



DNS

An introduction

Ricardo Azevedo
ricardo.azevedo@ua.pt

Cofinanciado por:





DNS – O que é?

- Trata-se de uma base de dados distribuída para mapear nomes de máquinas (*hostnames*) em endereços IP e vice-versa (mas não só)
- Base de dados é distribuída por questões de escalabilidade.
- Servidores são responsáveis por domínios bem definidos;
- Servidores são organizados de forma hierárquica a definição de nomes é delegada em servidores de redes menores;
- Existem vários domínios de topo de descendem de um domínio raiz e que pode ter vários sub-domínios.

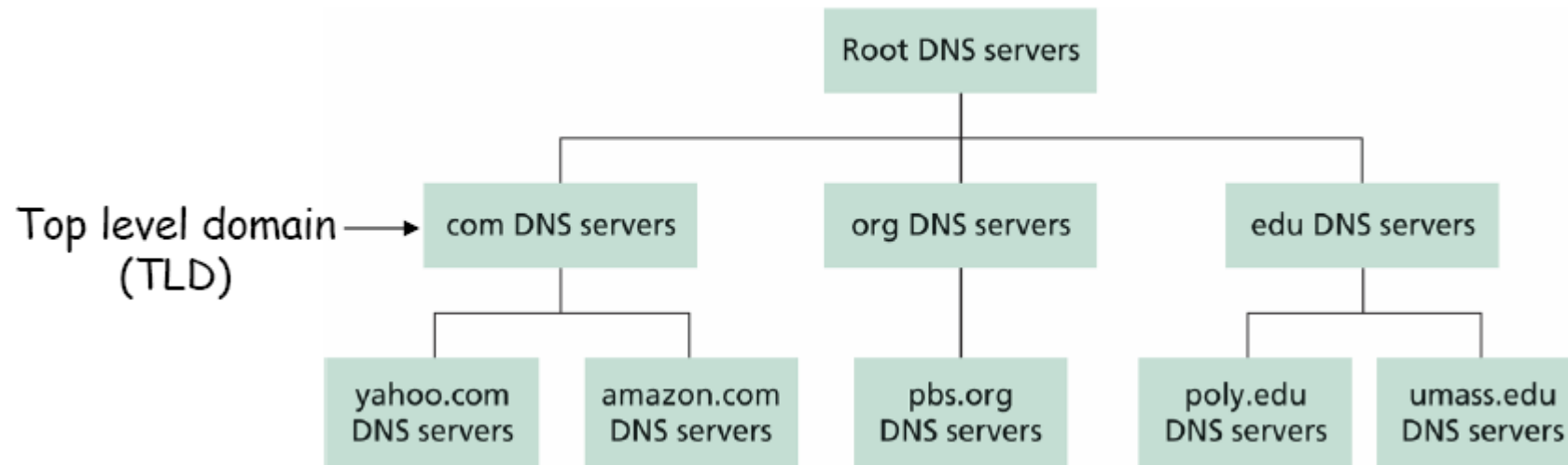


Conceitos básicos

- Dá-nos a funcionalidade de traduzir nomes em IPs e “vice-versa” (mas não só)
- Organização
 - Top-Level Domains (TLD)
 - Exemplos: .com; .net; .org
 - Second-Level Domains
 - Exemplos: google.com
- A ICANN (Internet Consortium of Assigned Names and Numbers) gere os TLD



Conceitos básicos





Conceitos básicos

- Os endereços são resolvidos baseados em **zonas**
- As **zonas** contêm informação dos computadores, serviços e endereços IPs de uma determinada colecção de máquinas
- Um DNS Server que tenha uma cópia *Readable e Writeable* de uma zona é considerado *authoritative*
- A existência de vários servidores DNS por domínio é possível, funcionando um como *authoritative* e o outro como secundário



Conceitos básicos (tipos de zonas)

- Existem dois tipos de zonas
 - *forward lookup zones* – resolvem nomes em IPs
 - %SystemRoot%\system32\dns existem ficheiros do tipo ASCII com a seguinte nomenclatura <nome do dominio>.dns (exemplo: guiapratico.local.dns)
 - Também pode estar dentro da AD
 - *Reverse lookup zones* – resolvem IPs em nomes

Classe endereçoamento

Class A (12.0.0.0/8)

Class B (152.100.0.0/16)

Class C
(209.197.152.0/24)

Resulting zone name and method

12.in-addr.arpa.

100.152.in-addr.arpa.

152.197.209.in-addr.arpa.



Conceitos básicos (zonas vs domínios)

- Uma zona é o intervalo de máquinas e endereços que o servidor DNS tem de ter em atenção
- Uma zona não corresponde (ou pode não corresponder) a um domínio
- Um domínio pode ter várias zonas



Conceitos básicos (conteúdo das zonas)

- Cada zona pode conter 1 ou mais **Resource Records**
- **Host (A) Records**
 - Fazem o mapeamento (simples) entre hostname e endereços IPs
 - Podemos ter várias entradas de IPs para o mesmo nome.
 - Assim podemos implementar técnica de *round-robin* para fazer distribuição de carga



Conceitos básicos (conteúdo das zonas)

- **Canonical Name (CNAME) Records**

- Permite atribuir um conjunto de nomes ao mesmo endereço IP
- No “mundo Windows” esta funcionalidade é também designada por *alias*

- **Mail Exchanger (MX) Records**

- Identificam o servidor de mail para um determinada zona
- É possível haver mais que um registo para o mesmo nome
- Cada registo tem associado uma prioridade. Caso o mais prioritário não responda o de prioridade a seguir é invocado



Conceitos básicos (conteúdo das zonas)

- **Nameserver (NS) Records**

- Especificam o servidor DNS responsável por uma determinada zona ou domínio

- **Start of Authority (SOA) Records**

- Identifica qual o servidor DNS *authoritative* para uma determinada zona
- Define também um conjunto de opções de configuração relativamente a esse servidor
 - Refresh interval, Retry interval, Minimum (default) TTL



Conceitos básicos (conteúdo das zonas)

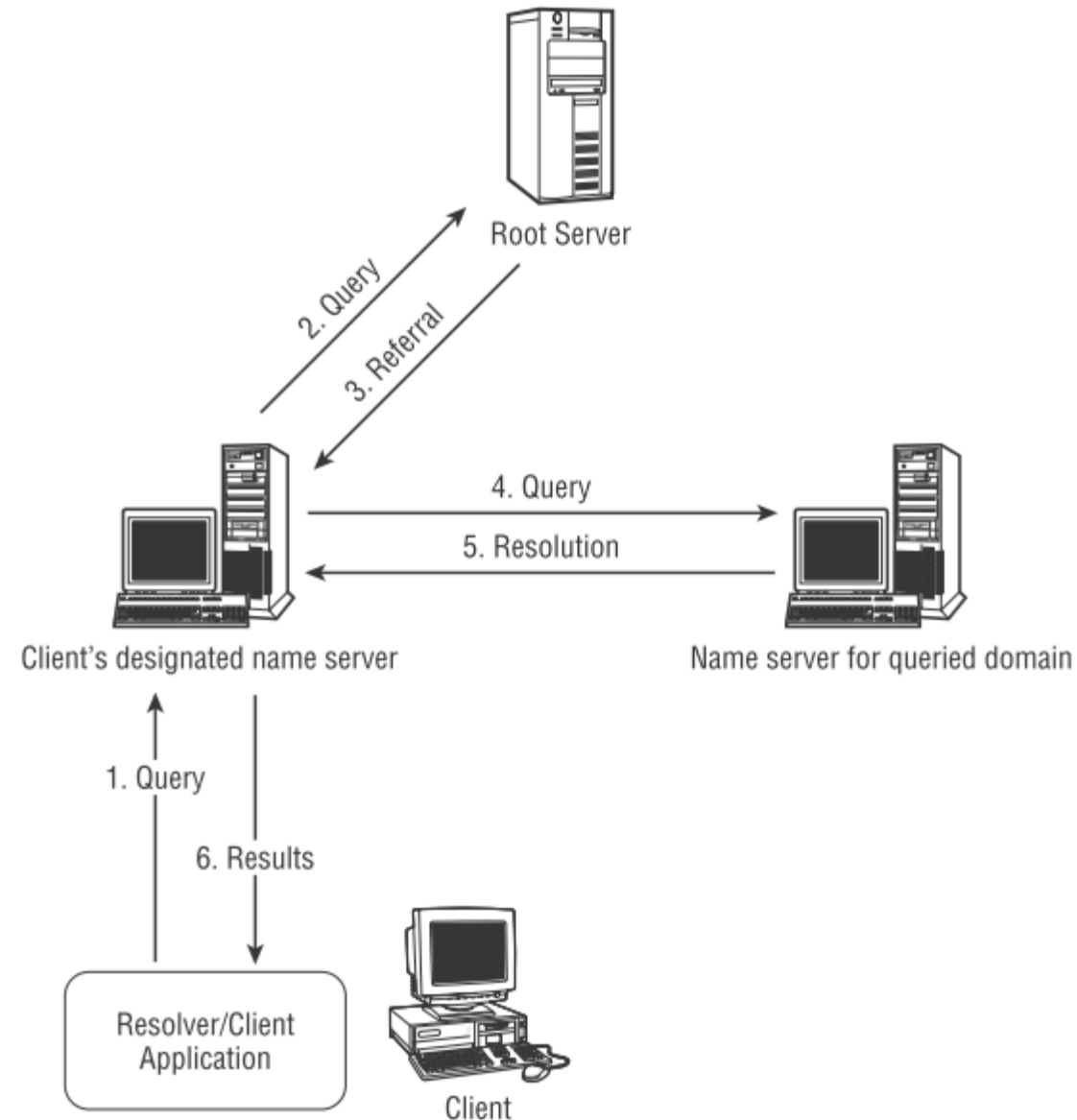
- **Pointer (PTR) Records**

- Funcionam exactamente como um A Record, mas para traduzir IPs em nomes

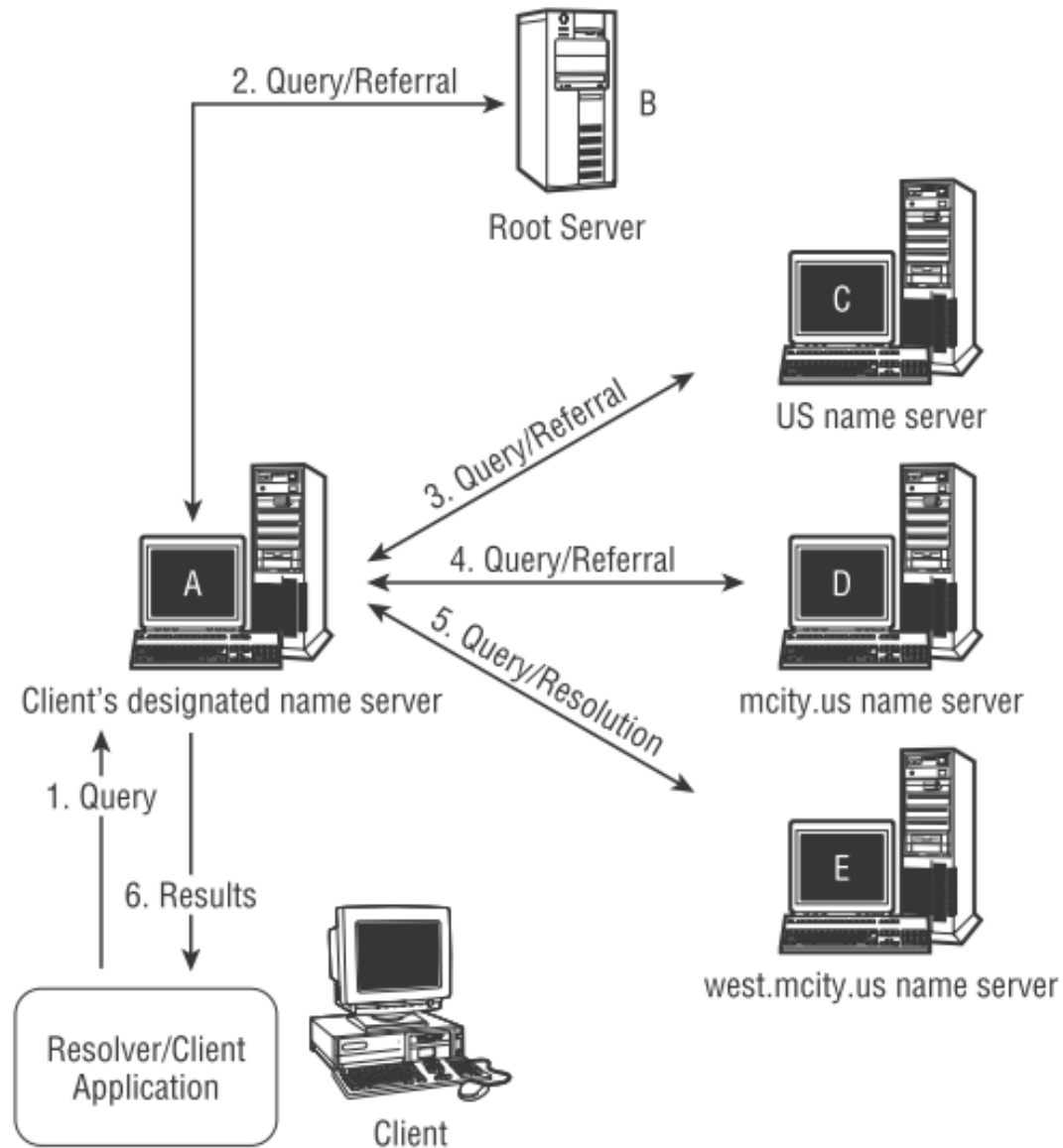
- **Service (SRV) Records**

- Indica a disponibilidade de serviços para uma determinada zona ou domínio
- Funciona como “as páginas amarelas” dos serviços que se encontram disponíveis na zona
- Este record é de extrema importância para a AD do windows 200X server

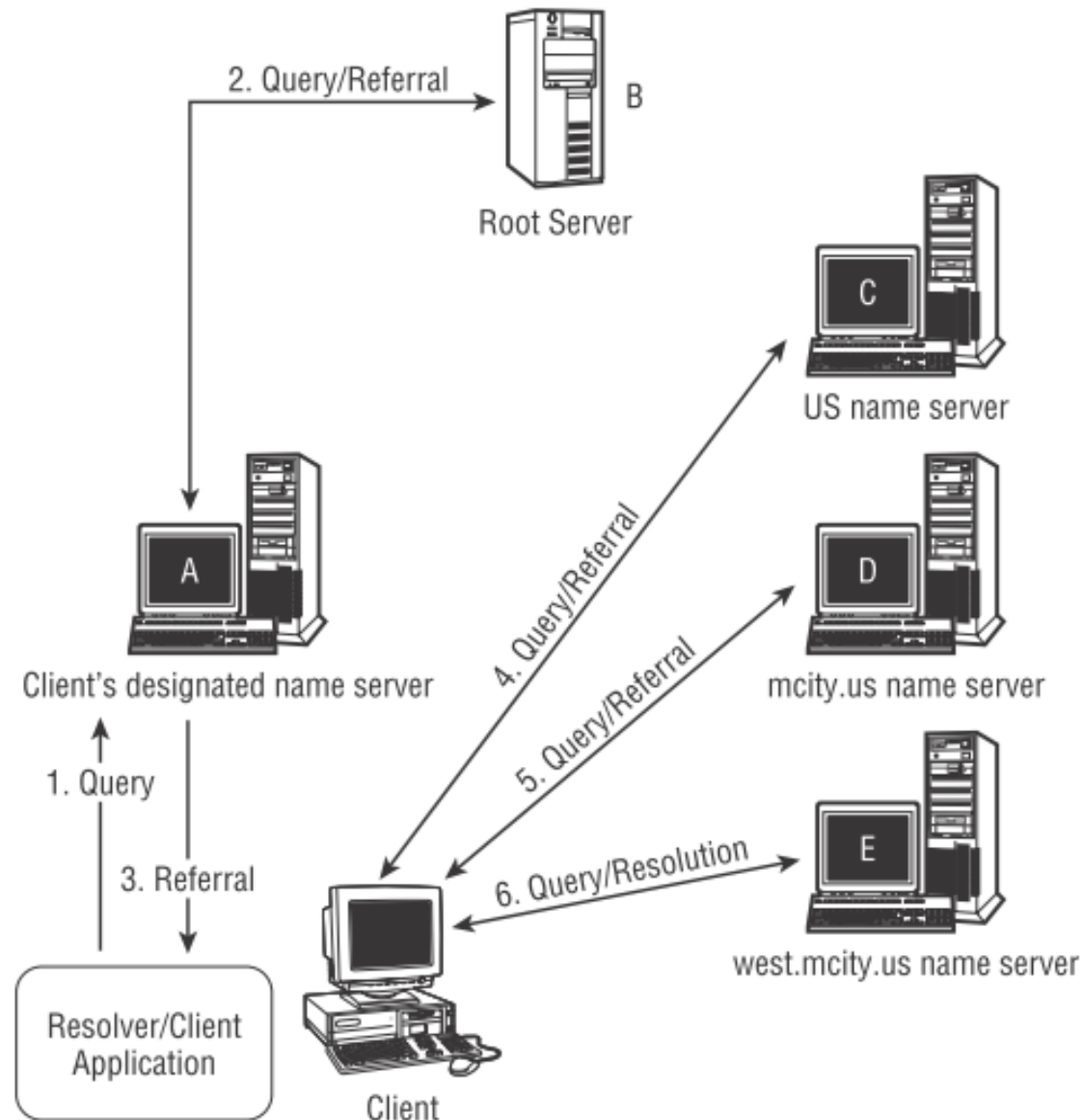
Funcionamento – básico



Funcionamento - Recursivo



Funcionamento - Iterativo





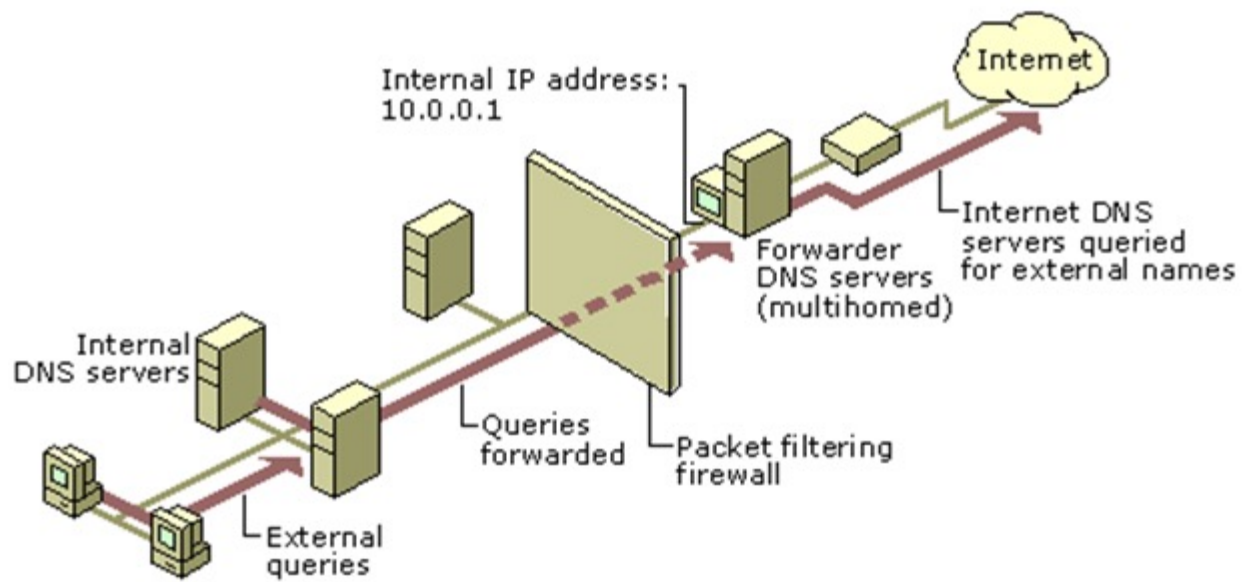
Configuração Servidor DNS

- Server Manager
 - Para instalar o novo *role*
- DNS Console
 - Start -> Administrative Tools -> click DNS
- Linha de comandos
 - dnscmd
 - /help -> para ver todas as opções

Forwarder



- São os DNS servers que recebem os pedidos que o DNS server da nossa rede não consegue resolver
- Nova funcionalidade do 2008 server
 - Conditional Forwarder
 - Capacidade para configurar um DNS Server para um determinado domínio



Se não houver *Forwarders* configurados o pedido é feito directamente aos *root* DNS



Comando útil – cliente e server

- ***nslookup***
 - Permite descobrir um conjunto de informação útil no que respeita ao serviço de DNS
 - Executar da linha de comandos **nslookup**
 - Para ver as opções basta escrever **help** na prompt
- **ipconfig /all**
 - Mostra informação dos servidores DNS instalados
- **netsh**



Windows Internet Name Service (WINS)

- Permite que computadores Windows possam comunicar usando o protocolo *NetBIOS* (Network Basic Input/Output System) numa rede local
- O nome associado ao IP é uma *label*



Funcionamento

1. Computador XPTO “entra” na rede. Regista-se no servidor WINS dando o seu nome e IP (o servidor WINS guarda na base de dados o nome e o IP)
2. Máquina SERVER precisa de aceder ao XPTO ([\\XPTO\SHARE](#))
 1. Faz um *request* ao servidor WINS
 2. Desiste à terceira tentativa e tenta contactar outro servidor WINS da lista.
 3. Se não conseguir resolver não à ligação à máquina XPTO
3. Se houver resolução é feita a ligação à máquina XPTO



Who runs the (DNS) Root Servers?

IANA only controls the data in the authoritative root DNS servers.

It does not run the root servers themselves.

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project