Universidade do Minho
Escola de Engenharia

Departamento de Informática

Comunicações por Computador

Trabalho Prático nº 3

Serviço de Resolução de Nomes (DNS)

Ano Letivo 2020/2021

Grupo 1 - PL1

Ana Filipa Pereira A89589
Carolina Santejo A89500
Raquel Costa A89464

Conteúdo

Parte I - Questões e Respostas

a)

Q: Qual o conteúdo do ficheiro /etc/resolv.conf e para que serve essa informação?

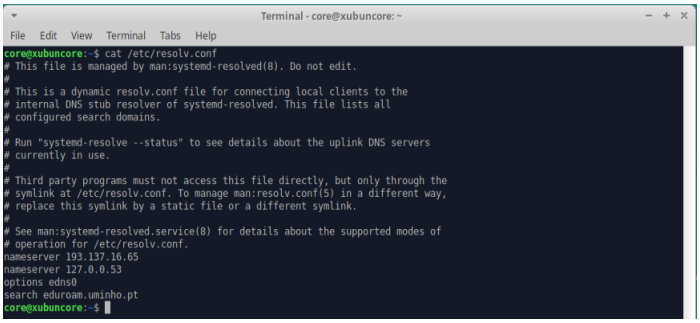

Figura 1: Conteúdo do ficheiro resolv.conf

Este ficheiro contém os servidores DNS por defeito da maquina, estabelecidos pelo administrador de rede, que serão os responsáveis por fazer a resolução de nomes e IPs.

b)

Q: Os servidores www.uminho.pt.e www.ubuntu.com. têm endereços IPv6? Se sim, quais?

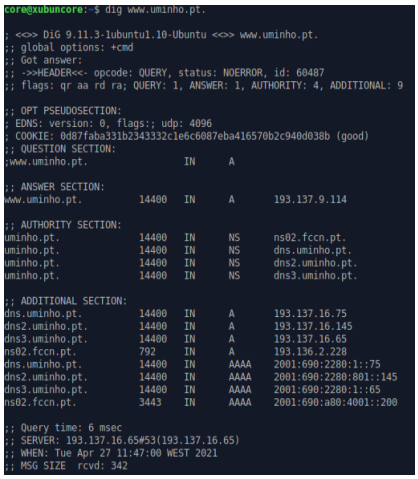

Figura 2: Comando dig para www.uminho.pt.

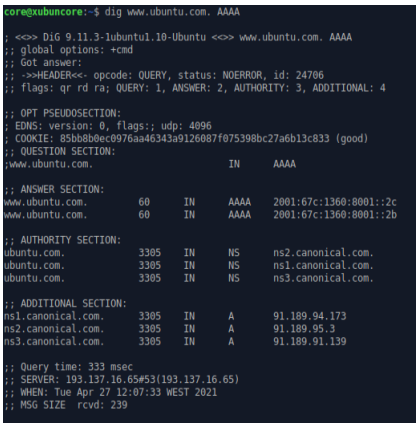

Figura 3: Comando dig para www.ubuntu.com.

Para verificar a existência de endereços IPv6 num servidor foi necessário procurar a ocorrencia do identificador AAAA nas informações do comando dig. Sendo assim, podemos verificar que para os servidores www.uminho.pt. identifica-se que os 4 existentes possuem endereços IPv6, sendo eles:
2001:690:2280:1::75
2001:690:2280:801::145
2001:690:2280:1::65
2001:690:a80:4001::200
Para o caso do www.ubuntu.com. também se verifica a existencia de 2 endereços IPv6:
2001:67c:1360:8001::2c
2001:67c:1360:8001::2b

c)

Q: Quais os servidores de nomes definidos para os domínios: "sapo.pt.", "pt." e "."?
Para identificar os servidores de nomes de um domínio foi necessário utilizar o comando dig com a flag NS. Para cada um dos domínios "sapo.pt.", "pt." e "." estão identificados os respetivos servidores na secção de resposta.

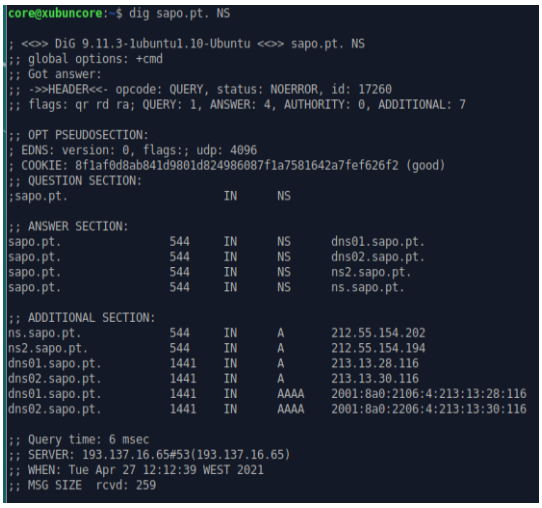

Figura 4: Comando dig para sapo.pt.

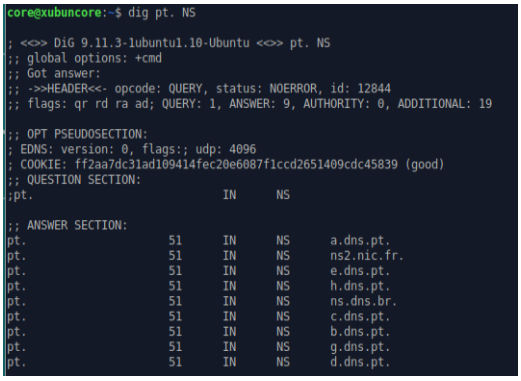

Figura 5: Comando dig para pt.

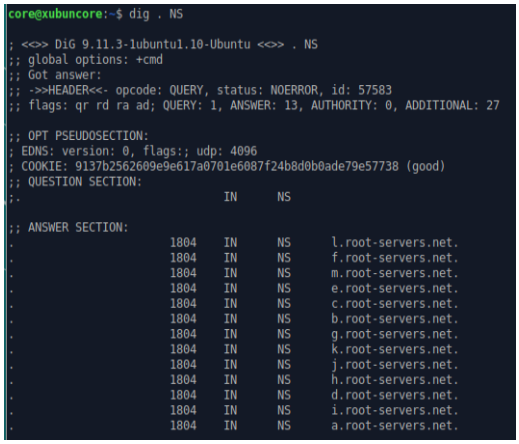

Figura 6: Comando dig para .

d)

Q: Existe o domínio open.money.? Será que open.money. é um host ou um domínio?
Sim, existe o domínio open.money. e é um host porque possui um endereço IP como pode verificar na figura abaixo.

```
core@xubuncore:~$ host open.money.
open.money has address 35.154.208.116
open.money mail is handled by 10 mailstore1.secureserver.net.
open.money mail is handled by 0 smtp.secureserver.net.
open.money mail is handled by 5 alt2.aspmx.l.google.com.
open.money mail is handled by 10 alt4.aspmx.l.google.com.
open.money mail is handled by 1 aspmx.l.google.com.
open.money mail is handled by 10 alt3.aspmx.l.google.com.
open.money mail is handled by 5 alt1.aspmx.l.google.com.
```

Figura 7: Comando host para open.money.

e)

Q: Qual é o servidor DNS primário definido para o domínio un.org.? Este servidor primário (master) aceita queries recursivas? Porquê?
DNS primário: ns1.un.org.
Este servidor aceita queries recursivas uma vez que na resposta ao comando dig está presente 'ra' que significa *recursion available*.

```
core@xubuncore:~$ host -t soa un.org.
un.org has SOA record ns1.un.org. root.un.org. 2021042400 1200 3600 1209600 300
```

Figura 8: Comando host para un.org.

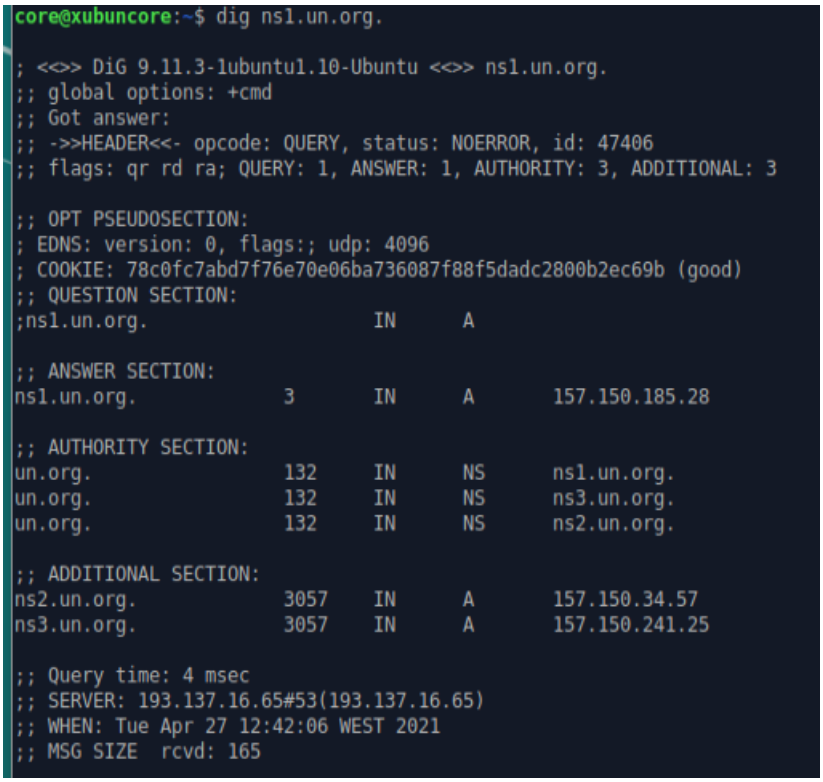

Figura 9: Comando dig para un.org.

f)

Q: Obtenha uma resposta "autoritativa" para a questão anterior. Para obter uma resposta autoritativa foi necessário a utilização de uma query do tipo NS. Para o domínio un.org. não foi possível obter uma resposta autoritativa

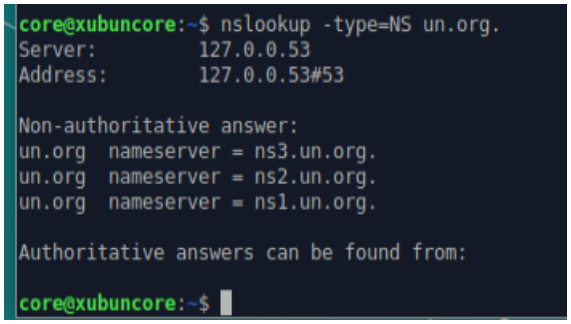

Figura 10: Comando nslookup -type=NS un.org.

g)

Q: Onde são entregues as mensagens de correio eletrónico dirigidas a presidency@eu.eu ou presidencia@2021portugal.eu?

Para verificar onde são entregues as mensagens de correio eletrónico utilizamos queries MX, isto é, "Mail Exchanger". Deste modo foi possível concluir o seguinte :

» No caso do eu.eu., as mensagens são entregues no servidor mxg.eu.mpssec.net.

```
core@xubuncore:/$ dig eu.eu. MX

; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> eu.eu. MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6104
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
eu.eu.                  3583    IN      MX      10 smtp01.level27.be.
eu.eu.                  3583    IN      MX      20 smtp02.level27.be.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Apr 27 11:55:58 WEST 2021
;; MSG SIZE  rcvd: 90
```

Figura 11: Comando dig para eu.eu.

»Para 2021portugal.eu., as mensagens são entregues nos servidores smtp01.level27.be. e smtp02.level27.be.

```
core@xubuncore:/$ dig 2021portugal.eu. MX

; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> 2021portugal.eu. MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46116
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;2021portugal.eu.               IN      MX

;; ANSWER SECTION:
2021portugal.eu.        300     IN      MX      10 mxg.eu.mpssec.net.

;; Query time: 941 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Apr 27 11:52:33 WEST 2021
;; MSG SIZE  rcvd: 77

core@xubuncore:/$ dig mxg.eu.mpssec.net.

; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> mxg.eu.mpssec.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35891
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;mxg.eu.mpssec.net.             IN      A

;; ANSWER SECTION:
mxg.eu.mpssec.net.      3600    IN      A       54.77.99.92

;; Query time: 194 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Apr 27 11:52:58 WEST 2021
;; MSG SIZE  rcvd: 62
```

Figura 12: Comando dig para 2021portugal.eu.

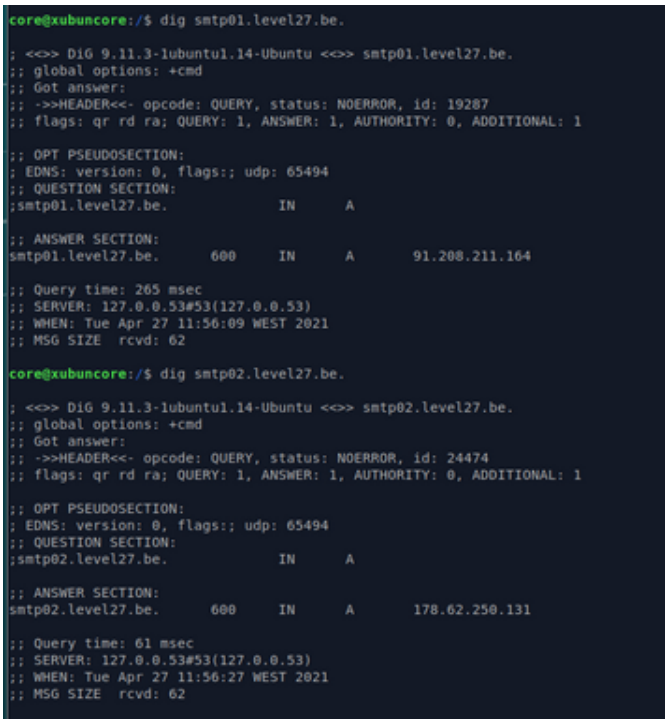

Figura 13: Comando dig para servidores smtp01.level27.be. e smtp02.level27.be.

h)

Q: Que informação é possível obter, via DNS, acerca de gov.pt?
Utilizando o comando dig com a flag ANY é possivel obter várias informações acerca do domínio gov.pt. Como se pode verificar na imagem abaixo foram obtidas 7 respostas onde as primeiras 5 identificam os servidores de nomes. Por outro lado, é possivel também observar que as opções *recursive available* e *recursive desirable* estão ativas.

Figura 14: Comando dig gov.pt.

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?

Utilizando o comando nslookup é possivel interrogar o DNS sobre este endereço. Da sua resposta podemos obter o nome do domínio associado a este IP, que é smtp01.fccn.pt.

Figura 15: Interrogação nslookup com o endereço IPv6

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: di.uminho.pt ou o domínio cc.pt que vai ser criado na topologia virtual).

O mecanismo de "Transferência de zona"permite replicar uma porção ou a totalidade da base de dados DNS do servidor primário para o secundário. Além disso, esta transferência é realizada sempre sobre TCP, assumindo a forma de uma transação cliente-servidor, onde o cliente que solicita a transferência trata-se de um servidor "slave"ou secundário.

Por exemplo, analisando os parâmetros definidos e os campos no Record do tipo SOA do domínio di.uminho.pt, é possível observar o campo SERIAL, que representa o número de série da zona em questão. Caso um servidor secundário observar um incremento neste número então irá assumir que esta zona já foi atualizada e irá inicializar a "transferência de zona", caso contrário, isto é, caso o número de série seja o mesmo ou inferior então a transferência não irá ocorrer, uma vez que o servidor secundário que está a solicitar o pedido contém uma versão da base de dados igual ou mais atual.

Note-se também na existência de outros campos no Record do SOA que contém valores temporais, tais como, o refresh, retry, expire e minimum.

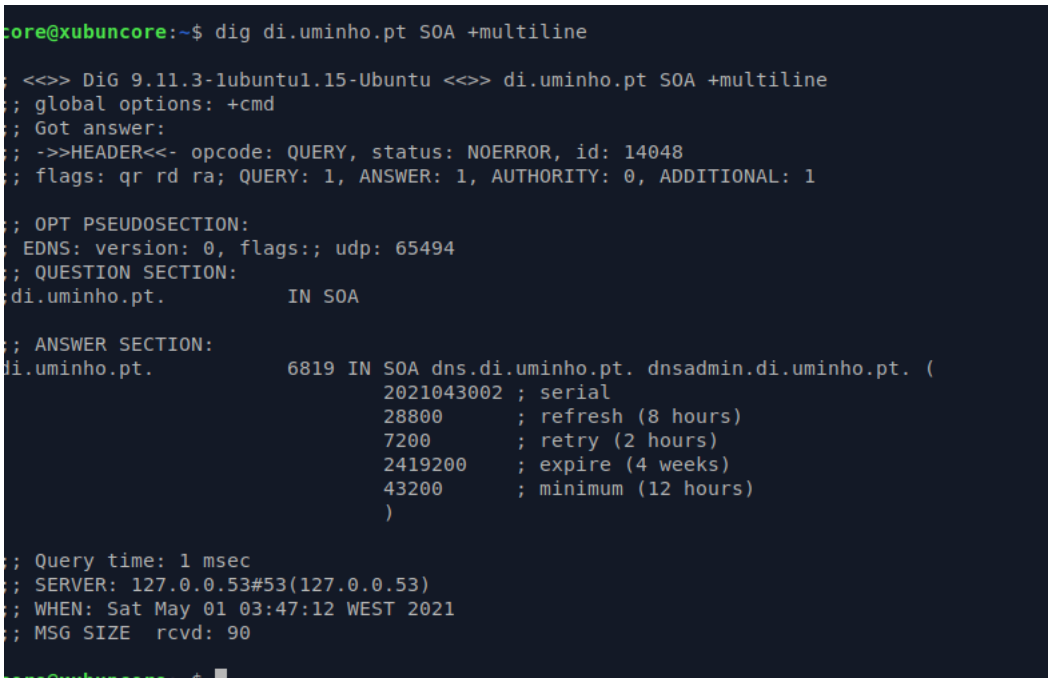

Figura 16: Comando dig di.uminho.pt. SOA

Parte II - Criação de um domínio de nomes cc.pt

```
// 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";


zone "cc.pt" {
        type master;
        file "/home/core/primario/db.cc.pt";
        allow-transfer{
                10.2.2.2;
        };
};

zone "1.1.10.in-addr.arpa"{
        type master;
        file "/home/core/primario/db.1-1-10.rev";
        allow-transfer{
                10.2.2.2;
        };
};
~
```

Figura 17: primario/named.conf

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     Server1.cc.pt. PL01G01.cc.pt. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@               IN      NS      Server1.cc.pt.
@               IN      NS      Mercurio.cc.pt.
;
ns              IN      CNAME   Server1.cc.pt.
ns2             IN      CNAME   Mercurio.cc.pt.
;
Server1         IN      A       10.1.1.1
Mercurio        IN      A       10.2.2.2
;
www             IN      CNAME   Server2.cc.pt.
mail            IN      CNAME   Server2.cc.pt.
pop             IN      CNAME   Server3.cc.pt.
imap            IN      CNAME   Server3.cc.pt.
;
Server2         IN      A       10.1.1.2
Server3         IN      A       10.1.1.3
;
g01             IN      CNAME   Laptop1.cc.pt.
;
Laptop1         IN      A       10.4.4.1
;
@               IN      MX 20   Server2
@               IN      MX 10   Server3
;
Venus           IN      A       10.2.2.3
Marte           IN      A       10.2.2.1
```

Figura 18: primario/db.cc.pt

```
;
; BIND reverse file for local loopback interface
;
$TTL    604800
1.1.10.in-addr.arpa.       IN      SOA  Server1.cc.pt. PL01G01.cc.pt. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@               IN      NS      Server1.cc.pt.
@               IN      NS      Mercurio.cc.pt.
;
1               IN      PTR     Server1.cc.pt.
2               IN      PTR     Server2.cc.pt.
3               IN      PTR     Server3.cc.pt.
~
~
```

Figura 19: primario/db.1-1-10.rev

```
// 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";

zone "cc.pt" {
        type slave;
        file "/var/cache/bind/db.cc.pt";
        masters{
                10.1.1.1;
        };
};

zone "1.1.10.in-addr.arpa" {
        type slave;
        file "/var/cache/bind/db.1-1-10.rev";
        masters{
                10.1.1.1;
        };
};
~
```

Figura 20: secundario/named.conf

Na próxima figura está representada a transferência da base de dados entre o servidor primário (*master*), que neste caso consiste no "Server1"e o secundário (*slave*), tratando-se do "Mercurio". Além disso, estão também demonstradas algumas queries feitas aos servidores de DNS.

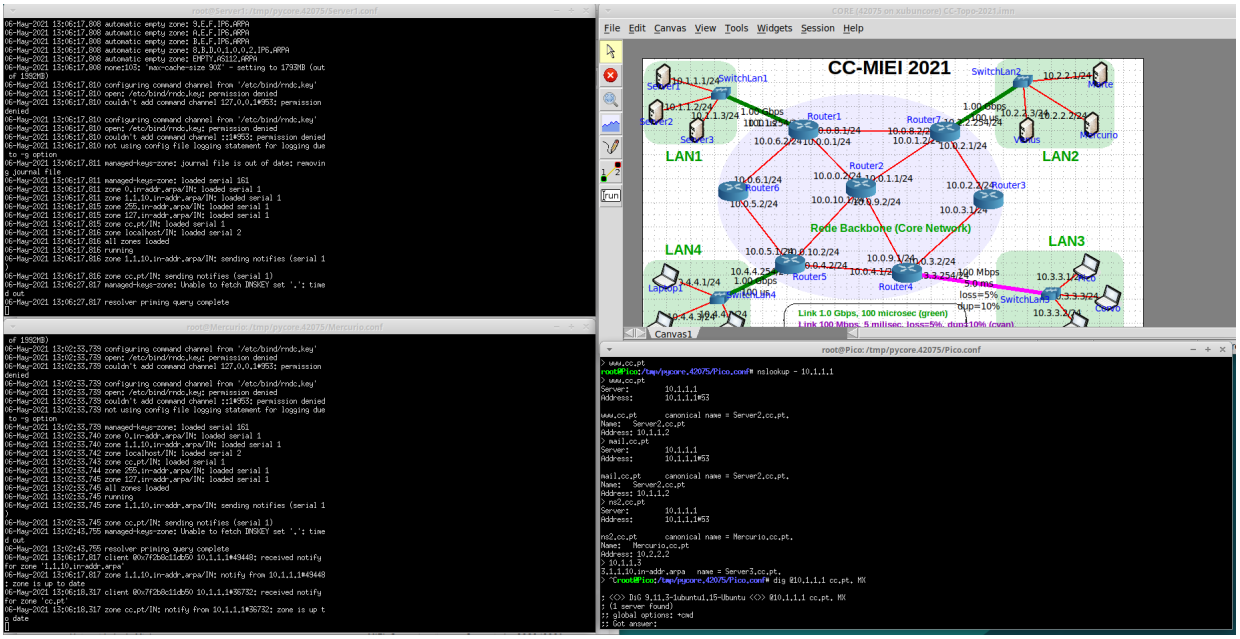

Figura 21: Demonstração da transferência da DB + queries nsloookup

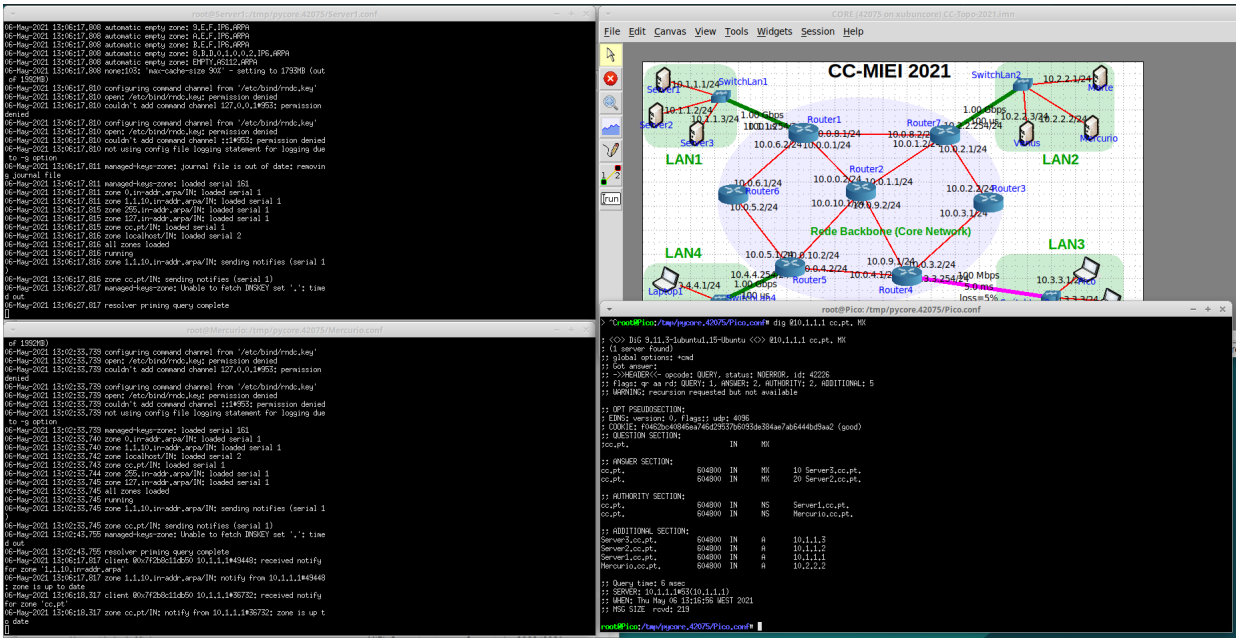

Figura 22: Query do tipo MX

Além disso, ainda foi capturado tráfego DNS através da ferramenta *wireshark*.

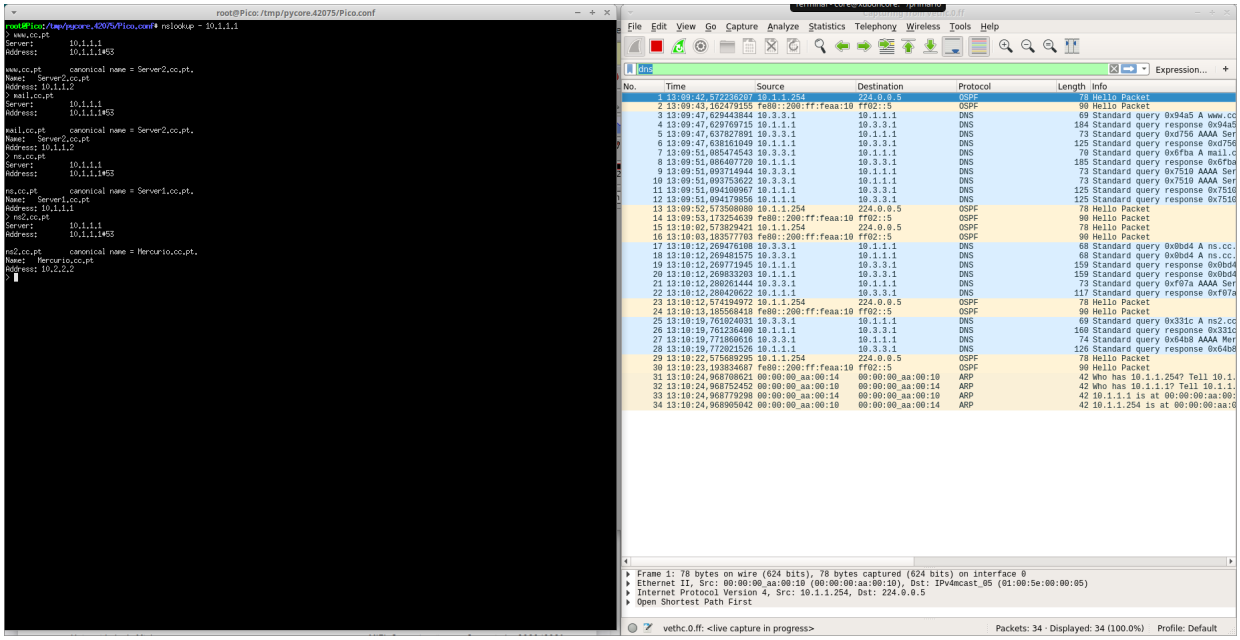

Figura 23: Tráfego DNS

Por fim, de forma a testar a redundância do sistema, isto é, se deitando o servidor primário abaixo, o secundário continuaria a funcionar, foram feitos vários testes através dos seguintes comandos representados nas figuras abaixo:

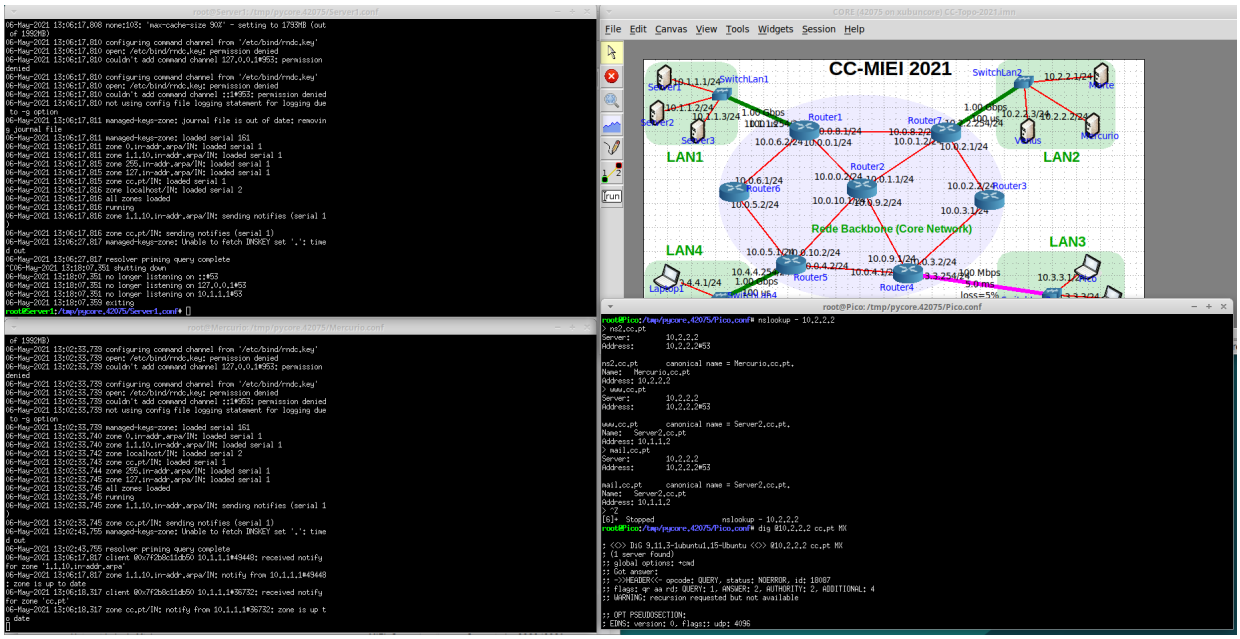

Figura 24: Query nslookup no servidor secundário

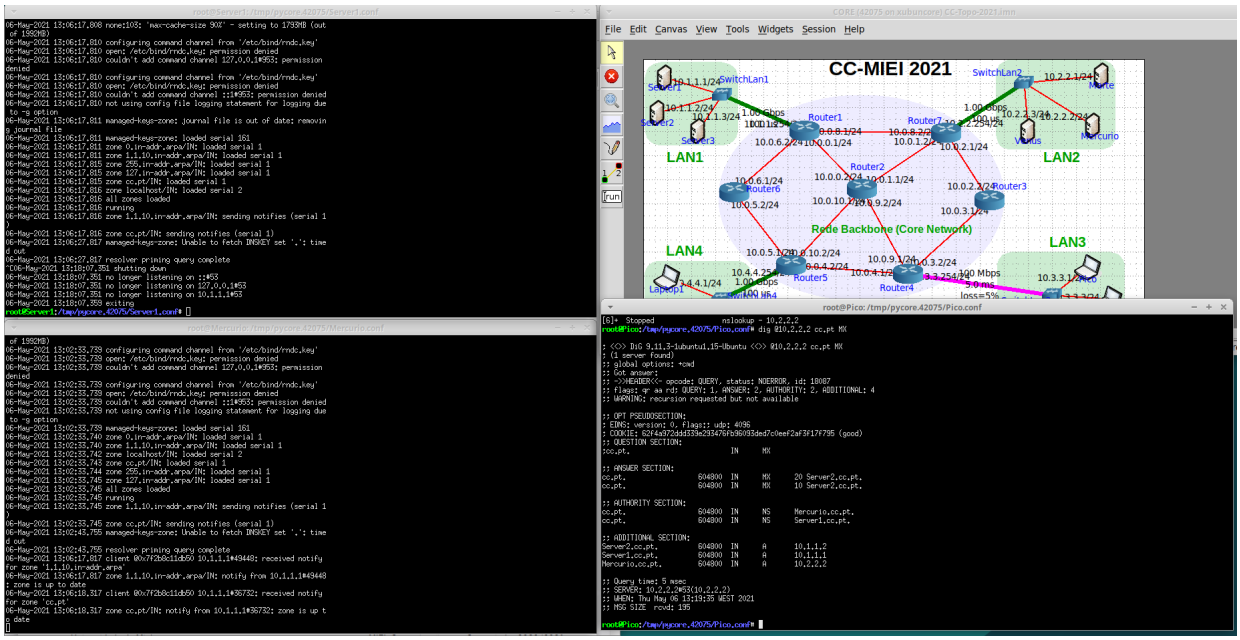

Figura 25: Query dig do tipo MX no servidor secundário

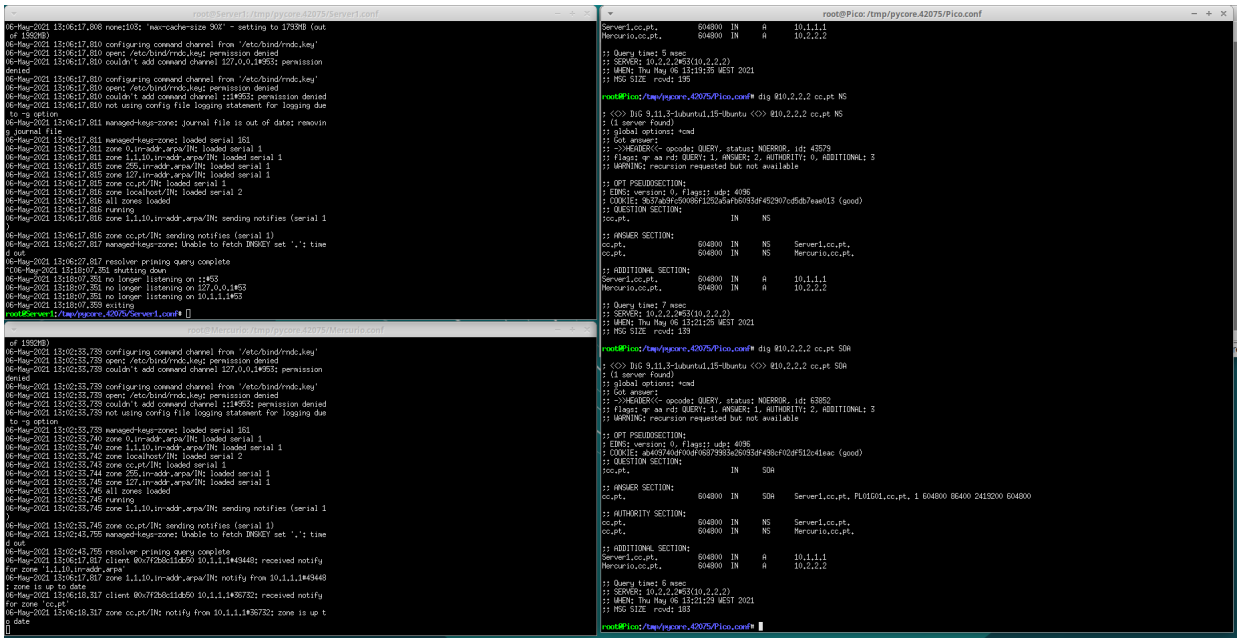

Figura 26: Query dig do tipo NS e SOA no servidor secundário

Conclusão

Ao longo deste trabalho prático, foi possível aplicar e consolidar todo o conhecimento adquirido ao longo das aulas teóricas e práticas de Comunicação por Computadores.

Na primeira parte, Questões e Respostas, foi necessário analisar o ficheiro que contém os servidores, */etc/resolv.conf*, além de ter sido pedido, nas várias alíneas, que se obtivesse outras informações , sendo utilizados para isso, os comandos dig e nslookup.

A segunda parte do trabalho, consistiu na instalação, configuração e teste de um domínio CC.PT.

Desta forma, o grupo considera que concluiu este desafio com sucesso, uma vez que todos os requisitos foram cumpridos e todas as funcionalidades pedidas foram implementadas.