

**Universidade do Minho**

# **Comunicações por Computador**

## **Trabalho Prático 3**

**Grupo 43**

**José João Cardoso Gonçalves a93204**  
**Bernardo Emanuel Magalhães Saraiva a93189**  
**Daniel Torres Azevedo a93324**

**17/12/2020**

**a) Qual o conteúdo do ficheiro /etc/resolv.conf e para que serve essa informação?**

O ficheiro resolv.conf é utilizado para configurar o DNS resolver. Este ficheiro contém a lista dos domínios configurados.

```
core@xubuncore:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search lan
```

**Figura 1**

**b) Os servidores [www.di.uminho.pt](http://www.di.uminho.pt). e [www.europa.eu](http://www.europa.eu). têm endereços IPv6? Se sim, quais?**

Ao questionar o servidor [www.di.uminho.pt](http://www.di.uminho.pt). (usando o DNS da uminho) quanto à existência de entradas IPv6 obtemos a resposta, como verificado no screenshot a seguir, que o nome de domínio verdadeiro do servidor é o [ww5.di.uminho.pt](http://ww5.di.uminho.pt).

```
saraiva@saraiva-OMEN:~$ dig @193.137.16.75 AAAA www.di.uminho.pt

; <<>> DiG 9.16.6-Ubuntu <<>> @193.137.16.75 AAAA www.di.uminho.pt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 7960
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: a578f1d4d20799721697053661928717ed88b7cd3fceff4d (good)
;; QUESTION SECTION:
;www.di.uminho.pt.      IN      AAAA

;; ANSWER SECTION:
www.di.uminho.pt.      14400   IN      CNAME   ww5.di.uminho.pt.

;; AUTHORITY SECTION:
di.uminho.pt.          14400   IN      SOA      dns.di.uminho.pt. dnsadmin.di.uminho.pt. 2021110201 28800 7200 2419200 43200

;; Query time: 16 msec
;; SERVER: 193.137.16.75#53(193.137.16.75)
;; WHEN: seg nov 15 16:13:11 WET 2021
;; MSG SIZE rcvd: 141
```

**Figura 2**

Prosseguindo a análise, questionamos agora o endereço obtido anteriormente acerca de entradas do tipo AAAA. Obtendo a resposta apresentada a seguir.

```
saraiva@saraiva-OMEN:~$ dig @193.137.16.75 AAAA www5.di.uminho.pt

; <<>> DiG 9.16.6-Ubuntu <<>> @193.137.16.75 AAAA www5.di.uminho.pt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23837
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2b6ad5c369bc44c01638fa9d61928d376d93469852aa1647 (good)
;; QUESTION SECTION:
;www5.di.uminho.pt.          IN      AAAA

;; AUTHORITY SECTION:
di.uminho.pt.               14400   IN      SOA     dns.di.uminho.pt. dnsadmin.di.uminho.pt. 2021110201 28800 7200 2419200 43200

;; Query time: 16 msec
;; SERVER: 193.137.16.75#53(193.137.16.75)
;; WHEN: seg nov 15 16:39:19 WET 2021
;; MSG SIZE rcvd: 123
```

Figura 3

Como é possível observar, não obtivemos nenhuma resposta, o que demonstra que o endereço [www.di.uminho.pt](http://www.di.uminho.pt) não possui nenhum endereço IPv6.

No que diz respeito ao servidor [www.europa.eu](http://www.europa.eu) ao executar a query AAAA obtemos a seguinte resposta:

```
saraiva@saraiva-OMEN:~$ dig AAAA www.europa.eu.

; <<>> DiG 9.16.6-Ubuntu <<>> AAAA www.europa.eu.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53064
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.europa.eu.            IN      AAAA

;; ANSWER SECTION:
www.europa.eu.             600     IN      CNAME   ip-europa.ec.europa.eu.
ip-europa.ec.europa.eu.    299     IN      AAAA    2a01:7080:24:100::666:25
ip-europa.ec.europa.eu.    299     IN      AAAA    2a01:7080:14:100::666:25

;; Query time: 228 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: seg nov 15 16:47:18 WET 2021
;; MSG SIZE rcvd: 125
```

Figura 4

Verificando assim, a existência de dois servidores IPv6 com os seguintes IPs : 2a01:7080:24:100::666:25 e 2a01:7080:14:100::666:25.

**c) Quais os servidores de nomes definidos para os domínios: “gov.pt.” e “.”?**

Através do comando dig gov.pt. NS obtém-se os os servidores de nomes definidos para este endereço através da seguinte resposta:

```
;; ANSWER SECTION:
gov.pt.      6      IN      NS      ns02.fccn.pt.
gov.pt.      6      IN      NS      nsp.dnsnode.net.
gov.pt.      6      IN      NS      europe1.dnsnode.net.
gov.pt.      6      IN      NS      a.dns.pt.
gov.pt.      6      IN      NS      dns1.gov.pt.
```

**Figura 5**

Repetindo este comando para o “.” (conhecido como root), obtemos a resposta de que existem 13 servidores DNS para este endereço.

```
;; ANSWER SECTION:
.            4515   IN      NS      j.root-servers.net.
.            4515   IN      NS      f.root-servers.net.
.            4515   IN      NS      i.root-servers.net.
.            4515   IN      NS      e.root-servers.net.
.            4515   IN      NS      k.root-servers.net.
.            4515   IN      NS      a.root-servers.net.
.            4515   IN      NS      h.root-servers.net.
.            4515   IN      NS      g.root-servers.net.
.            4515   IN      NS      b.root-servers.net.
.            4515   IN      NS      c.root-servers.net.
.            4515   IN      NS      m.root-servers.net.
.            4515   IN      NS      d.root-servers.net.
.            4515   IN      NS      l.root-servers.net.
```

**Figura 6**

**d) Existe o domínio efiko.academy.? Com base na informação obtida do DNS, nomeadamente os registos associados a esse nome, diga se o considera um host ou um domínio de nomes.**

Fazendo dig efiko.academy. ANY reparamos que apresenta um SOA, pelo que podemos confirmar diretamente que é um domínio. Posteriormente, foi-se verificar se era também um host através do endereço IPV4 que se verificou na Answer Section - 5.134.7.2.

```

core@xubuncore:~$ dig efiko.academy. ANY
; <<> DiG 9.16.1-Ubuntu <<> efiko.academy. ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48081
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;efiko.academy.                IN      ANY

;; ANSWER SECTION:
efiko.academy.        1790    IN      SOA     ns3.combell.net. hostmaster.efiko.academy. 2021033008 10800 3600 604800 40000
efiko.academy.        1790    IN      MX      10 alt4.aspmx.l.google.com.
efiko.academy.        1790    IN      MX      5 alt1.aspmx.l.google.com.
efiko.academy.        1790    IN      MX      5 alt2.aspmx.l.google.com.
efiko.academy.        1790    IN      MX      10 alt3.aspmx.l.google.com.
efiko.academy.        1790    IN      MX      1 aspmx.l.google.com.
efiko.academy.        1790    IN      AAAA    2a00:1c98:1000:11d4:0:2:8511:1ff8
efiko.academy.        1660    IN      A       5.134.7.2
efiko.academy.        1656    IN      NS      ns3.combell.net.
efiko.academy.        1656    IN      NS      ns4.combell.net.

;; Query time: 24 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui nov 11 08:40:23 WET 2021
;; MSG SIZE rcvd: 298

```

Figura 7

Para fazer essa verificação, fizemos dig efiko.academy. e verificamos que se apresentava novamente o mesmo endereço, pelo que se conclui que não é um host.

```

core@xubuncore:~$ dig efiko.academy.
; <<> DiG 9.16.1-Ubuntu <<> efiko.academy.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3908
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;efiko.academy.                IN      A

;; ANSWER SECTION:
efiko.academy.        1613    IN      A       5.134.7.2

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui nov 11 08:41:09 WET 2021
;; MSG SIZE rcvd: 58

```

Figura 8

e) Qual é o servidor DNS primário definido para o domínio gov.pt.? Este servidor primário (master) aceita queries recursivas? Porquê?

Ao efetuar o comando `dig gov.pt. SOA`, conseguimos descobrir o servidor DNS primário, sendo este o primeiro que aparece: **dnssec.gov.pt**

```
core@xubuncore:~$ dig gov.pt. SOA

; <<>> DiG 9.16.1-Ubuntu <<>> gov.pt. SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29621
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gov.pt.                                IN      SOA

;; ANSWER SECTION:
gov.pt.      492      IN      SOA      dnssec.gov.pt. dns.ceger.gov.pt. 2019072064 18000 7200 2419200 86400

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: sáb nov 13 18:03:58 WET 2021
;; MSG SIZE rcvd: 88
```

Figura 9

Para analisar se este servidor master aceita queries recursivas, basta analisar as flags ao fazer efetuar um `dig`, sendo que ao efetuar este comando nos são apresentadas as flags **rd** e **ra** (*recursive desired* e *recursive available*, respetivamente). Deste modo, confirmamos que este servidor aceita queries recursivas.

f) Obtenha uma resposta “autoritativa” para a questão anterior

Para obter uma resposta “autoritativa”, necessitamos de descobrir o endereço de um servidor DNS que responde pelo domínio gov.pt. Para isso usamos a query NS e apercebemo-nos que um dos DNS é o `dns1.gov.pt`.

```
saraiva@saraiva-OMEN:~$ dig gov.pt. ns

; <<>> DiG 9.16.6-Ubuntu <<>> gov.pt. ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62144
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gov.pt.                                IN      NS

;; ANSWER SECTION:
gov.pt.      447      IN      NS      nsp.dnsnode.net.
gov.pt.      447      IN      NS      nsp.dnsnode.net.
gov.pt.      447      IN      NS      ns02.fccn.pt.
gov.pt.      447      IN      NS      dns1.gov.pt.
gov.pt.      447      IN      NS      europe1.dnsnode.net.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui nov 18 10:04:17 WET 2021
;; MSG SIZE rcvd: 149
```

Figura 10

Posteriormente, descobriremos o IP deste servidor de DNS, como mostrado na figura

```
saraiva@saraiva-OMEN:~$ dig A dns1.gov.pt.

; <<>> DiG 9.16.6-Ubuntu <<>> A dns1.gov.pt.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31505
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;dns1.gov.pt.                IN      A

;; ANSWER SECTION:
dns1.gov.pt.                568     IN      A      193.47.185.3

;; Query time: 156 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui nov 18 10:06:48 WET 2021
;; MSG SIZE rcvd: 56
```

Figura 11

Por fim, será necessário questionar o domínio gov.pt à cerca de registos SOA, usando um DNS do domínio. Como, obtivemos a resposta com a flag 'aa' podemos confirmar que a resposta é autoritativa.

```
saraiva@saraiva-OMEN:~$ dig @193.47.185.3 gov.pt SOA

; <<>> DiG 9.16.6-Ubuntu <<>> @193.47.185.3 gov.pt SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63901
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;gov.pt.                     IN      SOA

;; ANSWER SECTION:
gov.pt.                      600     IN      SOA     dnssec.gov.pt. dns.ceger.gov.pt. 2019072064 18000 7200 2419200 86400

;; AUTHORITY SECTION:
gov.pt.                      600     IN      NS      a.dns.pt.
gov.pt.                      600     IN      NS      europe1.dnsnode.net.
gov.pt.                      600     IN      NS      nsp.dnsnode.net.
gov.pt.                      600     IN      NS      ns02.fccn.pt.
gov.pt.                      600     IN      NS      dns1.gov.pt.

;; ADDITIONAL SECTION:
dns1.gov.pt.                 600     IN      A      193.47.185.3

;; Query time: 71 msec
;; SERVER: 193.47.185.3#53(193.47.185.3)
;; WHEN: qui nov 18 10:09:41 WET 2021
;; MSG SIZE rcvd: 218
```

Figura 12

**g) Onde são entregues as mensagens de correio eletrónico dirigidas a [marcelo@presidencia.pt](mailto:marcelo@presidencia.pt)?**

Para concluir acerca de onde as mensagens dirigidas a [marcelo@presidencia.pt](mailto:marcelo@presidencia.pt) são entregues, primeiramente fez-se um dig para o Mail Exchanger do domínio presidencia.pt - **dig presidencia.pt MX**, pelo que reparamos que temos dois DNS para onde as mensagens são dirigidas, sendo estas **mail1.presidencia.pt** e **mail2.presidencia.pt**:

```
core@xubuncore:~$ dig presidencia.pt MX

; <<> DiG 9.16.1-Ubuntu <<> presidencia.pt MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28539
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;presidencia.pt.                IN      MX

;; ANSWER SECTION:
presidencia.pt.      359     IN      MX      50 mail1.presidencia.pt.
presidencia.pt.      359     IN      MX      10 mail2.presidencia.pt.

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui nov 11 08:57:52 WET 2021
;; MSG SIZE rcvd: 87
```

**Figura 13**

Posteriormente, analisou-se os IP's de cada um destes através de **dig mail1.presidencia.pt** e **dig mail2.presidencia.pt** e inferiram-se os seguintes resultados:

```
core@xubuncore:~$ dig mail1.presidencia.pt

; <<> DiG 9.16.1-Ubuntu <<> mail1.presidencia.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19268
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;mail1.presidencia.pt.         IN      A

;; ANSWER SECTION:
mail1.presidencia.pt. 1446    IN      A      192.162.17.31

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui nov 11 08:58:42 WET 2021
;; MSG SIZE rcvd: 65
```

**Figura 14**



```

core@xubuncore:~$ dig mail2.presidencia.pt

; <<>> DiG 9.16.1-Ubuntu <<>> mail2.presidencia.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59904
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;mail2.presidencia.pt.      IN      A

;; ANSWER SECTION:
mail2.presidencia.pt.      86400   IN      A      192.162.17.32

;; Query time: 28 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui nov 11 09:41:46 WET 2021
;; MSG SIZE rcvd: 65

```

Figura 15

**h) Que informação é possível obter, via DNS, acerca de gov.pt?**

Ao utilizar a query NS, obtemos a lista de todos os DNS que respondem por este endereço. Portanto, recorrendo a **dig gov.pt. NS**, obtemos os seguintes endereços:

```

core@xubuncore:~$ dig gov.pt. NS

; <<>> DiG 9.16.1-Ubuntu <<>> gov.pt. NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46517
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gov.pt.                  IN      NS

;; ANSWER SECTION:
gov.pt.                   370     IN      NS      a.dns.pt.
gov.pt.                   370     IN      NS      nsp.dnsnode.net.
gov.pt.                   370     IN      NS      dns1.gov.pt.
gov.pt.                   370     IN      NS      ns02.fccn.pt.
gov.pt.                   370     IN      NS      europe1.dnsnode.net.

```

Figura 16

Conseguimos saber que existem 5 servidores de DNS a responder pelo domínio gov.pt.

```

root@xubuncore:~# dig a.dns.pt ANY

<<>> DiG 9.16.1-Ubuntu <>> a.dns.pt ANY
;; global options: +cmd
;; Got answer:
;;->HEADER<<- opcode: QUERY, status: NOERROR, id: 47851
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 65494
;; QUESTION SECTION:
a.dns.pt.                IN      ANY

;; ANSWER SECTION:
a.dns.pt.                871     IN      RRSIG   AAAA 13 3 900 20211214230042 20211114230042 9534 dns.pt. KIy/ZiIRwZuetAnpKv5ln17Xku5zVsLKfAr7iRiPv6dEr30jPK4peJ I9dmSsKUU0IZodAUPSPvGudgIFllj5g
a.dns.pt.                871     IN      RRSIG   A 13 3 900 20211214230042 20211114230042 9534 dns.pt. /aAjw068fEd/CLiUo8dWl8kZMq2wQhidx3ByVvCkDHmrt0G+wS54+ZH L01H6lVvIIDjJ5dLbbPcIoaoF22dg==
a.dns.pt.                871     IN      AAAA    2a04:6d80:::1
a.dns.pt.                871     IN      A       185.39.208.1

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: sex nov 19 00:20:23 WET 2021
;; MSG SIZE rcvd: 285

```

### Figura 17

Posteriormente fazendo o comando **dig a.dns.pt ANY**, podemos saber que este servidor tem um IPv4 e também um IPv6.

**i) Consegue interrogar o DNS sobre o endereço IPv6 2001:690:2080:8005::38 usando algum dos clientes DNS? Que informação consegue obter? Supondo que teve problemas com esse endereço, consegue obter um contacto do responsável por esse IPv6?**

É possível interrogar o DNS sobre o endereço IPv6 2001:690:2080:8005::38 recorrendo a:

- dig -x 2001:690:2080:8005::38 - ou seja, fazendo uma reverse query ao servidor.

```
core@xubuncore:~$ dig -x 2001:690:2080:8005::38

; <<> DiG 9.16.1-Ubuntu <<> -x 2001:690:2080:8005::38
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 9844
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;8.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.8.0.8.0.2.0.9.6.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
8.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.8.0.8.0.2.0.9.6.0.1.0.0.2.ip6.arpa. 7121 IN PTR smtp01.fccn.pt.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: sáb nov 13 18:36:42 WET 2021
;; MSG SIZE rcvd: 129
```

### Figura 18

Com esta resposta, é possível descobrir o domínio do endereço inicialmente fornecido e questionar o mesmo acerca do seu registo SOA, sendo possível encontrar neste o email do responsável pelo servidor, verificando que se trata

```
saraiva@saraiva-OMEN:~$ dig SOA fccn.pt

; <<>> DiG 9.16.6-Ubuntu <<>> SOA fccn.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60291
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;fccn.pt.                IN      SOA

;; ANSWER SECTION:
fccn.pt.                10800   IN      SOA      ns01.fccn.pt. hostmaster.fccn.pt. 2021111601 21600 7200 1209600 300

;; Query time: 100 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui nov 18 10:25:16 WET 2021
;; MSG SIZE rcvd: 88
```

Figura 19

j) Os secundários usam um mecanismo designado por “Transferência de zona” para se atualizarem automaticamente a partir do primário, usando os parâmetros definidos no Record do tipo SOA do domínio. Descreve sucintamente esse mecanismo com base num exemplo concreto (ex: uminho.pt).

As transferências de zona são uns dos métodos disponíveis para replicar bancos de dados DNS. Este tipo de transação utiliza TCP para transporte e assume a forma de cliente-servidor.

O servidor secundário solicita a transferência de dados ao servidor primário.

Para realizar uma transferência de zona primeiramente temos que descobrir o servidor primário, por isso realizamos o comando **dig uminho.pt SOA**.

```
core@xubuncore:~$ dig uminho.pt SOA

; <<>> DiG 9.16.1-Ubuntu <<>> uminho.pt SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60725
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;uminho.pt.              IN      SOA

;; ANSWER SECTION:
uminho.pt.              14400   IN      SOA      dns.uminho.pt. servicos.scom.uminho.pt. 2021111501 14400 7200 1209600 300

;; Query time: 24 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: sex nov 19 21:20:45 WET 2021
;; MSG SIZE rcvd: 92
```

Figura 20

Seguidamente fazemos **dig uminho.pt NS**, para sabermos os restantes servidores da uminho.pt.

```
core@xubuncore:~$ dig uminho.pt NS

; <> DiG 9.16.1-Ubuntu <> uminho.pt NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59068
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;uminho.pt.                IN      NS

;; ANSWER SECTION:
uminho.pt.                14400   IN      NS      ns02.fccn.pt.
uminho.pt.                14400   IN      NS      dns3.uminho.pt.
uminho.pt.                14400   IN      NS      dns2.uminho.pt.
uminho.pt.                14400   IN      NS      dns.uminho.pt.

;; Query time: 92 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: sex nov 19 21:31:19 WET 2021
;; MSG SIZE rcvd: 118
```

Figura 21

Finalmente fazemos a transferência de zona, entre o servidor primário(dns.uminho.pt) e um dos servidor secundário (dns2.uminho.pt), recorrendo ao comando **dig @dns.uminho.pt @dns2.uminho.pt AXFR**.

```
core@xubuncore:~$ dig @dns.uminho.pt @dns2.uminho.pt AXFR

; <> DiG 9.16.1-Ubuntu <> @dns.uminho.pt @dns2.uminho.pt AXFR
; (2 servers found)
;; global options: +cmd
;; Query time: 96 msec
;; SERVER: 193.137.16.75#53(193.137.16.75)
;; WHEN: sex nov 19 21:38:44 WET 2021
;; MSG SIZE rcvd: 56
```

Figura 22

## PARTE II

Esta parte do trabalho pretende que o grupo instale, configure e teste um domínio DNS com o nome de **CC.PT**.

Começou-se por transferir os ficheiros da máquina remota para duas pastas (primário e **secundário**), e preparar todo o ambiente, alterando as configurações de **apparmor.service** e desligando o **bind9**.

Em seguida, tratou-se da configuração do servidor primário, seguindo o guião para tal, sendo que os passos 1, 2 e 3 foram seguidos à risca, sendo que no passo 3 se criou uma zona para cc.pt e uma zona cada rede (neste caso 4).

No passo 4, começou-se por criar uma base partindo do ficheiro db.local, e a partir daí foi-se complementando e alterando este ficheiro, pelo que se descreve em seguida:

1. Começou-se por alterar o servidor primário (**ns.cc.pt.**) e o email do administrador (**g43pl04.cc.pt.**), tomando atenção que o primeiro ponto substitui o @ do email.
2. Adicionou-se os servidores primário e secundário;
3. Definiu-se os três servidores de domínio;
4. Definiu-se o servidor de email principal, servidor web, servidor pop e imap;
5. Registou-se o portátil 1 com alias g43.cc.pt;
6. Registou-se no domínio de nomes Orca, Foca e Golfinho;
7. Registrar o domínio reverso;
8. Registrar os servidores de email (MX), assim como os domínios reversos;

De igual modo, para o passo 5 obteve-se uma base do ficheiro db.2-2-10.rev através do db.127 e foi-se progressivamente complementando e alterando este ficheiro.

Este procedimento foi replicado para mais 3 zonas (uma vez que temos 4 LAN's), sendo que se criou um ficheiro para cada uma das zonas e procedeu-se às alterações necessárias.

Em seguida explica-se como se procedeu para o ficheiro db.2-2-10.rev, sendo que todos os outros foram elaborados de forma semelhante:

1. Alterou-se o servidor primário e o email de administrador;
2. Adicionou-se os servidores primário e secundário;
3. Adicionou-se os três nodos correspondentes ao LAN2 (ou rede/LAN correspondente ao ficheiro);

## 2.2 - Configuração do cliente e teste do primário

Nesta secção apresentar-se-á os vários testes realizados, assim como os resultados obtidos.

### 1.

- Iniciar o core com a topologia CC-Topo-2022.imn;
- Abrir uma bash no nó "**Servidor1**" e executar o comando de arranque do servidor:  

```
sudo /usr/sbin/named -c /home/core/primario/named.conf -g
```

- Abrir uma bash no nó "**Portatil1**" e testar uma *query* ao servidor primário:

```
$ nslookup www.cc.pt. 10.2.2.1
... ou ...
$ nslookup - 10.2.2.1
> www.cc.pt
...
```

Figura 23

Resultado do teste:

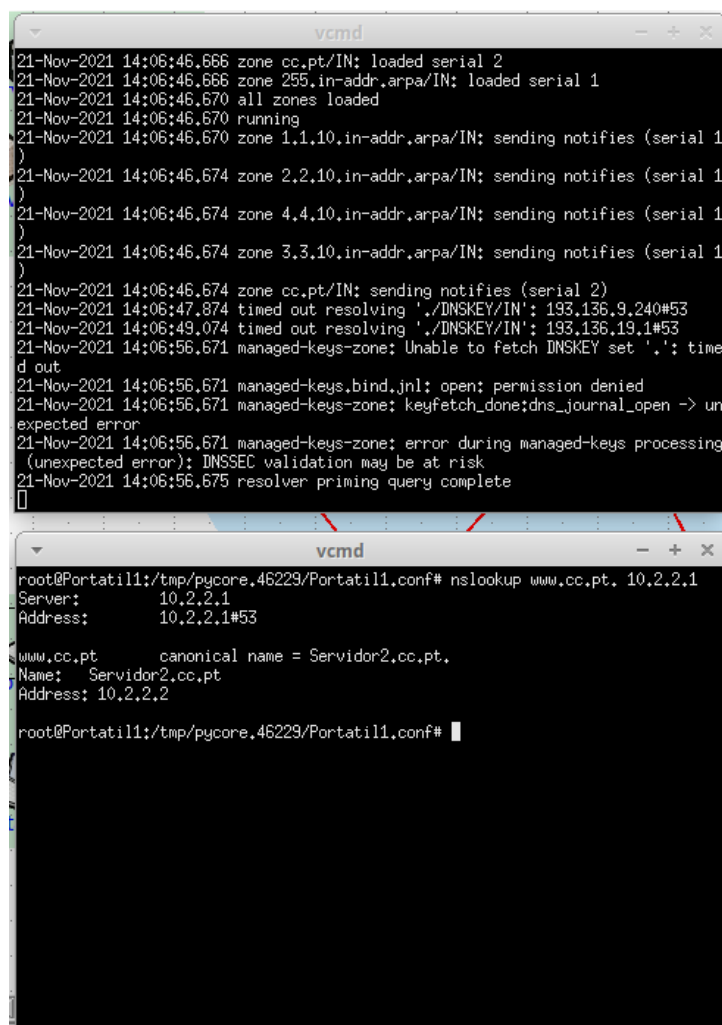


Figura 24

## 2.

- modificar o `/etc/resolv.conf` (editar fora do CORE) e testar de novo com `nslookup` ou `dig`:

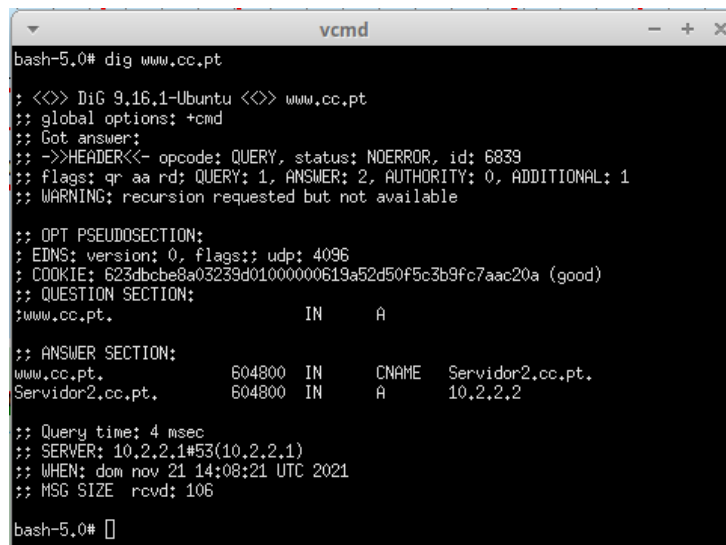
(nota: esta opção pode não ser necessária; evitar editar o `/etc/resolv.conf` se estiver na sua máquina de trabalho Linux nativa; caso edite o ficheiro para efeitos deste trabalho, pode voltar a repor o conteúdo original, se o copiar previamente para outro local)

```
$ cat /etc/resolv.conf
nameserver 10.2.2.1
domain cc.pt
search cc.pt

$ nslookup www.cc.pt
$ dig www.cc.pt
```

Figura 25

### Resultado do teste:



```
bash-5.0# dig www.cc.pt

; <<> DiG 9.16.1-Ubuntu <<> www.cc.pt
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 6839
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 623dbcb8a03239d0100000619a52d50f5c3b9fc7aac20a (good)
;; QUESTION SECTION:
;www.cc.pt.                IN      A

;; ANSWER SECTION:
www.cc.pt.                 604800  IN      CNAME   Servidor2.cc.pt.
Servidor2.cc.pt.          604800  IN      A       10.2.2.2

;; Query time: 4 msec
;; SERVER: 10.2.2.1#53(10.2.2.1)
;; WHEN: dom nov 21 14:08:21 UTC 2021
;; MSG SIZE rcvd: 106

bash-5.0#
```

Figura 26

## 2.3 - Configuração do servidor secundário

### 1.

4. Executar o core e abrir um bash no nó **Golfinho**. Executar o servidor, na linha de comando, fazendo por exemplo:

```
$ sudo /usr/sbin/named -c /home/core/secundario/named.conf -g
```

*Nota: verificar se os dados foram transferidos do primário para o secundário*

5. Teste simples com `nslookup`, em qualquer nó da topologia:

```
$ nslookup www.cc.pt. 10.3.3.2
(...)
$ nslookup - 10.3.3.2
> www.cc.pt
```

Figura 27

## Resultado do teste:

Estando os 2 servidores a correr : primário no servidor 1 e secundário no golfinho, obteve-se a seguinte resposta:

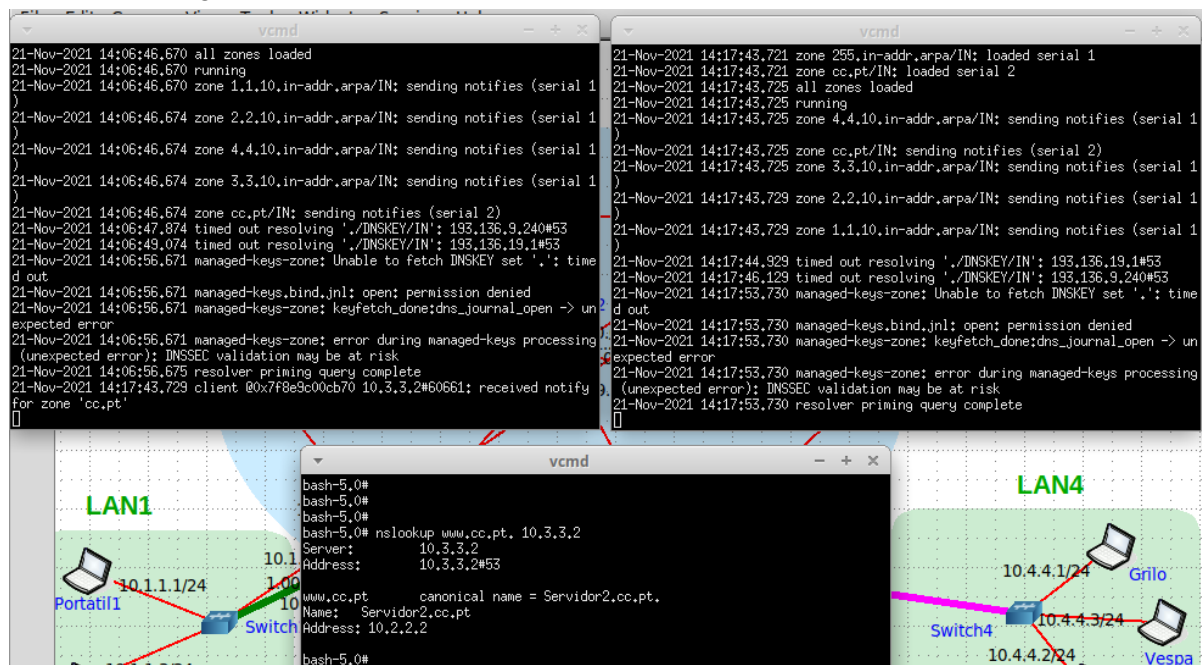
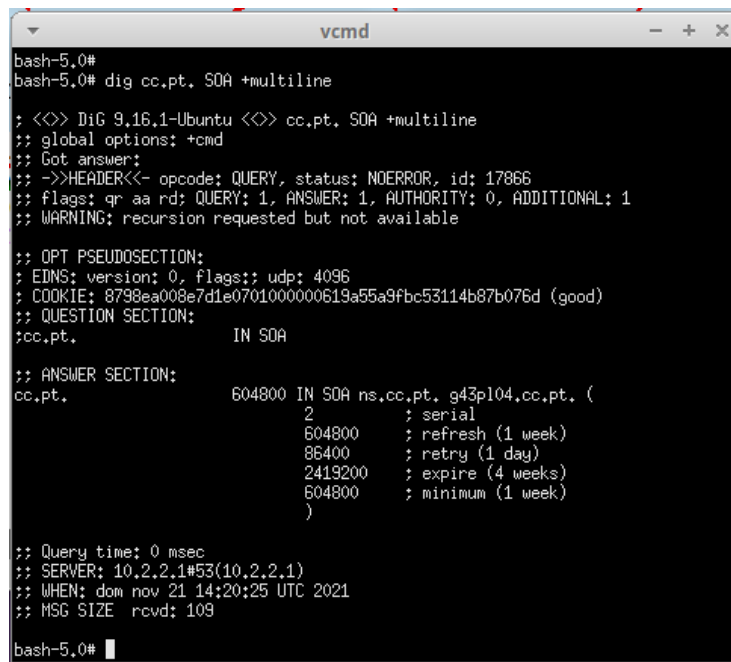


Figura 28



## Testes adicionais:

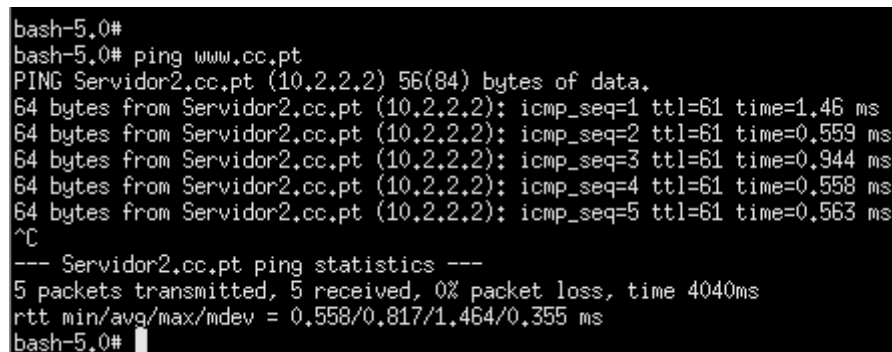
1. Verificar que nameserver responde a um dig quando temos o servidor primário e o secundário a correr:



```
bash-5.0#  
bash-5.0# dig cc.pt. SOA +multiline  
  
; <<> DiG 9.16.1-Ubuntu <<> cc.pt. SOA +multiline  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 17866  
;; flags: qr aa rd: QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
;; WARNING: recursion requested but not available  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
; COOKIE: 8798ea008e7d1e0701000000619a55a9fbc53114b87b076d (good)  
;; QUESTION SECTION:  
;cc.pt.  
      IN SOA  
  
;; ANSWER SECTION:  
cc.pt.      604800 IN SOA ns.cc.pt. g43p104.cc.pt. (  
              2      ; serial  
              604800 ; refresh (1 week)  
              86400  ; retry (1 day)  
              2419200 ; expire (4 weeks)  
              604800 ; minimum (1 week)  
              )  
  
;; Query time: 0 msec  
;; SERVER: 10.2.2.1#53(10.2.2.1)  
;; WHEN: dom nov 21 14:20:25 UTC 2021  
;; MSG SIZE rcvd: 109  
  
bash-5.0#
```

Figura 29

2. Efetuar um ping:



```
bash-5.0#  
bash-5.0# ping www.cc.pt  
PING Servidor2.cc.pt (10.2.2.2) 56(84) bytes of data:  
64 bytes from Servidor2.cc.pt (10.2.2.2): icmp_seq=1 ttl=61 time=1.46 ms  
64 bytes from Servidor2.cc.pt (10.2.2.2): icmp_seq=2 ttl=61 time=0.559 ms  
64 bytes from Servidor2.cc.pt (10.2.2.2): icmp_seq=3 ttl=61 time=0.944 ms  
64 bytes from Servidor2.cc.pt (10.2.2.2): icmp_seq=4 ttl=61 time=0.558 ms  
64 bytes from Servidor2.cc.pt (10.2.2.2): icmp_seq=5 ttl=61 time=0.563 ms  
^C  
--- Servidor2.cc.pt ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4040ms  
rtt min/avg/max/mdev = 0.558/0.817/1.464/0.355 ms  
bash-5.0#
```

Figura 30

### 3. Parar apenas o servidor primário e fazer novamente uma query sobre o domínio cc.pt:

The screenshot displays a network simulation environment with two main components: terminal logs and network diagrams.

**Terminal Logs (vcmd):**

- Left Window:** Shows logs for the primary server (10.3.3.2). It includes messages about DNSKEY set fetching, permission denied errors, and a resolver priming query complete. The server is identified as 'Servidor1'.
- Right Window:** Shows logs for the secondary server (10.3.3.2). It includes messages about zone loading, sending notifications, and a resolver priming query complete. The server is identified as 'Servidor2'.

**Network Diagrams:**

- LAN1:** A network diagram showing a switch connected to three laptops (Portatil1, Portatil2, Portatil3) with IP addresses 10.1.1.1/24, 10.1.1.2/24, and 10.1.1.3/24 respectively.
- LAN4:** A network diagram showing a switch connected to three laptops (Grilo, Vespa, Cigarra) with IP addresses 10.4.4.1/24, 10.4.4.2/24, and 10.4.4.3/24 respectively.

**Central Terminal Output:**

```

rtt min/avg/max/ndev = 0.958/0.817/1.464/0.355 ms
bash-5.0# dig cc.pt. SOA +multiline
; <<> Dig 9.16.1-Ubuntu <<> cc.pt. SOA +multiline
; global options: +vcmd
; Got answer:
; ->HEADER<- opcode: QUERY, status: NOERROR, id: 4108
; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version 0, flags: udp: 4096
; COOKIE: 6e7451a4ac240220100000619a5653ca8a9909284c3746 (good)
;; QUESTION SECTION:
;cc.pt.                IN SOA
;; ANSWER SECTION:
cc.pt.                 604800 IN SOA ns.cc.pt. g43p104.cc.pt.cc.pt. (
                        2          ; serial
                        604800    ; refresh (1 week)
                        86400    ; retry (1 day)
                        2419200  ; expire (4 weeks)
                        604800    ; minimum (1 week)
                        )
;; Query time: 0 msec
;; SERVER: 10.3.3.2#53(10.3.3.2)
;; WHEN: dom nov 21 14:23:15 UTC 2021
;; MSG SIZE rcvd: 120
bash-5.0#
  
```

Figura 31

## **Adicionalmente, fez-se também testes com queries reversas:**

### **1. Com o primário e o secundário online:**

```
bash-5.0# dig -x 10.3.3.3
; <<> DiG 9.16.1-Ubuntu <<> -x 10.3.3.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1040
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
; COOKIE: 0a2449011b61c49e01000000619a57259791fb39b02def17 (good)
;; QUESTION SECTION:
;3.3.3.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
3.3.3.10.in-addr.arpa. 604800 IN      PTR      Foca.cc.pt.

;; Query time: 0 msec
;; SERVER: 10.2.2.1#53(10.2.2.1)
;; WHEN: dom nov 21 14:26:45 UTC 2021
;; MSG SIZE rcvd: 102
```

**Figura 32**

### **2. Apenas com o secundário online:**

```
bash-5.0# dig -x 10.1.1.1
; <<> DiG 9.16.1-Ubuntu <<> -x 10.1.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30493
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
; COOKIE: 35f1c10e0d0fe8be01000000619a6548061735904ef4d8fc (good)
;; QUESTION SECTION:
;1.1.1.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.1.1.10.in-addr.arpa. 604800 IN      PTR      Portatil1.cc.pt.

;; Query time: 0 msec
;; SERVER: 10.3.3.2#53(10.3.3.2)
;; WHEN: dom nov 21 15:27:04 UTC 2021
;; MSG SIZE rcvd: 107
```

**Figura 33**