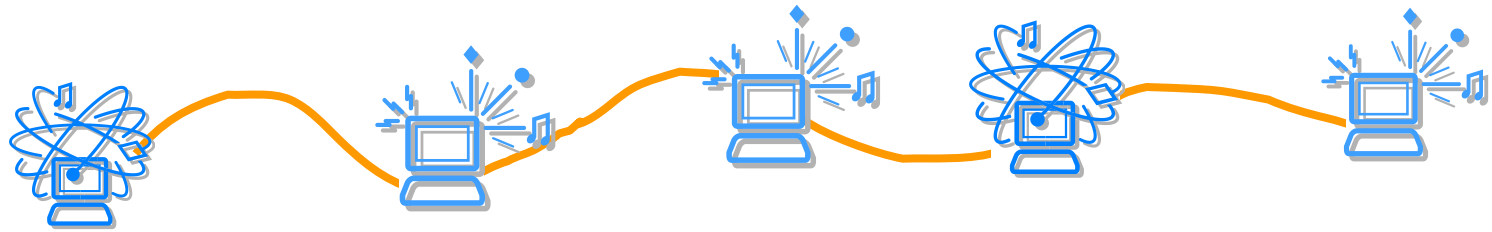
Sistema de Distribuição de Nomes de Domínios (DNS)



Instituto Superior de Engenharia de Lisboa

Departamento de Engenharia de Electrónica e Telecomunicações e de Computadores

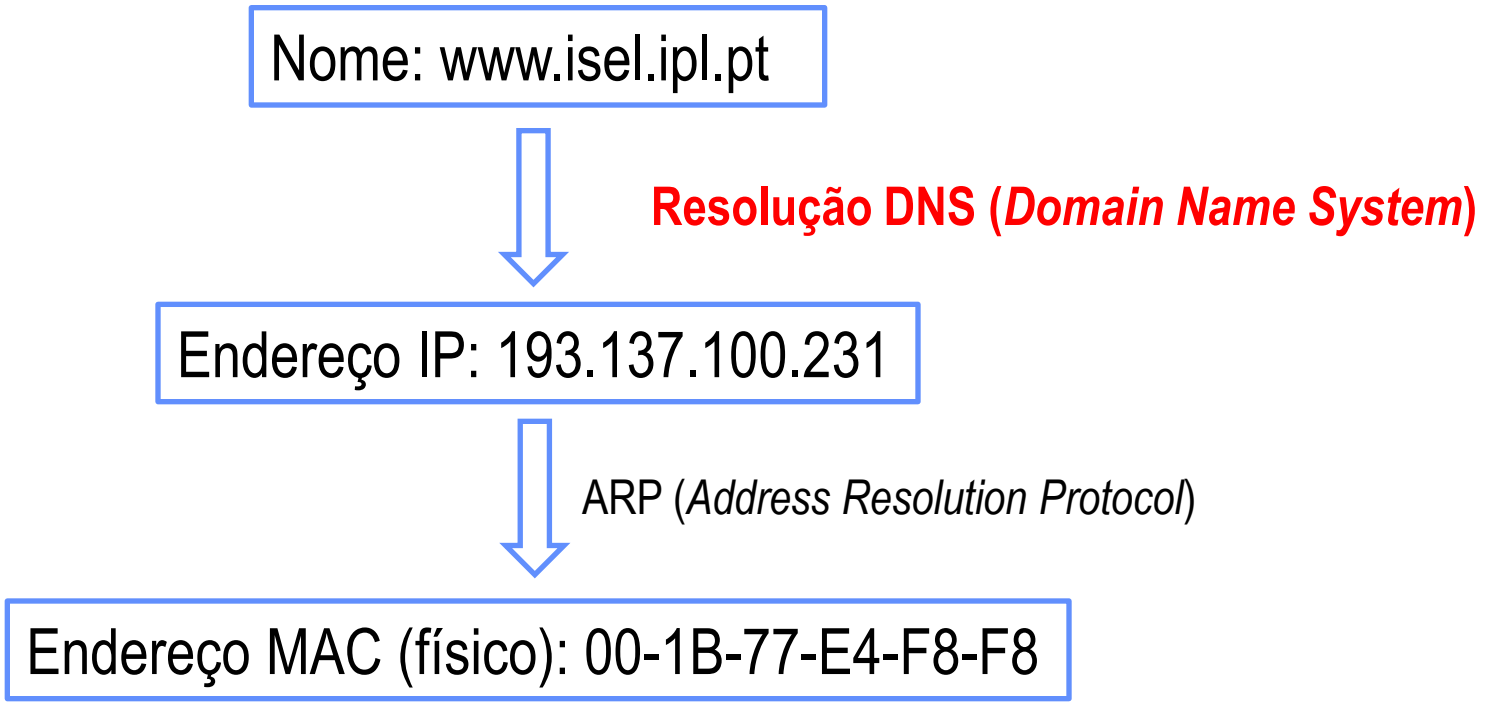
Redes de Computadores

Sumário: *Domain Name System* (DNS)

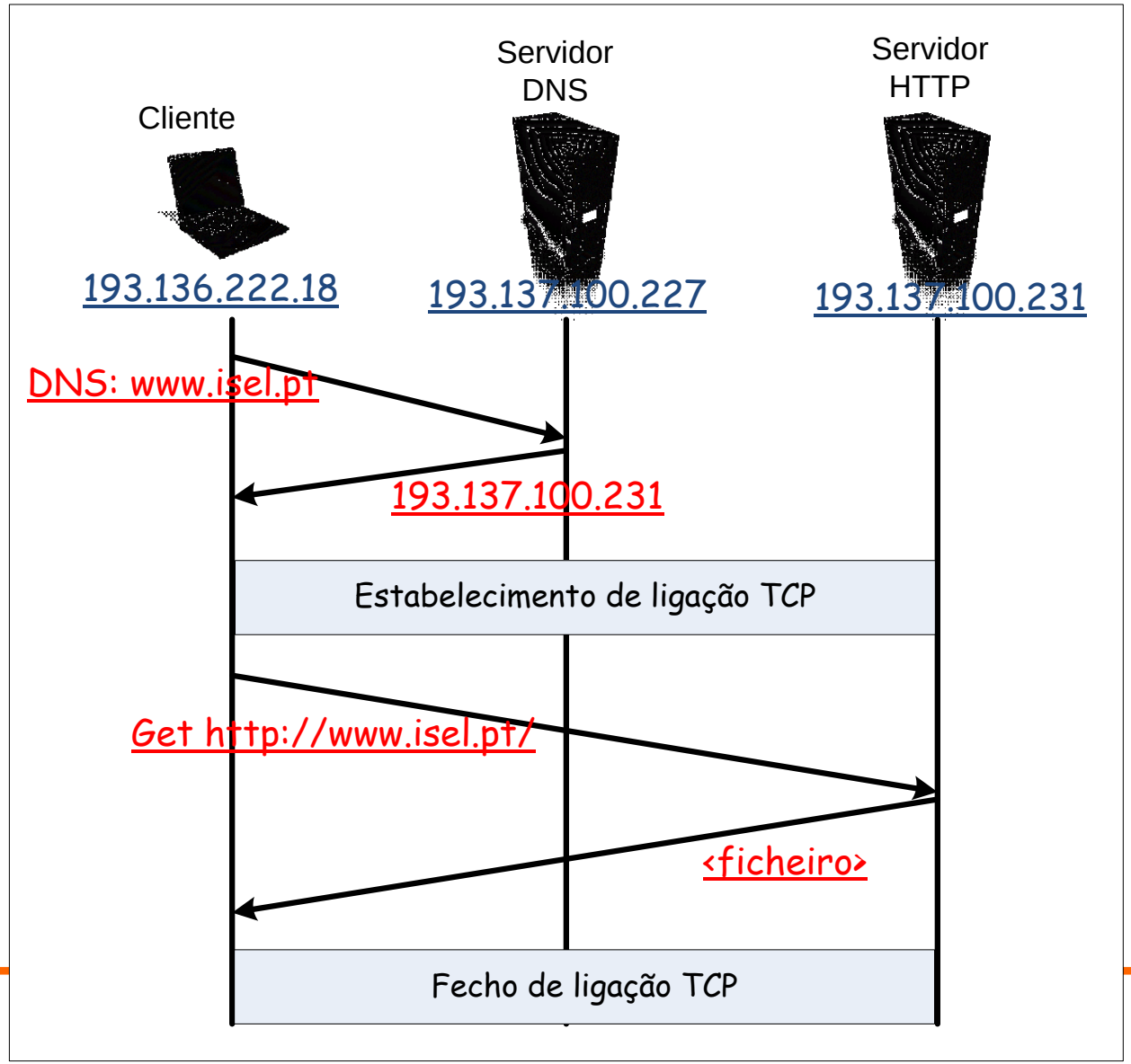
- Contexto
- Introdução ao DNS
- Hierarquia de nomes
- Hierarquia de servidores
- Processo de resolução de nomes
- Protocolo DNS
- Arquitectura de servidores
- Balanceamento de carga
- Distribuição de conteúdos
- Segurança

Contexto

- De uma forma geral existem múltiplos mapeamentos:



DNS: para que é preciso ?

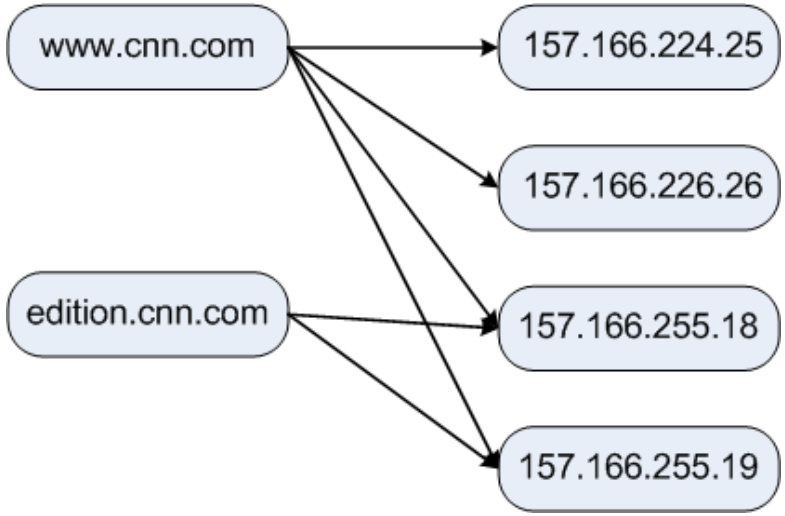


Introdução ao *Domain Name System* (DNS)

- Identificação das máquinas na rede:
  - Endereço IP de 32 bits: utilizados no endereçamento de datagramas
    - Formato fácil de processar pelos computadores
  - Nome (p.e. www.isel.pt) utilizados pelos humanos
    - Fácil memorização pelos humanos
- **Problema**: como mapear um nome num endereço IP ?
- *Domain Name System*:
  - Implementa uma função essencial para o funcionamento da Internet a uma escala planetária !
  - Base de dados distribuída implementada num conjunto de servidores
  - Protocolo do nível de aplicação que permite o processo de resolução de nomes
  - Pode ser utilizado para outros serviços, ex. tradução nº telefone - endereço IP

Mapeamento DNS

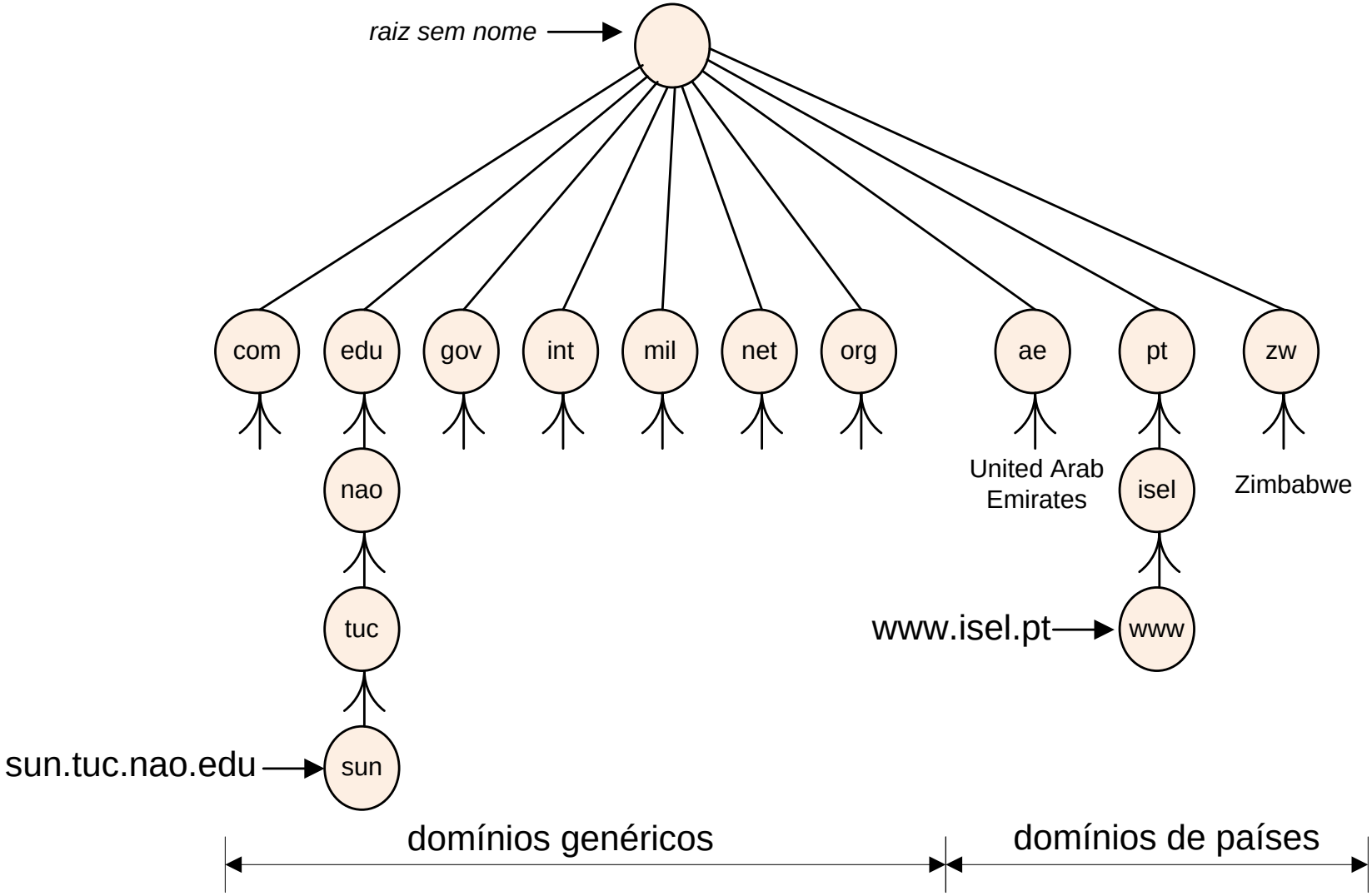
- Múltiplos nomes podem ser mapeados no mesmo endereço IP:
  - www.cnn.com e edition.cnn.com podem ser mapeados para a mesma máquina (i.e., o mesmo endereço IP)
- Um nome pode ser mapeado em múltiplos endereços IP:
  - www.cnn.com pode ser mapeado em múltiplas máquinas



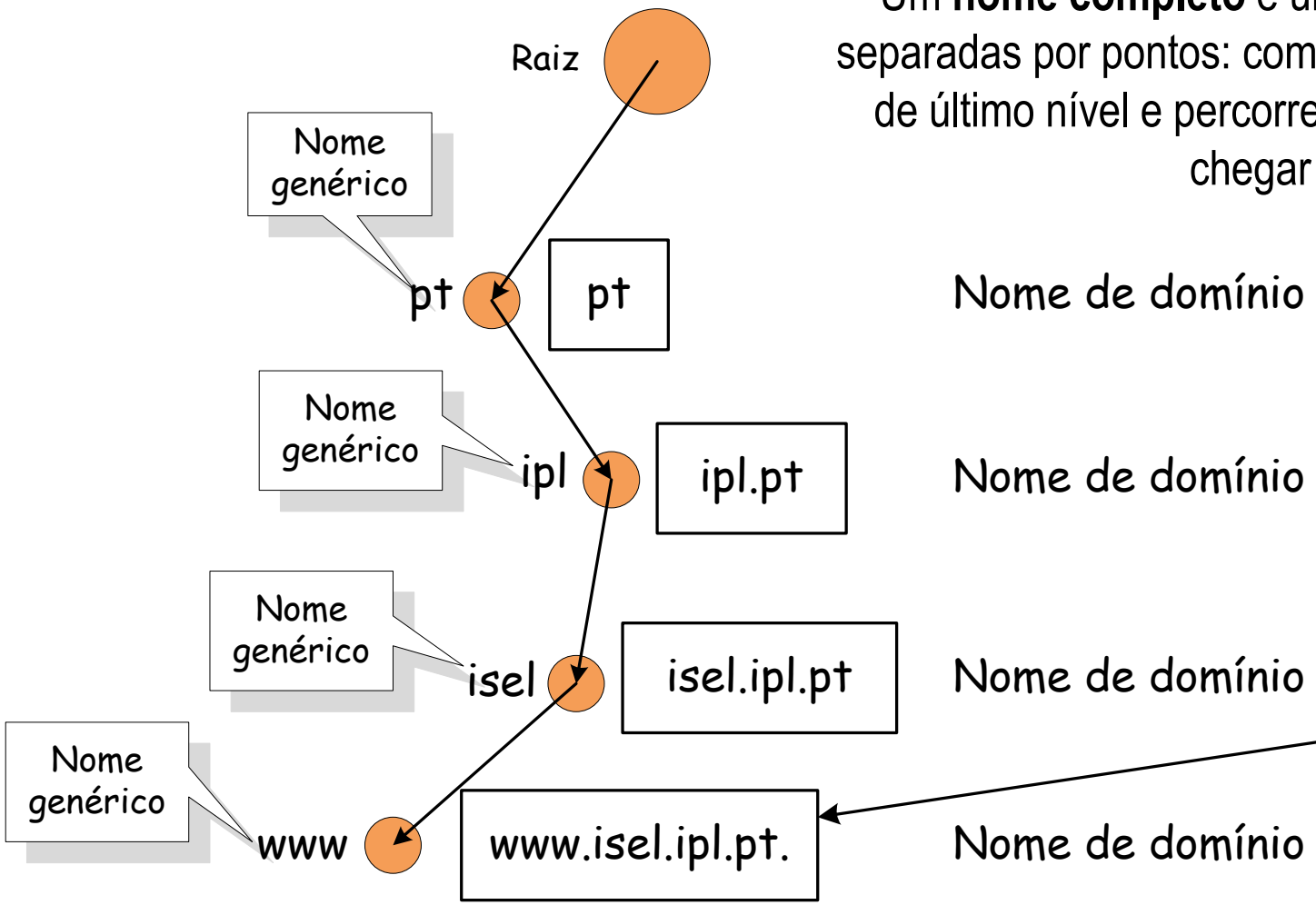
Nomes genéricos (*labels*)

Nome genérico	Descrição
com	Organizações comerciais
edu	Instituições de ensino pós-secundario
gov	Instituições governamentais
mil	Grupos militares
org	Organizações sem fins lucrativos
net	Infraestrutura de rede
int	Organizações internacionais
aero	Companhias de navegação aérea
biz	Negócios ou firmas (semelhante ao com)
coop	Cooperativas
info	Locais de informação sem restrições
museum	Museus
name	Famílias e indivíduos
pro	Profissões

Hierarquia de nomes

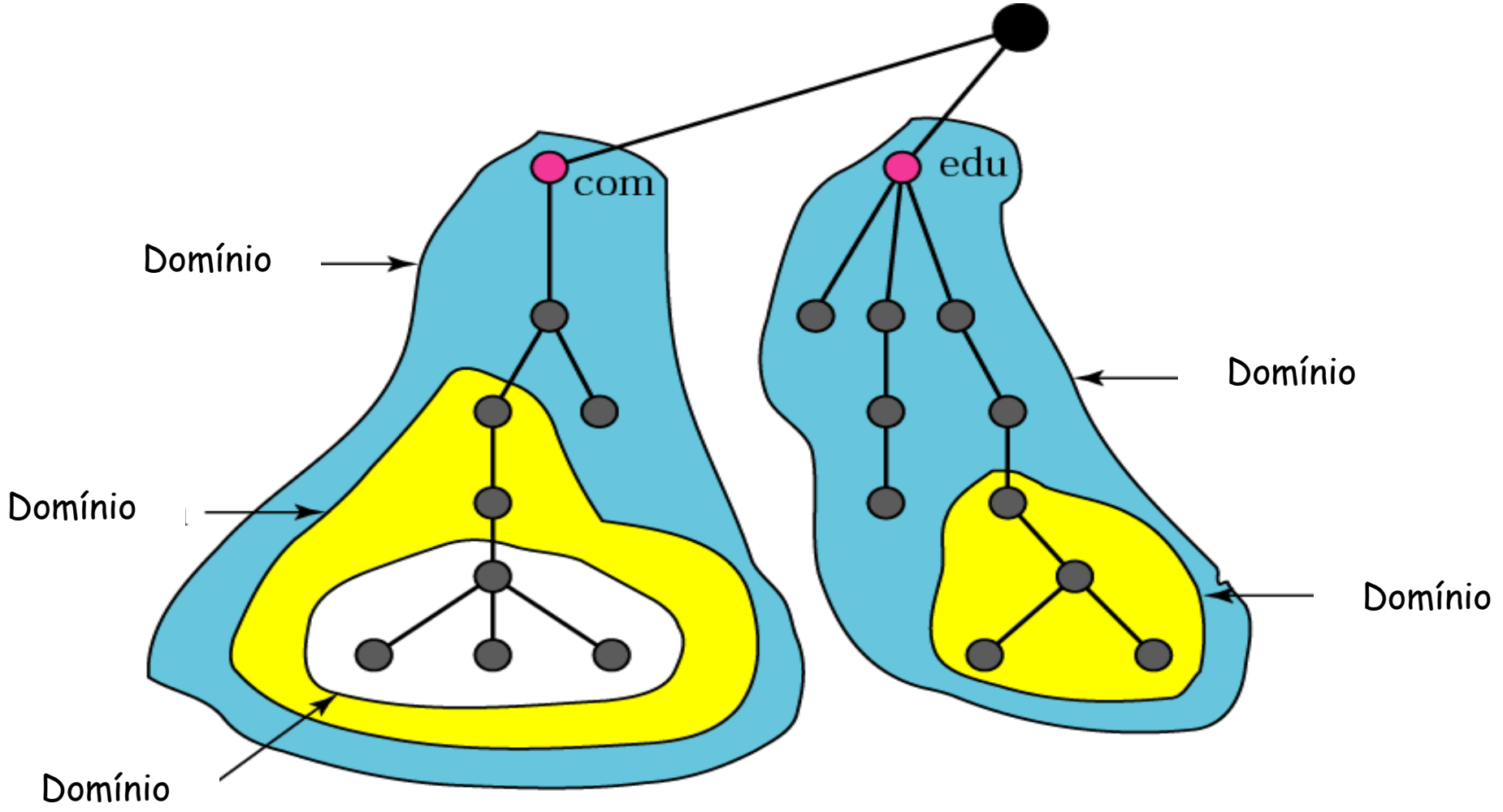


Nomes de domínios e *labels*



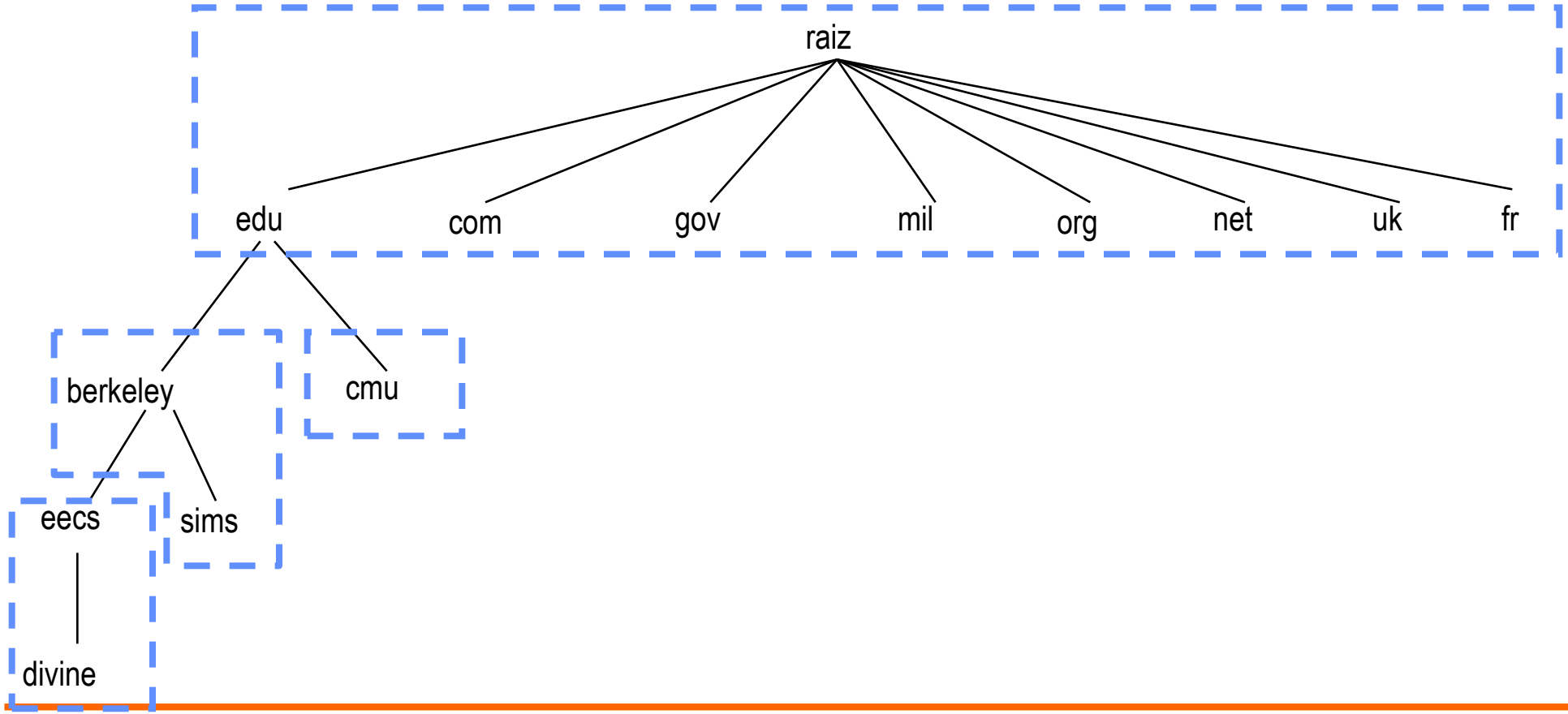
Um **nome completo** é uma sequência de *labels* separadas por pontos: começa com a *label* de um nó de último nível e percorre um ramo da árvore até chegar à raiz

Domínios

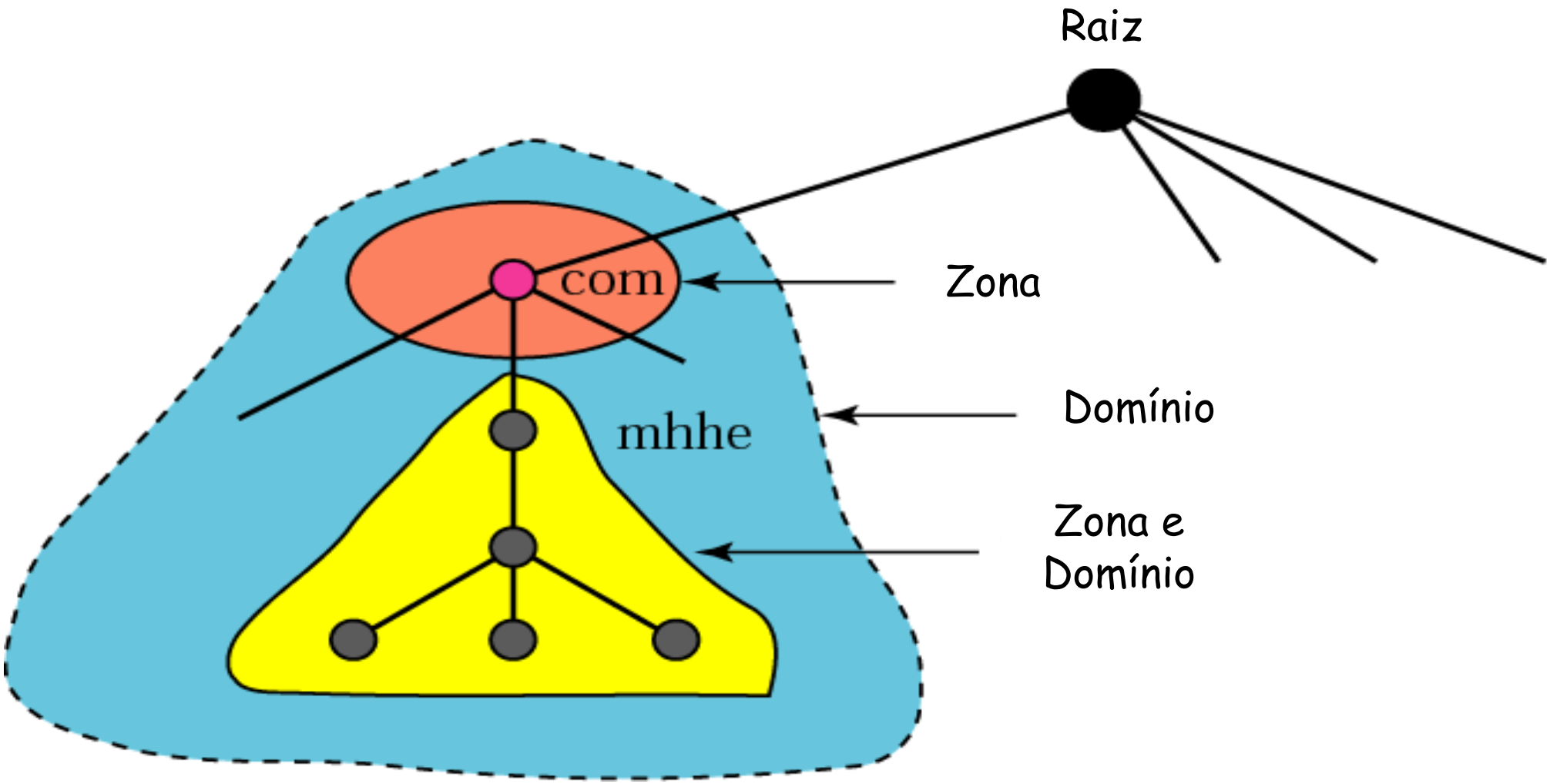


Autoridade: zonas

- Uma zona corresponde a uma autoridade administrativa que é responsável por uma parte da hierarquia de nomes



Zonas e domínios



Sistema de nomes DNS

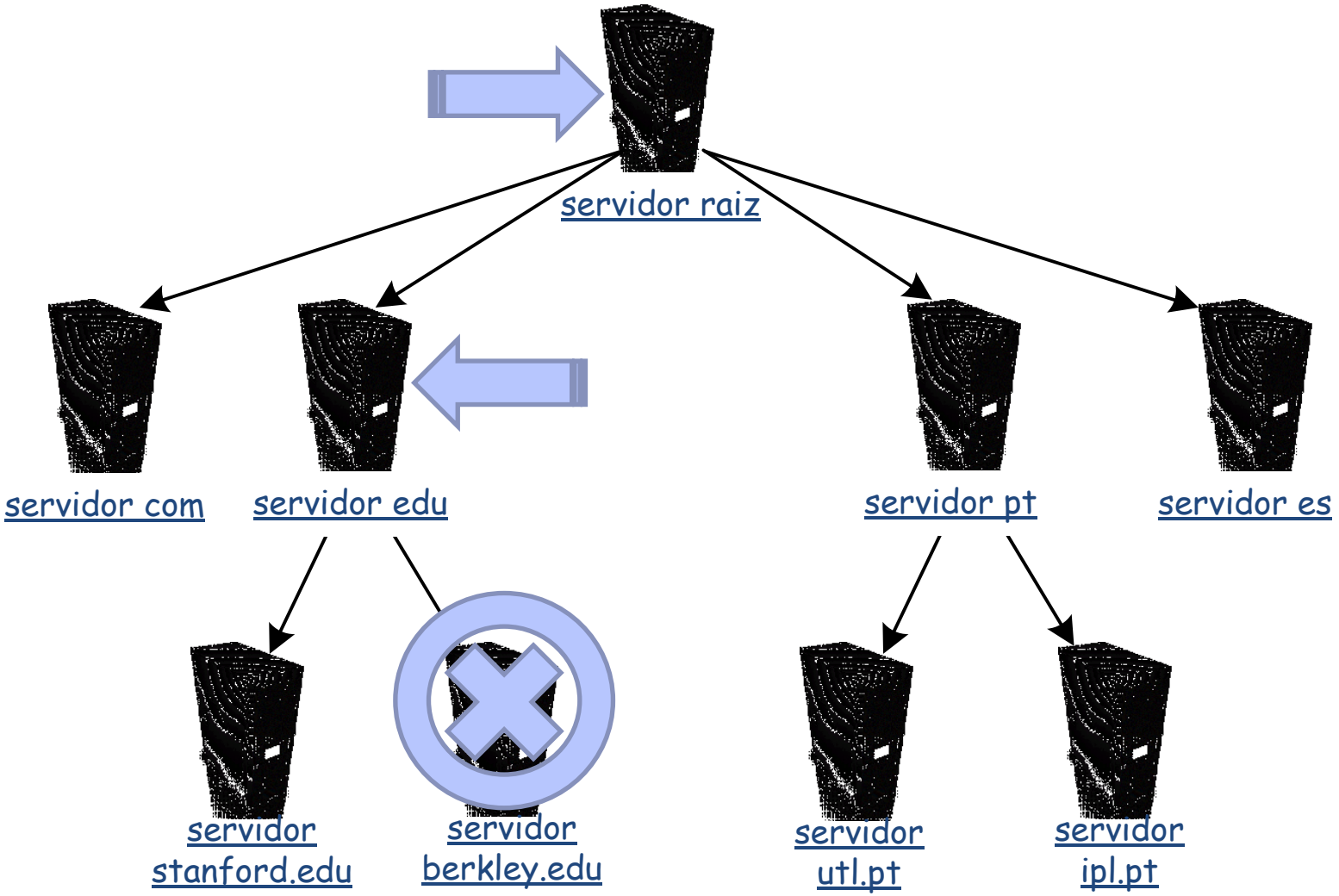
- Exemplos de serviços DNS:
  - Tradução de um nome de uma máquina para um endereço IP
  - Nomes canónicos
  - Endereçamento (*alias*) de servidores de email
  - Distribuição de carga entre servidores web replicados
    - Conjunto de endereços IP para um só nome

- Centralizar o DNS ? Porque não ?
  - Volume de tráfego
  - Único ponto de falha
  - Distância à base de dados centralizada
  - Manutenção
  - Falta de escalabilidade

Hierarquia de servidores

- Os servidores DNS são organizados de forma hierárquica
- Autoridade: servidor com a responsabilidade de manter uma tabela de resolução para todos os nomes no espaço de nomes que controla
- Cada servidor tem autoridade sobre uma parte da hierarquia
  - Um único nó na mesma hierarquia de nomes não pode ser dividido
  - Um servidor mantém apenas um subconjunto de todos os nomes
  - Necessita de conheçer outros servidores que são responsáveis por outras partes da hierarquia

Base de dados hierárquica e distribuída



Servidores de nomes raiz

- Servidores de nomes raiz: contactados por outros servidores de nomes quando estes não conseguem resolver o nome

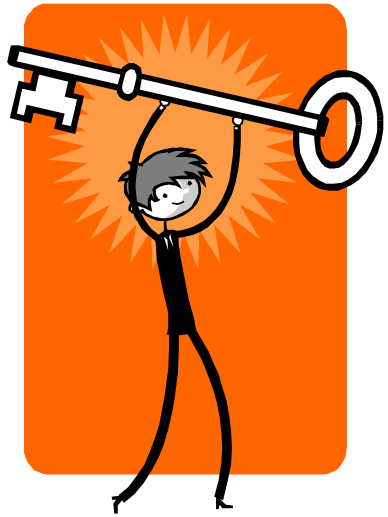
13 servidores raiz conheçidos (A-M)

Servidores TLD

- Servidores *top-level domain* (TLD):
  - Responsáveis por com, org, net, edu, ..., e todos os domínios de países de TLD pt, uk, fr, ca, jp, ...
  - Os servidores TLD são conhecidos pelo servidor de nomes raiz
  - Registos de topo (por exemplo isel.pt) são realizados nos *registrars*
  - Os operadores de registos mantêm a base de dados de nomes de domínios actualizada para um ou mais TLDs dos quais são responsáveis
- Alguns exemplos:
  - *Network Solutions* mantém os servidores para o TLD com
  - FCCN mantém os servidores para o TLD pt e alberga fisicamente um servidor raiz "F" gerido pela ISC

Servidores autoritários

- Servidores de DNS autoritários:
  - Servidores de DNS das instituições (empresas, universidades, etc) que fornecem mapeamentos autoritários (end. IP – nome) para algumas máquinas da instituição (e.g., web, mail).
  - Podem ser mantidos pela instituição ou pelo fornecedor de conectividade da Internet (ISP)

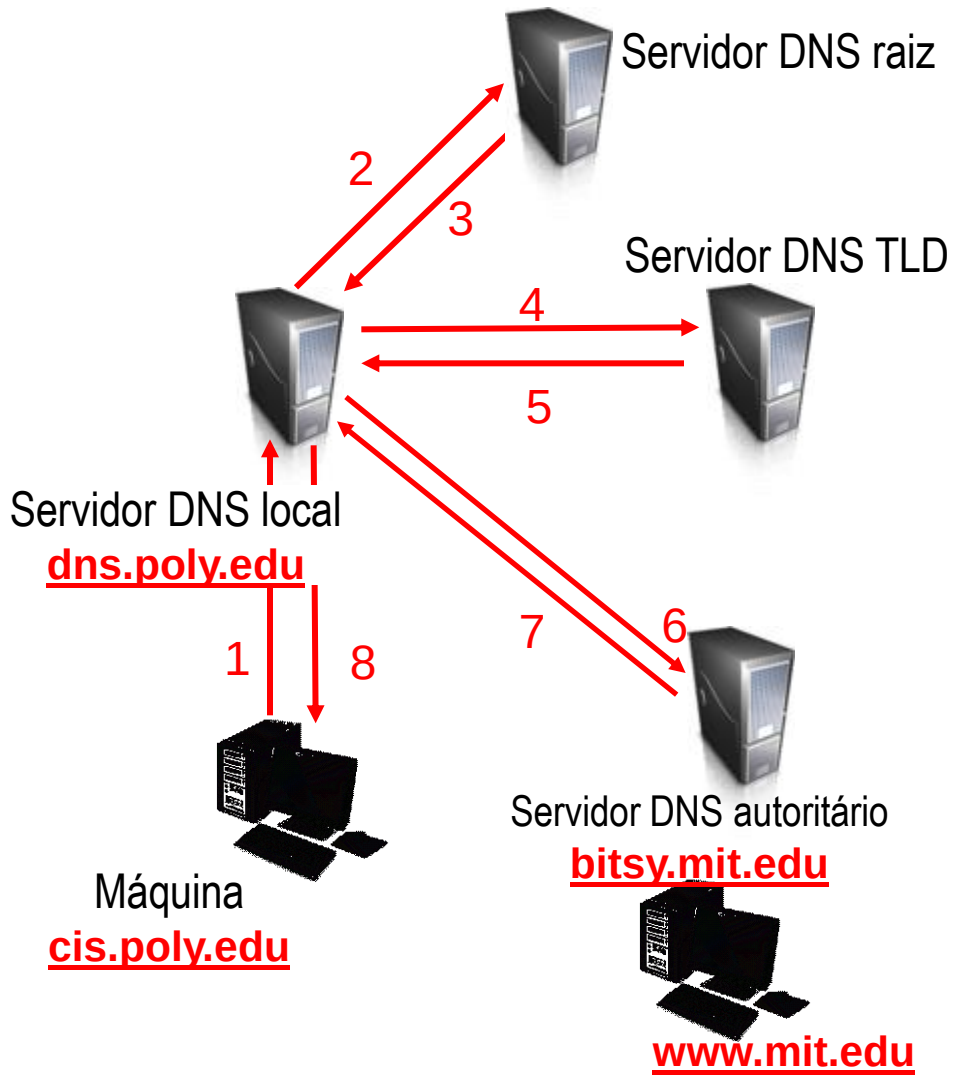


Servidores de nomes local

- Não faz parte da hierarquia de servidores
- Cada ISP (residencial, empresa, universidade) tem um
- Quando uma máquina faz um pedido de DNS, este é enviado para o servidor de nomes local
  - Funciona como um proxy, reencaminha os pedidos na hierarquia de servidores de DNS
- Conhece os servidores de nomes raiz

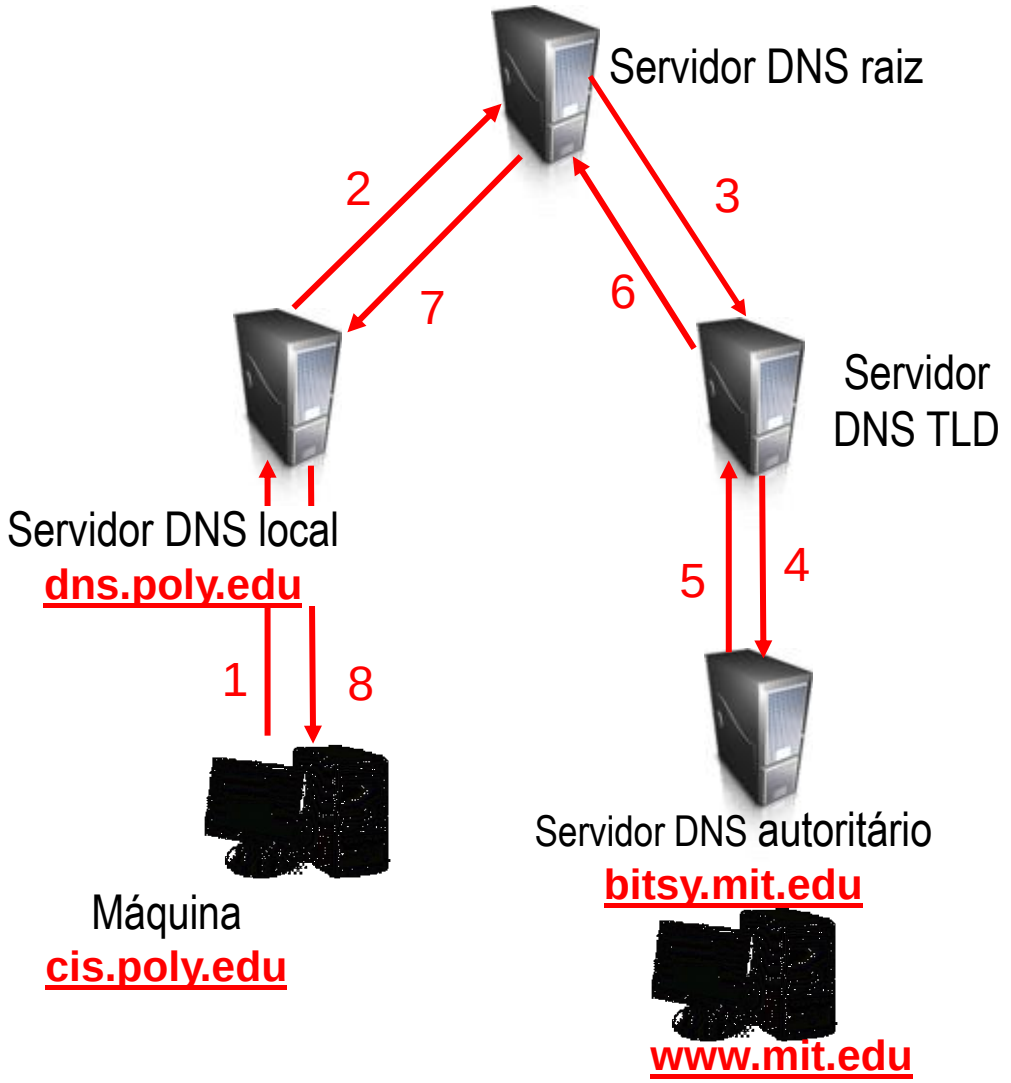
Processo de resolução de nomes: iterativo

- Máquina em cis.poly.edu quer o endereço IP de www.mit.edu
- Servidor de nomes local responde com a resposta final (endereço IP)
- Pedido iterativo:
  - Um servidor DNS pode responder com o nome do servidor DNS a contactar
  - "Eu não conheço este nome, mas sei qual é o servidor que o pode conheçer"



Processo de resolução de nomes: recursivo

- Coloca a tarefa de resolução do pedido no servidor contactado
- Carga elevada ?



Protocolo DNS: campos

- DNS: base de dados distribuída e organizada em campos RR (*resource records*)

  RR format: **`(Nome, Valor, Tipo, TTL)`**

- Tipo A:
  - **Nome** é o nome da máquina (*hostname*)
  - **Valor** é o endereço IP
- Tipo NS:
  - **Nome** é o domínio (p.e. foo.com)
  - **Valor** é o nome do servidor de nomes autoritário para aquele domínio
- Tipo CNAME:
  - **Nome** é um alias para algum nome canónico (nome real)
  - **Valor** é o nome canónico
  - Exemplo: www.ibm.com é na realidade www.ibm.com.cs186.net
- Tipo MX:
  - **Valor** é o nome do servidor de email associado ao **nome**

Protocolo DNS: tipos de RRs

Tipo	Abreviatura	Descrição
1	A	Endereço IPv4 de 32 bits. Utilizado para converter um nome de domínio num endereço IPv4
2	NS	Servidor de nomes. Identifica um servidor autoritário para uma zona.
5	CNAME	Nome canónico. Define uma *alias* para o nome oficial de uma máquina
6	SOA	Secção de autoridade. Marca o início de uma zona. Primeiro campo de um ficheiro de zona.
11	WKS	Serviços conhecidos. Define serviços de rede que a máquina fornece.
12	PTR	Resolução inversa. Permite converter um endereço IP num nome de domínio.
13	HINFO	Informação da máquina. Descrição do hardware e software de uma máquina
15	MX	Permite conhecer os servidores de email responsáveis pelo domínio.
28	AAAA	Endereço IPv6 de 128 bits. Utilizado para converter um nome de domínio num endereço IPv6.
252	AXFR	Um pedido para a transferência de toda a zona. Permite a replicação dos dados do DNS.
255	ANY	Um pedido para todos os campos.

Cache e actualização de RRs

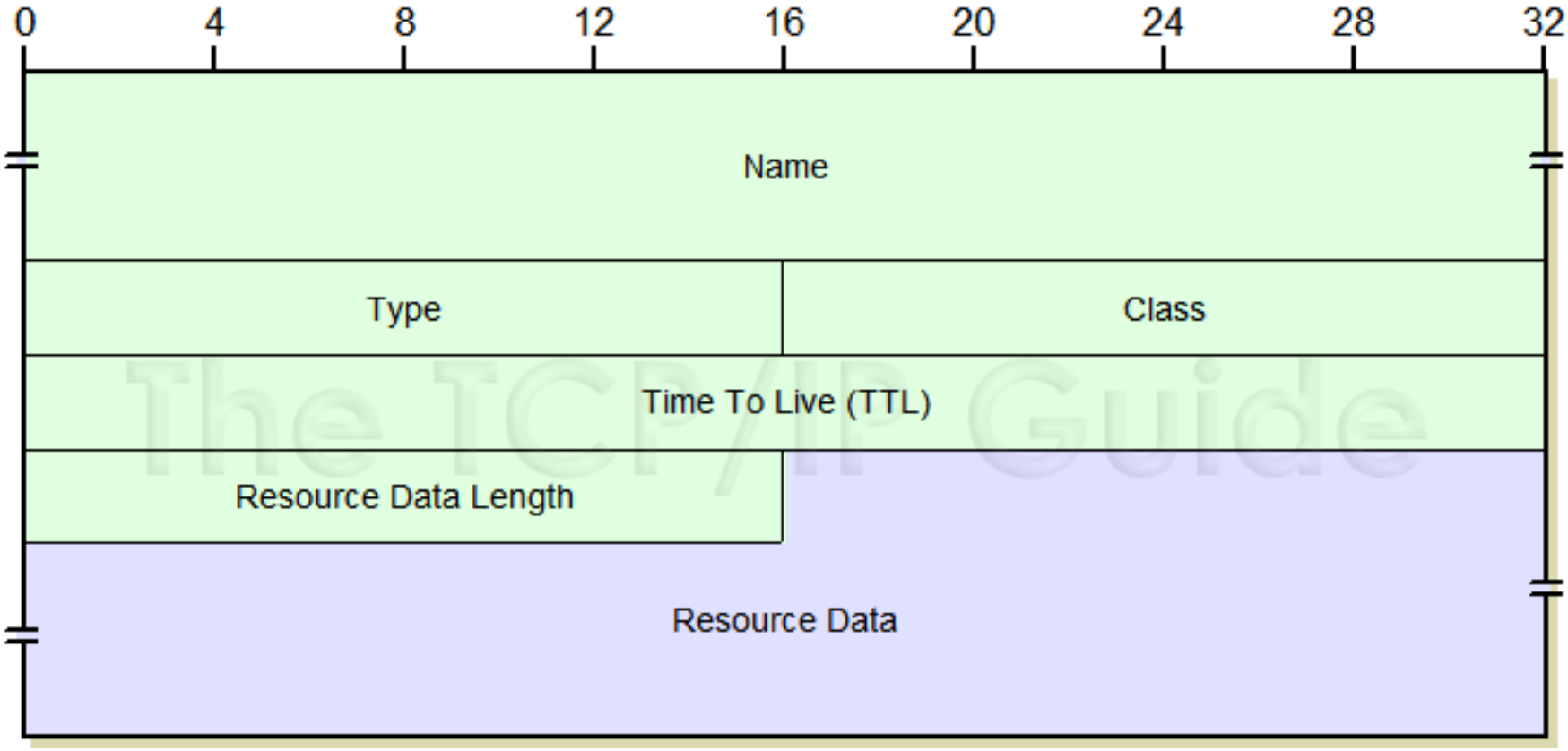
- O processo de resolução de nomes pode ser altamente ineficiente:
  - Cada máquina a contactar por nome gera um pedido de DNS
  - Um pedido de DNS pode passar por múltiplos servidores na hierarquia
- Servidores e máquinas usam um sistema de cache para reduzir o número de pedidos
  - Cache contém os mapeamentos recentemente resolvidos
  - As entradas na cache expiram depois de um certo tempo *Time to Live* (TTL)
  - Os servidores TLD são guardados em cache nos servidores de nomes locais
    - Desta forma alevia-se os servidores de nomes raiz

Protocolo DNS: mensagens

- Protocolo DNS: define mensagens de pedidos e respostas, ambas com o mesmo formato
- Cabeçalho:
  - Identificação: 16 bit para identificar pedidos, resposta usa o mesmo valor
  - Flags:
    - Questão ou resposta ?
    - Recursão desejada ?
    - Recursão disponível ?
    - Resposta é autoritativa ?

Identificação	Flags
Nº de questões	Nº de respostas
Nº de RRs autoritários	Nº de RRs adicionais
Questões	
Respostas	
Servidores autoritários	
Informação adicional	

Protocolo de DNS: mensagens



Protocolo DNS: transporte

- Protocolo UDP (porto 53):
  - Normalmente os pedidos e respostas DNS são transportados num datagrama UDP
  - As mensagens UDP de DNS são limitadas a 512 bytes
  - Mensagens maiores são truncadas e a flag *truncated* é activada

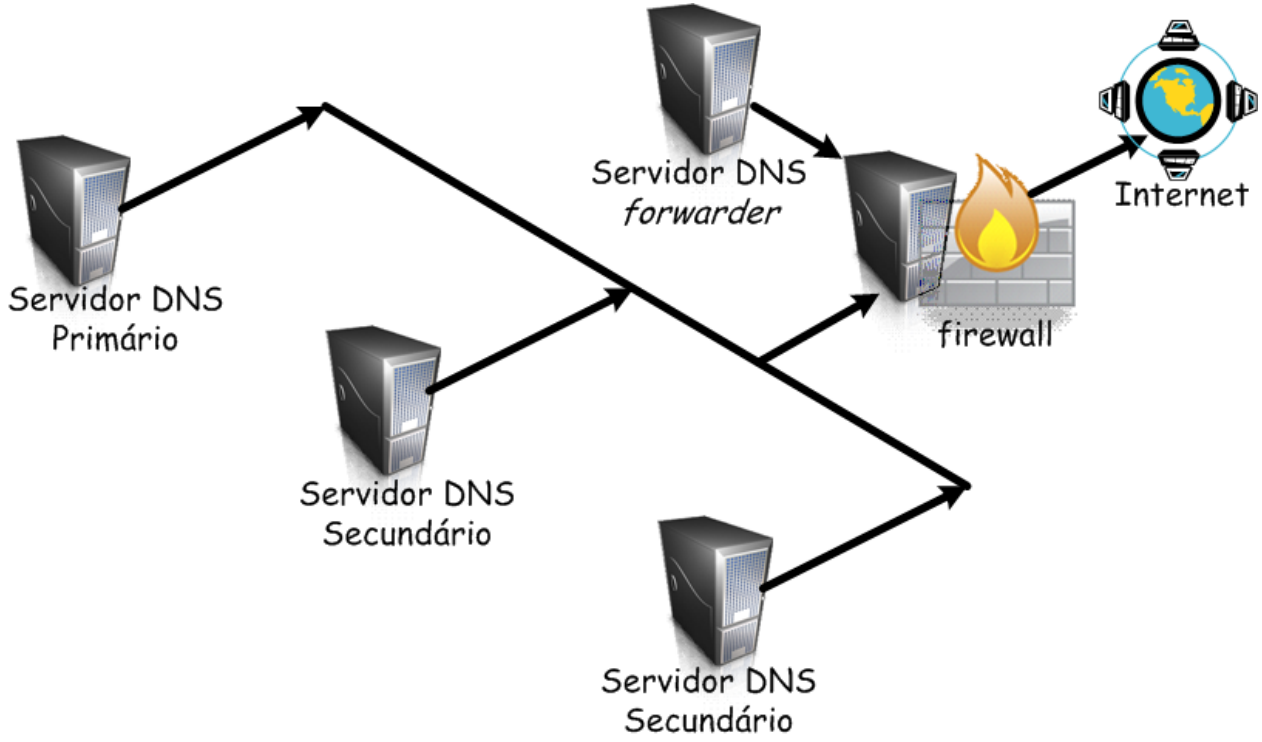
- Protocolo TCP (porto 53):
  - Para transferência de informação de zonas do servidor primário para os secundários (sincronização)
  - O cliente DNS estabelece uma ligação TCP com o servidor DNS para realizar a transferência
  - Quando é recebida uma resposta com a flag *truncated* activada

Arquitectura de servidores DNS

- Para receber pedidos de resolução da própria zona existem dois servidores de nomes: um servidor **primário** e zero ou mais servidores **secundários**
  - Redundância: permite a resolução mesmo que o servidor primário falhe
  - Manutenção: quando existem servidores secundários pode-se efectuar manutenção ao servidor primário sem impacto significativo
  - Balanceamento de carga: permite espalhar a carga em múltiplos servidores DNS melhorando assim a eficiência no acesso aos servidores de dados da zona
  - Eficiência: colocar servidores o mais perto possível dos clientes, por exemplo em ambos os lados de uma ligação WAN
- O servidor primário carrega toda a informação de um ficheiro local
- Um servidor secundário carrega toda a informação do servidor primário:
  - Transferência de zona
- Para encaminhar pedidos de resolução de outras zonas
  - Servidores locais: *Forwarders*, *Cache*, *Cache-Only*

Exemplo de uma topologia DNS

- Servidores DNS primário e secundários:
  - Normalmente autoritários para um ou mais domínios
- Servidores *forwarder* (local):
  - Encaminham as perguntas DNS realizados pelos clientes (com cache ou não)



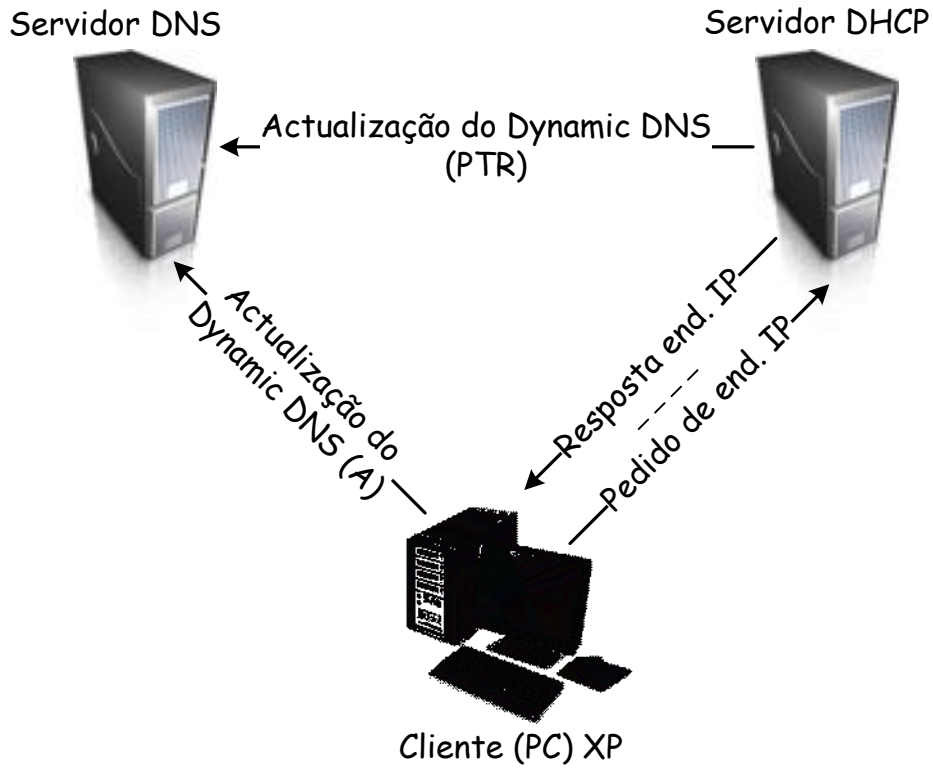
Inserir um registo no DNS

- Exemplo: nova empresa startup “Network Utopia”
  - Registar o nome networkuptopia.pt no DNS registrar (FCCN)
  - Providenciar nomes, endereços IP dos servidores de nomes autoritários (primário e secundário)
  - O operador de registo FCCN insere dois RRs no servidor TLD pt:
    - (networkutopia.pt, dns1.networkutopia.pt, NS)
    - (dns1.networkutopia.pt, 212.212.212.1, A)
- Criar um servidor autoritário (e.g. BIND) com um campo do Tipo A para www.networkuptopia.pt e um campo Tipo MX para networkutopia.pt
- De que forma se obtém o endereço IP de www.networkutopia.pt ?
- De que forma se obtém o servidor de email do endereço jascenso@networkutopia.pt ?

DNS dinâmico

- DDNS (*Dynamic Domain Name System*)
  - Mecanismo de actualização dos servidores de DNS quando máquinas ou domínios são adicionadas/apagadas/modificadas
  - Mecanismo de update/notify (RFC 2136)

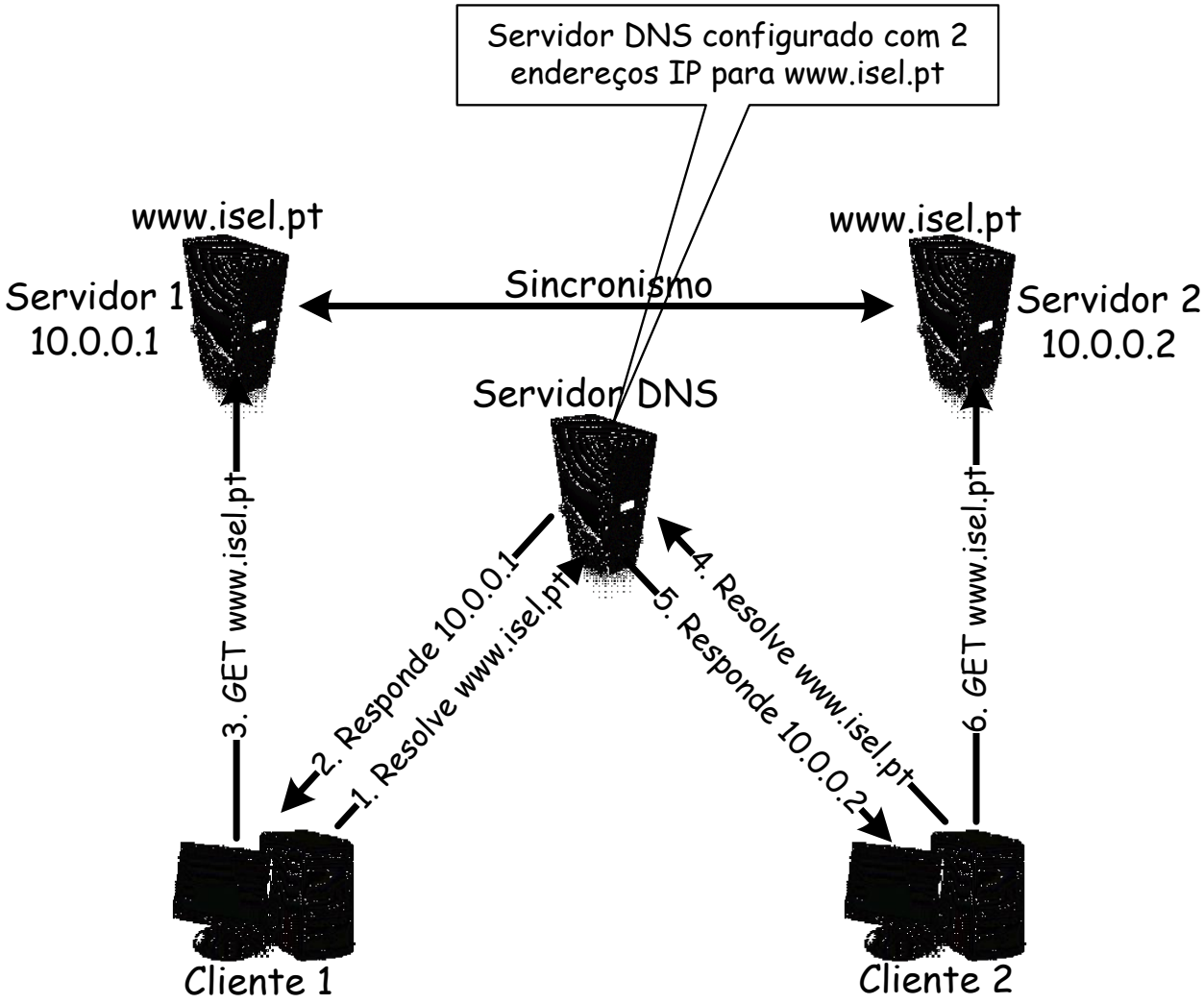
- Permite a interacção entre DHCP e DNS:
  - Actualização automática do endereço IP e nome (FQDN) de uma máquina



Balanceamento de carga

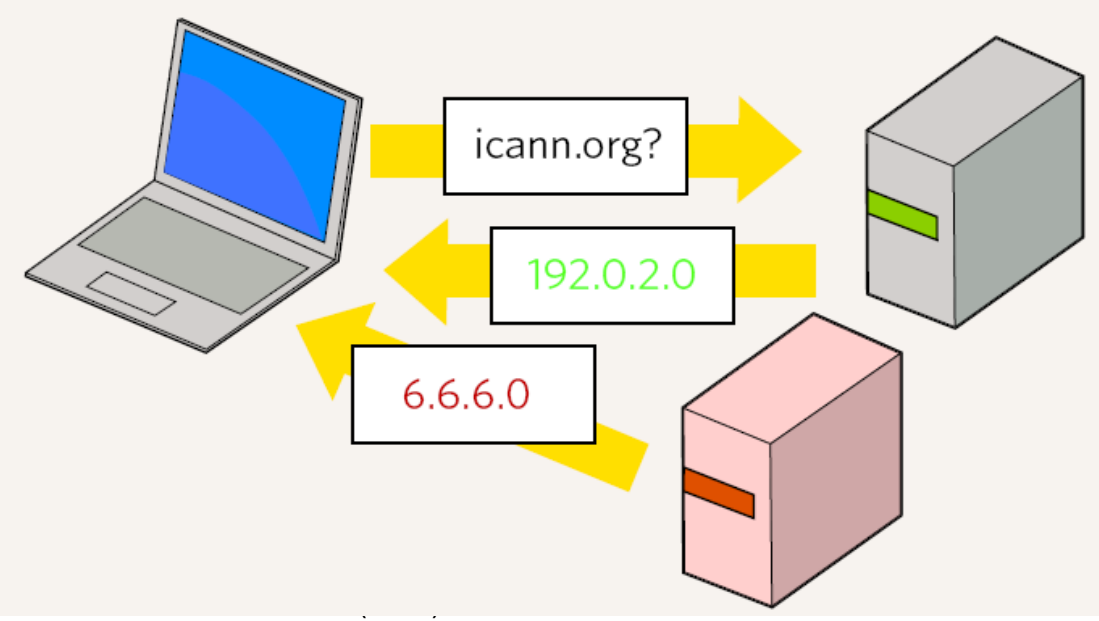
- Um balanceamento de carga simples pode ser conseguido no DNS utilizando múltiplos registos A para um nome:
  - Três servidores WWW assim configurados:
    - www.domain.tld. 60 IN A 123.45.67.1
      www.domain.tld. 60 IN A 123.45.67.2
      www.domain.tld. 60 IN A 123.45.67.3
  - Quando um *resolver* perguntar por www.domain.tld, o servidor DNS efectua uma rotação e responde à pergunta com os registos em ordem diferente:
    - www.domain.tld. 60 IN A 123.45.67.3
      www.domain.tld. 60 IN A 123.45.67.1
      www.domain.tld. 60 IN A 123.45.67.2
  - Os clientes irão utilizar o primeiro registo e ignorar os restantes
  - A carga é distribuída por três máquinas permitindo responder a um número maior de pedidos HTTP para www.domain.tld

Balanceamento de carga: exemplo



Segurança

- DNS é um serviço muito importante e por isso frequentemente atacado:
  - Direccionar os pedidos de www.bes.pt para um servidor web malicioso
  - Negação de serviço (DoS): muitos serviços de rede dependem do DNS
  - Guarda informação sensível sobre a rede: nº máquinas, endereços IP, etc..
- Possível solução: DNSSec = *DNS Security*
  - Garante comunicação segura entre servidores de nomes e clientes
  - Garante integridade de dados
  - A origem da informação é verificada



Referências

- “Computer Networking, a top down approach featuring the Internet (4th edition)”, James F. Kurose (Author), Keith W. Ross, Addison-Wesley Longman.

- “TCP/IP Protocol Suite”, Behrouz A. Forouzan, Sophia C. Fegan, McGraw-Hill Professional.