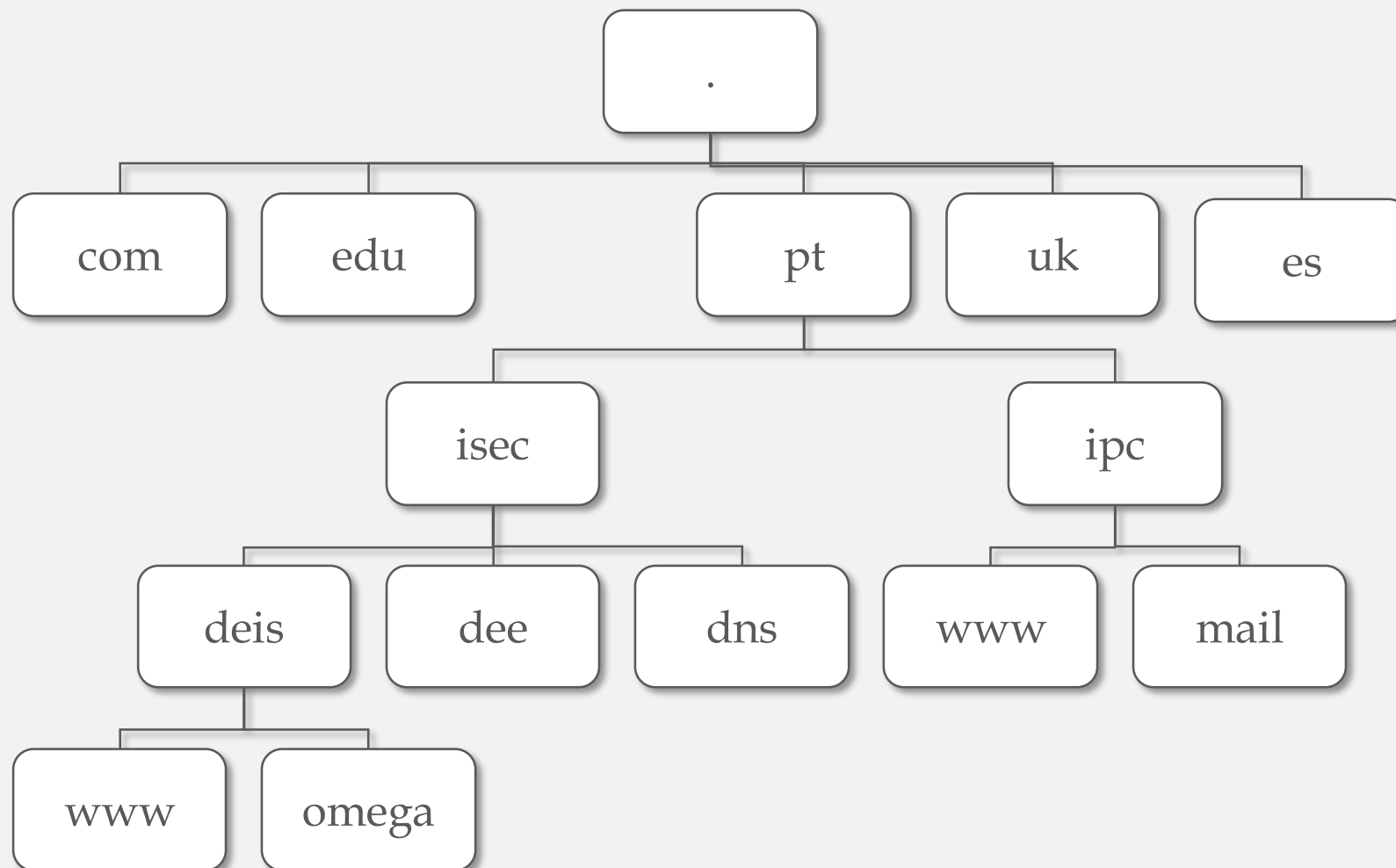
# Domínios

- Atualmente podem registrar-se nomes sob vários domínios de topo:
  - com, aero, biz, cat, coop, edu, gov, info, int, jobs, mil, mobi, museum, name, net, org, pro, travel, tv ...
  - Domínios para os países ou regiões: pt, eu, es, fr, uk, ...
  - Veja a lista em <https://www.iana.org/domains/root/db>
- O nome de cada nó/identificador (exceto o do nó *root*) tem de ter, no máximo, **63 caracteres**, e é indiferente a utilização de maiúsculas ou minúsculas. Os identificadores têm de começar por uma letra e podem consistir apenas de letras, algarismos e traços (-).
- No conjunto, um nome de domínio completo **não pode exceder os 255 caracteres**.



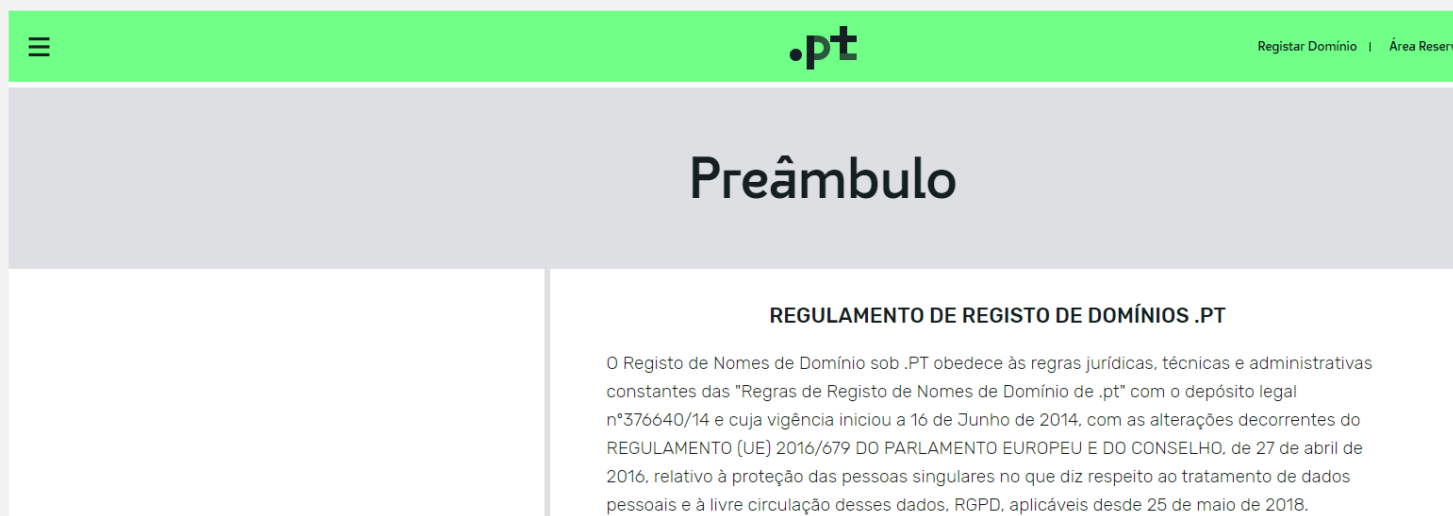


# Domínios



# Domínios

- Em Portugal, a FCCN disponibiliza também domínios de segundo nível para o domínios 'pt': com, edu, gov, int, net, nome, org, publ.
- As regras para o registo de um domínio em Portugal está definida em:
  - <https://www.dns.pt/pt/dominio/regras-de-dominios/preambulo/>



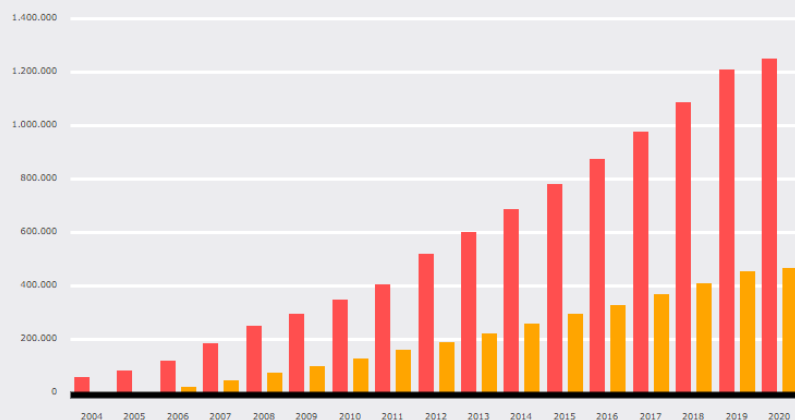
# Domínios

- As entidades que aceitam registo de nomes designam-se por Registrars.
- São entidades especializadas no registo e gestão de nomes de domínios.
- Em Portugal são credenciados pela FCCN através de protocolo que reconhece direitos e obrigações recíprocos, permitindo uma maior flexibilidade e agilidade na gestão de nomes de domínio por estas entidades.
- Para se candidatar a Agente de Registo (Registrar) credenciado da FCCN deverá garantir um conjunto de requisitos que pode consultar em:  
<https://www.dns.pt/pt/registrar/ser-registrar-pt/>
- Pode consultar a lista em (atualmente estão registadas 101 empresas) :  
<http://www.dns.pt/pt/registrars/>

# Números

- Evolução do registo e domínios ativos

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
------	---------	---------

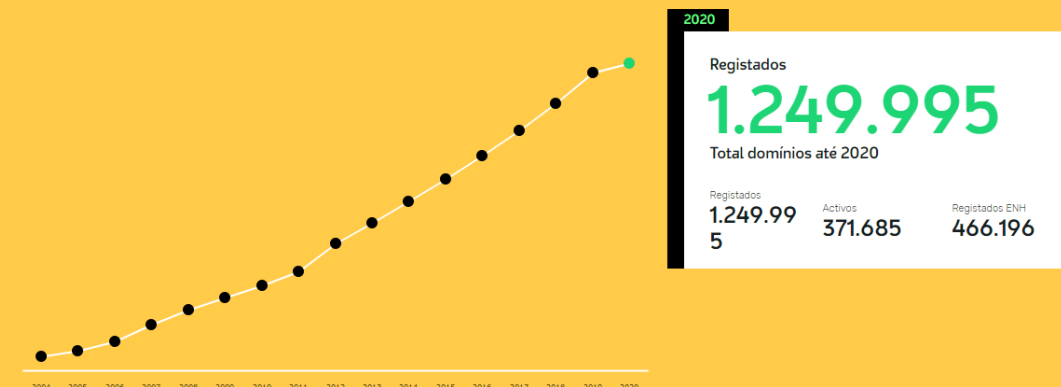
2011	403.574	159.430
------	---------	---------

2010	346.779	126.740
------	---------	---------

2009	295.796	99.210
------	---------	--------

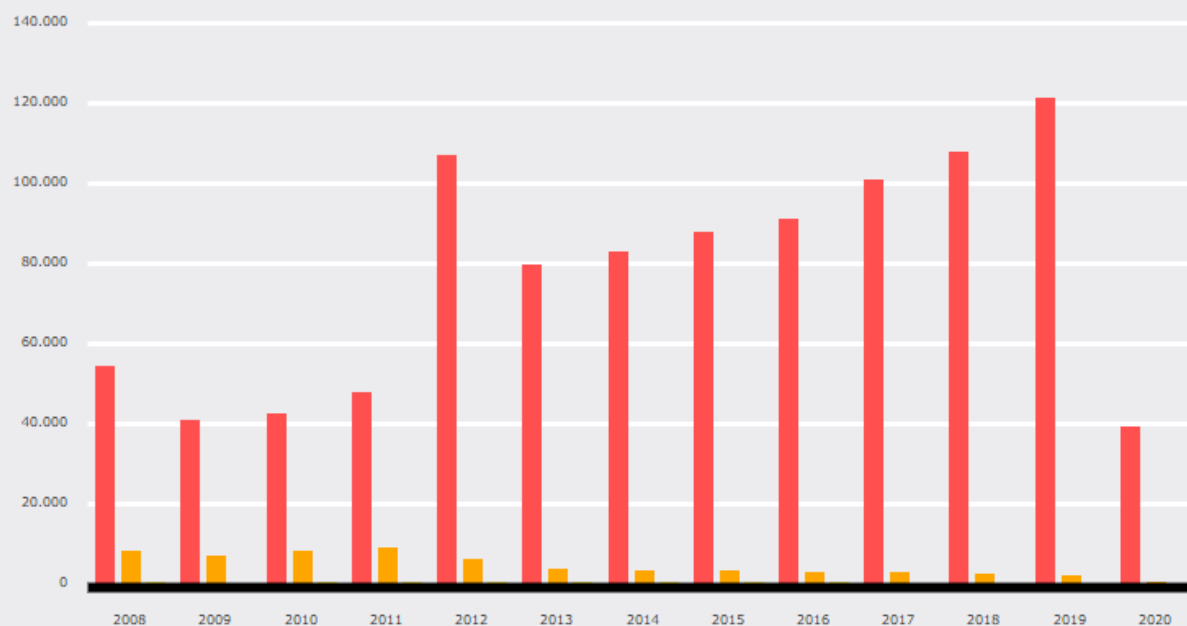
2008	247.898	72.703
------	---------	--------

Evolução do Registo de Domínios



# Números

## Domínios Registados por Ano



Fonte: <https://www.dns.pt>

# Números



Fonte: <https://www.dns.pt>

# Custos

- O registo de domínios é habitualmente pago.
- Os preços podem variar consoante o tipo de domínio
  - Entre 10 € e 60 € por ano (por vezes, existe uma taxa inicial de submissão)
  - Para Portugal são estes os custos:

		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 €

Fonte: <https://www.dns.pt/pt/dominio/precos/>

- Quem registar um nome pode disponibilizá-lo a outra entidade (leia-se... vendê-lo ;-))



# Domínios e Zonas

- **Domínio/Subdomínio**

- Subárvore do espaço de nomes definido pelo DNS.
- Exemplos:
  - isec.pt.
  - deis.isec.pt.
- O domínio deis.isec.pt. é um subdomínio de isec.pt.

- **Zona**

- Conteúdo de uma secção contígua do espaço de nomes normalmente delimitada por fronteiras administrativas que pode ser ou não coincidente com um domínio ou subdomínio.

# Zonas

- Os computadores e organizações que estejam pendurados no mesmo nó da árvore do DNS partilham uma parte do nome dos respetivos domínios.
- Por exemplo, todos os computadores e departamentos existentes no ISEC utilizam o domínio isec.pt. Pode-se então definir uma zona para essa subárvore do DNS que pode ser um domínio nacional de topo (TLND - Top Level National Domain) ou ao nível do departamento/organização.
- Dentro de uma zona o serviço DNS para zonas subsidiárias pode ser delegado conjuntamente com um domínio subsidiário.
- Desta forma, embora exista uma entidade responsável pela administração do domínio pt, que é a FCCN, a responsabilidade da administração do domínio isec.pt foi delegada ao ISEC.

# Nomes de Domínios

- **Nome absoluto (FQDN – Fully Qualified Domain Name)**
  - É estruturado da seguinte forma: "*host.3rd-level-domain.2nd-level-domain.top-leveldomain*"
  - O número de níveis não é fixo.
  - Caso nenhum domínio seja definido, o domínio default localdomain será usado.
  - Exemplo: `www.isec.pt`
- **Nome relativo**
  - Sequência não terminada por "."
  - Exemplo: `www`

# Servidores de ROOT

- São servidores autoritários com papéis especiais, sem eles a Internet não funciona.
- Existem 13 servidores (10 nos Estados Unidos, 2 na Europa e 1 na Ásia). O conteúdo de cada um é replicado 2 vezes por dia de forma automática.
- Existem replicas destes servidores espalhadas por todo o mundo.
- Possuem uma tabela que indica qual o servidor DNS responsável pela resolução de cada um dos *Top Level Domains*.

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



# Servidores *Top Level Domains*

- O domínio de primeiro nível, é um dos componentes dos endereços. Cada nome de domínio consiste de alguns nomes separados por pontos, e o último desses nomes é o domínio de topo.
- Existem de dois tipos:
  - **Generic Top level domains – relacionados com as funções das organizações**
    - **Generic** – usados para organizações genéricas (.com, .info, .net, .org)
    - **Generic restricted** – usados para determinadas funções (.biz, .name, .pro )
    - **Infrastructure** – utilizado apenas na infraestrutura do DNS (.arpa)
    - **Sponsored domains** – só podem ser utilizados por empresas ou entidades vinculadas a esses setores (.edu, .gov, .mil, . Travel etc)
  - **Country Code Top Level Domain – relacionados com a localização das organizações(.pt, .br, .fr, etc)**

# Servidores *Top Level Domains .pt*

## Name Servers

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

# Servidores Locais

- A entidade responsável pela zona deve possuir um único servidor primário e, preferencialmente, um ou mais servidores secundários.
- A grande diferença entre estes dois tipos de servidores é que um servidor primário carrega toda a informação da zona em causa a partir de ficheiros (base de dados) existentes em disco, enquanto os servidores secundários obtêm toda a informação a partir do servidor primário.
- Quando um servidor secundário obtém a informação do primário respetivo, essa operação tem o nome de *zone transfer*.
- Quando um novo computador é adicionado à zona, o administrador adiciona a informação apropriada (nome e endereço IP) a um ficheiro em disco existente no servidor primário (que constitui a base de dados DNS local). O servidor de nomes primário é então notificado que tem de reler os ficheiros de configuração.
- Os servidores secundários contactam o primário de uma forma regular (normalmente cada 3 horas), e se o primário possuir novos dados, os secundários obtêm esses dados através do mecanismo de *zone transfer* (porta 53 TCP).
- Um determinado servidor pode ser primários ou secundário de diversas zonas.



# Servidores Primários

- Trata-se de um servidor DNS responsável pelo menos por uma zona, obtendo os dados dessa Zona a partir de ficheiros locais (Zone files).
- Diz-se que é Autoritário para essa Zona, sendo que a alteração da informação relativa à mesma (adição de domínios ou máquinas) apenas pode ser feita localmente.
- Em geral o Master Name Server é o servidor primário da zona.
- Não precisa de correr na rede (física e lógica) da autoridade responsável pela Zona:
  - pode estar a correr numa rede distinta.
  - os Zone files podem ser importados por FTP ou email quando houver necessidade de atualizar a informação da zona.

# Servidores Secundários

- Servidor que obtém os dados da zona a partir de outro servidor de DNS (*Master Zone Server* – servidor primário ou secundário)
- Periodicamente ou sempre que o servidor arranca é verificada a necessidade de efetuar uma atualização dos dados da zona (*Zone Transfer*)
- Cada ISP, instituição, etc. tem vários servidores locais que são usados diretamente pelos utilizadores as *queries* DNS dos utilizadores são dirigidas a estes servidores
- Vantagens de possuir servidores secundários:
  - **Redundância** - Se um dos servidores falhar os restantes poderão ser contactados em alternativa (mecanismo de *timeout*).
  - **Localização remota** - Para evitar a latência das ligações WAN é boa política os subdomínios possuírem um servidor secundário do seu domínio pai.
  - **Distribuição da carga de processamento** - Para evitar a congestão de um único servidor deve-se distribuir as consultas a um domínio por diversos servidores.

# Outros Servidores

- ***Forward***

- Trata-se do servidor de uma organização eleito para interagir com os servidores exteriores à mesma quando há necessidade de resolver nomes não locais.
- É uma configuração feita por servidor e não por Zona.
- Se os servidores internos ao contactar o forwarder não virem os seus pedidos resolvidos tentam pelos seus próprios meios efectuar a resolução contactando o exterior.

- ***Stub Server***

- Mantém apenas uma cópia abreviada da zona (*stub zone*), contendo a lista dos servidores '*authoritative*' para essa zona.

- ***Caching-only server***

- Apesar de todos os servidores fazerem caching de todas as consultas recebidas e resoluções corretamente realizadas existem servidores que são exclusivamente ativados para essa tarefa não efetuando a manutenção de nenhuma Zona.

# *Resolvers*

- São servidores utilizados pelas aplicações cliente para consultar o DNS.
- Necessitam de conhecer pelo menos a localização de um servidor de nomes.
- Usam a informação fornecida pelo servidor de nomes conhecido para responder às consultas dos clientes.
- A resposta pode ser diretamente fornecida pelo servidor de nomes conhecido ou por contacto sucessivo de outros servidores referidos.
- São tanto mais eficientes quanto maior for a abrangência da sua cache.

# Registos DNS

- **SOA** – *Start of Authority* - define as características gerais da zona
  - **NAMESERVER**: indica o servidor DNS autoritário daquela zona;
  - **MNAME** - nome de domínio do nameserver (ex. isec.pt);
  - **RNAME** - endereço de email do administrador da zona (domínio);
  - **SERIAL** - versão do ficheiro de zona. Este valor deve ser incrementado sempre que alguma parte da informação do ficheiro de zona é alterada. A tática vulgarmente usada é escrever um número com o formato de data (ano/mês/dia/versão - 0..99): 2001053000.
  - **REFRESH** - periodicidade (em segundos) com que os servidores secundários consultam o primário para averiguar a versão atual da zona. Valor típico: 3600 = 1h
  - **RETRY** - Periodicidade (em segundos) com que os servidores secundários repetem a tentativa de averiguar o número de série do master file após falharem um contacto. Valor típico: 600 = 10m
  - **EXPIRE** - Limite máximo (em segundos) de retenção de réplica da zona sem conseguir averiguar o número de série. Após este valor expirar os secundários deixam de poder responder pela zona. Valor típico: 3600000 -> 42d;
  - **MINIMUM TTL** - define quanto tempo o registro dessa zona deverá permanecer no cache de um servidor DNS antes que seja feita uma atualização. Valor típico: 864000 -> 10d

# Registos DNS

- **A** – trata-se do tipo básico que estabelece a correspondência entre um nome canónico e um endereço IP (IP V4)
- **AAAA** – igual ao anterior mas para IP V6.
- **CNAME** – mapeia um alias para um nome de domínio verdadeiro ou canónico. Ou seja, indica que um nome é um nome alternativo para um outro nome. É particularmente útil para fornecer nomes alternativos que correspondem aos diferentes serviços de uma mesma máquina
- **MX** – *Mail Exchanger* – Informa os IPs dos servidores SMTP de um domínio. Esse tipo de registro tem como particularidade um campo a mais, que informa a prioridade do servidor SMTP. Quanto mais baixo o valor, maior a prioridade. Cada registro MX deve corresponder a um registro A.
- **SRV** – *Service Location* - permitem definir quais os servidores que suportam um determinado serviço para um domínio.
- **NS** – *nome do domínio* – é o que faz com que a hierarquia de nomes funcione. Indica o nome (canónico) de uma máquina que aloja um servidor DNS para o domínio referido.
- **TXT** - servem para associar informação ao domínio. Estas informações são com que pequenos ficheiros de texto, que podem conter qualquer informação pública que se pretenda associar ao domínio.
- **PTR** – *Pointer* (IP => nome) - Associa um endereço IP a um hostname para a resolução de DNS reverso.

# Exemplo

```
#####  
  
@      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 prmx2.isec.pt.
isec.pt.	IN	MX	30 prmx2.isec.pt.
isec.pt.	IN	MX	40 prmx1.isec.pt.
isec.pt.	IN	MX	10 prmx2.isec.pt.
isec.pt.	IN	NS	ns.isec.pt.
isec.pt.	IN	NS	ns2.isec.pt.
isec.pt.	IN	TXT	"v=spf1 ip4:193.137.78.24 ip4:193.137.78.26 ip4:193.137.78.20 ip4:193.137.78.21 -all"

## ► Additional

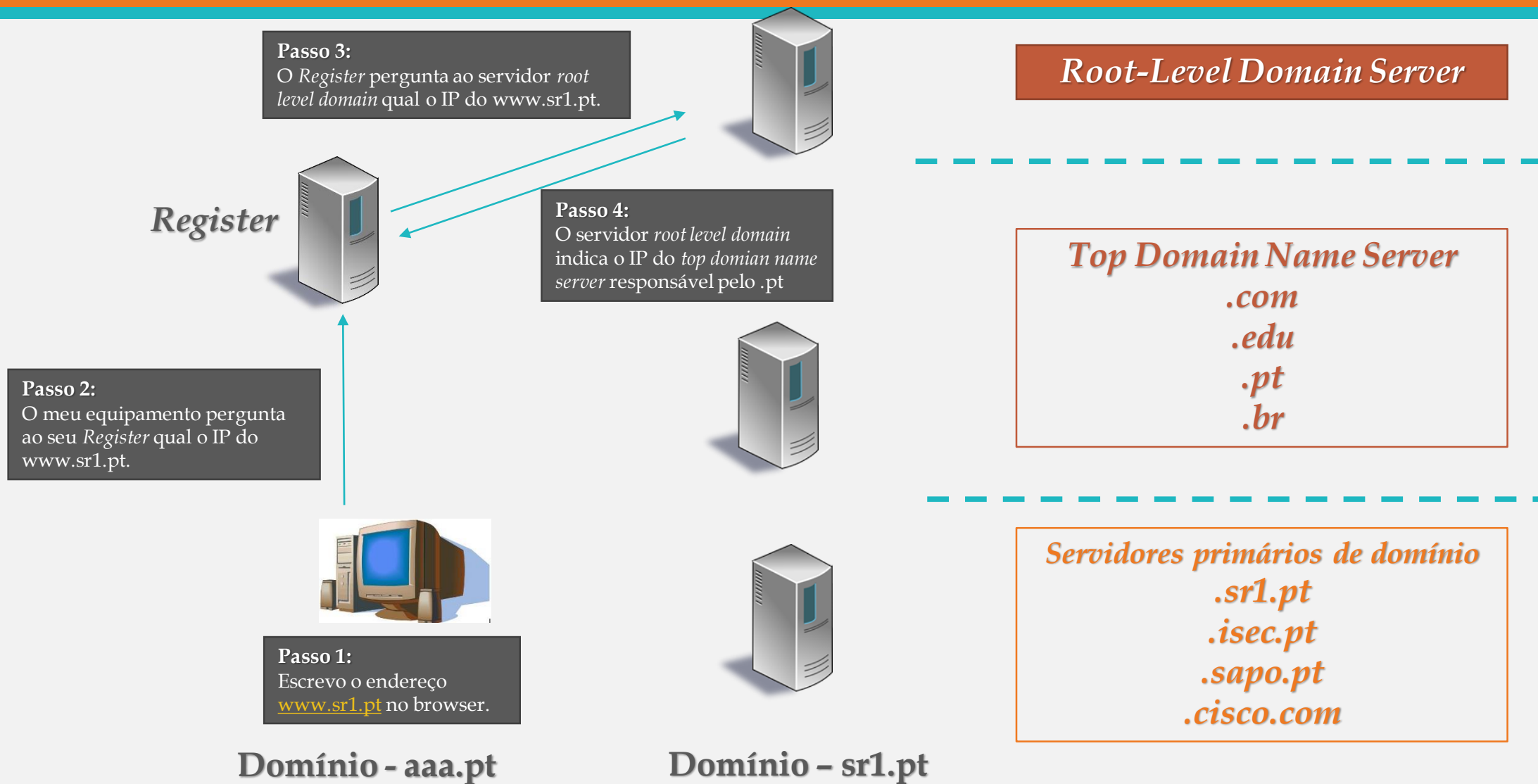
prmx2.isec.pt.	IN	A	193.137.78.26
prmx1.isec.pt.	IN	A	193.137.78.24
ns.isec.pt.	IN	A	193.137.78.1
ns2.isec.pt.	IN	A	193.137.78.3

# Funcionamento

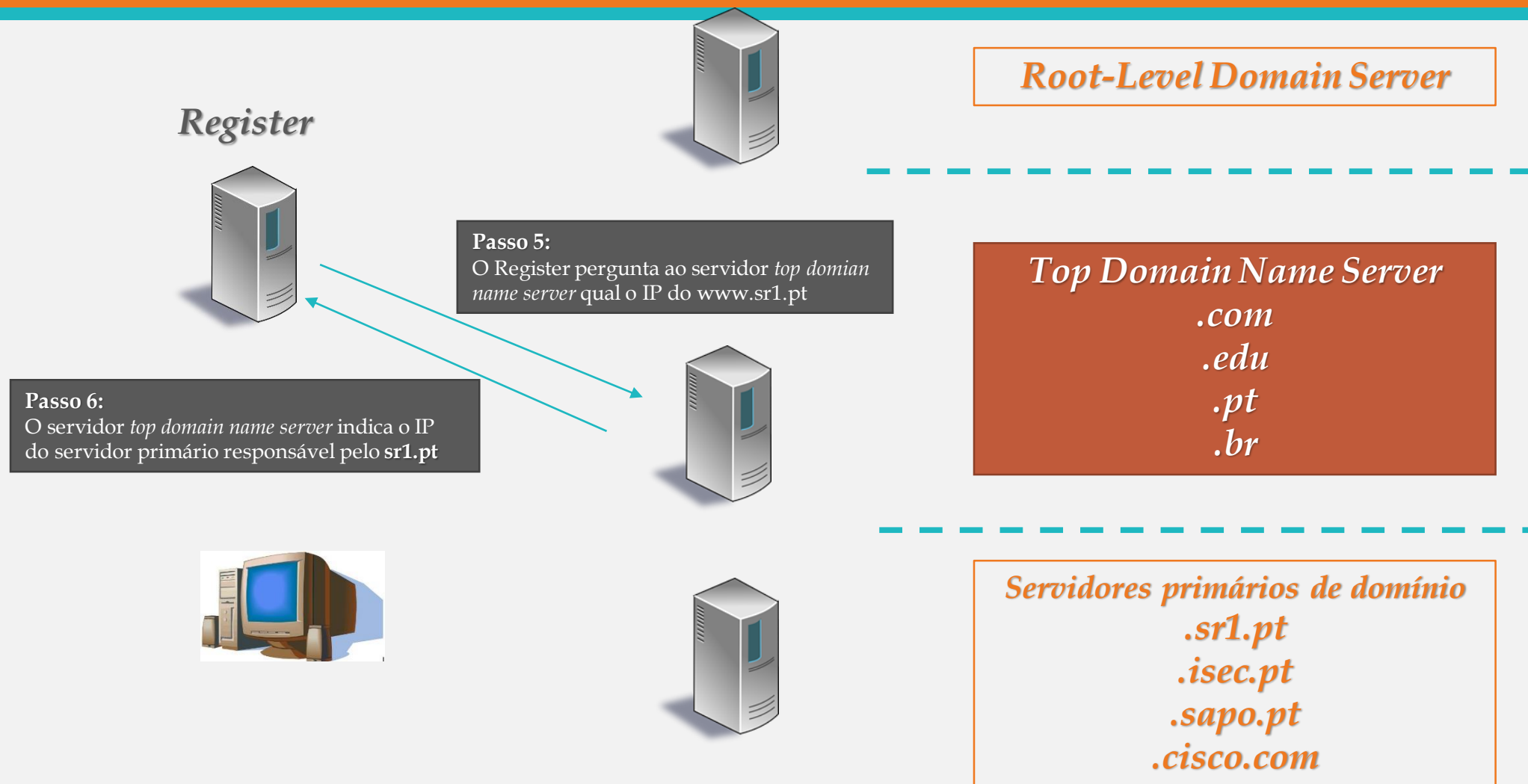
- Já vimos em outras aulas, que a ligação entre duas máquinas só é possível com o conhecimento de duas informações fundamentais:
  - Endereço IP.
  - Endereço físico (MAC).
- Então para que a máquina A se ligue à máquina B é necessário saber o endereço IP e depois o MAC dessa máquina.
- Mas se no browser eu escrevo o nome da máquina destino, como é que a minha máquina sabe o IP da máquina destino?
- Sim, eu sei que esse é o papel d DNS, mas como funciona?



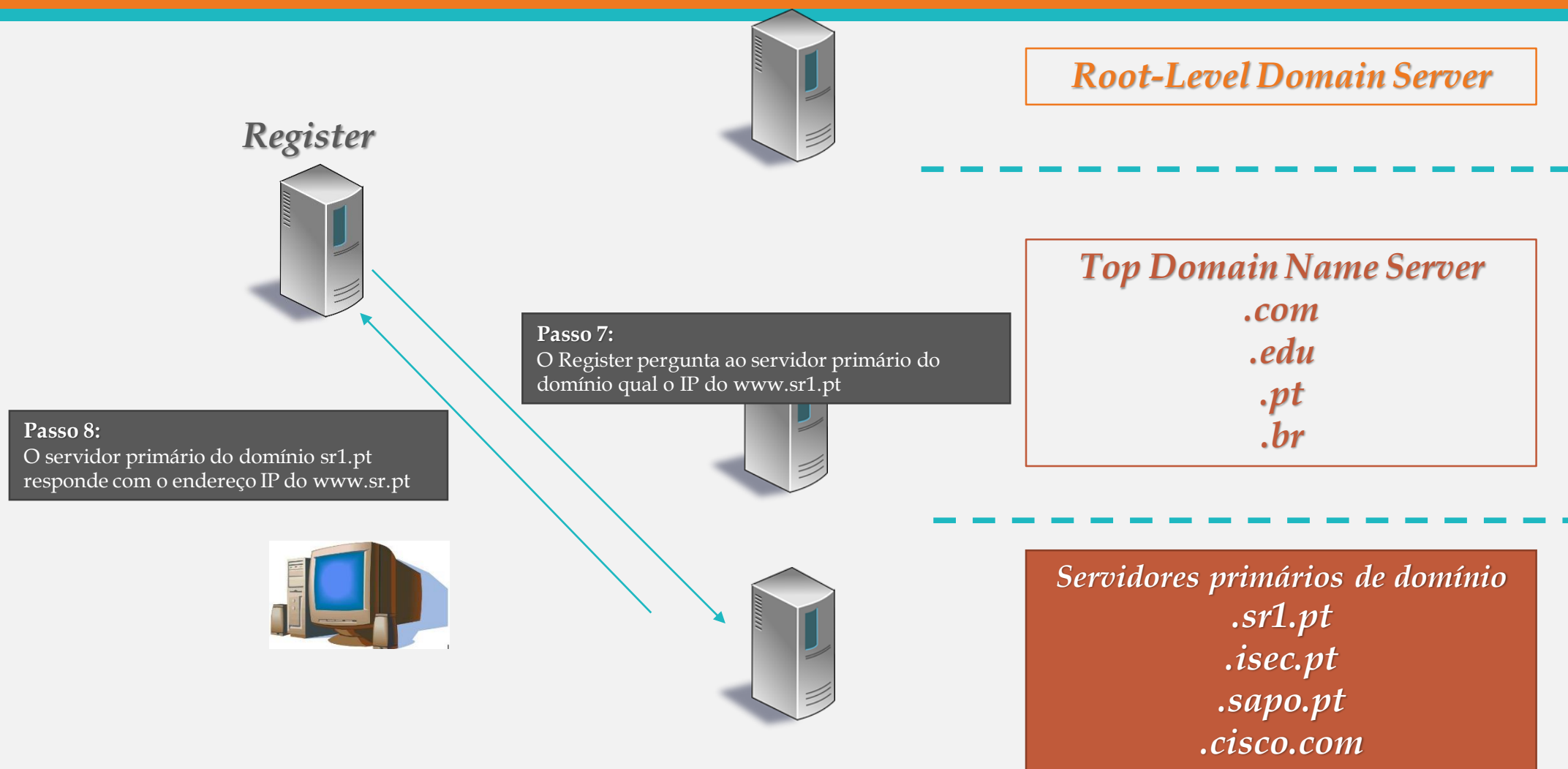
# Funcionamento



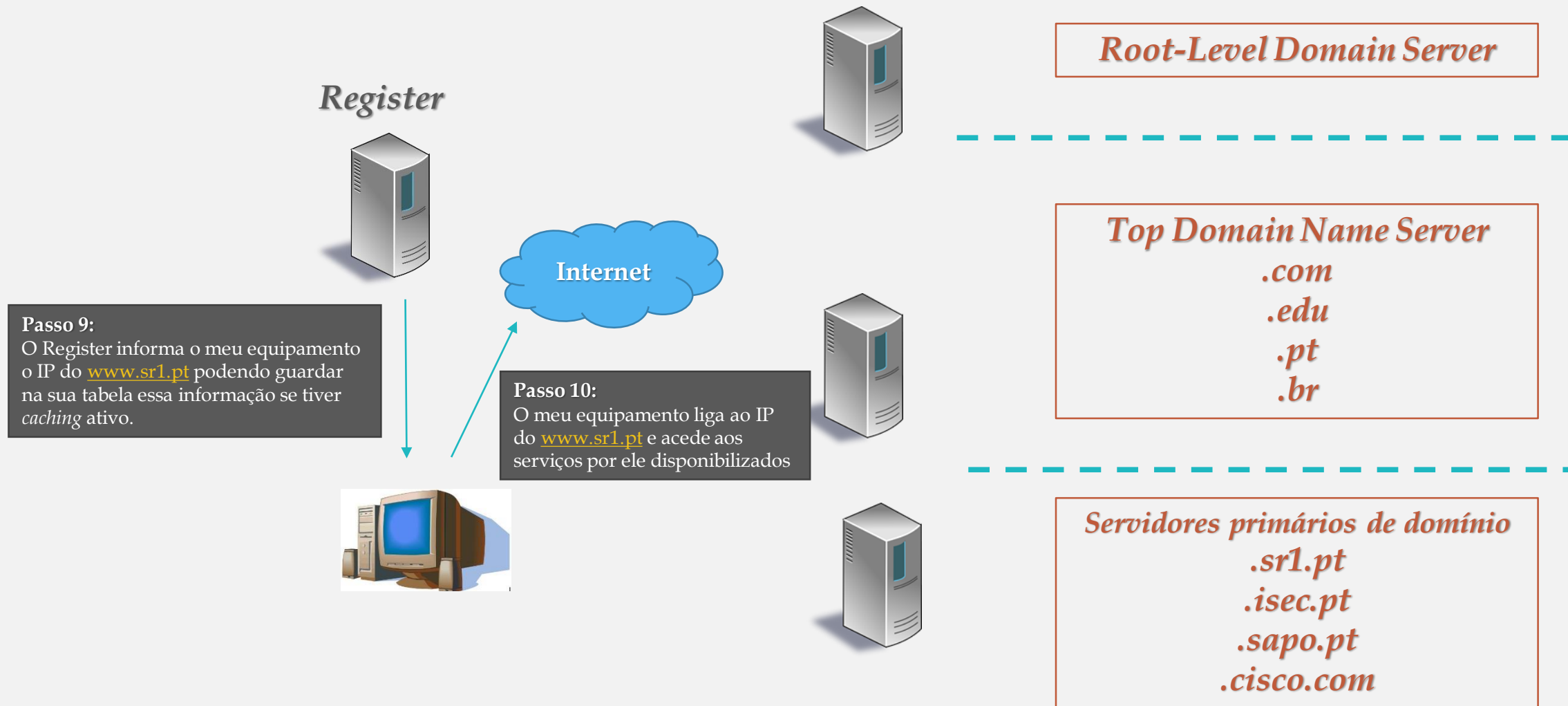
# Funcionamento



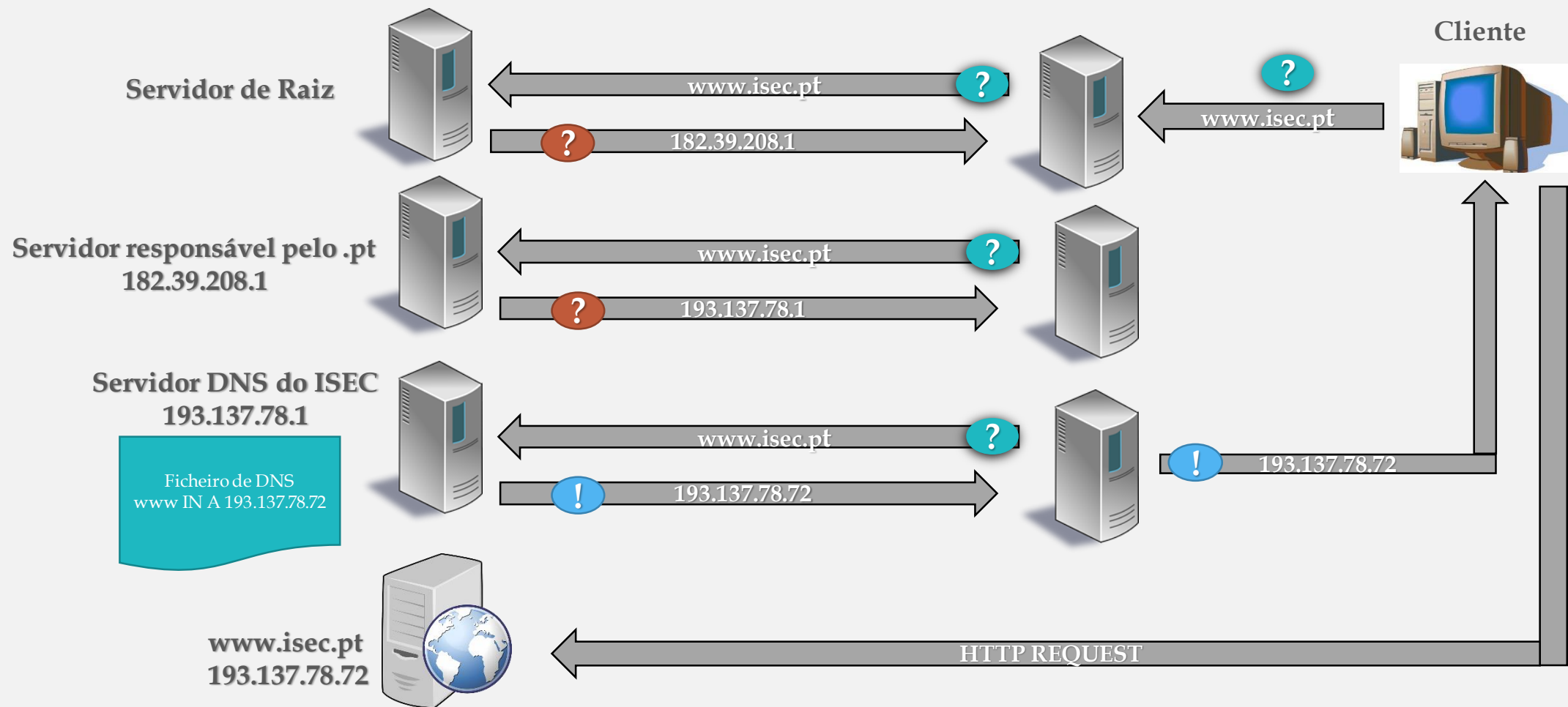
# Funcionamento



# Funcionamento

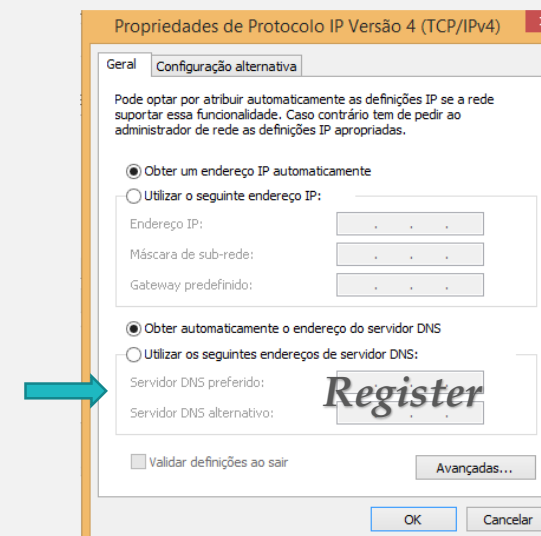


# Funcionamento



# Funcionamento

- **O *Register* é o primeiro local que a minha máquina usa para tentar obter o IP?**
  - Não. A sua máquina a primeira ação que faz é consultar o ficheiro hosts e só no caso de neste ficheiro não estar esta correspondência é que pergunta ao seu *register*.
- **Qual o endereço IP do *Register* que a máquina local utiliza?**
  - O IP que coloca na placa de rede do seu equipamento no campo DNS ou que está definido no seu serviço DHCP como o seu servidor DNS.
- **Qual o endereço IP que o servidor primário de um domínio devolve quando é questionada?**
  - O que estiver configurado na sua tabela. Assim, no exemplo anterior, se na tabela do servidor responsável pelo domínio sr1.pt estivesse criado um registo do tipo A com o IP 203.100.2001.1 para a maquina www seria esse o valor que ele respondia.
- **O *Register* que tenho definido no meu PC tem de ser uma máquina da minha rede local?**
  - Não, pode ser uma máquina fora da minha rede.
- **O *Register* pode ser o servidor primário do meu domínio DNS?**
  - Pode. O servidor de um dado domínio pode ser também o *Register* das máquinas desse domínio.



# Caching

- Uma característica fundamental do DNS é o *caching*. Isto é, quando um servidor de nomes recebe informação sobre um mapeamento de um computador, faz o *caching* dessa informação para futuras utilização em perguntas iguais.
- Então, uma consulta posterior relativo a esse mapeamento pode utilizar o resultado *cached*, evitando assim inquéritos adicionais a outros servidores.
- O DNS utiliza o *caching* para otimizar o custo da pesquisa.
- Desta forma, os endereços dos servidores TLD (Top Level Domin) estão sempre em cache.
- Uma entrada é mantida na cache até um limite de tempo controlado pelo administrador do servidor responsável pelo nome *cached* através do atributo TTL (Time To Live).
- Entrada é automaticamente removida da cache quando seu TTL expira.

# Caching

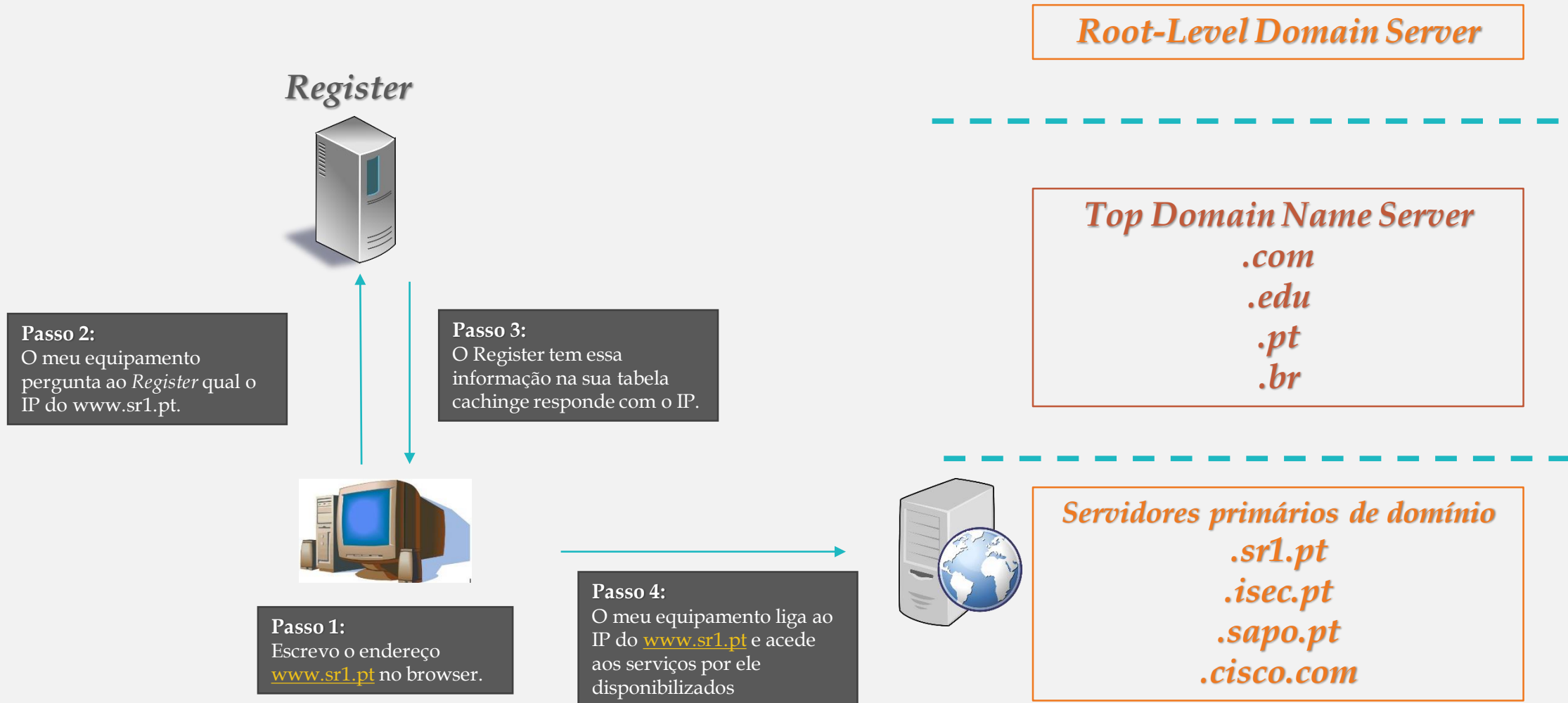
- Dado que a informação sobre um determinado nome pode ser alterada, um servidor pode possuir informação incorreta na sua tabela de *caching*.
- Utiliza-se então o valor TTL para decidir quando é que a informação não pode ser mais considerada como válida.
- Se um servidor responder a alguma consulta com informação em cache deve:
  - atualizar o TTL da RR fornecida na resposta
  - indicar que se trata de informação não autoritária bit AA (*authoritative answer*) colocado a 0 (false).



# Caching

- O DNS suporta, opcionalmente, *caching* de respostas negativas.
  - Exemplo: um servidor pode distribuir um TTL com uma indicação de “name error”.
- O cliente que receber esta informação pode assumir que o nome em causa não existe durante TTL sem consultar dados autoritários.
- Da mesma forma pode ser realizada uma consulta com um QTYPE que represente múltiplos tipos e armazenar em cache uma resposta com a indicação de que parte dos tipos não estão presentes.
- Os servidores que forneçam serviço recursivo devem estar bem apetrechados de memória!

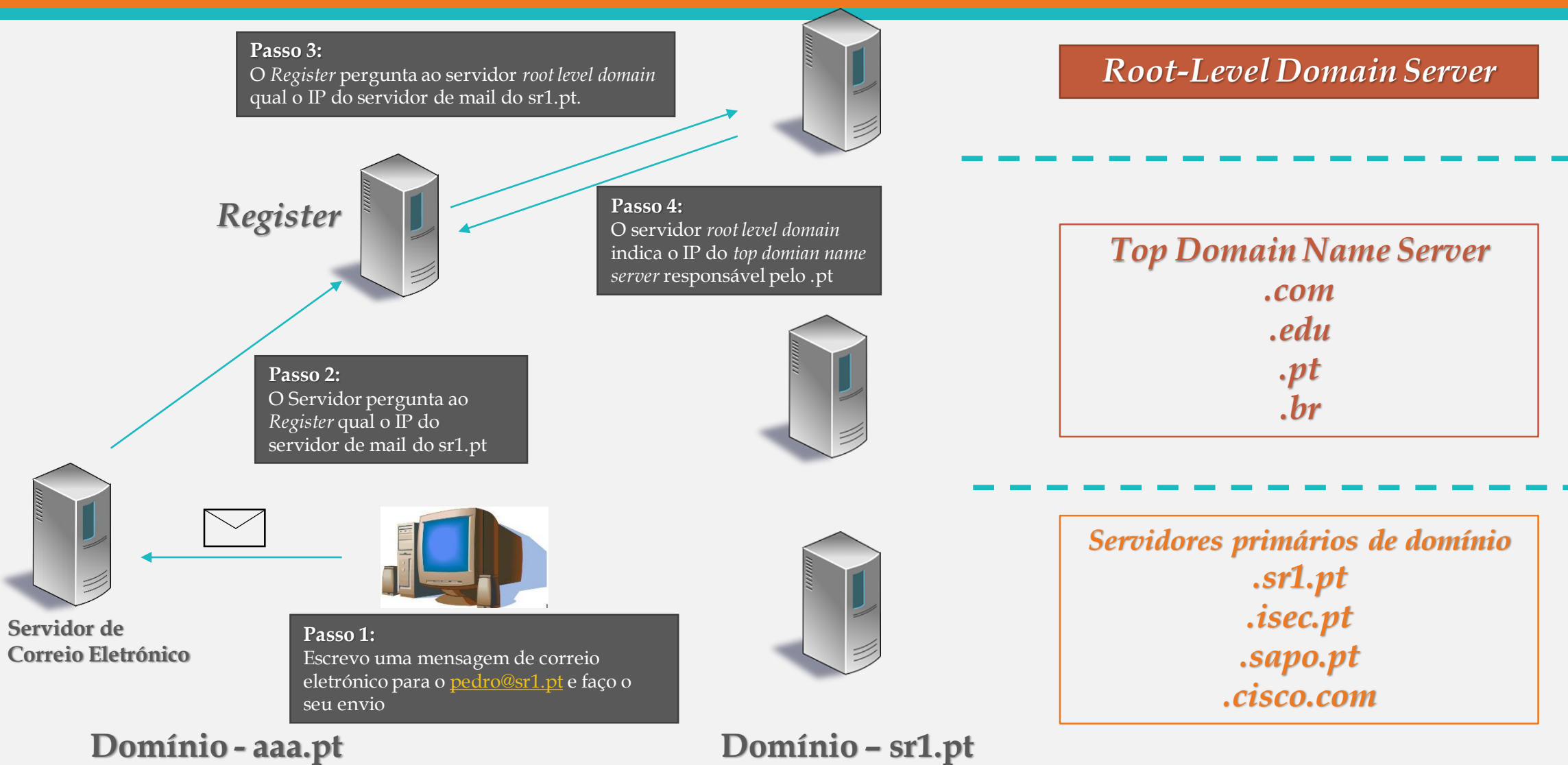
# Funcionamento - *Caching* e no caso de o *Register* já tenha informação do IP do *www.sr1.pt*



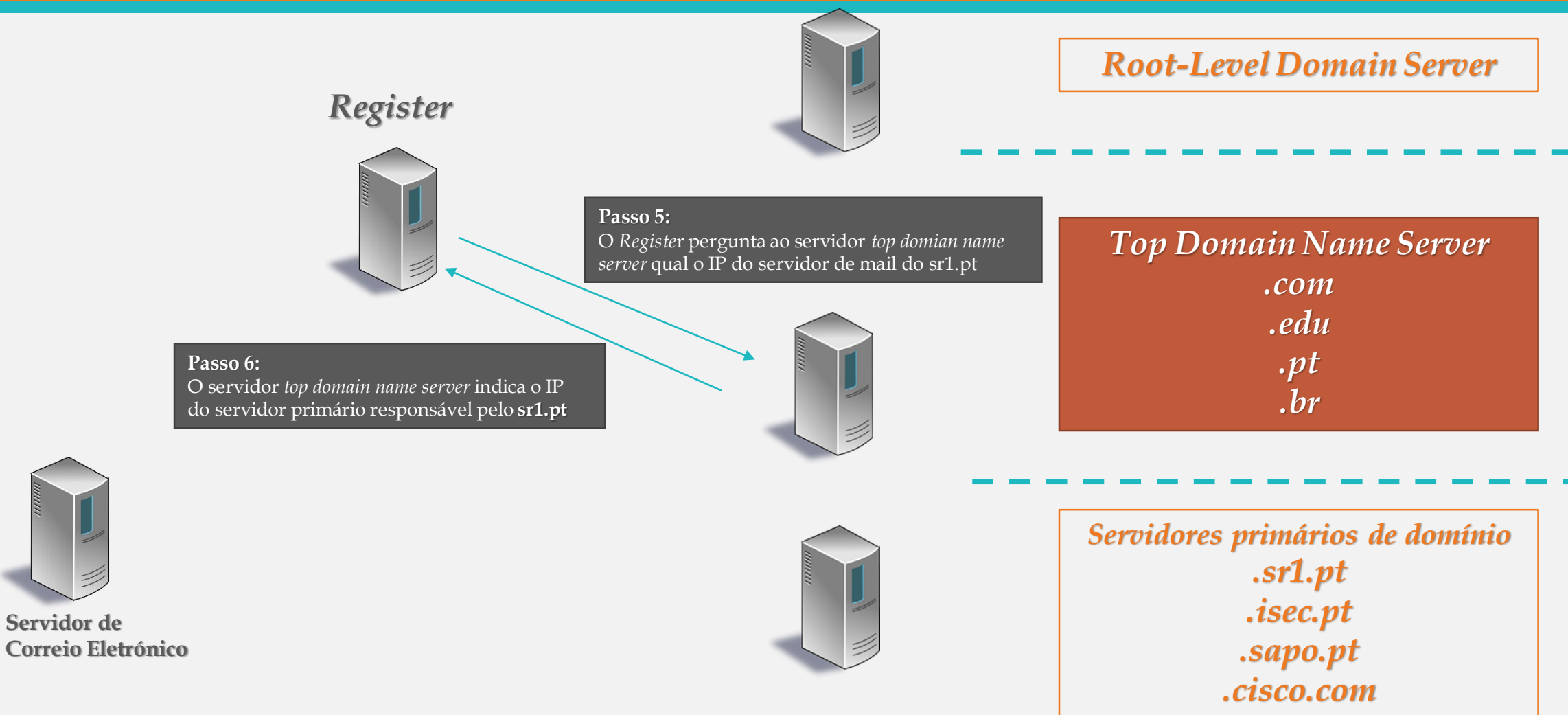
# Funcionamento – Correio Eletrónico (MX)

- No caso de pretender enviar uma mensagem de correio eletrónico, o seu servidor não sabe o nome da máquina onde tem de entregar a mensagem. Conhece apenas o endereço de correio eletrónico do destinatário e consequentemente o domínio.
- O funcionamento será idêntico ao descrito para saber o IP do nome de uma máquina, mas agora a pergunta não terá como resposta o IP de um nome mas sim do registo MX do domínio destino.

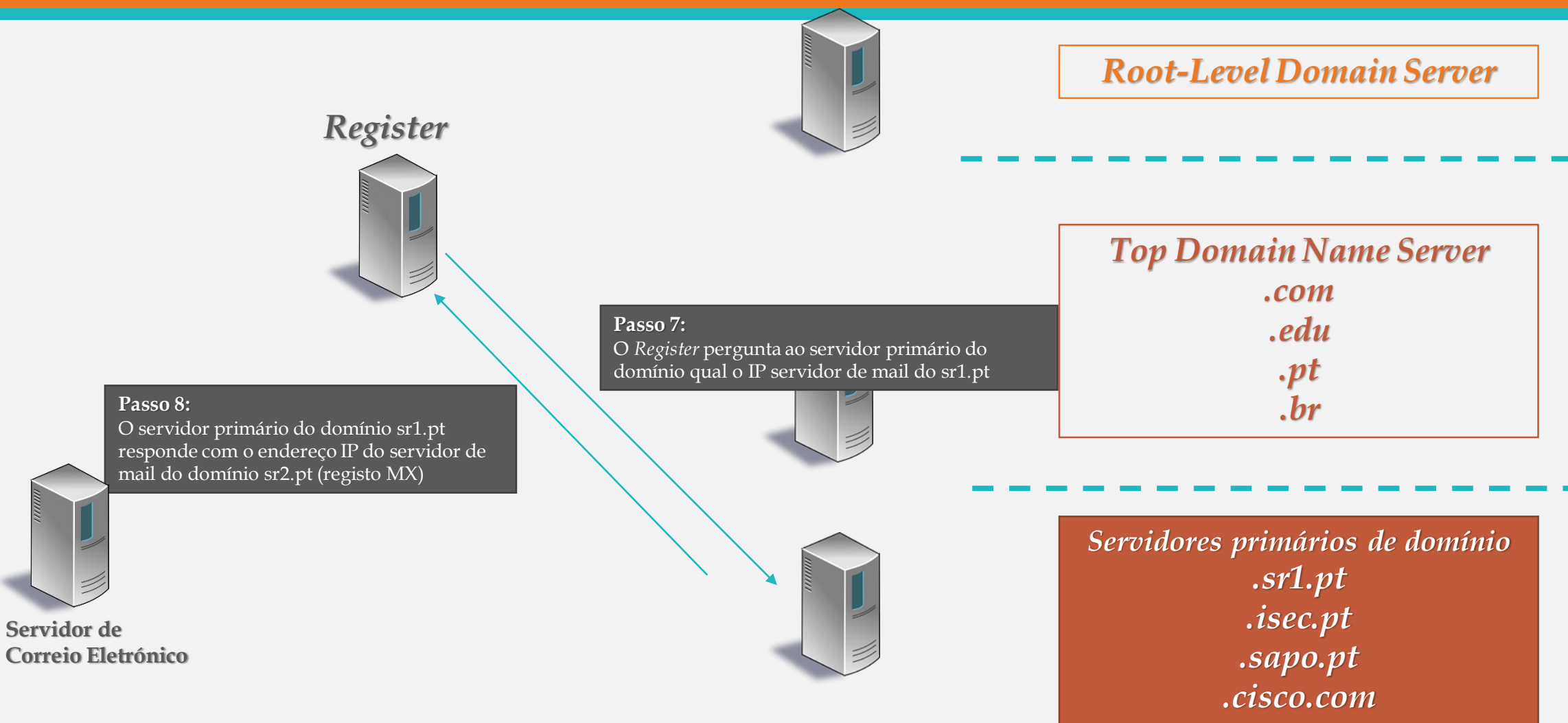
# Funcionamento – Correio Eletrónico (MX)



# Funcionamento – Correio Eletrónico (MX)



# Funcionamento – Correio Eletrónico (MX)



# Funcionamento – Correio Eletrónico (MX)

*Register*



**Passo 9:**  
O *Register* informa servidor de mail do IP do servidor de mail de sr2.pt podendo guardar na sua tabela essa informação se tiver *caching* ativo.



**Servidor de  
Correio Eletrónico  
do domínio aaa.pt**



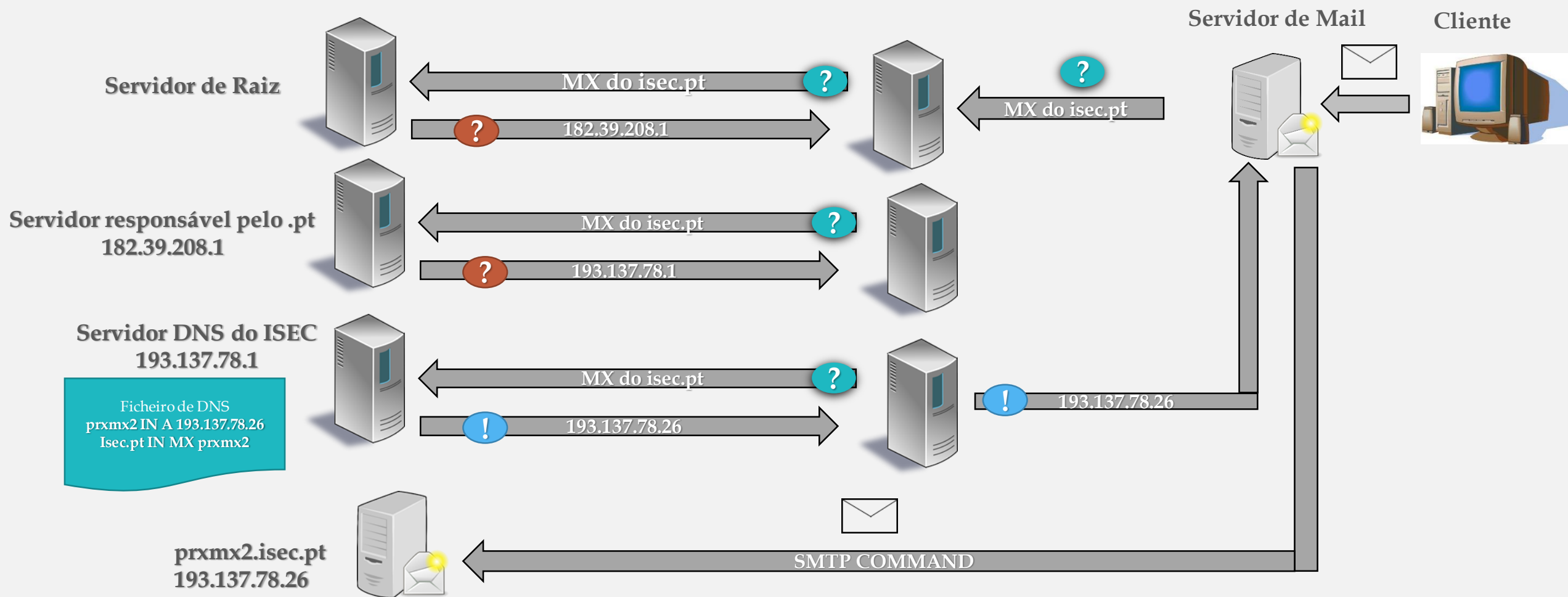
Internet



**Servidor de  
Correio Eletrónico  
do domínio sr1.pt**

**Passo 10:**  
O servidor de mail de aa.pt estabelece a ligação com o servidor de mail sr1.pt e entrega a mensagem de mail para o pedro@sr1.pt

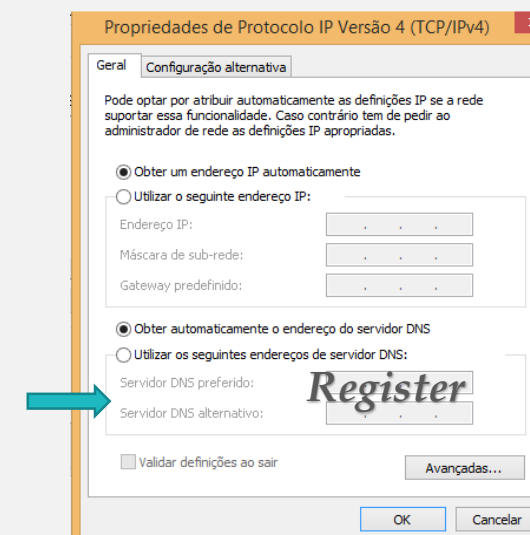
# Funcionamento – Correio Eletrónico (MX)





# Funcionamento

- **Qual o endereço IP do *Register* do servidor de mail do domínio aa.pt?**
  - O IP que coloca na placa de rede do seu servidor no campo DNS. Nos servidores não devemos utilizar endereços atribuídos por DHCP
- **Qual o endereço IP que o servidor primário de um domínio devolve quando é questionado, se não sabe o nome da máquina?**
  - Quando o servidor de mail inicia o processo não sabe nome da máquina destino, mas só o nome do endereço do destinatário da mensagem (a mensagem é para ser entregue em *utilizador@dominio*). Então a resposta do servidor DNS do domínio destino não será de uma máquina (registo do tipo A) mas sim da máquina que tem o registo MX.



# Tipo de consultas

- **Interativa**

- Trata-se de uma consulta à qual o servidor contactado responde com informação disponível localmente.
- A resposta pode consistir:
  - No endereço IP- se for informação autoritária ou estiver em cache.
  - Numa referência a um servidor mais “próximo” da resposta.
  - Num erro - em caso de consultas mal formuladas.
- Quem realiza estas consultas?
  - os servidores DNS que tentam responder a uma consulta recursiva.
  - os resolvers (raramente).
- Os servidores são obrigados a aceitar este modo.

# Tipo de consultas

- **Recursiva**

- Trata-se de uma consulta à qual o servidor contactado responde sempre com a resolução pedida ou com uma indicação de erro (i.e. fornece a resposta final!)
- Quem realiza estas consultas?
  - os resolvers (tipicamente)
  - os servidores DNS configurados para usar um forwarder
- Nenhum servidor DNS é obrigado a aceitar este tipo consulta (e.g.: os root servers não aceitam!)
- Deve existir um servidor DNS, por rede local, capaz de aceitar consultas recursivas.
- Centralizar a interação com o exterior melhora o efeito de *caching*!

# Respostas

- **Com autoridade** (*authoritative*)- Gerada por servidores que possuem autoridade no domínio do nome resolvido. Resposta bastante confiável, mas pode estar incorreta (se fornecida por um servidor secundário e não pelo primário)
- **Sem autoridade** (*non-authoritative*) - Gerada por servidores que não possuem autoridade no domínio do nome resolvido. A resposta não é tão confiável, pois as informações podem ter sido modificadas.

# Ferramentas

- Existem sites na Internet que permitem validar a correcta configuração do seu servidor de DNS .
- Um que pode utilizar é fornecido pela DNS.PT:

<http://www.dns.pt/pt/ferramentas/avaliador-tecnico/>

The screenshot shows the 'Avaliador Técnico' (Technical Evaluator) tool on the DNS.PT website. The interface has a green header with the '.pt' logo and a navigation menu. Below the header, there are three main sections: 'Ferramentas', 'WHOIS', and 'Avaliador Técnico' (highlighted in yellow). The 'Avaliador Técnico' section contains a description of the tool's purpose, an example of how to use it, and a form to enter domain and IP information for evaluation.

**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**

**Avaliar**

# nslookup

- É uma ferramenta, que existe no Windows e no Linux, e que é utilizada para obter informações sobre registros de DNS de um determinado domínio, máquina ou IP.
- Numa consulta padrão, o servidor DNS definido na placa de rede da máquina é o consultado, e responde com as informações sobre o domínio ou máquina pesquisado.
- A informação "*Non-authoritative answer*" significa que o servidor DNS utilizado não responde por este domínio, em outras palavras, isto significa que foi feita uma consulta externa aos servidores DNS. Imagine que está em sua casa que faz uma consulta sobre uma máquina do ISEC, se for o seu servidor a responder a essa questão a resposta será *Non-authoritative answer* se for o servidor do ISEC será *Authoritative answer*.

# nslookup - Modos

- **Modo não-interativo**

- Este modo é utilizado para apresentar o nome e informação associada relativa a um computador (*host*) ou domínio.
- O nome ou endereço Internet é fornecido como primeiro parâmetro. O segundo parâmetro é opcional e corresponde ao nome ou endereço de um servidor de nomes de domínios (*name server*).

- **Modo interativo**

- Com o modo interativo, o utilizador pode questionar servidores de nomes de domínios de modo a obter informação sobre vários computadores e domínios ou para imprimir a lista de computadores existentes num domínio.
- Este modo é invocado quando especifica o comando nslookup sem parâmetros, sendo então utilizado o servidor de nomes de domínios pré-definido.
- Pode ainda invocar este modo interativo se o primeiro parâmetro utilizado for um - e o segundo parâmetro for o nome de um computador ou endereço Internet de um servidor de nomes de domínios.

# nslookup - Consultas

- O tipo de consulta pretendida é definido pelo comando set q=
  - **A**
    - Uma simples consulta solicitando o endereço IP correspondente a um computador.
  - **CNAME**
    - Um dado computador pode possuir diversos nomes DNS. Um destes é o nome canónico (canonical name) ou de referência.
  - **MX**
    - Uma consulta para saber quem é o servidor de correio eletrónico de um determinado domínio.
  - **SOA**
    - Uma consulta ao Start of Authority de um determinado domínio .
  - **PTR**
    - Uma consulta PTR, que demonstra a resolução inversa (inverse ou reverse). Repare na forma algo esquisita da consulta, o que acontece parcialmente devido ao facto dos endereços IP possuírem a parte mais significativa no lado esquerdo enquanto os endereços DNS possuem-na no lado direito do endereço.



# nslookup - Exemplos

```
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 = prmxmx1.isec.pt
isec.pt MX preference = 30, mail exchanger = prmxmx1.isec.pt
isec.pt MX preference = 10, mail exchanger = prmxmx1.isec.pt
isec.pt MX preference = 40, mail exchanger = prmxmx2.isec.pt

isec.pt nameserver = ns2.isec.pt
isec.pt nameserver = ns.isec.pt
prmxmx1.isec.pt internet address = 193.137.78.24
prmxmx2.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

- Para visualizar a *cache* de resolução de nomes num cliente pode fazer:
  - **ipconfig/displaydns**
- Para limpar e repor uma cache de resolução de clientes:
  - **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
```

# Propagação DNS

- É o tempo necessário para que um domínio seja publicado e divulgado em todos os servidores DNS existentes. Assim, entre a ativação do domínio e os servidores DNS receberem o novo domínio criado, demora um intervalo temporal, que é então o tempo de propagação de DNS.
- Este tempo também acontece quando altera a configuração do seu DNS por exemplo com a adição ou a alteração de um novo registro.
- A propagação leva de 8 a 48 horas. Durante este tempo o serviço fica instável, podendo funcionar em determinados momentos e dependente do *Register* que os clientes usem.
- Há várias razões, mas o que torna a operação lenta é justamente a necessidade de se informar outros servidores DNS do novo domínio ou da alteração efetuada como são alguns milhões de servidores demora o seu tempo...
- O processo de publicação é feito pelos órgãos responsáveis pelo registro de domínios. Estas entidades atualizam nos seus servidores e publicam uma "lista" de novos registros de domínios e alterações de servidores DNS, para domínios já registrados.
- Seguidamente ocorre o que chamamos de propagação, durante a qual as bases de dados dos servidores DNS dos ISP (Fornecedores de serviço de Internet) são atualizadas. Após esse processo, os domínios passam a apontar para o endereço IP do servidor onde estão as informações do site.
- Normalmente, a publicação não ultrapassa 48 horas, mas podem ocorrer situações, principalmente no caso de domínios internacionais, no qual este prazo pode ser maior. Isso depende exclusivamente da política da entidade que realiza os registros. Para além disso, a propagação dessas informações para os servidores DNS dos ISP pode também levar algum tempo e atrasar todo o processo.

# Protocolos de Transporte

- **UDP**

- Normalmente os pedidos e respostas DNS são transportados num *datagrama* UDP (inicialmente e enquanto a resposta < 512 bytes)
- No caso de a informação a transportar ser superior ao tamanho desse *datagrama*, a resposta é enviada incompleta e a *flag Truncated* é ativada.

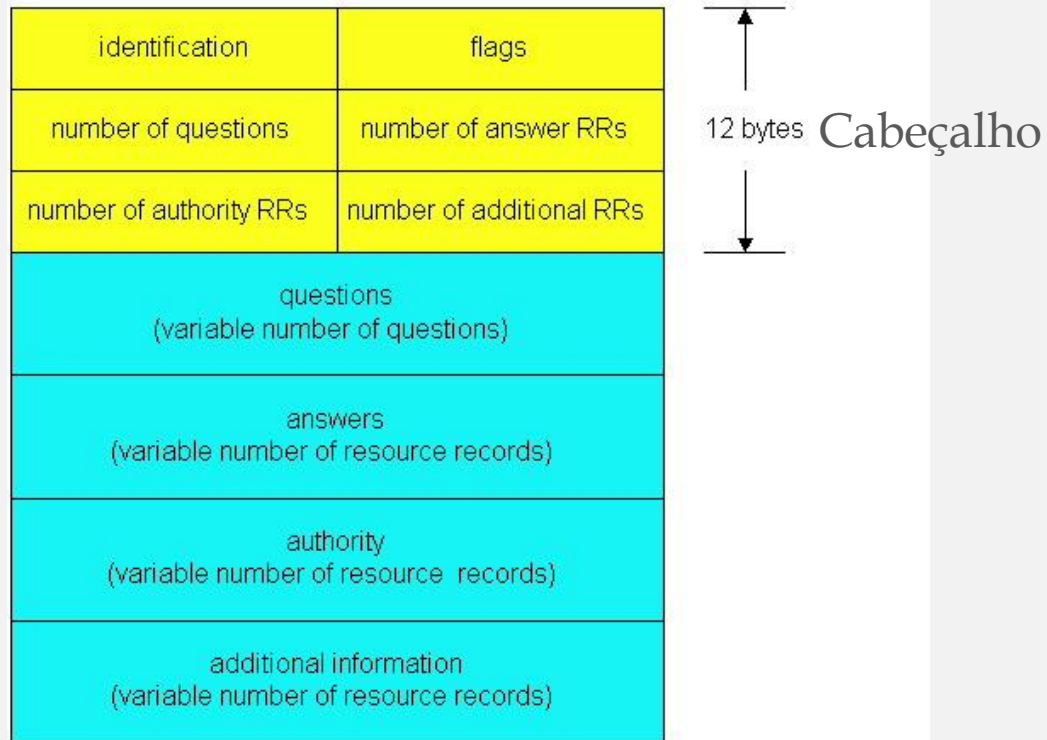
- **TCP**

- Quando o volume de informação a transferir não cabe num *datagrama* UDP (>512 bytes), o cliente DNS estabelece uma ligação TCP com o servidor para realizar a transferência. Ou seja:
  - quando é recebida uma resposta com a *flag Truncated* ativada.
  - para transferência de informação de zonas do servidor primário para os secundários.

- Em ambos o porto utilizado é o 53.

# O Protocolo do DNS

- As mensagens de pergunta e de resposta têm ambas o mesmo formato:



# Campos da mensagem

- **Cabeçalho** - identifica o tipo de operação DNS.
- **Questions** - pergunta a fazer ou feita.
- **Answers** - o que o servidor consegue saber em resposta a essa pergunta (pode ser informação *cached*).
- **Authority** - dados sobre os *name servers* com autoridade sobre os dados listados na resposta.
- **Additional information**- dados que podem vir a ser úteis (informações suplementares que podem evitar mais perguntas).

# Cabeçalho

- **Campo *Identification***

Trata-se de um valor estabelecido pelo cliente e devolvido pelo servidor para que quem consulte saiba que a mensagem é a resposta a determinada questão.

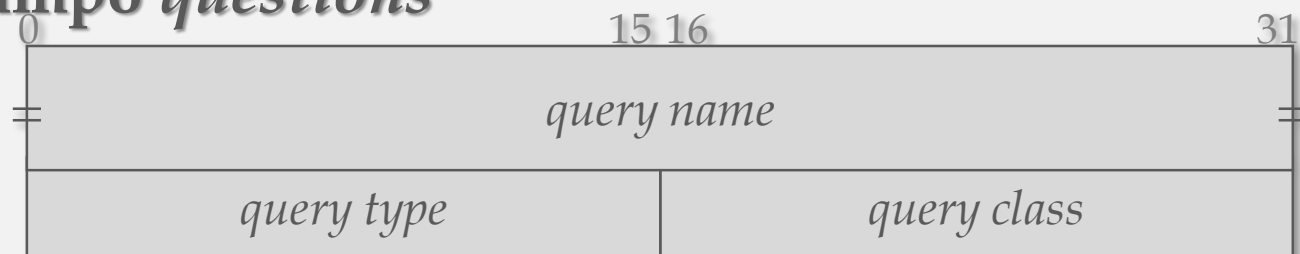
- **Campo *Flags***



- 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) | ... }

# Protocolo

- **Campo *questions***



- *query name*: o domínio que se questiona

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

- *query type*: tipo de informação requisitada

Código	Nome	Descrição
1	A	IP address
2	NS	name server
5	CNAME	canonical name
252	AXFR	req. zone transfer

Código	Nome	Descrição
12	PTR	pointer records
13	HINFO	host info
15	MX	mail exchange
255	*ANY	req. all records



# Protocolo

- **Campo *Answers***

- Domain Name
  - Chave de procura (Ex.: Nome de máquina)
- Type
  - Tipo de resposta
- Class
  - Tip. 1 - Internet
- Time To Live
  - Validade da informação (*cache*)
- Resource Data Domain Name
  - Informação adicional

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

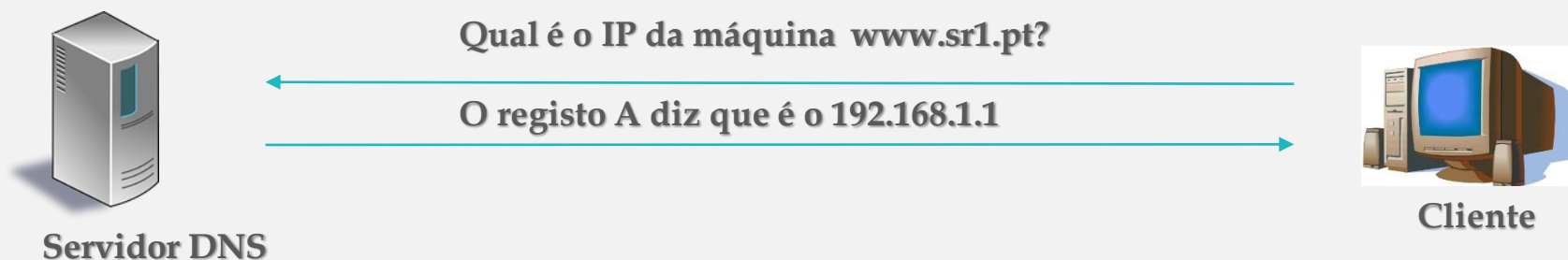
domain name	
type	class
time to live (TTL)	
resource lenght	
resource data	

# Resolução inversa - Reverse DNS resolution

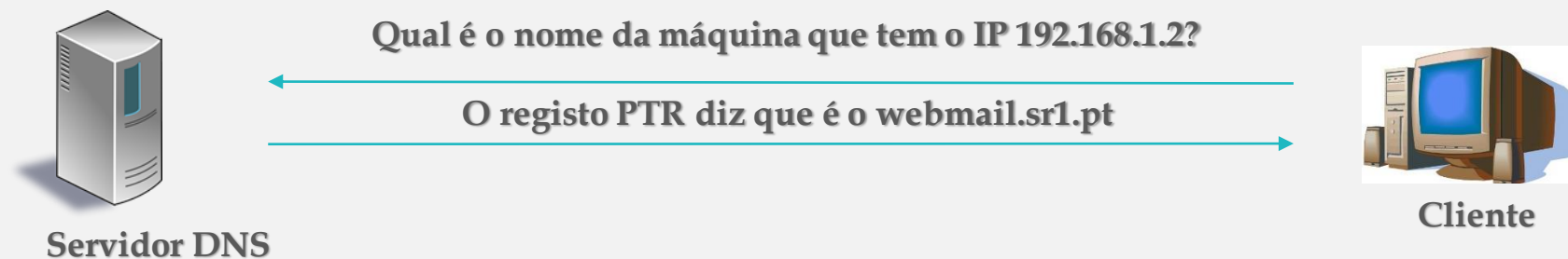
- Recurso utilizado para resolver um nome através de um endereço IP ou seja a operação inversa a DNS
- Utilizado para garantir a confiabilidade do nome a ser apresentado, conferindo o nome com o endereço IP.
- Vantagens
  - Segurança (por exemplo: filtragem por nome ou zona geográfica).
  - Leitura facilitada de ficheiros de log.
  - Redução do SPAM (servidor destino pode questionar se o MX do domínio que lhe está a tentar entregar a mensagem tem o IP da maquina que lhe está a ligar).

# Resolução inversa

## Resolução Direta



## Resolução Inversa



# Resolução inversa

- A configuração da resolução inversa é efectuada através de domínios definidos para o efeito, pertencentes ao domínio 'in-addr.arpa.'
  - Os subdomínios são definidos através da introdução dos octetos do endereço de rede, por ordem inversa
    - Exemplo (ISEC): 78.137.193.in-addr.arpa
- A gestão de um domínio 'in-addr.arpa.' só pode ser delegada se os endereços da classe (classe C, classe B,...) tiverem sido todos atribuídos a uma única entidade:
  - Exemplo (ISEC): o ISEC pode gerir o domínio 78.137.193.in-addr.arpa porque lhe foi delegada essa gestão por quem tem delegada a gestão da classe B 193.137.0.0 (FCCN).
  - A gestão de classes não completas é possível mas possui um nível de complexidade mais elevado, principalmente ao nível da sua manutenção.
- No caso do IPv6 a resolução inversa é efectuada através do domínio IP6.ARPA
  - o domínio inicial existente para este efeito, IP6.INT, está a ser abandonado.

# Resolução inversa

```
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

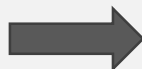
; Ativos de rede Gondor

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
```

Direta



```
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.
```

Inversa

# Resolução inversa

Direta

Inversa

```
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

- Balanceamento de carga nesta perspetiva consiste em distribuir os clientes de um recurso (servidor ftp, www, mail, ...) pelos diversos fornecedores do recurso.
- Assume-se portanto uma replicação do mesmo recurso por vários sistemas da rede.
- Uma técnica comum (RFC 1794 ) de, com base no DNS, efetuar balanceamento de carga consiste em ordenar de maneira diferente (e.g. por **round-robin**) os registos do mesmo domínio, classe e tipo em cada resposta a um pedido de resolução.
- Para tornar efetiva esta técnica a tais registos associam-se em geral valores TTL reduzidos.

# Load Balancing

- Pode fazer um balanceamento de cargas dos seus servidores utilizando o DNS para tal. Tem apenas que ter múltiplos registros A, para um nome.
- Por exemplo, se existirem três servidores WWW com os endereços 10.0.0.1, 10.0.0.2 e 10.0.0.3, um conjunto de registros tal como os que se seguem implica que os clientes se irão ligar um terço do tempo a cada máquina:

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

- Quando um *resolver* perguntar por estes registros, o DNS irá rodá-los e responder à pergunta com os registros em ordem diferente. No exemplo acima os clientes irão receber aleatoriamente os registros pela ordem 1, 2, 3; 2, 3, 1; e 3, 1, 2. Muitos clientes irão usar o primeiro registo e ignorar os restantes.



# Segurança

- O DNS sempre foi, e pretende continuar a ser, um repositório de informação pública e portanto não é fornecido nenhum mecanismo de suporte à confidencialidade da informação que manipula e troca.
- Contudo, com o evoluir e massificação da sua utilização começou a ser vulnerável a ataques. Por isso foi pensado forma de lhe introduzir alguma segurança.
- Os primeiros passos foram dados com o Secure DNS:
  - RFC 2065 - January 1997 *"Domain Name System Security Extensions"*
- Mais tarde, na sequência da proposta de atualização dinâmica do DNS (RFC 2136), e com base no DNSSEC, foi apresentado o
  - RFC 2137 - April 1997 *"Secure Domain Name System Dynamic Update"*
- Em 1999 são redefinidas as extensões de segurança do DNS de forma mais abrangente em quatro documentos:
  - 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"*

# Segurança

- O DNSSEC (*Domain Name System Security Extensions*) é o nome dado às extensões de segurança ao protocolo DNS concebidas para proteger e autenticar o seu tráfego.
- Os mecanismos de segurança previstos no DNSSEC são complementares e transparentes para o utilizador, não interferindo, desta forma, com o normal funcionamento do protocolo DNS.
- As extensões visam melhorar a confiabilidade dos utilizadores nos serviços prestados, nomeadamente:
  - Suprimir fragilidades;
  - Prevenir ataques;
  - Reduzir o risco de manipulação;
  - Prestar um serviço seguro;
  - Reforçar a segurança.
- Para que se obtenha total proveito deste serviço é necessário haver uma implementação do lado dos ISPs para que este serviço chegue ao cliente final.

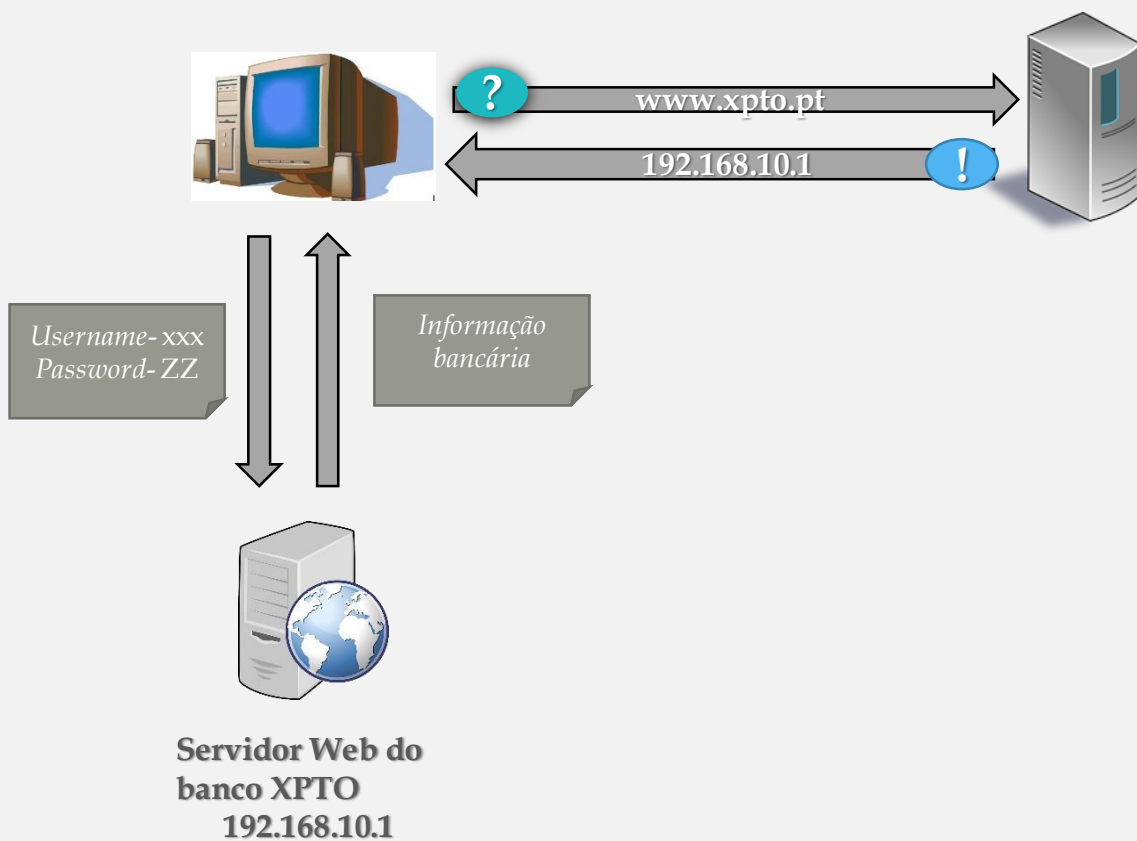
# Segurança

---

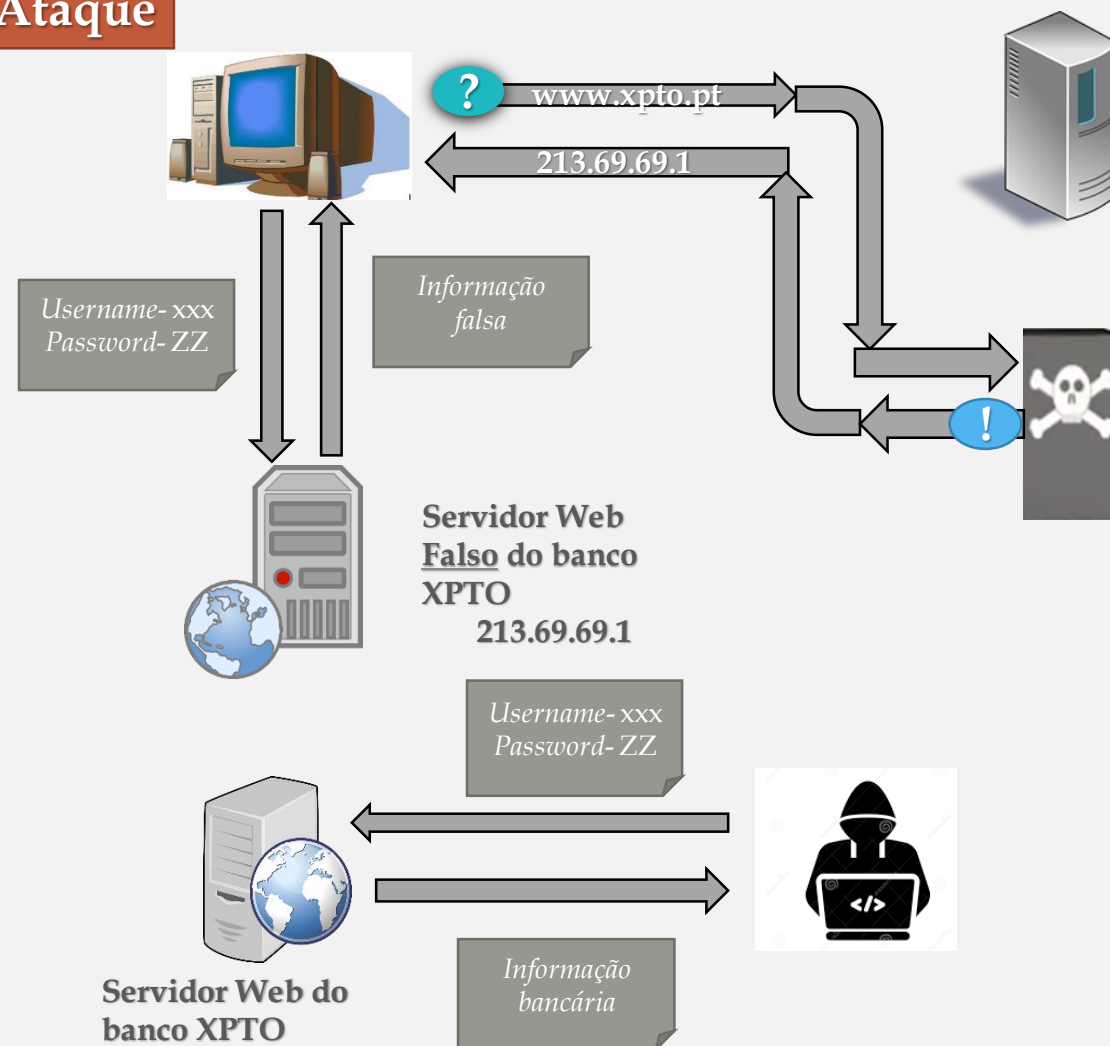
- As extensões de segurança assentam essencialmente nas tecnologias de criptografia de chave pública e em assinaturas digitais baseadas em chave pública.
- As extensões de segurança propostas no RFC 2535 consideram três serviços:
  - Distribuição de Chaves.
  - Autenticação da Origem dos Dados e Integridade.
  - Autenticação de Transações e Pedidos DNS.

# Segurança – Ataque *man-in-the middle*

## Situação Normal

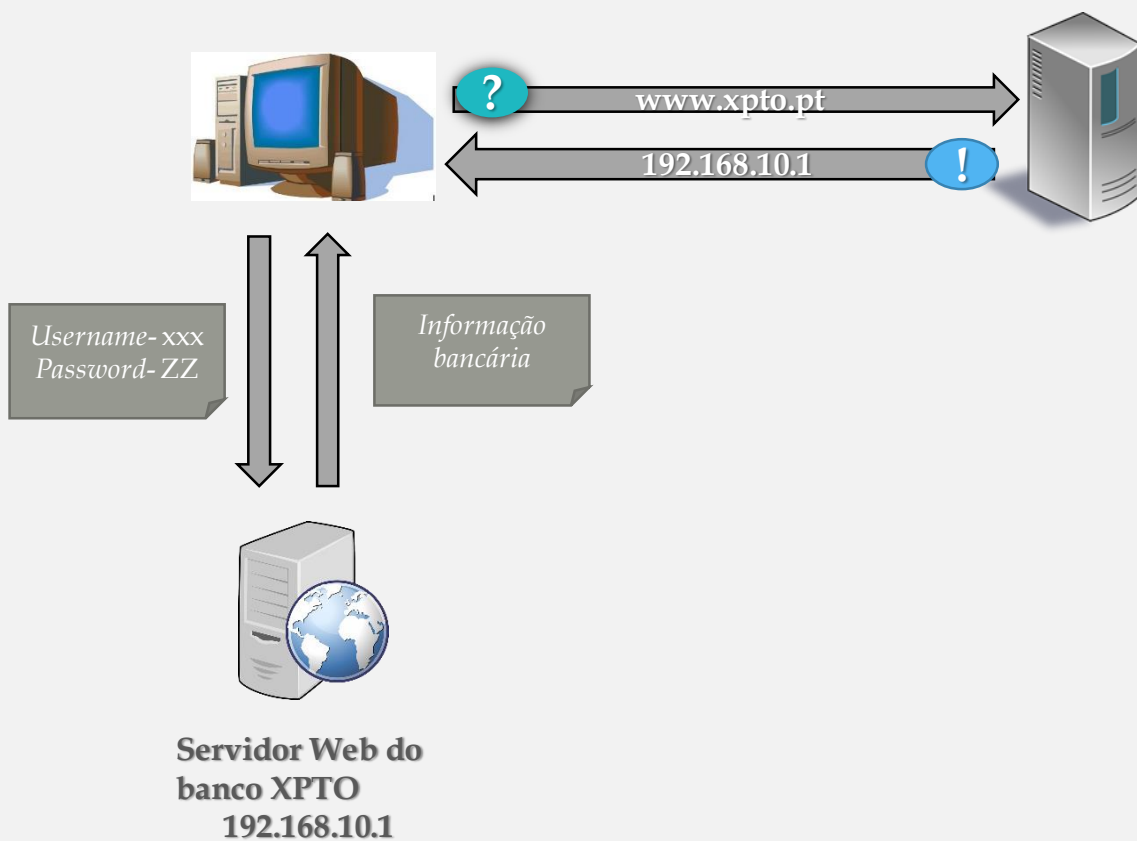


## Ataque

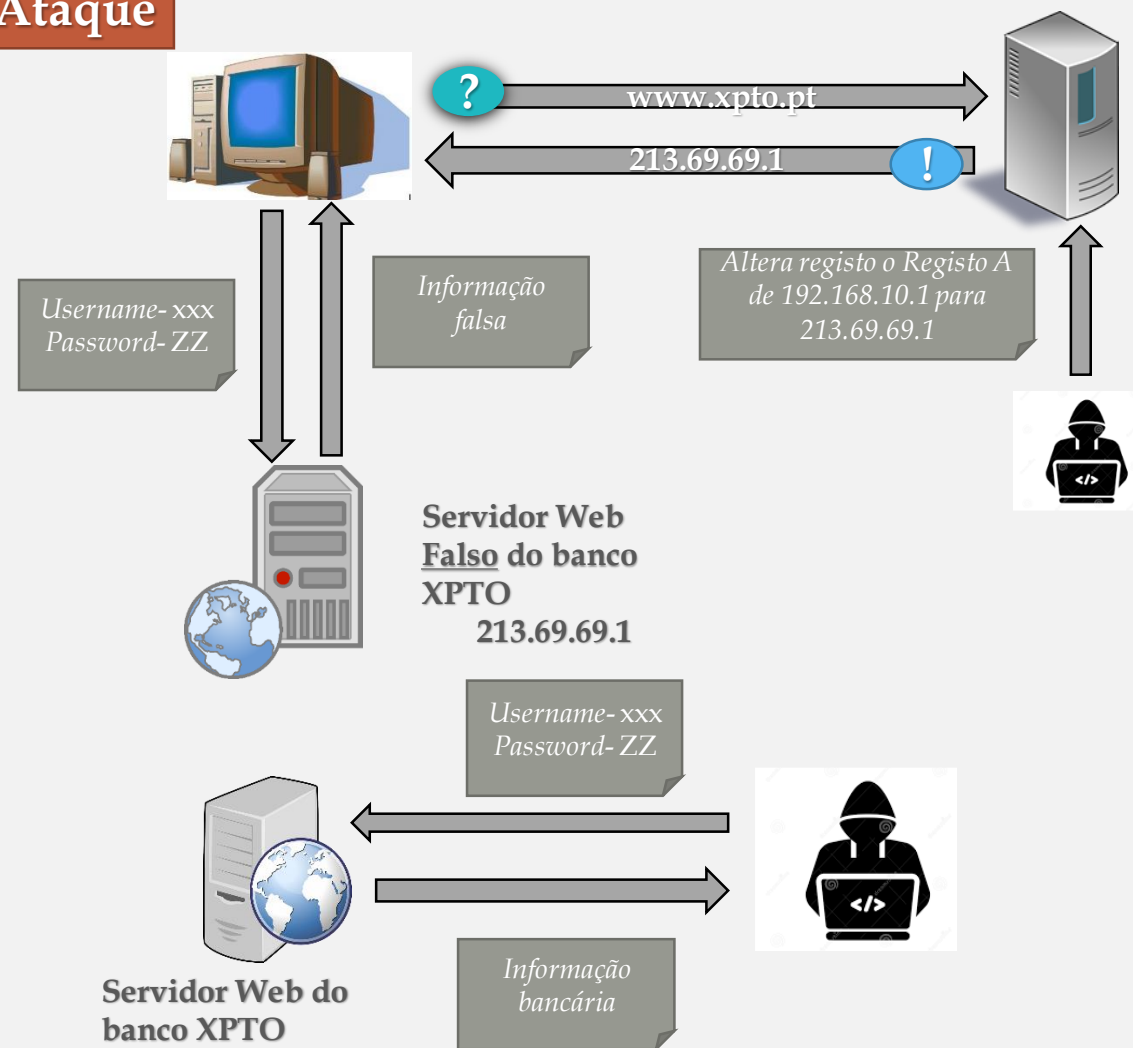


# Segurança – Ataque *cache poisoning*

## Situação Normal

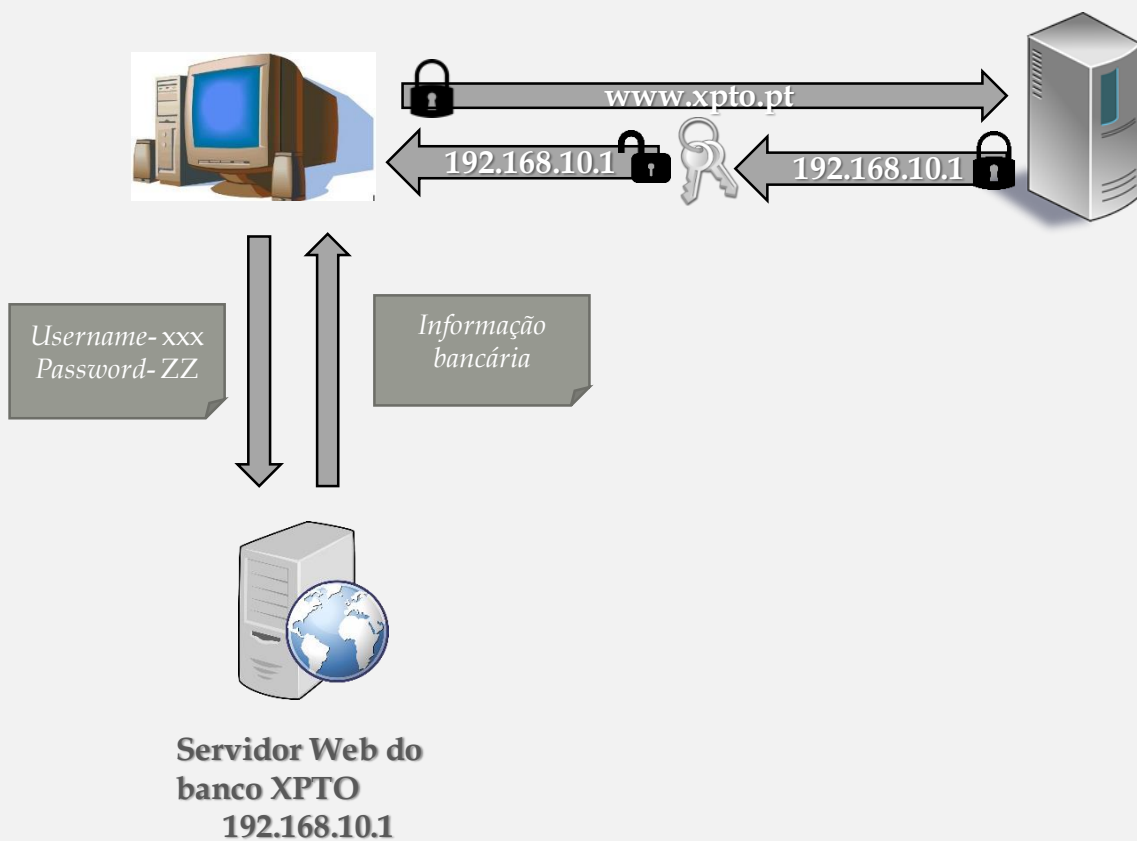


## Ataque

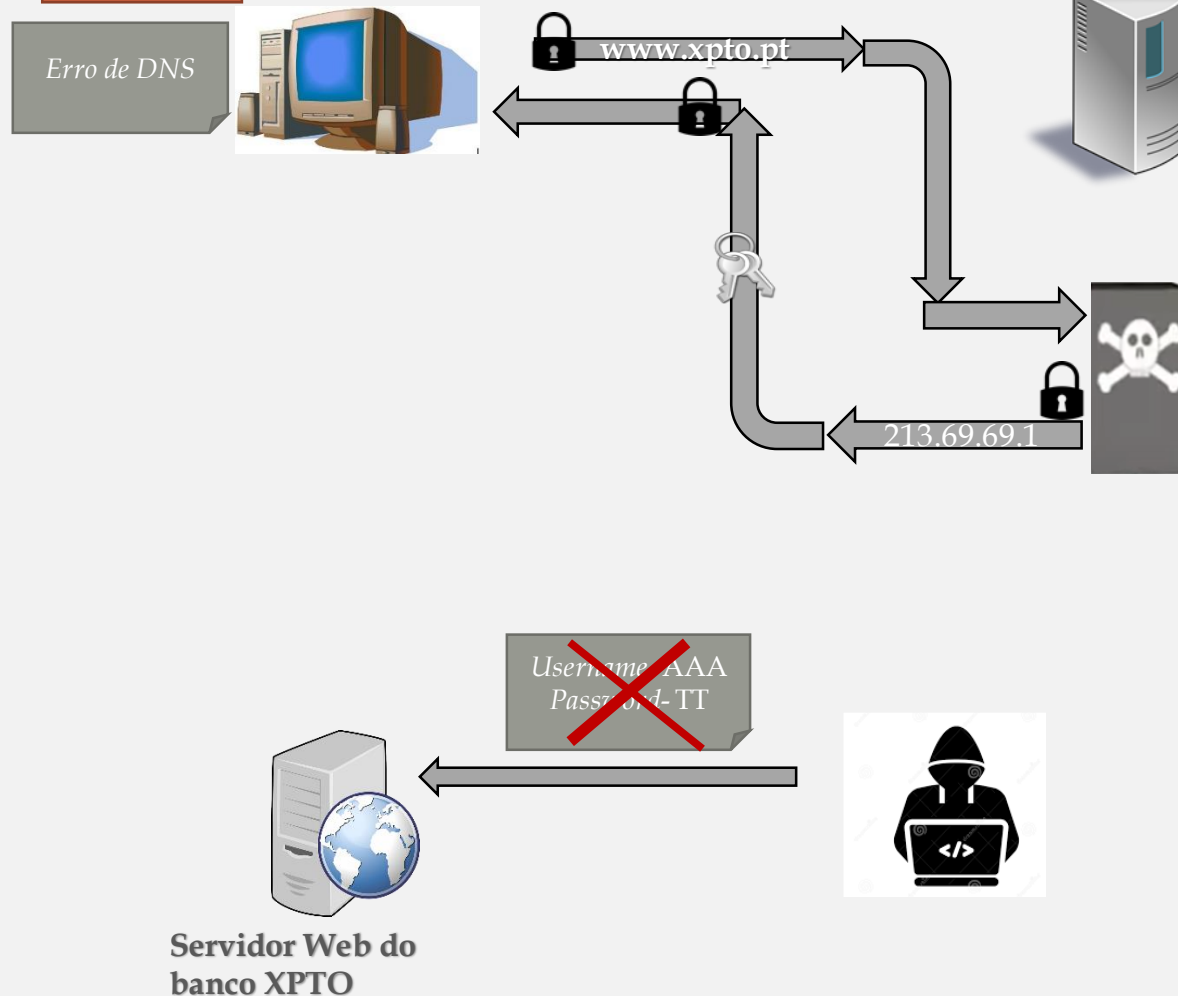


# Segurança – A solução DNSSEC

## Situação Normal



## Ataque



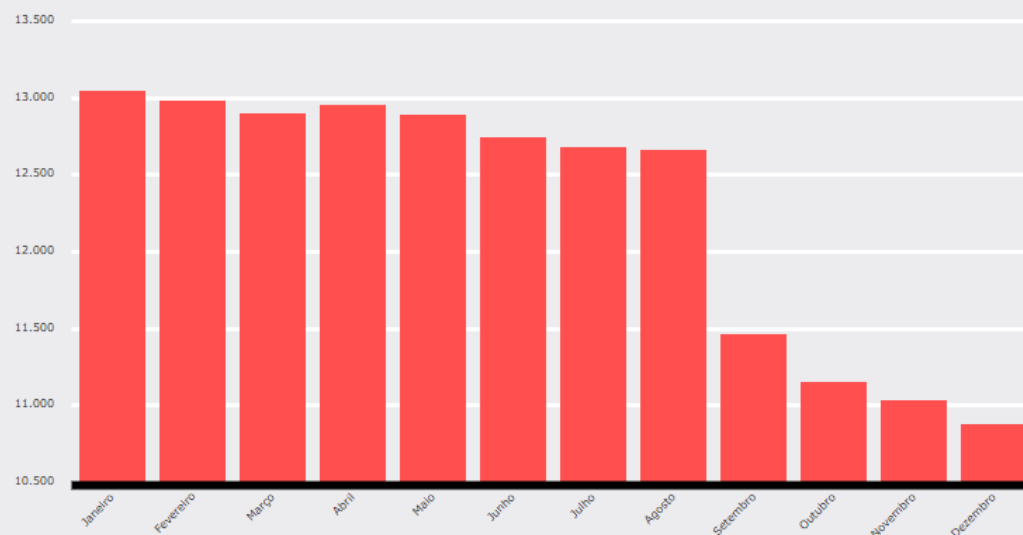
# Segurança

---

- O que garante?
  - Origem (Autenticidade).
  - Integridade.
- O que não garante?
  - Confidencialidade.
  - Proteção contra ataques de negação de serviço.

# Segurança – Números em Portugal

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>



# Segurança

- O DNSSEC introduz registos adicionais que se dividem em quatro tipos diferentes:
  - DNSKEY - Chave pública;
  - RRSIG - Assinatura Digital do RRset;
  - NSEC/NSEC3 - Resposta autenticada da não existência de um domínio ou conjunto de Resource Records associado a um domínio;
  - DS - Síntese da chave pública que faz a ligação entre um domínio e subdomínio de modo a construir uma cadeia de confiança;

# Public DNS

- Quando a Google lançou no final do ano de 2009 o seu serviço público de DNS, este prometia ser o mais rápido, simples e robusto de utilizar.
- A ideia da empresa tornar a Internet ainda mais rápida, recorrendo a servidores distribuídos de DNS, mas que todos respondiam pelos mesmos endereços IP.
- Este projeto cresceu e atualmente é já um serviço maduro. É também já o serviço de DNS mais usado na Internet, processando por dia mais de 70 mil milhões de pedidos.



# Public DNS

- Que vantagens:
  - Performance
  - Segurança
  - Taxa de acertos
- Pode ver mais detalhes deste serviço em
  - <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

## **Comodo Secure DNS**

8.26.56.26

8.20.247.20

## **Opennicproject**

151.236.6.156

118.88.20.195

## **OpenDNS**

208.67.222.222

208.67.220.220

## **SafeDNS**

195.46.39.39

195.46.39.40

## **DynDNS**

216.146.35.35

216.146.36.36

## **Dnsadvantage**

156.154.70.1

156.154.71.1

# Atualizações dinâmicas

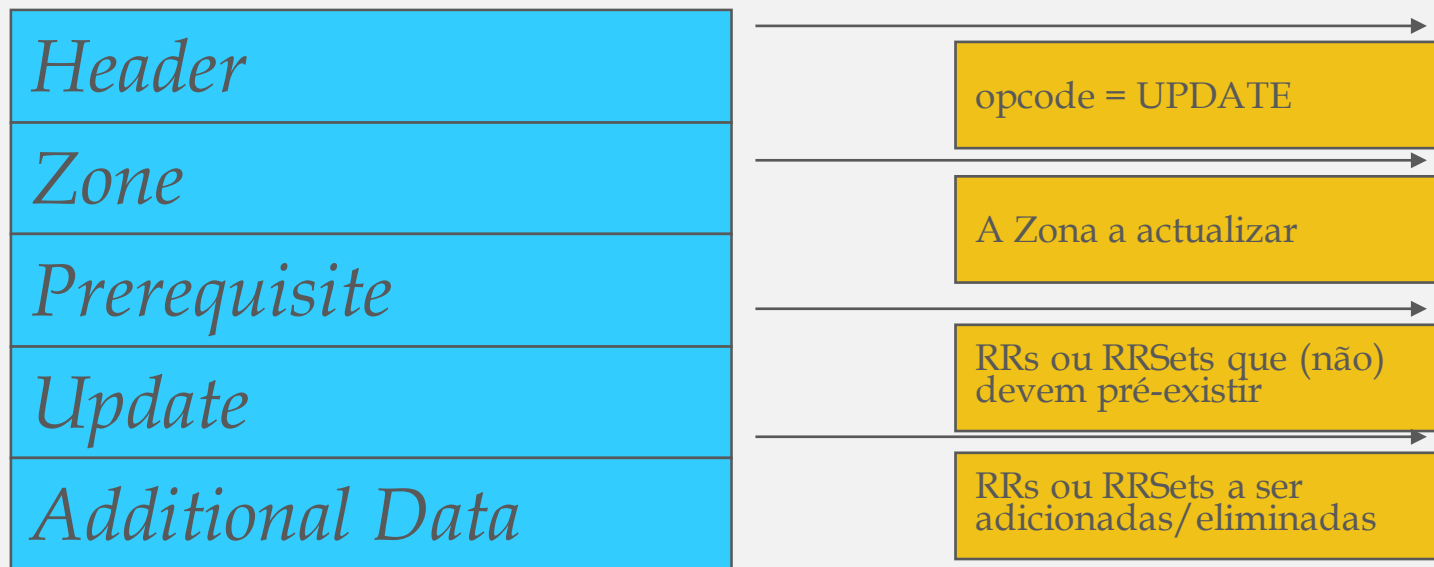
- O DNS é um serviço de diretoria que assume que a informação nas Zonas muda muito raramente.
- É, portanto, aceitável que o mecanismo de atualização dos ficheiros de Zona seja exterior ao próprio protocolo (geralmente por edição manual dos próprios ficheiros).
- Contudo, em ambientes com endereços dinâmicos (por exemplo: DHCP) torna-se útil um sistema de resolução de nomes que se atualize também dinamicamente.
- Estas atualizações podem ser requeridas pelos clientes ou por servidores de DHCP.
- Os serviços de DNS presentes nos sistemas operativos mais recentes permitem atualizações dinâmicas.

# Atualizações dinâmicas

- O RFC 2136 define uma nova operação (opcode = UPDATE) que vai permitir:
  - adicionar ou eliminar RRs ou RRSets a uma zona específica
  - especificar pré-requisitos a verificar para efetivar tais operações de atualização:
  - a existência prévia (ou não) de um RRSet
  - a existência prévia (ou não) de uma RR específica
- A operação UPDATE apenas se verifica se todos os pré-requisitos forem verificados e nunca em paralelo com outra operação de UPDATE.

# Atualizações dinâmicas

- Formato do pacote do UPDATE

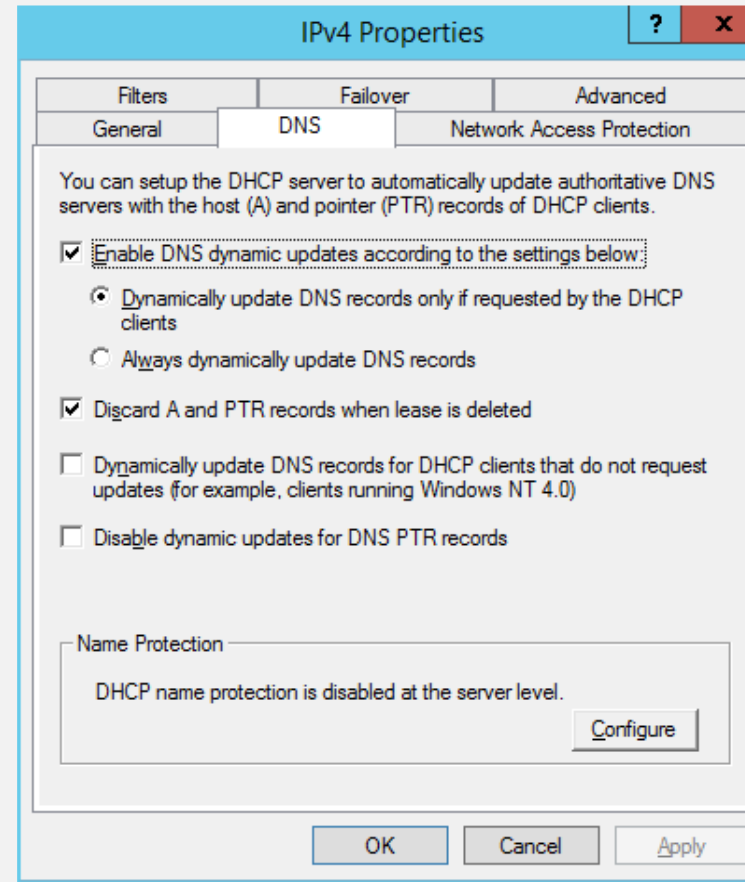
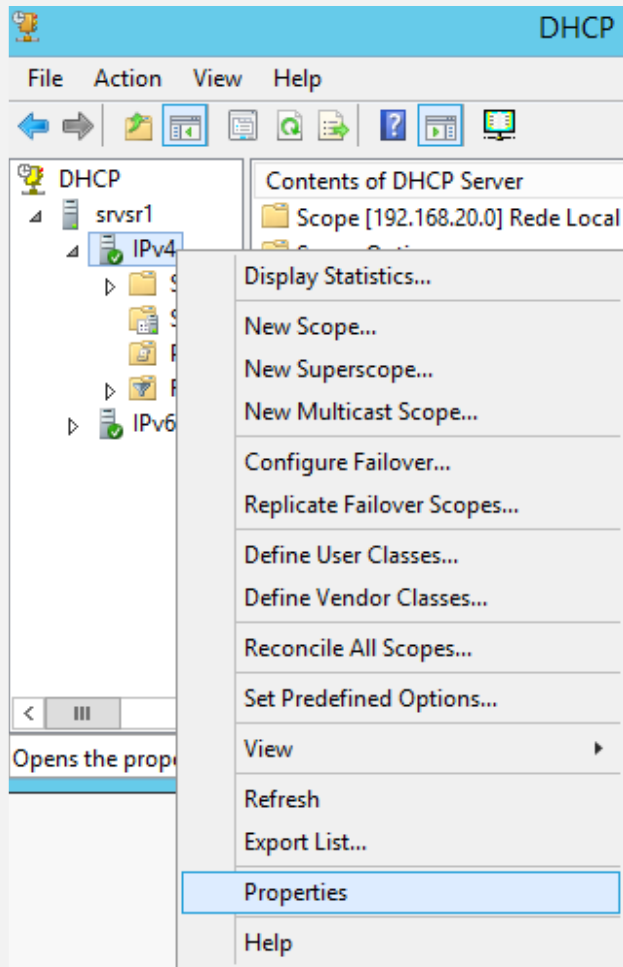


# Atualizações dinâmicas

- O requisitante de uma operação de UPDATE (e.g. servidor DHCP) deve tentar dirigir o pedido diretamente 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.



# Atualizações dinâmicas - DHCP - DNS



# Dúvidas e Referências



# Referências - Vídeos

- **Governança da Internet e domínios**

- <https://youtu.be/GGhAXVKlUfo> - acessado em abril de 2020

- **Como funciona o DNS?**

- <https://www.youtube.com/watch?v=ACGuo26MswI> - acessado em abril de 2020

- **A importância do DNS na sua rede?**

- <https://www.youtube.com/watch?v=epWv0-eqRMw> - acessado em abril de 2020

# 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