Universidade do Minho

Mestrado Integrado em Engenharia Informática
Licenciatura em Engenharia Informática

Comunicações por Computador

TP3 - Serviço de Resolução de Nomes (DNS)

Grupo 7.6

Ana Canelas
(A93872)

Ana Henriques
(A93268)

Ana Murta
(A93284)

15 de novembro de 2021

Conteúdo

1 PARTE I

Questões e Respostas

1.1 Questão A

Qual o conteúdo do ficheiro *etc/resolv.conf* e para que serve essa informação?
O ficheiro */etc/resolv.conf* contém várias diretorias:

- *nameserver* - endereço IP do nameserver.
- *domain* - nome do domain local.
- *search* - contém uma lista de domain search paths que é necessária para vários servidores.
- *options* - permite definir parâmetros, como timout, ndots, rotate entre outros.

Esta informação é variável porque depende da rede em que o host se encontra. Quando um utilizador quer aceder a um domínio, o nome do servidor é o primeiro a ser interrogado, procurando pelo mesmo nos registos.

```
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 home
```

Figura 1: Conteúdo do ficheiro /etc/resolv.conf

1.2 Questão B

Os servidores www.di.uminho.pt. e www.europa.eu. têm endereços IPv6? Se sim, quais?

- www.di.uminho.pt. - Não tem endereços IPv6
- www.europa.eu. - ”2a01:7080:24:100::666:25”e ”2a01:7080:14:100::666:25”

```
core@xubuncore:~$ nslookup
> set TYPE=AAAA
> www.di.uminho.pt.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.di.uminho.pt        canonical name = www5.di.uminho.pt.
>
> www.europa.eu.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.europa.eu   canonical name = ip-europa.ec.europa.eu.
Name:   ip-europa.ec.europa.eu
Address: 2a01:7080:24:100::666:25
Name:   ip-europa.ec.europa.eu
Address: 2a01:7080:14:100::666:25
>
```

Figura 2: Execução do comando nslookup para os endereços www.di.uminho.pt. e www.europa.pt.

1.3 Questão C

Quais os servidores de nomes definidos para os domínios: *"gov.pt."* e *"."*?
Os nameservers para o domínio *"gov.pt."* são os assinalados na figura 3:

```
core@xubuncore:~$ nslookup
> set type=NS
> gov.pt.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
gov.pt  nameserver = a.dns.pt.
gov.pt  nameserver = dns1.gov.pt.
gov.pt  nameserver = nsp.dnsnode.net.
gov.pt  nameserver = ns02.fccn.pt.
gov.pt  nameserver = europe1.dnsnode.net.

Authoritative answers can be found from:
>
```

Figura 3: Execução do comando nslookup do endereço *"gov.pt."*

Podemos, agora, analisar que, ao domínio *"."*, já estão associados mais name servers (ao certo 13 servidores), estando os mesmos assinalados na figura 4:

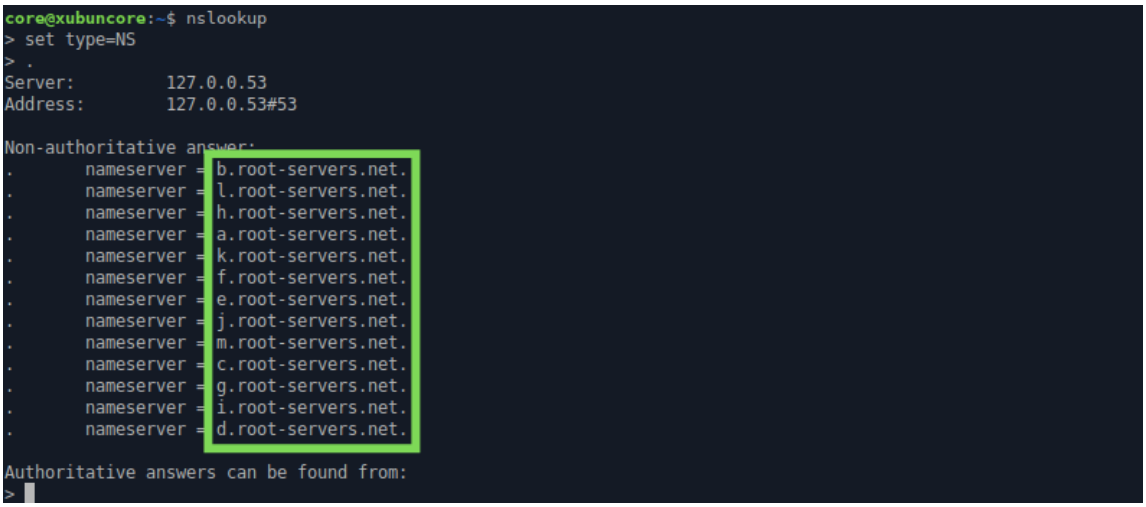

Figura 4: Execução do comando nslookup do endereço *"."*

1.4 Questão 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?

Consideramos que *efiko.academy.* é um host. Isto porque, atráves do comando dig, podemos chegar à conclusão que o *resource record* de *efiko.academy.* corresponde a 'A' e, como tal, é um host porque tem associado a ele o endereço IP 5.132.7.2, tal como podemos observar na figura 5. .

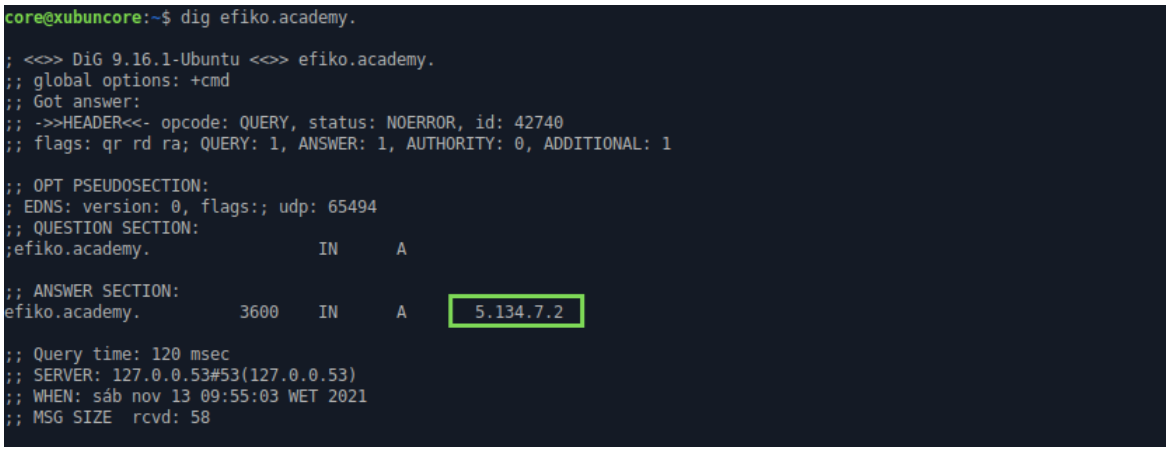

Figura 5: Execução do comando dig do enderelo *"efiko.academy"*

1.5 Questão E

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

Recorrendo ao comando *nslookup* e definindo o tipo de *resource record* como SOA (*Start of Authority*), conseguimos confirmar com o campo *origin* que o servidor DNS primário definido para o domínio *"gov.pt."* é *"dnssec.gov.pt"*.

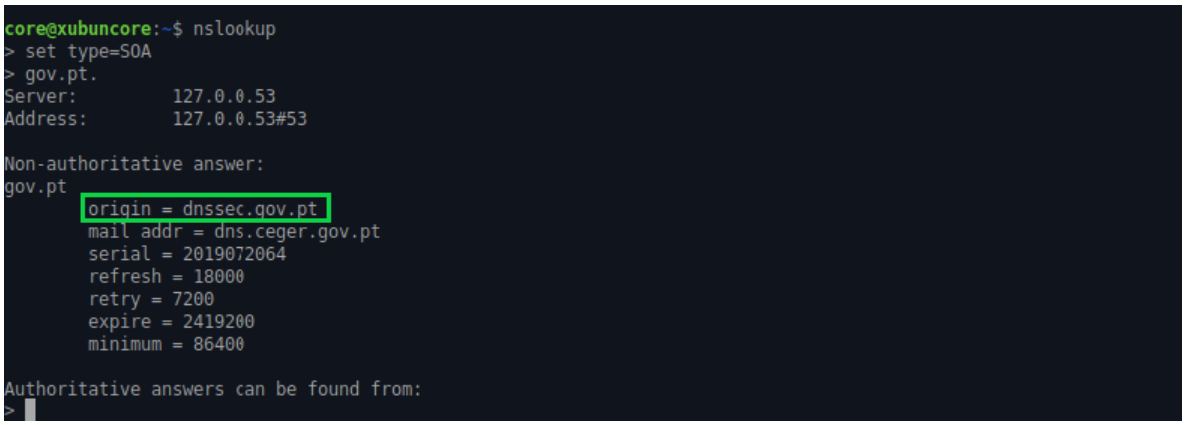

Figura 6: Execução do comando nslookup para *"gov.pt."*

Perante este resultado, basta utilizarmos o comando *dig dnssec.gov.pt* para podermos ver que este servidor primário aceita, de facto, queries recursivas já que, na figura 7, se confirma a presença das flags *"rd"* (*recusion desired*) e *"ra"* (*recusion available*).

Figura 7: Execução do dig para *"dnssec.gov.pt"*

1.6 Questão F

Obtenha uma resposta "autoritativa"para a questão anterior.

A partir do comando *nslookup* com uma query do tipo SOA, obtivemos o resultado *Non-authoritative answer* e, portanto, não existem quaisquer respostas autoritativas para *"gov.pt."*.

```
core@xubuncore:~$ nslookup
> set type=SOA
> gov.pt.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
gov.pt
        origin = dnssec.gov.pt
        mail addr = dns.ceger.gov.pt
        serial = 2019072064
        refresh = 18000
        retry = 7200
        expire = 2419200
        minimum = 86400

Authoritative answers can be found from:
>
```

Figura 8: nslooup de *"gov.pt."*

1.7 Questão G

Onde são entregues as mensagens de correio eletrónico dirigidas a marcelo@presidencia.pt?

Para obter a informação acerca do destino das mensagens dirigidas àquele correio eletrónico, temos de executar o comando *nslookup* com *type=MX*, que filtra os nomes dos servidores de email associados ao nome domínio. Consequentemente, obtivemos os seguintes resultados:

```
core@xubuncore:~$ nslookup
> set type=MX
> presidencia.pt
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
presidencia.pt  mail exchanger = 10 mail2.presidencia.pt.
presidencia.pt  mail exchanger = 50 mail1.presidencia.pt.

Authoritative answers can be found from:
```

Figura 9: nslookup de *"presidencia.pt"*

As mensagens de correio eletrónico dirigidas a *marcelo@presidencia.pt* podem ser entregues em duas opções diferentes: *mail2.presidencia.pt.* ou *mail1.presidencia.pt.*. Todavia, o servidor prioritário é o que possui o menor *priority value*. Como tal, as mensagens serão

primeiro entregues ao *mail2*, cujo *priority value* é 10, e só em caso de indisponibilidade, é que serão entregues ao *mail1*, cujo *priority value* é 50.

1.8 Questão H

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

Tal como ilustrado na figura 10, podemos aceder a informação como o email do administrador do domínio assim como os valores de vários campos de atualiação do servidor secundário.

Figura 10: nslookup com *type=SOA*

Figura 11: nslookup com *type=A*

1.9 Questão I

Consegue interrogar o DNS sobre o endereço IPv6 2001:609:2080:8005::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?

Recorrendo ao comando *nslookup* com uma query do tipo AAA, que corresponde ao IPv6, consegue-se determinar o domínio associado ao endereço dado. Perante isto, temos, então,

acesso ao nome do servidor (associado ao domínio) e ao endereço internet IPv6 (associado a cada servidor).

Figura 12: nslookup de 2001:609:2080:8005::38 com type=AAA

1.10 Questão 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. Descreve sucintamente esse mecanismo com base num exemplo concreto(ex:uminho.pt).

A "trasnferência de zona"é um tipo de transação de DNS, um dos muitos mecanismos disponíveis para os administradores replicarem bases de dados DNS num conjunto de servidores DNS secundários. Uma "transferência de zona"recorre ao TCP para transporte e assume a forma de uma transação cliente-servidor. Ou seja, um cliente solicita uma transferência de dados de um servidor primário para um secundário, sendo a parte replicada da base de dados conhecida por "zona".

A partir das modificações feitas na Parte II deste trabalho prático, foi possível utilizar o exemplo *cc.pt* criado na topologia virtual.

Existem vários parâmetros definidos como tempo de atualização do servidor secundário de acordo com as informações do primário:

- *Serial* - Número de série da zona. Este valor apenas incrementa quando os dados do servidor primário são alterados de modo a que o servidor secundário saiba quando deve atualizar os seus próprios dados, o que permite estar constantemente atualizado.

- *Refresh* - Tempo (em segundos) após o qual o servidor secundário contactará o servidor primário para atualizar informações e para detetar possíveis alterações na zona. No nosso caso, corresponde a 604800 segundos.

- *Retry* - Tempo (em segundos) que o secundário aguarda antes de tentar novamente conectar-se ao servidor primário em caso de falha, sendo que o *retry* deve ser sempre inferior ao *refresh*. No nosso caso, corresponde a 86400 segundos.

- *Expire* - Tempo (em segundos) que o secundário aguarda até considerar os dados atuais como desatualizados de modo a, depois, parar de fazer solicitações para a zona específica caso o servidor primário não responda. No nosso caso, corresponde a 2419200 segundos.

- *Negative* Cache TTL - Tempo (em segundos) que um nome de domínio demora a ser armazenado totalmente em cache antes de expirar, retornando, também, aos servidores de nomes oficiais para obter informações atualizadas. No nosso caso, corresponde a 604800 segundos.

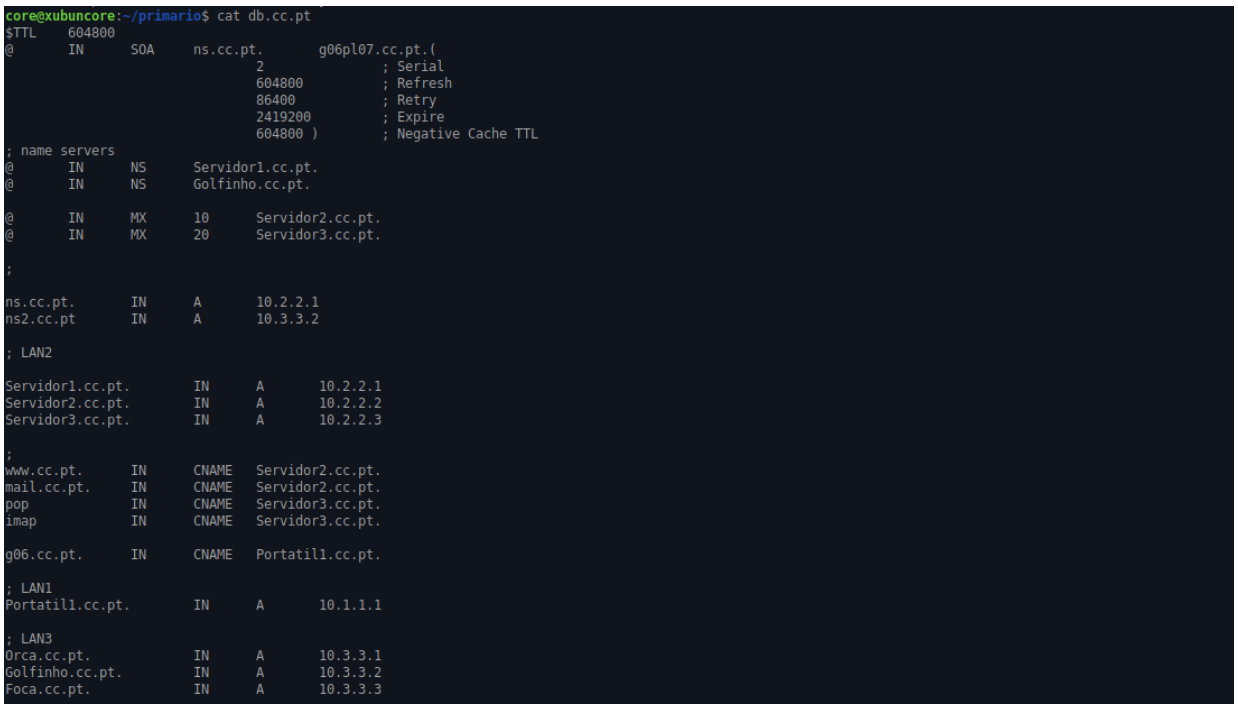

Figura 13: Ficheiro db.cc.pt que foi criado na Parte II

Concluindo, o servidor secundário deverá contactar o primário para se atualizar após 604800 segundos terem passado; depois de falhar inicialmente, deve esperar 86400 segundos até poder tentar uma nova conexão com o servidor primário; e se o servidor primário não responder durante 2419200 segundos, o servidor secundário deixar de tentar a conexão.

2 PARTE II

2.1 Servidor Primário

Para a configuração do servidor primário, limitámo-nos a respeitar as regras e seguir as instruções presentes no enunciado.

Após editar os ficheiros */etc/hosts* e *primario/named.conf.options*, modificámos o ficheiro *named.conf*. Neste, incluímos as zonas *"cc.pt"* e *"2.2.10.in-addr.arpa*, tal como indicado no enunciado. No entanto, a topologia apresenta 4 redes LAN diferentes, o que levou, também, a incluir as zonas de procura inversa para as redes que faltavam: *"1.1.10.in-addr.arpa"*, *"3.3.10.in-addr.arpa"* e *"4.4.10.in-addr.arpa"*.

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

zone "cc.pt"{
        type master;
        file "/home/core/primario/db.cc.pt";
        allow-transfer { 10.3.3.2; };
};


zone "1.1.10.in-addr.arpa"{
        type master;
        file "/home/core/primario/db.1-1-10.rev";
        allow-trasnfer { 10.3.3.2; };
};

zone "2.2.10.in-addr.arpa"{
        type master;
        file "/home/core/primario/db.2-2-10.rev";
        allow-transfer { 10.3.3.2; };
};

zone "3.3.10.in-addr.arpa"{
        type master;
        file "/home/core/primario/db.3-3-10.rev";
        allow-trasnfer { 10.3.3.2; };
};

zone "4.4.10.in-addr.arpa"{
        type master;
        file "/home/core/primario/db.4-4-10.rev";
        allow-trasnfer { 10.3.3.2; };
};
```

Figura 14: Ficheiro *named.conf* do servidor primário

Em seguida, procedeu-se à criação e configuração do ficheiro *"db.cc.pt"*. Para tal, configurámos o SOA (*Start of Authority*), titulando o *Servidor1.cc.pt* como o DNS principal (já que se trata do servidor principal) e colocando *g06pl07.cc.pt* como administrador.

Entretanto, para o bom funcionamento do nosso servidor DNS, introduzimos os *nameservers*, *Servidor1* e *Golfinho*, com a cláusula *NS*, e os servidores de e-mail, *Servidor2* (servidor de e-mail principal) e *Servidor3* (servidor de e-mail secundário), com a cláusula *MX*. Depois, para todos os elementos, colocámos os seus nomes mencionados na topologia e o seu endereço IP, usando a cláusula *A*. Para além disto, adicionámos *alias* para alguns dos elementos, como

requisitado no enunciado, e definimos o servidores web e e-mail, presentes em **Servidor2**, e o servidor pop e imap, presentes em *Servidor3*.

```
$TTL    604800
@       IN      SOA     ns.cc.pt.       g06pl07.cc.pt. (
                                2               ; Serial
                                604800          ; Refresh
                                86400           ; Retry
                                2419200         ; Expire
                                604800 )        ; Negative Cache TTL
; name servers
@       IN      NS      Servidor1.cc.pt.
@       IN      NS      Golfinho.cc.pt.

@       IN      MX      10      Servidor2.cc.pt.
@       IN      MX      20      Servidor3.cc.pt.

;

ns.cc.pt.       IN      A       10.2.2.1
ns2.cc.pt       IN      A       10.3.3.2

; LAN2

Servidor1.cc.pt.        IN      A       10.2.2.1
Servidor2.cc.pt.        IN      A       10.2.2.2
Servidor3.cc.pt.        IN      A       10.2.2.3

;
www.cc.pt.      IN      CNAME   Servidor2.cc.pt.
mail.cc.pt.     IN      CNAME   Servidor2.cc.pt.
pop             IN      CNAME   Servidor3.cc.pt.
imap            IN      CNAME   Servidor3.cc.pt.

g06.cc.pt.      IN      CNAME   Portatil1.cc.pt.

; LAN1
Portatil1.cc.pt.        IN      A       10.1.1.1

; LAN3
Orca.cc.pt.             IN      A       10.3.3.1
Golfinho.cc.pt.         IN      A       10.3.3.2
Foca.cc.pt.             IN      A       10.3.3.3
```

Figura 15: Ficheiro *db.cc.pt* com configuração *type=SOA*

Terminando a configuração do ficheiro *"db.cc.pt"*, abrimos uma bash no nó *Portatil1* e testando a seguinte query ao servidor primário:

```
root@Portatil1:/tmp/pycore.39819/Portatil1.conf# nslookup www.cc.pt. 10.2.2.1
Server:         10.2.2.1
Address:        10.2.2.1#53

www.cc.pt       canonical name = Servidor2.cc.pt.
Name:   Servidor2.cc.pt
Address: 10.2.2.2

root@Portatil1:/tmp/pycore.39819/Portatil1.conf#
```

Figura 16: Teste de conexão através do comando *nslookup* no Portatil1

Consequentemente, procedemos à configuração dos restantes ficheiros que permitirão a procura inversa. Embora havendo 4 redes LAN diferentes, o processo é semelhante para todos, acabando por ter a mesma configuração SOA e a adição dos dois *nameservers*: *Servidor1* e *Golfinho*.

Falta apenas fazer o *reverse mapping*, para o qual introduzimos o endereço da máquina em questão e o seu nome, usando a cláusula *PTR*.

```
$TTL 604800
@       IN      SOA     ns.cc.pt.       g06pl07.cc.pt. (
                                1               ; Serial
                           604800          ; Refresh
                            86400          ; Retry
                          2419200          ; Expire
                           604800 )        ; Negative Cache TTL
; name servers
@       IN      NS      Servidor1.cc.pt.
@       IN      NS      Golfinho.cc.pt.

; PTR records
1       IN      PTR     Servidor1.cc.pt.
2       IN      PTR     Servidor2.cc.pt.
3       IN      PTR     Servidor3.cc.pt.
```

Figura 17: Exemplo de reverse mapping para a rede 10.2.2.0/24

2.2 Servidor secundário

Na configuração do servidor secundário, foi apenas necessário alterar o ficheiro *named.conf*, adicionando as zonas existentes no servidor primário com algumas alterações. O *type*, que antes era *master*, agora passa a ser *slave*; a cláusula *allow-transfer* foi substituída pela cláusula *masters* {*10.2.2.1;*}; e o path para o ficheiro também foi alterado.

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

zone "cc.pt"{
        type slave;
        file "/var/cache/bind/db.cc.pt";
        masters { 10.2.2.1; };
};

zone "1.1.10.in-addr.arpa"{
        type slave;
        file "/var/cache/bind/db.1-1-10.rev";
        masters { 10.2.2.1; };
};

zone "2.2.10.in-addr.arpa"{
        type slave;
        file "/var/cache/bind/db.2-2-10.rev";
        masters { 10.2.2.1; };
};

zone "3.3.10.in-addr.arpa"{
        type slave;
        file "/var/cache/bind/db.3-3-10.rev";
        masters { 10.2.2.1; };
};

zone "4.4.10.in-addr.arpa"{
        type slave;
        file "/var/cache/bind/db.4-4-10.rev";
        masters { 10.2.2.1; };
};
```

Figura 18: Ficheiro *named.conf* do servidor secundário

Terminando a configuração do ficheiro *"named.conf"*, escolhendo abrir uma bash no nó *Portatil1* e testando a seguinte query ao servidor secundário:

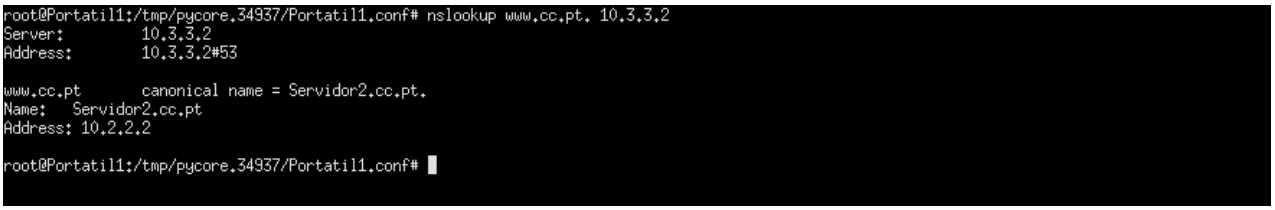

Figura 19: Teste de conexão através do comando *nslookup* no Portatil1

3 Conclusão

Com a realização deste trabalho prático, conseguimos aprofundar e assimilar melhor os nossos conhecimentos sobre a Unidade Curricular de Comunicações por Computador, pondo em prática os conteúdos aprendidos nas aulas teóricas.

Na primeira fase, de questões e respostas, praticámos diversas formas de interrogar o DNS e, na segunda parte, procedemos à instalação, configuração e teste de um domínio *cc.pt*.

Apesar das dificuldades enfrentadas ao longo do desenvolvimento deste projeto, conseguiu-se cumprir todas as indicações propostas com sucesso. Além disto, o grupo ficou satisfeito com o resultado final deste trabalho.