

Questões

1.

```
[root@localhost etc]# host -t mx dept.lr-g11.pt
dept.lr-g11.pt mail is handled by 10 mail.lr-g11.pt.
```

2. Não obtivemos uma *query* DNS bem sucedida. A resolução partiu da root “.” e *Top-Level-Domain* “.pt” e como o domínio “lr-g11” não está registrado, a resolução de nome falhou.

```
[root@Labs5610 ar]# host -t mx lr-g11.pt
Host lr-g11.pt not found: 3(NXDOMAIN)
```

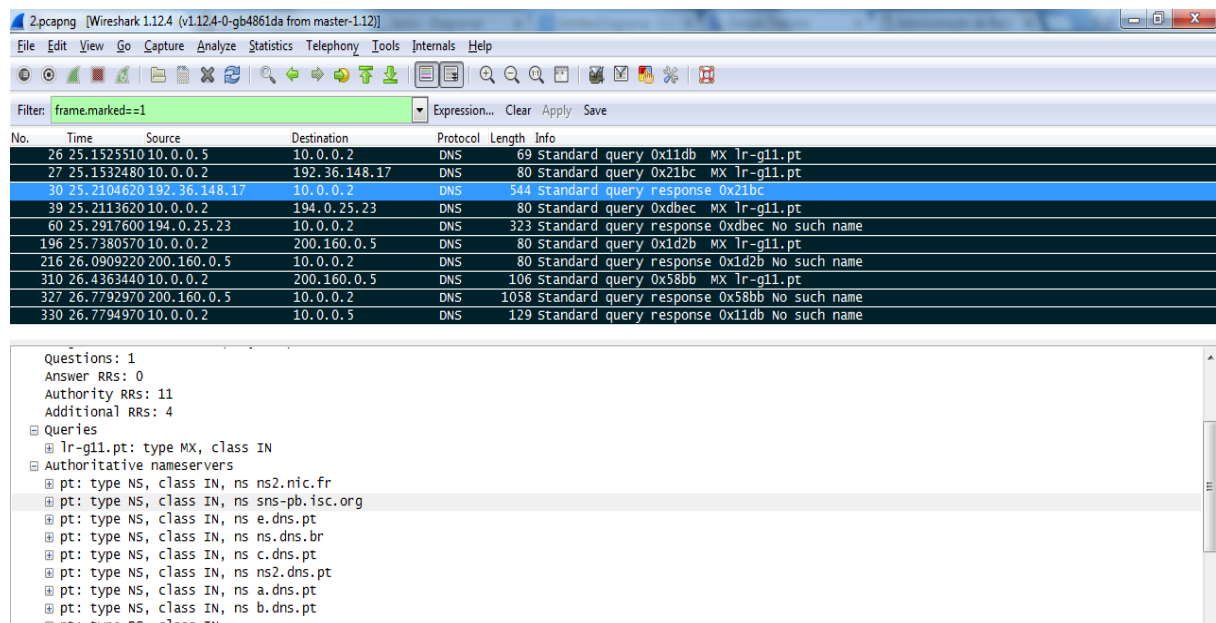


Figura 2: Captura *wireshark* no dns.dept.lr-gX.pt.

3.

```
[root@Labs5610 ar]# dig www.jn.pt

; <<>> DiG 9.10.3-P2-RedHat-9.10.3-7.P2.fc23 <<>> www.jn.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 34829
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.jn.pt. IN A

;; ANSWER SECTION:
www.jn.pt. 300 IN A 80.251.169.144
```

```

www.jn.pt. 300 IN A 80.251.169.145
www.jn.pt. 300 IN A 80.251.169.146
www.jn.pt. 300 IN A 80.251.169.147

;; AUTHORITY SECTION:
jn.pt. 7200 IN NS dns3.jn.pt.
jn.pt. 7200 IN NS dns2.jn.pt.
jn.pt. 7200 IN NS dns1.jn.pt.
jn.pt. 7200 IN NS dns.jn.pt.

;; ADDITIONAL SECTION:
dns.jn.pt. 7200 IN A 194.65.90.97
dns1.jn.pt. 7200 IN A 80.251.161.203
dns2.jn.pt. 7200 IN A 194.65.90.101
dns3.jn.pt. 7200 IN A 83.240.201.246

;; Query time: 339 msec
;; SERVER: 10.0.0.2#53(10.0.0.2)
;; WHEN: Wed May 25 10:45:21 WEST 2016
;; MSG SIZE rcvd: 241

```

a. O `term1` pede ao `dns.dept.lr-g11.pt` (servidor de nomes local) para resolver o nome `www.jn.pt`, este verifica que o nome não faz parte do seu domínio e por isso, interroga o servidor de nomes da raiz (`193.0.14.129`), este devolve ao servidor de nomes local uma referência para o servidor de nomes do subdomínio `pt`. O servidor de nomes local interroga o o servidor de nomes de `pt` (`194.0.25.23`) sobre o endereço IP de `www.jn.pt` e obtém assim, uma referência para o servidor do nomes `jn.pt` que devolve ao servidor de nomes local. Este interroga, finalmente o servidor de `jn.pt` (`194.65.90.97`) que tem condições de resolver o endereço IP pedido. Termina então o processo de resolução e o `dns.dept.lr-g11.pt` devolve ao `term1` o endereço IP correspondente ao nome solicitado.

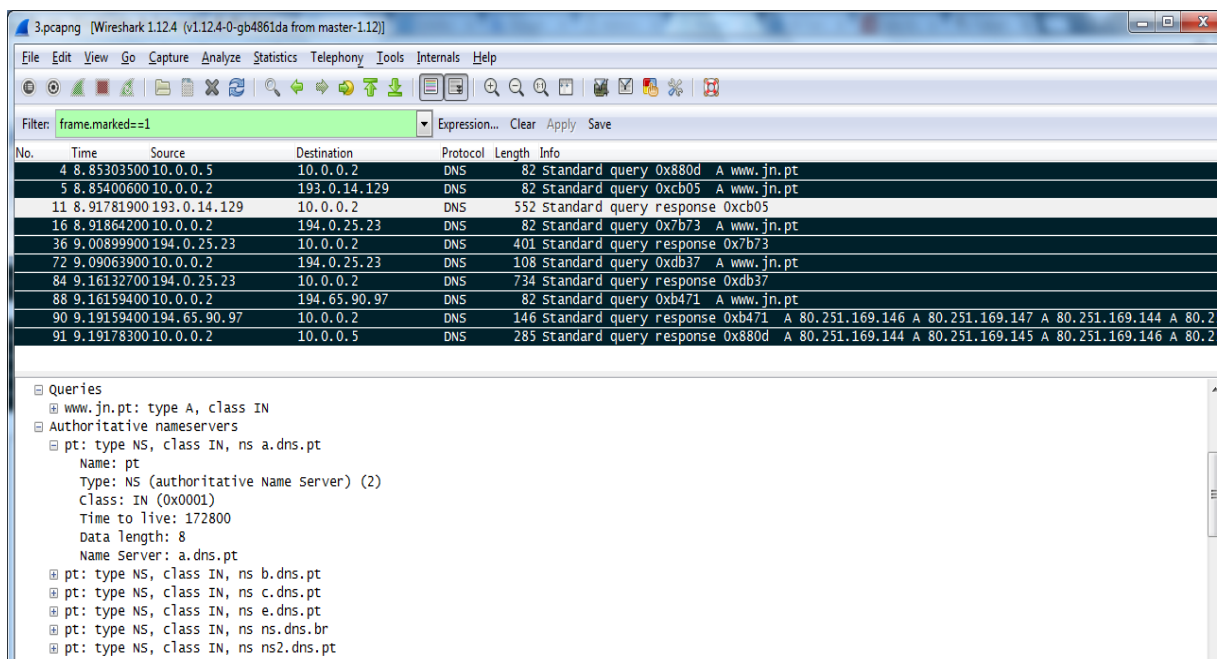


Figura 3: Captura *wireshark* do(s) pedido(s) do registo A no `dns.dept.lr-g11.pt`.

b. Sim, a resposta dada ao terminal 1 é autoritativa, como podemos ver pelos campos marcados na figura abaixo Authority RRs: 4:

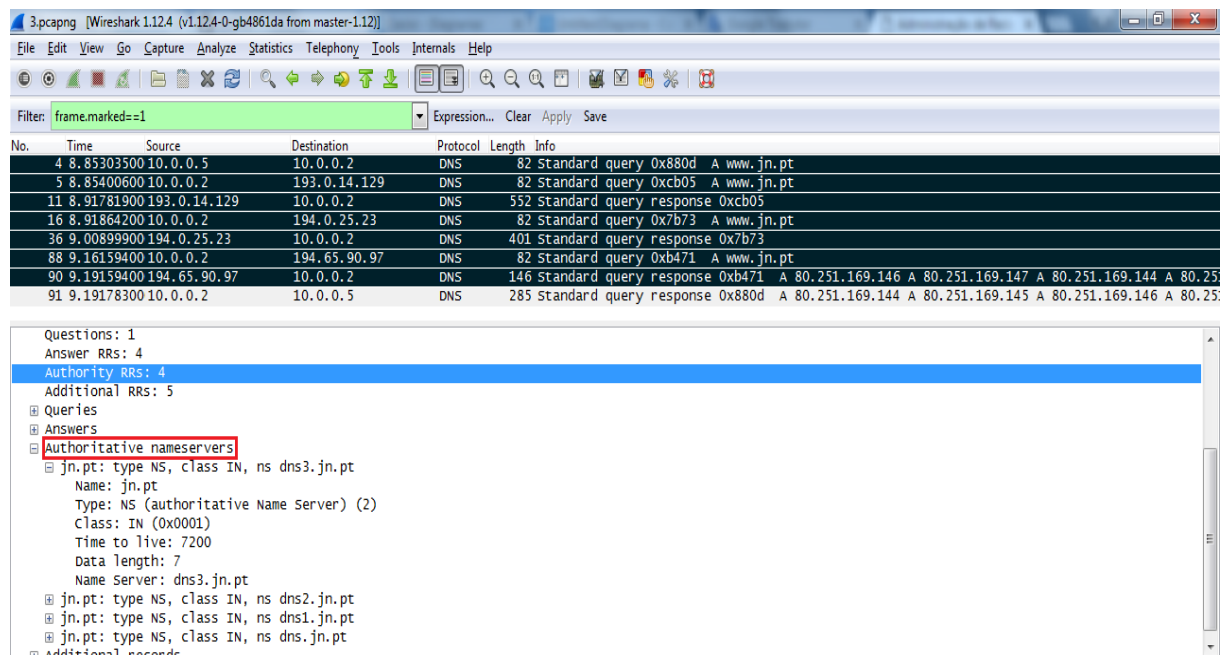


Figura 4: Captura *wireshark* da resposta dada ao terminal no dns.dept.lr-gX.pt.

c. *jn.pt* Não, a resposta obtida pelo dns.dept.lr-gX.pt não é autoritativa.

d. Na resposta obtida a esta pergunta é nos fornecido mais do que um endereço para este nome, na qual a ordem dos endereços é *round-robin*.

Round robin é um mecanismo de equilíbrio local de carga (*load balancing*), usado pelos servidores DNS para compartilhar e distribuir cargas (pedidos de resolução de nomes) entre dois ou mais servidores da rede, e é esta a principal vantagem do uso deste mecanismo.

Usando o *round robin*, a um único nome DNS são associados mais do que um endereços IP. À medida que as requisições vão chegando, o servidor DNS responde cada consulta com um dos endereços IP e depois faz uma **reordenação** da lista de endereços, para que na próxima requisição, um endereço IP diferente seja o primeiro da lista. Isto resulta numa distribuição igual de carga entre os diferentes servidores.

4. *Glue record*, ou registo-cola, é a associação de um nome *host* (servidor de nomes ou DNS) a um endereço IP. Este tipo de registo é necessário quando queremos definir servidores de nomes de um domínio para um nome *host* que é um subdomínio desse domínio, (que leva a uma dependência cíclica).

Por exemplo, no nosso caso, para resolver dept.lr.g11.pt é necessário consultar dns.dept.lr-g11.pt (servidor de nomes), mas para isso é necessário resolver dns.dept.lr-g11.pt, o que implica consultar dns.dept.lr-g11.pt, entrando assim numa **dependência cíclica**. Perante isto, na nossa montagem, foi necessário usar um *glue record* na máquina dns.lr-gX.pt, de modo a evitar essa dependência cíclica.

Glue records só devem ser usados na situação descrita acima, onde o servidor DNS se encontra dentro do domínio delegado.

5.

a. No ficheiro `named.conf`, como podemos ver abaixo, na cláusula `options` alteramos a declaração `recursion` para `no`, e configuramos duas vistas, uma para rede interna e outra para o exterior.

```
options {
    ...
    recursion no;
    ...
};

view "interior" {
    match-clients {localhost; localnets; 172.16.0.0/24; 10.0.0.0/24;};
    recursion yes;
    zone "lr-g11.pt" IN {
        type master;
    file "master/dns.lr-g11.pt.zone";
    };
    zone "0.16.172.in-addr.arpa" IN {
        type master;
        file "reverse/172.16.0.zone";
    };
    zone "." IN {
type hint;
file "named.ca";
    };
};

view "exterior" {
    match-clients {"any";};
    recursion no;
    zone "lr-g11.pt" IN {
        type master;
    file "master/dns.lr-g11.pt.exterior.zone";
    };
    zone "80.168.192.in-addr.arpa" IN {
        type master;
        file "reverse/192.168.80.zone";
    };
    zone "." IN {
type hint;
file "named.ca";
    };
};
```

Também configuramos os ficheiros de zona para resolução direta:

```
$ORIGIN lr-g11.pt.
$TTL 86400
@ 1D SOA dns.lr-g11.pt. miguelferreira108.google.com. (
2016051904
```

```
3h
15
1w
3h
)
```

```
NS dns.lr-g11.pt.
MX 10 mail.lr-g11.pt.
```

```
dept NS dns.dept
dns.dept A 10.0.0.2
```

```
dns A 192.168.80.2
mail A 192.168.80.7
router A 192.168.80.1
```

```
www.lr-g11.pt CNAME dns.lr-g11.pt.
```

e zona para resolução inversa:

```
$ORIGIN 80.168.192.in-addr.arpa.
$TTL 86400
@ 1D SOA dns.lr-g11.pt. miguelferreira108.google.com. (
2016051902
3h
15
1w
3h
)
```

```
NS dns.lr-g11.pt.
MX 10 mail.lr-g11.pt.
```

```
1 PTR router.lr-g11.pt.
2 PTR dns.lr-g11.pt.
7 PTR mail.lr-g11.pt.
```

b.

```
[root@localhost named]# host router.lr-g11.pt
router.lr-g11.pt has address 172.16.0.1
```

c.

```
[root@localhost network-scripts]# host router.lr-g11.pt. 192.168.80.2
Using domain server:
Name: 192.168.80.2
Address: 192.168.80.2#53
Aliases:

router.lr-g11.pt has address 192.168.80.1
```

6.

- a. Ao ficheiro `named.conf`, como podemos ver abaixo, acrescentamos as seguintes zonas:

```
zone "dept.lr-g11.pt" IN {
    type slave;
    masters {10.0.0.2;};
    file "slave/dns.dept.lr-g11.pt.zone";
};

zone "0.0.10.in-addr.arpa" IN {
    type slave;
    masters {10.0.0.2;};
    file "slave/10.0.0.zone";
};
```

E também configuramos os ficheiros de zona para resolução direta:

```
$ORIGIN dept.lr-g11.pt.
$TTL 86400
@ 1D SOA dns.dept.lr-g11.pt. miguelferreira108.google.com. (
2016051905
3h
15
1w
3h
)

NS dns.dept.lr-g11.pt.
MX 10 mail.lr-g11.pt.

dept NS dns.dept
dns.dept A 10.0.0.2

dns A 172.16.0.2
mail A 172.16.0.7
router A 172.16.0.1

www.lr-g11.pt CNAME dns.lr-g11.pt.
```

e zona para resolução inversa:

```
$ORIGIN 0.0.10.in-addr.arpa.
$TTL 86400
@ 1D SOA dns.dept.lr-g11.pt. miguelferreira108.google.com. (
2016051900
3h
15
1w
3h
)
```

NS dns.dept.lr-g11.pt.
MX 10 mail.lr-g11.pt.

1 PTR router.dept.lr-g11.pt.
2 PTR dns.dept.lr-g11.pt.
7 PTR mail.lr-g11.pt.

b. Na captura *wireshark* apresentada abaixo, podemos detetar a transferência do domínio dept.lr-gX.pt do master para o slave, AXFR (*Authority Transfer*):

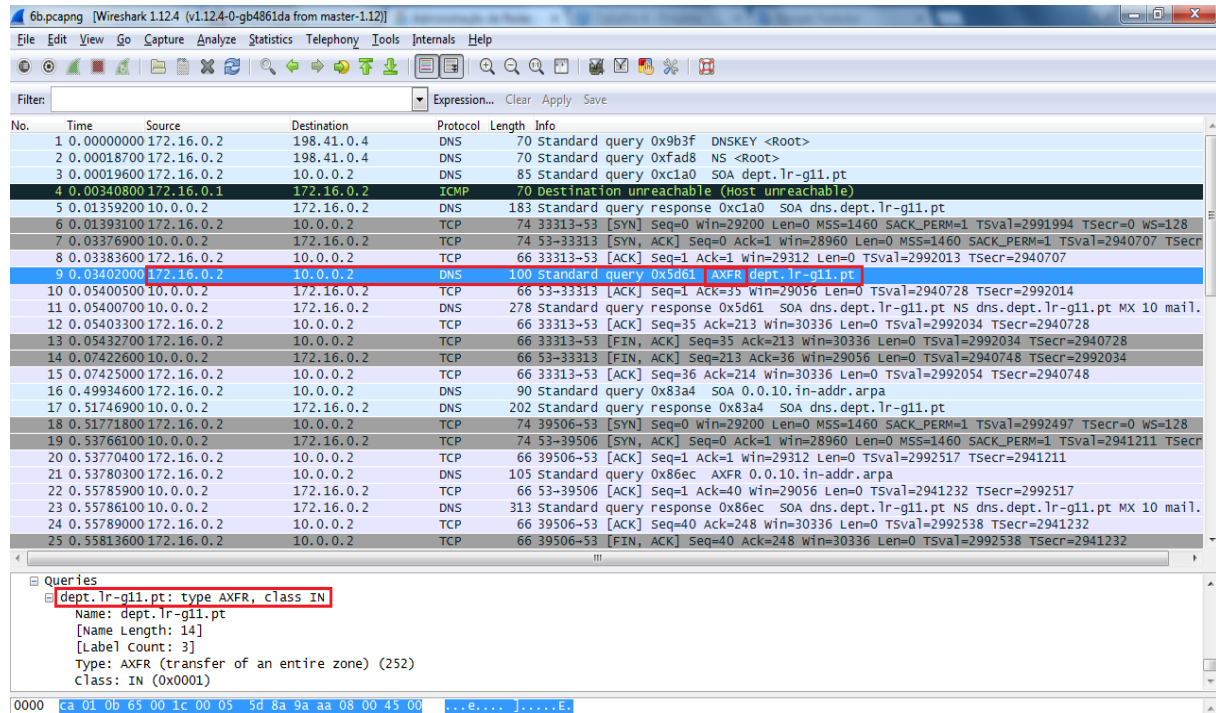


Figura 5: Captura *wireshark* no dns.dept.lr-gX.pt.

c. O registo SOA (*Start Of Authority*), como o próprio nome indica, significa início de autoridade. Este é o registo mais importante dentro do DNS, é sempre o primeiro registo de qualquer zona, e sozinho consegue determinar grande parte das informações necessárias para a correta resolução de um domínio, tais como:

- nome da zona;
- servidor DNS principal (*primary master*), servidor que é a autoridade para a referida zona;
- endereço de email do administrador da zona;
- número de série, que é um indicativo se houve ou não alterações na zona;
- período de refrescamento (transferência de domínio para os *slaves*);
- período para nova tentativa se falhar a transferência de domínio;
- período de expiração da zona, após o qual um *slave* deixa de ser autoritário para esta zona (se não a conseguir refrescar);

- período para *caching* negativo, da indicação de que um dado nome não existe nesta zona.

SOA da zona é pedido antes de fazer a transferência de domínio para comparar o número de série com o que tem atualmente, se este for o mesmo, significa que não houve alterações na zona, e se for diferente, significa que é necessário transferir novamente a zona (pedido AXFR (transferência completa) ou IXFR (transferência incremental)).

d. Sim, o protocolo de transporte usado para a transferência de domínio é o **TCP**, enquanto que o que é normalmente usado para as outras perguntas DNS é o **UDP**, uma vez que normalmente os pedidos e respostas são curtos e cabem num único pacote, o que gerava um desperdício se usa-se TCP. Como as transferências de zona, entre *master* e *slave*, são normalmente um grande volume de informação, que precisa de fiabilidade, e as mensagens são precedidas por um número de 16 bits indicando o tamanho das mesmas (TCP não faz delineação de mensagens), é indispensável a utilização do TCP como protocolo de transporte.

- e. Captura de pacotes na pseudo-interface any no dns.lr-gX.pt:

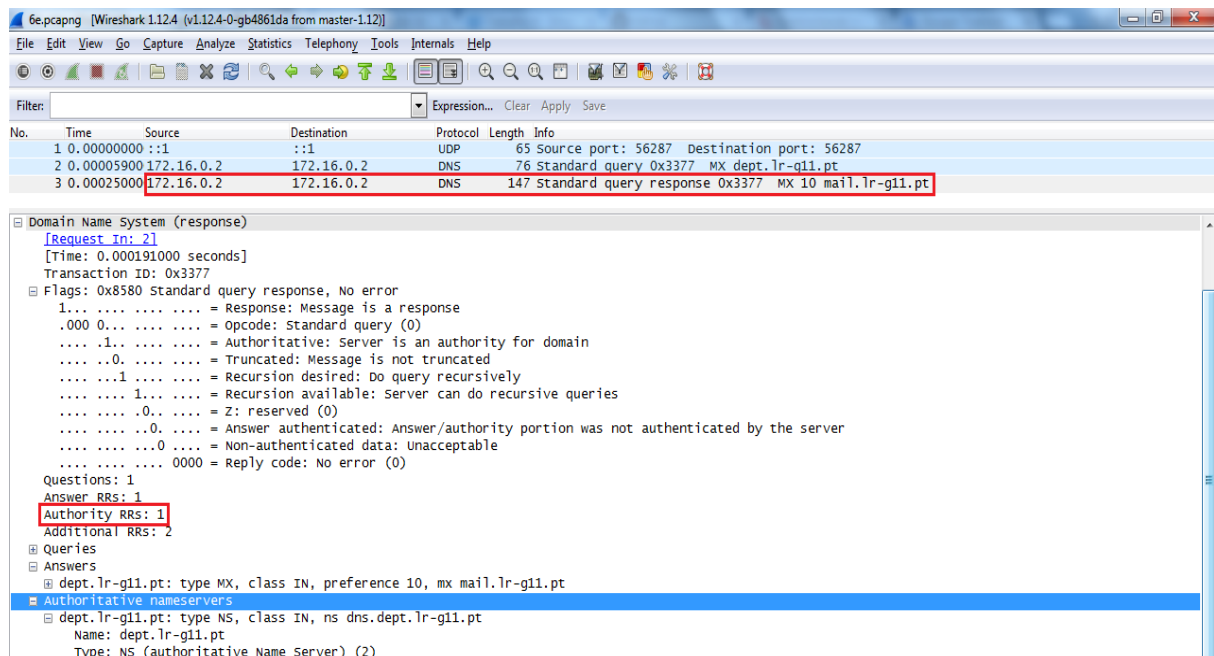


Figura 6: Captura *wireshark* no dns.lr-gX.pt.

f. A resposta que obteve na alínea anterior é autoritativa? Justifique. (texRes) Sim, a resposta obtida é autoritativa, como podemos ver na figura abaixo (*Authoritative nameservers*). Também sabemos que os servidores *master* e *slave* são autoritativos para a zona.

7. Conteúdo do ficheiro named.ca:

```
; <<>> DiG 9.9.2-P1-RedHat-9.9.2-6.P1.fc18 <<>> +bufsize=1200 +norec
@a.root-servers.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25828
```

```

;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 23

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;. IN NS

;; ANSWER SECTION:
. 518400 IN NS a.root-servers.net.
. 518400 IN NS b.root-servers.net.
. 518400 IN NS c.root-servers.net.
. 518400 IN NS d.root-servers.net.
. 518400 IN NS e.root-servers.net.
. 518400 IN NS f.root-servers.net.
. 518400 IN NS g.root-servers.net.
. 518400 IN NS h.root-servers.net.
. 518400 IN NS i.root-servers.net.
. 518400 IN NS j.root-servers.net.
. 518400 IN NS k.root-servers.net.
. 518400 IN NS l.root-servers.net.
. 518400 IN NS m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 3600000 IN A 198.41.0.4
a.root-servers.net. 3600000 IN AAAA 2001:503:ba3e::2:30
b.root-servers.net. 3600000 IN A 192.228.79.201
c.root-servers.net. 3600000 IN A 192.33.4.12
d.root-servers.net. 3600000 IN A 199.7.91.13
d.root-servers.net. 3600000 IN AAAA 2001:500:2d::d
e.root-servers.net. 3600000 IN A 192.203.230.10
f.root-servers.net. 3600000 IN A 192.5.5.241
f.root-servers.net. 3600000 IN AAAA 2001:500:2f::f
g.root-servers.net. 3600000 IN A 192.112.36.4
h.root-servers.net. 3600000 IN A 128.63.2.53
h.root-servers.net. 3600000 IN AAAA 2001:500:1::803f:235
i.root-servers.net. 3600000 IN A 192.36.148.17
i.root-servers.net. 3600000 IN AAAA 2001:7fe::53
j.root-servers.net. 3600000 IN A 192.58.128.30
j.root-servers.net. 3600000 IN AAAA 2001:503:c27::2:30
k.root-servers.net. 3600000 IN A 193.0.14.129
k.root-servers.net. 3600000 IN AAAA 2001:7fd::1
l.root-servers.net. 3600000 IN A 199.7.83.42
l.root-servers.net. 3600000 IN AAAA 2001:500:3::42
m.root-servers.net. 3600000 IN A 202.12.27.33
m.root-servers.net. 3600000 IN AAAA 2001:dc3::35

;; Query time: 78 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Mon Jan 28 15:33:31 2013
;; MSG SIZE rcvd: 699

```

O ficheiro básico named.ca contém registos NS que nomeiam os root servers, e registos A

que fornecem os respectivos endereços dos root servers. Este ficheiro distingue a resolução de domínios ligados e não ligados à Internet: numa rede não ligada à Internet, cada servidor DNS tem entradas no `named.ca` designando um root server dentro da rede não ligada; numa rede ligada à Internet o `named.ca` terá de nomear os root servers da Internet (é possível obter o `named.ca` em `ftp.rs.internic.net`).