

# Tecnologias de Redes de Computadores - 90398

## Apresentação 10 – Domain Name System

*Pedro Gonçalves - pasg@ua.pt*

# Sumário

- Serviço de tradução de nomes
- Tipos de servidores
- Processo de configuração
  - Conceito de zonas
  - Tipos de registos
  - Processo de delegação de autoridade
  - Conceito de views





# Serviço de nomes



# Serviço de Nomes – DNS

- Forma binária e decimal dos endereços pouco apropriada para utilizadores humanos.
- A forma mais adaptada fácil de humanos conseguirem referir maquinas é de associar um nome ao endereço.
- Falta um serviço de nomes que indique endereço de uma maquina com determinado nome.
- Internet possui serviço de nomes - *Domain Name System* (DNS) – que possibilita que máquina possa também ser identificada por um nome.



ns.lr.estga.ua.pt

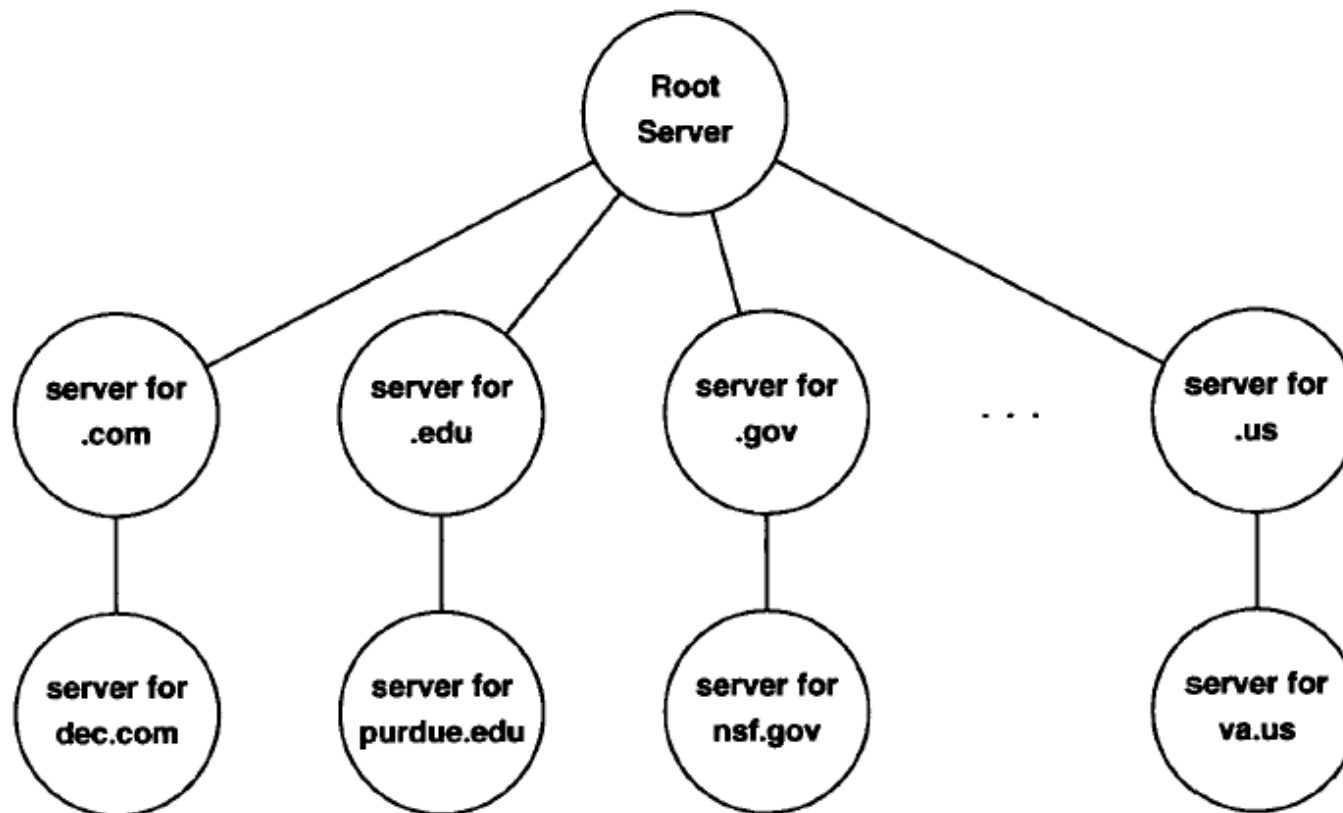
192.168.229.2

# DNS

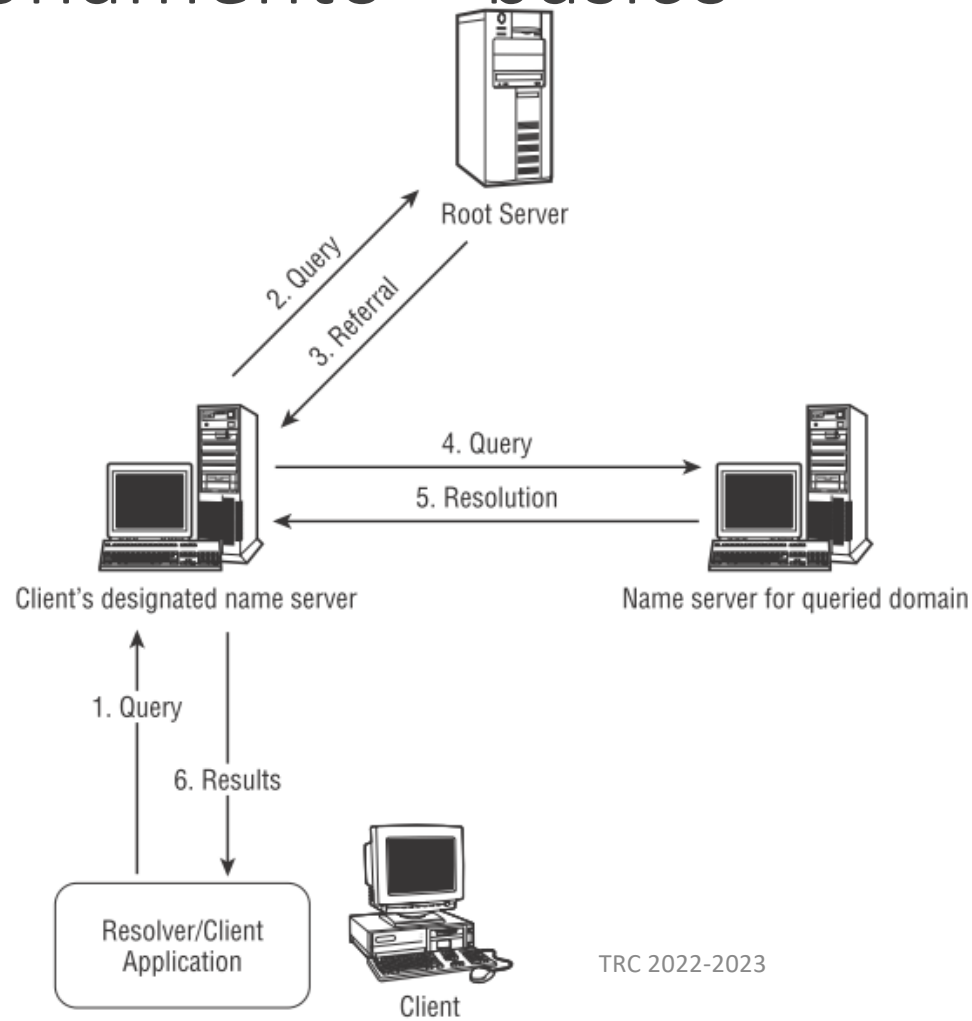
- Trata-se de uma base de dados distribuída para mapear nomes de máquinas (*hostnames*) em endereços IP e vice-versa.
- Base de dados é distribuída por questões de escalabilidade.
- Servidores são responsáveis por domínios bem definidos;
- Servidores são organizados de forma hierárquica a definição de 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.



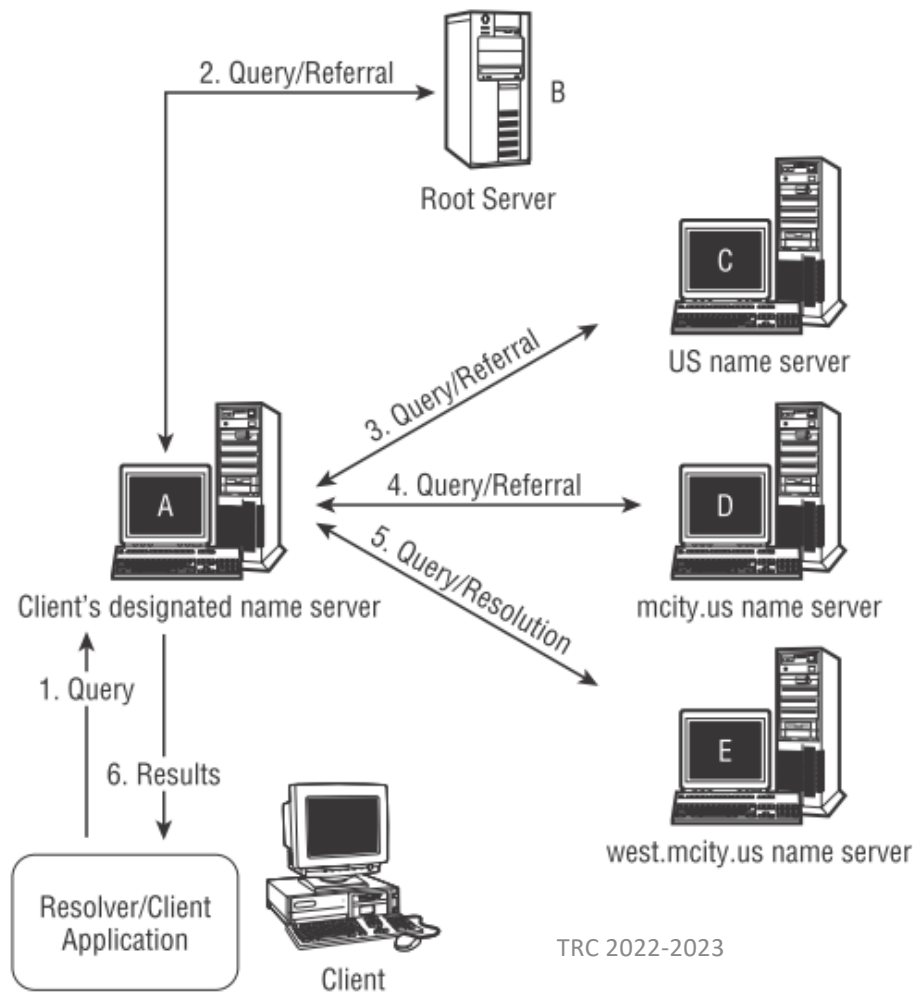
# Hierarquia dos servidores



# Funcionamento – básico

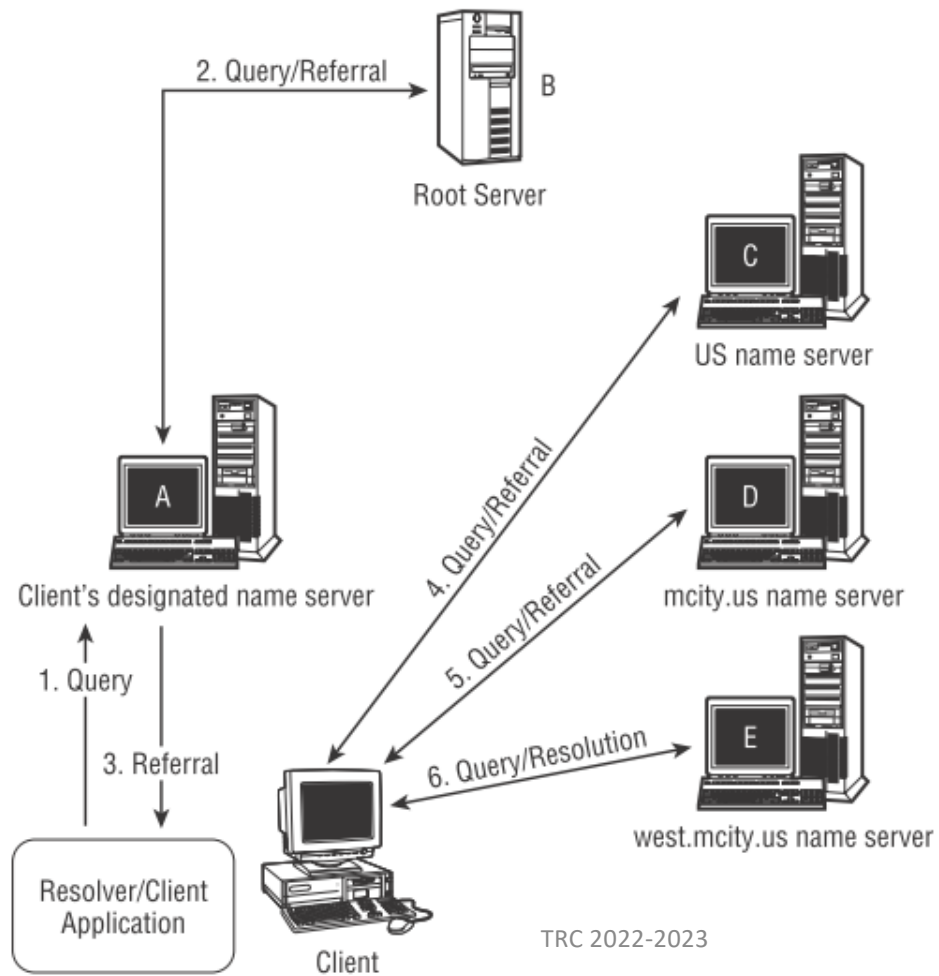


# Funcionamento - Recursivo





# Funcionamento - Iterativo



# Estrutura do pacote

0	16	31
<b>IDENTIFICATION</b>		<b>PARAMETER</b>
<b>NUMBER OF QUESTIONS</b>		<b>NUMBER OF ANSWERS</b>
<b>NUMBER OF AUTHORITY</b>		<b>NUMBER OF ADDITIONAL</b>
<b>QUESTION SECTION</b> ...		
<b>ANSWER SECTION</b> ...		
<b>AUTHORITY SECTION</b> ...		
<b>ADDITIONAL INFORMATION SECTION</b> ...		



# Tipos de servidores

- Authoritative – representante oficial acerca da zona
- Master – Servidor principal da zona; obtém informação do seu disco
- Primary – Sinónimo de master
- Slave – Copia informação do master
- Secondary - Sinónimo de slave
- Distribution – Servidor só utilizado dentro de domínio
- Nonauthoritative – Responde a informação da sua cache, mas não sabe se ainda é válida
- Caching – Guarda informação de queries anteriores, não tem zonas locais
- Forwarder – Faz consultas em nome dos clientes; obtém uma cache enorme
- Recursive – Faz todas as queries até obter resolução ou erro
- Nonrecursive – Devolve referral para clientes fazerem questões subsequentes



# Formato dos registos DNS

- [name] [ttl] IN type data
- name: nome do objecto de DNS.
- ttl: time-to-live em segundos para o registo.
- IN: identifica o registo como registo DNS da Internet.
- type: tipo de registo.
- data: dados do registo.



# Registos DNS

- Start of Authority – **SOA** - Marks the beginning of a zone's data, and defines parameters that affect the entire zone.
- Nameserver – **NS** - Identifies a domain's nameserver.
- Address – **A** - Converts a hostname to an address.
- Pointer – **PTR** - Converts an address to a hostname.
- Mail Exchange – **MX** - Identifies where to deliver mail for a given domain name.
- Canonical Name – **CNAME** - Defines an alias hostname.
- Host Information – **HINFO** - Describes a host's hardware and OS.
- Well-Known Service – **WKS** - Advertises network services.
- Text – **TXT** - Stores arbitrary text strings.



# Start Of Authority (SOA)

```
@      IN      SOA      ns1r.lr.estga.ua.pt. pasg.ua.pt. (  
                2011101501      ; Serial number  
                7200      ; Refresh      [1h]  
                120      ; Retry      [10m]  
                2419200 ; Expire      [1d]  
                604800) ; Default TTL [1h]
```



- **Source host** – a máquina que representa o servidor de nomes do domínio.
- **Contact e-mail** – Endereço de e-mail da pessoa responsável pelo ficheiro da zona. De notar que "@" do endereço é substituído pelo "."

# Valores do SOA

- **Serial number** – Número de revisão do ficheiro da zona que é incrementado sempre que a zona é editada. O incremento permite que a alteração seja propagada por todos os servidores de DNS secundários.
- **Refresh Time** - Tempo em segundos, que o servidor de DNS secundário espera até pedir o registo de SOA do servidor primário e verificar se existem alterações. Quando o *refresh time* expira, o servidor de DNS secundário pede uma cópia do registo de SOA ao servidor primário. O servidor secundário compara o *serial number* do DNS primário com o seu e se forem diferentes, o secundário pede a transferência da zona do servidor de DNS primário. O valor por defeito é de 3600.



# Valores do SOA

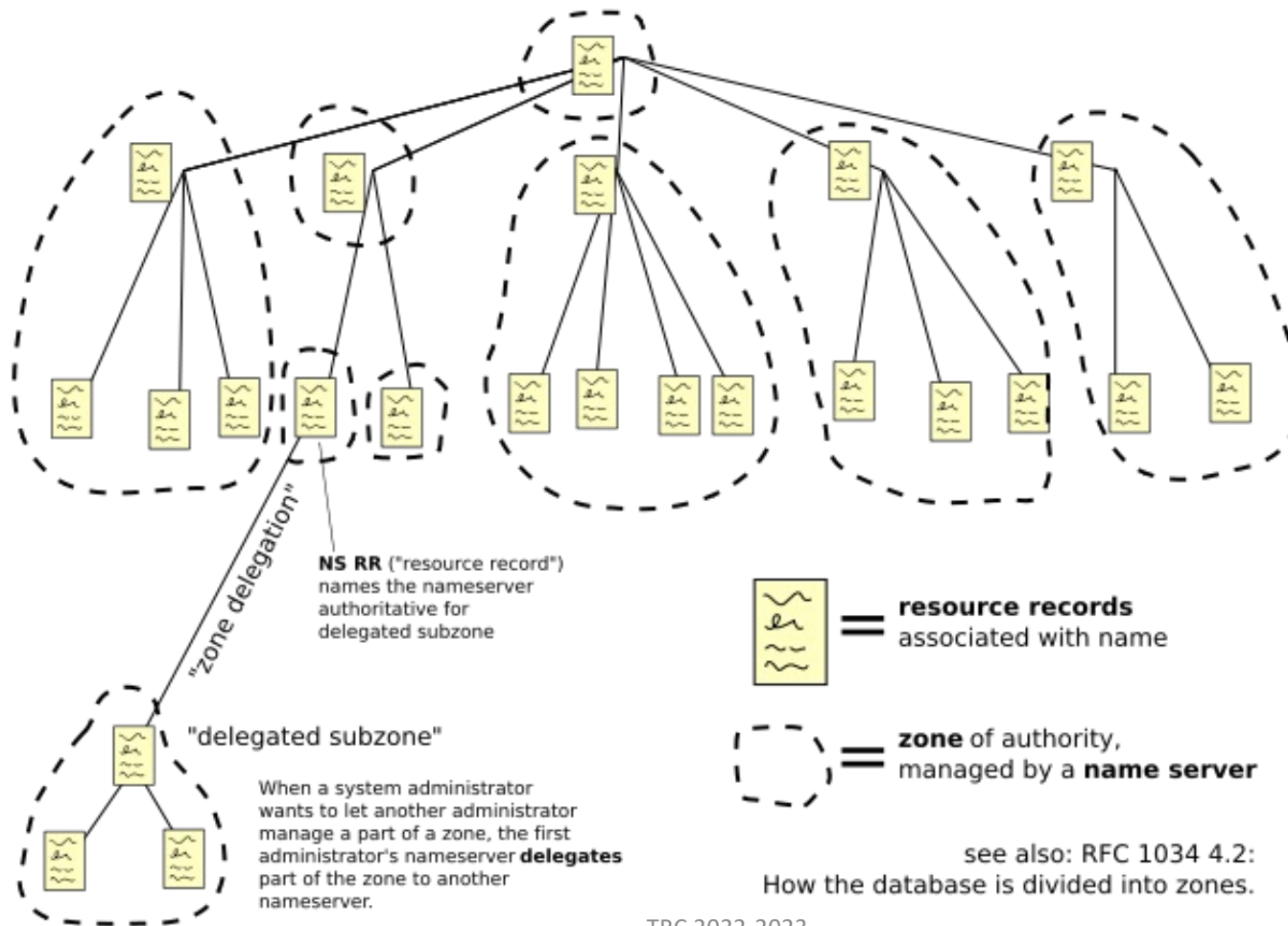
- **Retry time** – Tempo em segundos, que um servidor secundário espera antes de tentar novamente uma transferência de uma zona falhada. Normalmente, o *retry time* é menor do que o *refresh time*. O valor por defeito é 600.
- **Expire time** - Tempo em segundos, que um servidor secundário continua a tentar transferir uma zona. Se o tempo espirar o servidor espira a zona, deixando de responder às queries dessa zona. O valor por defeito é 86400.
- **Minimum TTL** – Tempo (time-to-live) dos registos de uma zona. O tempo é anunciado nas respostas de forma a que os servidores saibam quanto tempo o podem manter em cache. . O valor por defeito é 3600.







# Domain Name Space



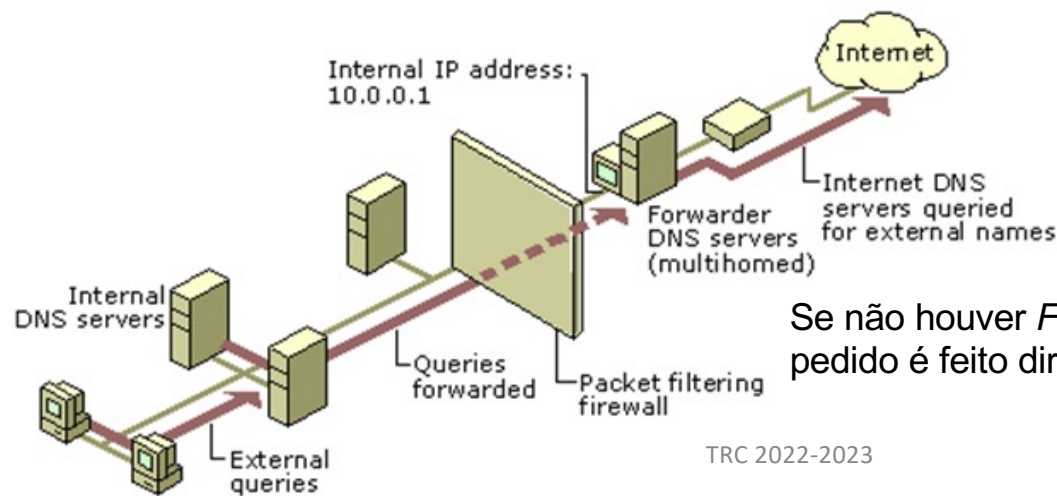
# Zonas, domínios e autoridade

- Conceito de zona e domínio por vezes são confundidos:
- Domínio é um conjunto de nomes que partilham o mesmo sufixo
- Zona é uma parte contígua do espaço de nomeação
- Pode até conter informação acerca de múltiplos domínios
- Domínio tem pelo menos zona directa e zona inversa
- Servidores têm autoridade sobre domínios
- Que entretanto podem delegar partes desse domínio



# 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

# Servidores disponíveis

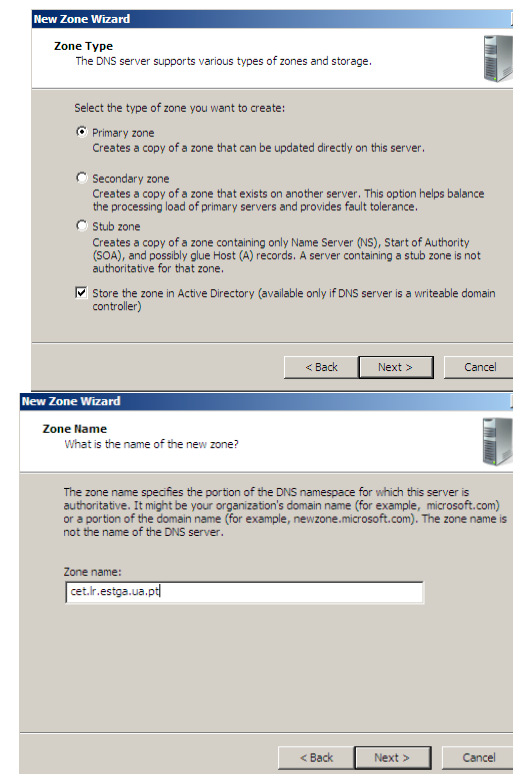
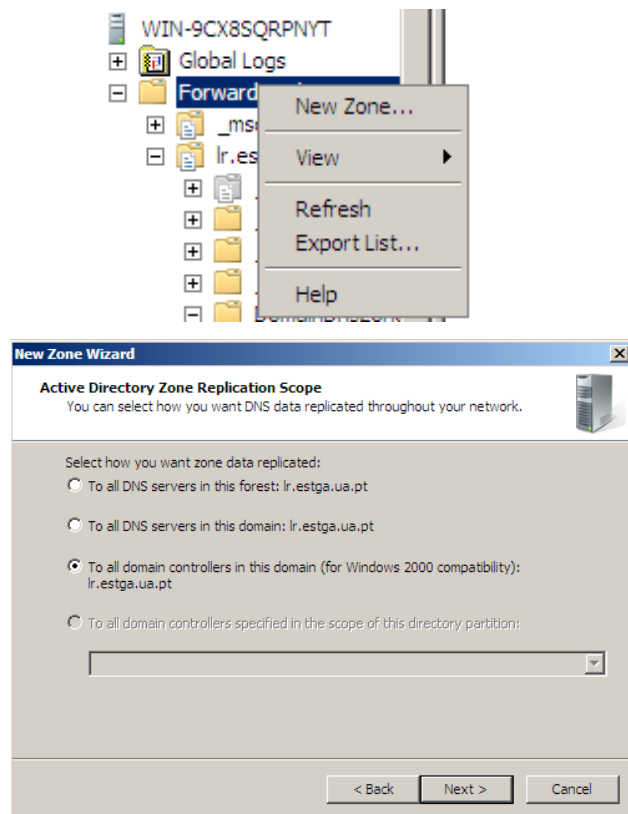
- BIND - <http://www.isc.org/products/BIND/>.
- Djbdns <http://djbdns.org>.
- PowerDNS - [www.powerdns.com/](http://www.powerdns.com/)
- MS DNS Server.
- <http://mydns.bboy.net/survey/>

70.105%	24,335,752	<a href="#">BIND</a>
16.571%	5,405,266	<a href="#">TinyDNS</a>
6.237%	2,165,143	<a href="#">Microsoft DNS Server</a>
2.792%	969,097	<a href="#">MyDNS</a>
1.964%	681,614	<a href="#">PowerDNS</a>
1.250%	433,905	<a href="#">Simple DNS Plus</a>
1.138%	395,206	Unknown
0.277%	96,232	<a href="#">Plant DNS Server</a>
0.203%	70,455	<a href="#">NSD</a>
0.144%	49,921	<a href="#">UltraDNS</a>
0.104%	36,195	<a href="#">Net::DNS::Nameserver</a>
0.083%	28,656	<a href="#">QuickDNS</a>
0.064%	22,087	<a href="#">Incognito DNS Commander</a>
0.025%	8,508	<a href="#">MaraDNS</a>
0.024%	8,174	<a href="#">rbindsd</a>
0.018%	6,135	<a href="#">Totd</a>
0.001%	386	<a href="#">ATLAS</a>
0.001%	371	<a href="#">Posadis</a>
0.001%	312	<a href="#">NonSequitur DNS</a>
0.000%	12	<a href="#">Nominum ANS/CNS</a>

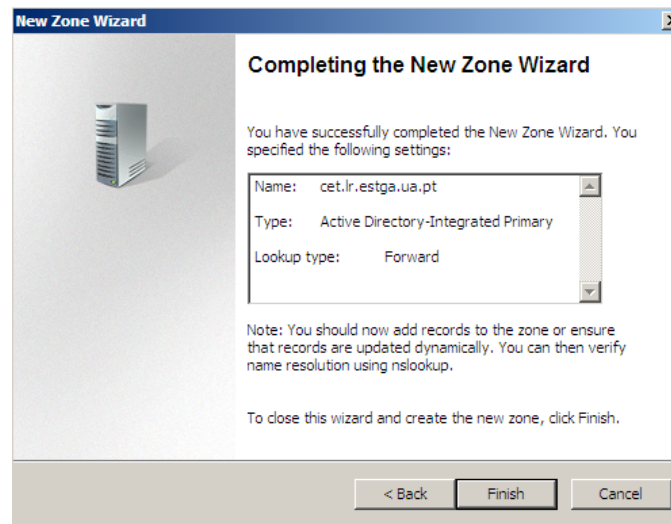
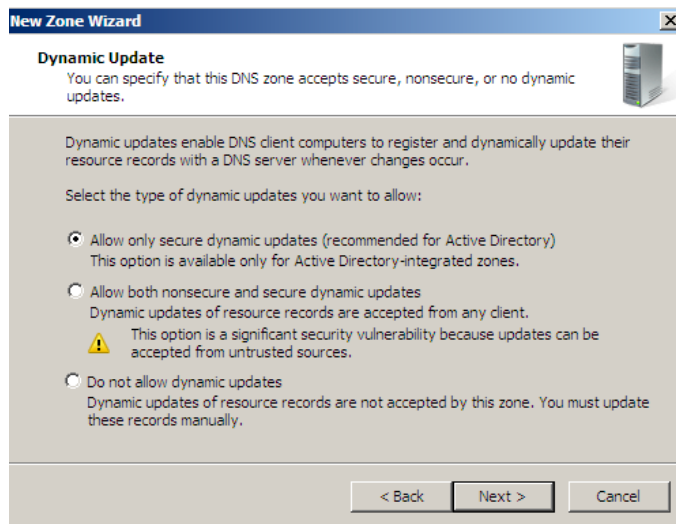


## Windows Server

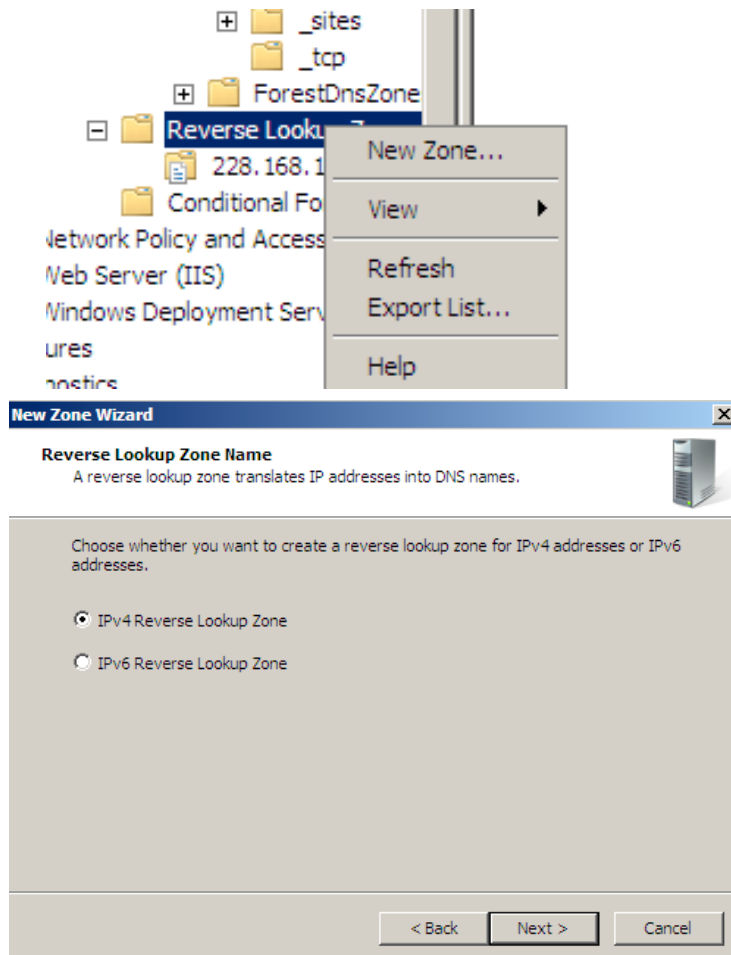
# Criação de zonas directas



# Criação de zonas directas

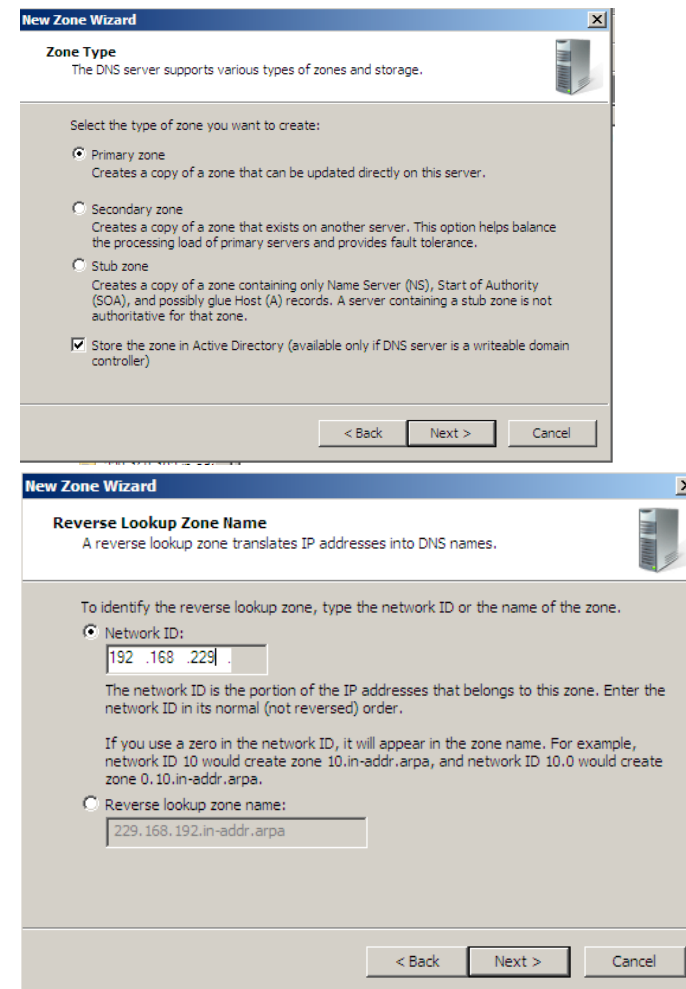


# Criação zona inversa



12/04/23

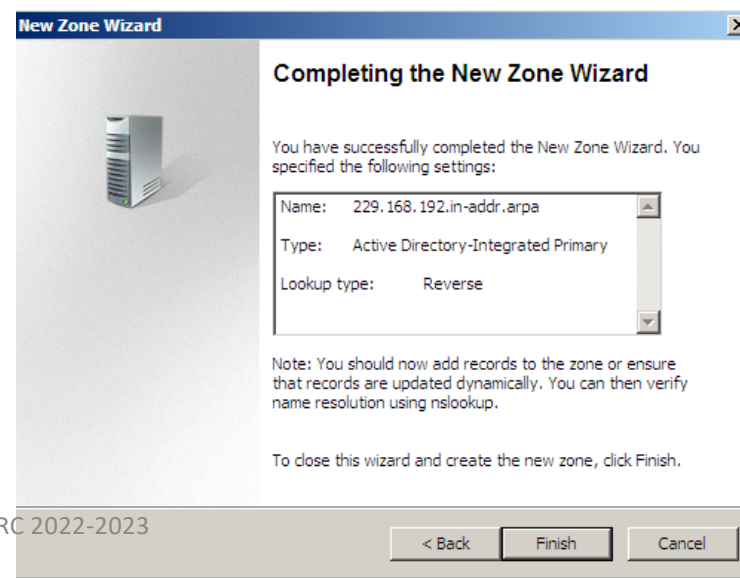
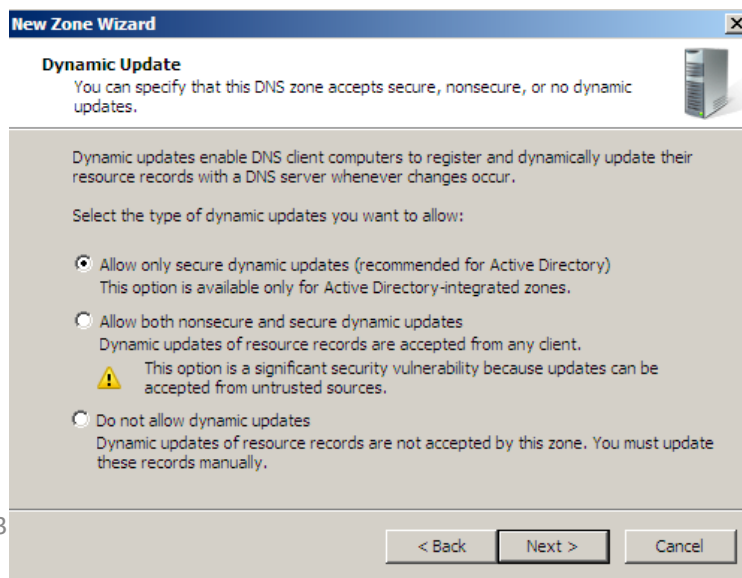
TRC 2022-2023



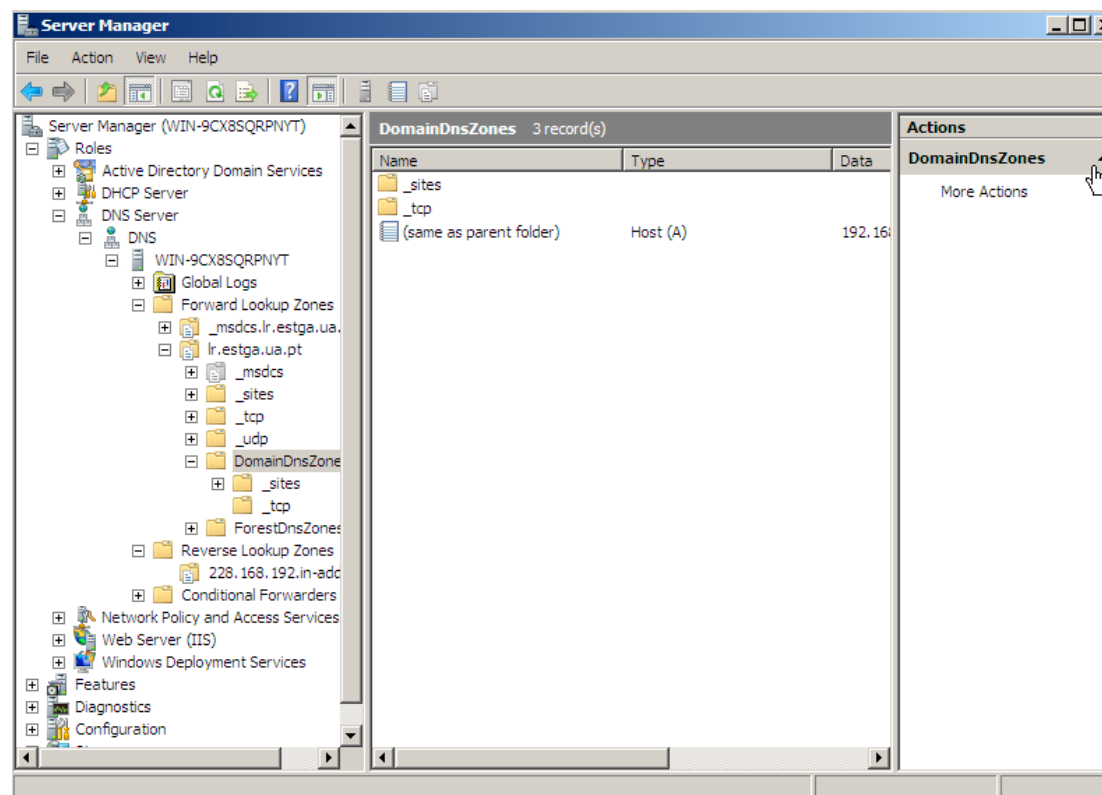
24



# Criação de zona inversa



# Conteúdo da zona



# Criação de registos



- New Host (A or AAAA)...
- New Alias (CNAME)...
- New Mail Exchanger (MX)...
- New Domain...
- New Delegation...
- Other New Records...
- Refresh
- Export List...
- View ▶
- Arrange Icons ▶
- Line up Icons
- Help

**New Host** [X]

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

☐ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

# Forwarders condicionais



**New Conditional Forwarder** [X]

DNS Domain:

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...		

[Delete] [Up] [Down]

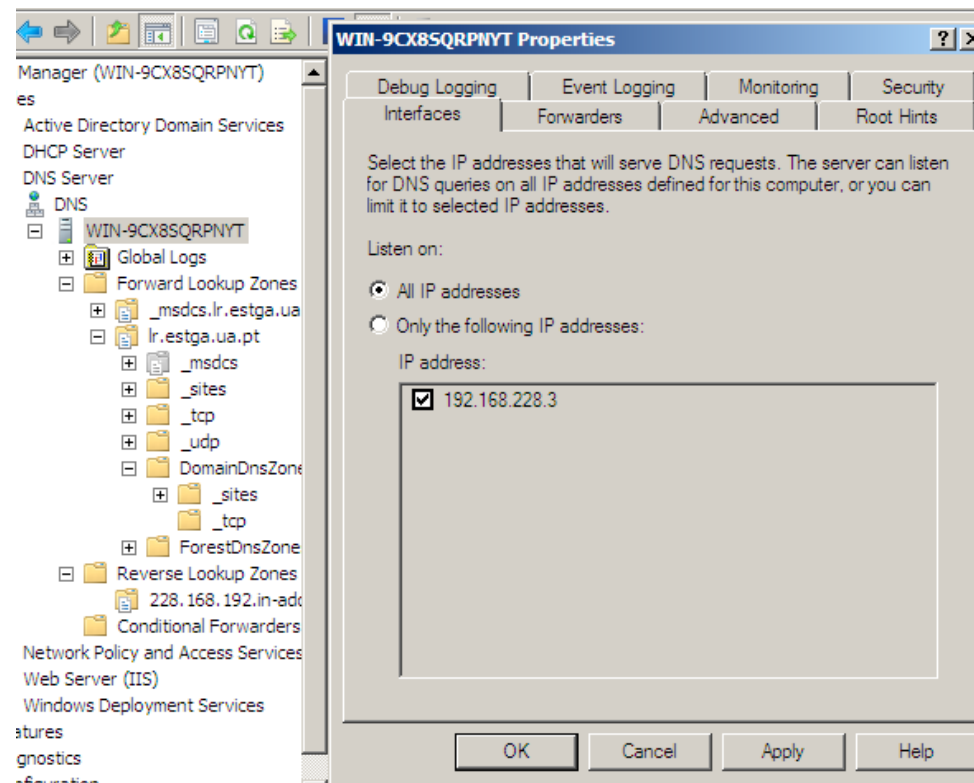
☐ Store this conditional forwarder in Active Directory, and replicate it as follows:

Number of seconds before forward queries time out:

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

[OK] [Cancel]

# Configuração do servidor






BIND9

# Ficheiros

- named.conf
- named.conf.local
- named.conf.options
- 1 ficheiro por zona
  - db.zona
  - dn.zona.rev



# named.conf



```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```



# named.conf.local

```
zone "lr.estga.ua.pt" IN {  
    type master;  
    file "/etc/bind/zones/lr.estga.ua.pt";  
    allow-query{any;};  
};  
zone "1.168.192.IN-ADDR.ARPA" IN {  
    type master;  
    file "/etc/bind/zones/192.168.1.rev";  
};
```



# named.conf.options

```
options {  
    directory "/var/cache/bind";  
  
    // If there is a firewall between you and nameservers you want  
    // to talk to, you may need to fix the firewall to allow multiple  
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113  
  
    // If your ISP provided one or more IP addresses for stable  
    // nameservers, you probably want to use them as forwarders.  
    // Uncomment the following block, and insert the addresses replacing  
    // the all-0's placeholder.  
  
    forwarders {  
        192.168.229.254;  
    };  
};
```




# Start Of Authority (SOA)

- Registo presente em todas as zonas
- Define um conjunto de valores relacionados com toda a zona.
- Exemplo:

\$ORIGIN lr.estga.ua.pt.

\$TTL 604800



```
@      IN      SOA      ns1r.lr.estga.ua.pt. root.lr.estga.ua.pt. (  
        1              ; Serial  
        8H             ; Refresh  
        2H             ; Retry  
                4W             ; Expire  
        1D)            ; Default TTL  
        NS      ns1r.lr.estga.ua.pt.  
@      IN      MX      10 mail.lr.estga.ua.pt.
```

# SOA

- Na falta de um origin o nome do domínio é definido através do nome da zona definida em `named.conf.local`
- Segundo parâmetro define o nome do servidor de nomes daquele domínio
- Terceiro parâmetro define o endereço de correio electrónico do administrador do servidor
  - Apesar de não ter @
- Serial é um número de série de configuração
  - Serve para servidores verificarem se a versão da informação é mais recente do que a versão que está em cache
  - Deve ser incrementado de cada vez que a configuração for editada
- Tempos podem ser especificados em segundos
  - Nesse caso são apresentados sem unidades
- Último argumento define o servidor de correio para o domínio



# Zona direta

```
$ORIGIN lr.estga.ua.pt.  
$TTL 604800  
@ IN SOA ns1r.lr.estga.ua.pt. pasg.ua.pt. (  
    2011101501 ; Serial  
    7200      ; Refresh  
    120       ; Retry  
    2419200   ; Expire  
    604800)   ; Default TTL
```

```
@ IN NS ns1r.lr.estga.ua.pt.  
@ IN MX 10 mail.lr.estga.ua.pt.
```

```
ns1r IN A 192.168.1.12  
mail IN A 192.168.1.12
```

```
$ORIGIN cet.lr.estga.ua.pt.  
$TTL 604800  
@ IN NS nscet.cet.lr.estga.ua.pt.  
nscet IN A 192.168.1.11
```



# Zona inversa

\$TTL 3D

```
@      IN      SOA      ns1r.lr.estga.ua.pt. pasg.ua.pt. (
                                2011101501      ; Serial
                                7200      ; Refresh
                                120      ; Retry
                                2419200      ; Expire
                                604800)      ; Default TTL
```

```
      IN      NS      ns1r.lr.estga.ua.pt.
12      IN      PTR      mail.lr.estga.ua.pt.
9      IN      PTR      mail.lab1.lr.estga.ua.pt.
10     IN      PTR      mail.lab2.lr.estga.ua.pt.
8      IN      PTR      ns1lab3.lab3.lr.estga.ua.pt.
11     IN      PTR      mail.cet.lr.estga.ua.pt.
```



# Validação da configuração do BIND

- Validação da configuração do servidor

`named-checkconf`



- Validação do conteúdo de uma zona

`named-checkzone {zonename} {filename}`

- Exemplo:

`named-checkzone lr.estga.ua.pt /etc/bind/lr.estga.ua.pt`



## Ferramentas de debug



# nslookup

- Exemplo de resolução direta:

```
garlic:~ pasg$ nslookup www.ua.pt
```

```
Server:                193.136.172.20
```

```
Address:      193.136.172.20#53
```

```
Name:          www.ua.pt
```

```
Address: 193.136.173.25
```

- Exemplo de resolução inversa:

```
garlic:~ pasg$ nslookup 193.136.173.25
```

```
Server:                193.136.172.20
```

```
Address:      193.136.172.20#53
```

```
25.173.136.193.in-addr.arpa name = bombadil.servers.ua.pt.
```



# nslookup

- Aplicação permite o pedido de outras informações além dos registos A e PTR:
  - Saber qual o servidor de correio do domínio ua.pt?

```
nslookup -query=MX ua.pt
```

- Que tradução é que a máquina 193.136.172.20 faz do nome www.ua.pt


```
nslookup www.ua.pt 193.136.172.20
```

- Qual é o servidor de nomes do domínio ua.pt?

```
nslookup -query=NS ua.pt
```



# Dig



```
garlic:~ pasg$ dig www.ua.pt
; <<>> DiG 9.7.3-P3 <<>> www.ua.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55473
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;www.ua.pt.                                IN      A
;; ANSWER SECTION:
www.ua.pt.      28800    IN      A      193.136.173.25
;; AUTHORITY SECTION:
ua.pt.          28800    IN      NS      ns2.ua.pt.
ua.pt.          28800    IN      NS      ns.ua.pt.
;; ADDITIONAL SECTION:
ns.ua.pt.       28800    IN      A      193.136.172.18
ns2.ua.pt.      28800    IN      A      193.136.172.19
;; Query time: 4 msec
;; SERVER: 193.136.172.20#53(193.136.172.20)
;; WHEN: Tue Apr 17 17:53:19 2012
;; MSG SIZE rcvd: 110
```

# Mais informação

- "Computer Networks", Andrew Tanenbaum, 3rd ed. Prentice Hall, 1996.
- DNS How to, <http://www.tldp.org/HOWTO/DNS-HOWTO.html#toc10>.
- "Internetworking with TCP-IP", Douglas E. Comer.



# E é tudo...

- Questões?
- Comentários?

