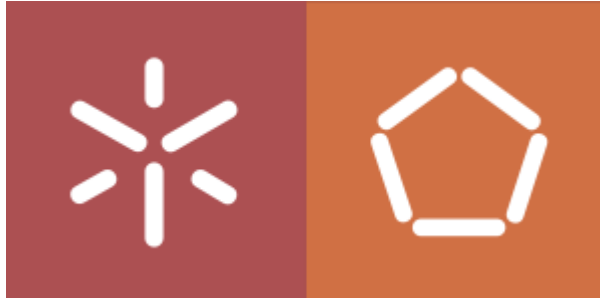


Universidade do Minho
Departamento de Informática



Mestrado Integrado em Engenharia Informática

Comunicações por Computador

TP3 - Serviço de Resolução de Nomes (DNS)

A84430 Bruno Teixeira
A84752 Diogo Rio
A85573 Jorge Cerqueira
14 de Abril de 2020

1 Questões e Respostas

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

```
teixeira@teixeira:~$ 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 "systemd-resolve --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
```

Figura 1

R: O ficheiro contém informação que determina os parâmetros operacionais dos servidores DNS, assim como os servidores DNS por defeito para resolução de domain names e IPs.

b) Os servidores `www.sapo.pt.` e `www.yahoo.com.` têm endereços IPv6? Se sim, quais?

```
teixeira@teixeira:~$ host www.yahoo.com
www.yahoo.com is an alias for atsv2-fp-shed.wg1.b.yahoo.com.
atsv2-fp-shed.wg1.b.yahoo.com has address 87.248.98.7
atsv2-fp-shed.wg1.b.yahoo.com has address 87.248.98.8
atsv2-fp-shed.wg1.b.yahoo.com has IPv6 address 2a00:1288:110:1c::4
atsv2-fp-shed.wg1.b.yahoo.com has IPv6 address 2a00:1288:110:1c::3
teixeira@teixeira:~$ host www.sapo.pt
www.sapo.pt has address 213.13.146.142
www.sapo.pt has IPv6 address 2001:8a0:2102:c:213:13:146:142
teixeira@teixeira:~$
```

Figura 2

R: Sim, ambos os servidores têm endereços IPV6, como se pode observar pela figura 2.

c) Quais os servidores de nomes definidos para os domínios: “`uminho.pt.`”, “`pt.`” e “`.`”?

```
teixeira@teixeira:~$ nslookup
> set q=NS
> uminho.pt.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
uminho.pt    nameserver = dns.uminho.pt.
uminho.pt    nameserver = dns3.uminho.pt.
uminho.pt    nameserver = ns02.fccn.pt.
uminho.pt    nameserver = dns2.uminho.pt.

Authoritative answers can be found from:
>
```

Figura 3

R: Os nameserver apresentados representam os servidores de nomes definidos para o domínio `uminho.pt.`

```

teixeira@teixeira:~$ nslookup
> set q=NS
> pt.
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
pt      nameserver = ns.dns.br.
pt      nameserver = b.dns.pt.
pt      nameserver = f.dns.pt.
pt      nameserver = e.dns.pt.
pt      nameserver = d.dns.pt.
pt      nameserver = c.dns.pt.
pt      nameserver = h.dns.pt.
pt      nameserver = g.dns.pt.
pt      nameserver = a.dns.pt.
pt      nameserver = ns2.nic.fr.

Authoritative answers can be found from:
> 

```

Figura 4

R: Os nameserver apresentados representam os servidores de nomes definidos para o domínio pt.

```

teixeira@teixeira:~$ nslookup
> set q=NS
> .
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
.      nameserver = d.root-servers.net.
.      nameserver = m.root-servers.net.
.      nameserver = i.root-servers.net.
.      nameserver = g.root-servers.net.
.      nameserver = l.root-servers.net.
.      nameserver = j.root-servers.net.
.      nameserver = a.root-servers.net.
.      nameserver = h.root-servers.net.
.      nameserver = e.root-servers.net.
.      nameserver = c.root-servers.net.
.      nameserver = f.root-servers.net.
.      nameserver = k.root-servers.net.
.      nameserver = b.root-servers.net.

Authoritative answers can be found from:
> 

```

Figura 5

R: Os nameserver apresentados representam os servidores de nomes definidos para o domínio .

d) Existe o domínio nice.software.? Será que nice.software. é um host ou um domínio?

```
teixeira@teixeira:~$ nslookup
> set q=NS
> nice.software.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
nice.software nameserver = nsqbr.comlaude.co.uk.
nice.software nameserver = nssui.comlaude.ch.
nice.software nameserver = nsusa.comlaude.net.

Authoritative answers can be found from:
> 
```

Figura 6

```
teixeira@teixeira:~$ nslookup
> set q=A
> nice.software.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   nice.software
Address: 213.212.81.71
> 
```

Figura 7

R: Tem name servers, logo existe o domínio nice.software. É um host pois tem endereço IP.

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

```
teixeira@teixeira:~$ host -t soa msf.org.
msf.org has SOA record ns1.dds.nl. postmaster.msf.org. 1407464621 16384 2048 1048576 2560
teixeira@teixeira:~$ 
```

Figura 8

R: O servidor primário é ns1.dds.nl.

```

teixeira@teixeira:~$ host uminho.pt ns1.dds.nl
;; connection timed out; no servers could be reached
teixeira@teixeira:~$ host google.pt ns1.dds.nl
;; connection timed out; no servers could be reached
teixeira@teixeira:~$ nslookup
> set q=SOA
> msf.org
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
msf.org
    origin = ns1.dds.nl
    mail addr = postmaster.msf.org
    serial = 1407464621
    refresh = 16384
    retry = 2048
    expire = 1048576
    minimum = 2560

Authoritative answers can be found from:
> server ns1.dds.nl
Default server: ns1.dds.nl
Address: 91.142.253.70#53
> uminho.pt
;; connection timed out; no servers could be reached
>

```

Figura 9

R: O servidor primário não aceita queries recursivas uma vez que sempre que se tenta aceder a outros domínios dá *Connection timed out*; como se pode verificar pelas várias tentativas ilustradas na figura 9.

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

```

teixeira@teixeira:~$ dig +noall +authority @ns1.dds.nl. msf.org
msf.org.      259200 IN      NS      ns1.dds.nl.
msf.org.      259200 IN      NS      ns2.dds.eu.
msf.org.      259200 IN      NS      ns4.dds-city.com.
msf.org.      259200 IN      NS      ns3.dds.amsterdam.
teixeira@teixeira:~$

```

Figura 10

g) Onde são entregues as mensagens de correio eletrônico dirigidas aos presidentes `marcelo@presidencia.pt` e `bolsonaro@casacivil.gov.br`?

```
teixeira@teixeira:~$ nslookup
> set query=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 11

R: As mensagens são entregues nos servidores `mail2.presidencia.pt` e `mail1.presidencia.pt`.

```
teixeira@teixeira:~$ nslookup
> set query=MX
> casacivil.gov.br.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
casacivil.gov.br mail exchanger = 5 esa01.presidencia.gov.br.
casacivil.gov.br mail exchanger = 10 esa02.presidencia.gov.br.

Authoritative answers can be found from:
> 
```

Figura 12

R: As mensagens são entregues nos servidores `esa01.presidencia.gov.br` e `esa02.presidencia.gov.br`.

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

```
teixeira@teixeira:~$ dig www.whitehouse.gov.

;<<>> DiG 9.11.3-lubuntu1.11-Ubuntu <<>> www.whitehouse.gov.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58777
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.whitehouse.gov.  291     IN      CNAME   wildcard.whitehouse.gov.edgekey.net.
wildcard.whitehouse.gov.edgekey.net. 29 IN CNAME e4036.dscb.akamaiedge.net.
e4036.dscb.akamaiedge.net. 18 IN A 92.122.238.175

;; Query time: 63 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Mar 31 11:34:53 WEST 2020
;; MSG SIZE rcvd: 148

teixeira@teixeira:~$
```

Figura 13

R: É possível obter a identificação dos servidores de nomes, alguns dos pseudónimos deste domínio e também observar que as flags recursive available e recursive desirable estão ativas. É também possível ver que o endereço IPv4 associado é 92.122.238.175. Além disso é possível obter as identificações presentes na figura 13.

i) Consegue interrogar o DNS sobre o endereço IPv6 2001:690:a00:1036:1113::247 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?

```
teixeira@teixeira:~$ nslookup 2001:690:a00:1036:1113::247
7.4.2.0.0.0.0.0.0.0.0.0.0.3.1.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      name = www.fccn.pt.

Authoritative answers can be found from:

teixeira@teixeira:~$ nslookup
> set query=SOA
> fccn.pt.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
fccn.pt
  origin = ns01.fccn.pt
  mail addr = hostmaster.fccn.pt
  serial = 2020033001
  refresh = 21600
  retry = 7200
  expire = 1209600
  minimum = 14400

Authoritative answers can be found from:
>
```

Figura 14

R: Sim, é possível interrogar o DNS sobre o endereço IPV6. A informação obtida com essa interrogação é o nome de domínio (www.fccn.pt). Sim, é possível obter um contacto do responsável por este IPV6, neste caso hostmaster.fccn.pt.

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).

R: A transferência de zona DNS, às vezes também conhecida pelo tipo de consulta DNS indutor AXFR, é um tipo de transação de DNS. É uma query usada para os administradores replicarem bancos de dados DNS num conjunto de servidores DNS. Uma transferência de zona usa o TCP começando pela verificação do preâmbulo que contém um número de série. Esta verificação determina se a transferência ocorre, pois se o número de série for igual ou inferior ao do servidor que envia o pedido, a transferência não ocorre uma vez que este contém uma versão da base de dados igual ou mais recente.

O cliente solicitando uma transferência de zona pode ser um servidor slave ou servidor secundário, solicitando dados de um servidor mestre, às vezes chamado de servidor principal. A parte do banco de dados que é replicada é uma zona.

2 Criação de um domínio de nomes CC.PT

```
;
; BIND data file for cc.pt
;
$TTL      604800
@         IN      SOA      dns.cc.pt. grupo10.cc.pt. (
                        4      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;

@         IN      NS       dns.cc.pt.
@         IN      NS       dns2.cc.pt.

mail      IN      MX       10      Serv1
www       IN      CNAME    Serv1
dns       IN      A        10.3.3.1
dns2      IN      A        10.4.4.1
mail      IN      MX       20      Serv2

Serv1     IN      A        10.3.3.1
Hermes    IN      A        10.4.4.1
Serv2     IN      A        10.3.3.2

pop       IN      CNAME    Serv2
imap      IN      CNAME    Serv2

Portatil1 IN      A        10.1.1.1
Grupo10   IN      CNAME    Portatil1
Atena     IN      A        10.4.4.3
Zeus      IN      A        10.4.4.2
~
~
~
```

Figura 15: primario/db.cc.pt

```

; BIND reverse data file for 10.3.3.1
$TTL      604800
@         IN      SOA      cc.pt. admin.cc.pt. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       dns.cc.pt.
@         IN      NS       dns2.cc.pt.
1         IN      PTR      dns.cc.pt.
1         IN      PTR      Serv1.cc.pt.
2         IN      PTR      Serv2.cc.pt.

```

Figura 16: primario/db.3-3-10.rev

```

1 // This is the primary configuration file for the BIND DNS server named.
2 //
3 // Please read /usr/share/doc/bind9/README.Debian.gz for information on the
4 // structure of BIND configuration files in Debian, *BEFORE* you customize
5 // this configuration file.
6 //
7 // If you are just adding zones, please do that in /etc/bind/named.conf.local
8
9 include "/etc/bind/named.conf.options";
10 include "/etc/bind/named.conf.local";
11 include "/etc/bind/named.conf.default-zones";
12
13 zone "cc.pt" {
14     type master;
15     file "/home/rio/primario/db.cc.pt";
16     allow-transfer{10.4.4.1;};
17 };
18
19 zone "3.3.10.in-addr.arpa" {
20     type master;
21     file "/home/rio/primario/db.3-3-10.rev";
22     allow-transfer{10.4.4.1;};
23 };

```

Figura 17: primario/named.conf

```

1 options {
2 >   directory "/var/cache/bind";
3
4 >   // If there is a firewall between you and nameservers you want
5 >   // to talk to, you may need to fix the firewall to allow multiple
6 >   // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
7
8 >   // If your ISP provided one or more IP addresses for stable•
9 >   // nameservers, you probably want to use them as forwarders.♦♦
10 >   // Uncomment the following block, and insert the addresses replacing•
11 >   // the all-0's placeholder.
12
13 >   forwarders {
14 >     >   8.8.8.8;
15 >     >   8.8.4.4;
16 >   };
17
18 >   //=====
19 >   // If BIND logs error messages about the root key being expired,
20 >   // you will need to update your keys.  See https://www.isc.org/bind-keys
21 >   //=====
22 >   dnssec-validation auto;
23
24 >   listen-on-v6 { any; };
25
26   allow-recursion { any; };
27 };

```

Figura 18: primario/named.conf.options

```

1 // This is the primary configuration file for the BIND DNS server named.
2 //
3 // Please read /usr/share/doc/bind9/README.Debian.gz for information on the•
4 // structure of BIND configuration files in Debian, *BEFORE* you customize•
5 // this configuration file.
6 //
7 // If you are just adding zones, please do that in /etc/bind/named.conf.local
8
9 include "/etc/bind/named.conf.options";
10 include "/etc/bind/named.conf.local";
11 include "/etc/bind/named.conf.default-zones";
12
13 zone "cc.pt"{
14     type slave;
15     file "/var/cache/bind/db.cc.pt";
16     masters{ 10.3.3.1; };
17 };
18
19 zone "3.3.10.in-addr.arpa"{
20     type slave;
21     file "/var/cache/bind/db.3-3-10.rev";
22     masters{ 10.3.3.1; };
23 };

```

Figura 19: secundario/named.conf

```
[rio@rio-pc] : [ ~ ] $ /usr/sbin/named-checkconf -z /home/rio/primario/named.conf
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
zone cc.pt/IN: loaded serial 4
zone 3.3.10.in-addr.arpa/IN: loaded serial 2
[rio@rio-pc] : [ ~ ] $ /usr/sbin/named-checkzone cc.pt /home/rio/primario/db.cc.pt
zone cc.pt/IN: loaded serial 4
OK
[rio@rio-pc] : [ ~ ] $ /usr/sbin/named-checkzone 3.3.10.in-addr.arpa /home/rio/primario/db.3-3-10.rev
zone 3.3.10.in-addr.arpa/IN: loaded serial 2
OK
[rio@rio-pc] : [ ~ ] $
```

Figura 20: Teste

```
[rio@rio-pc] : [ ~ ] $ cat /etc/resolv.conf
nameserver 10.3.3.1
domain cc.pt
search cc.pt
```

Figura 21: resolv.conf

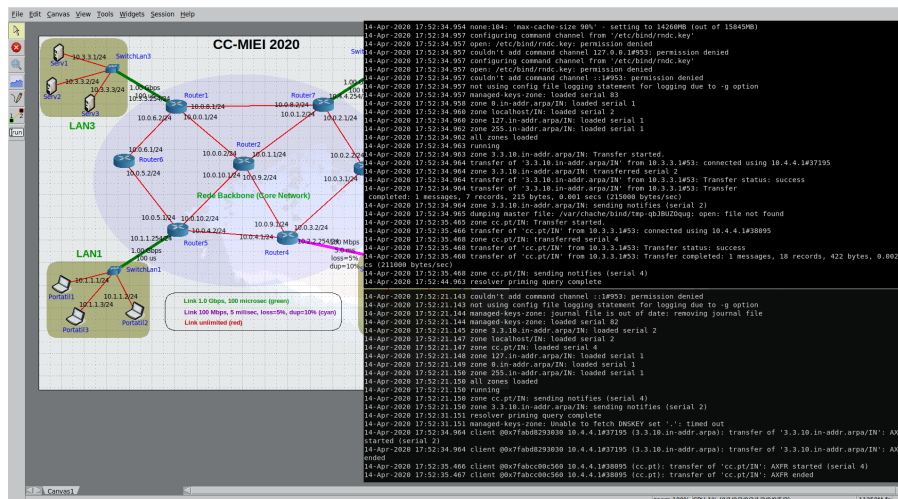


Figura 22: Transferência da base de dados de master para o slave

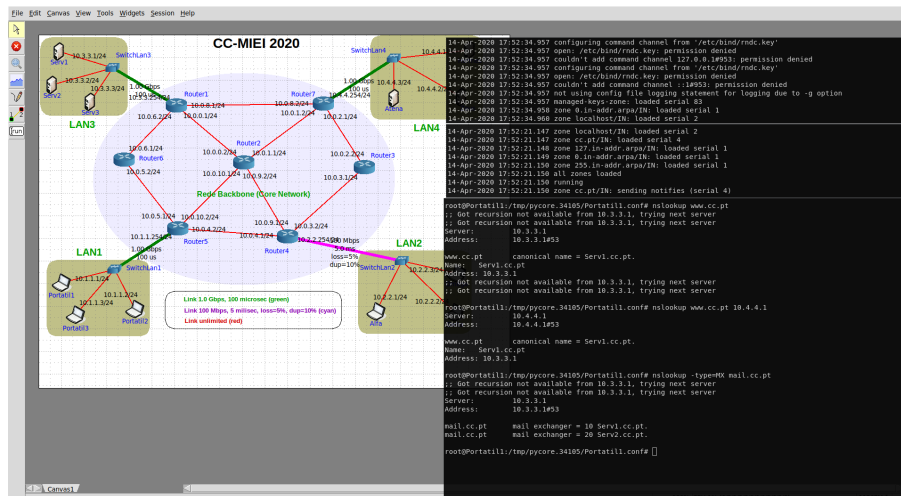


Figura 23: Queries aos servidores DNS

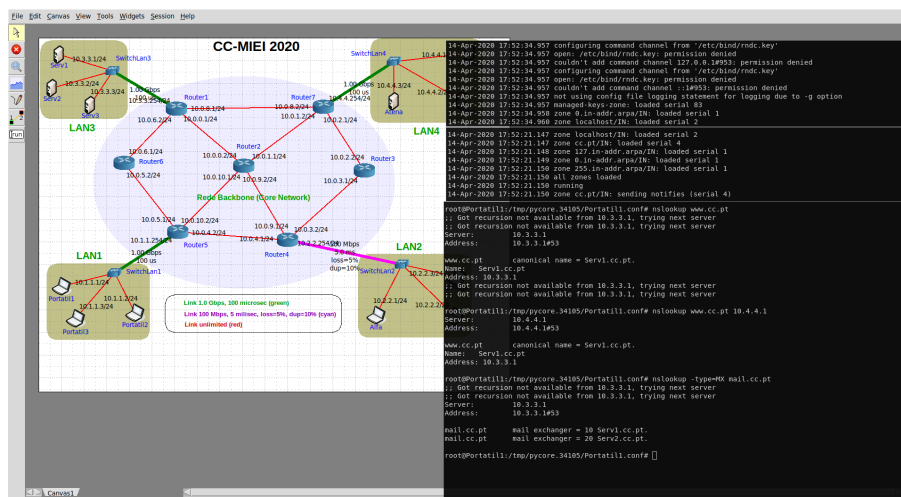


Figura 24: Queries aos servidores DNS

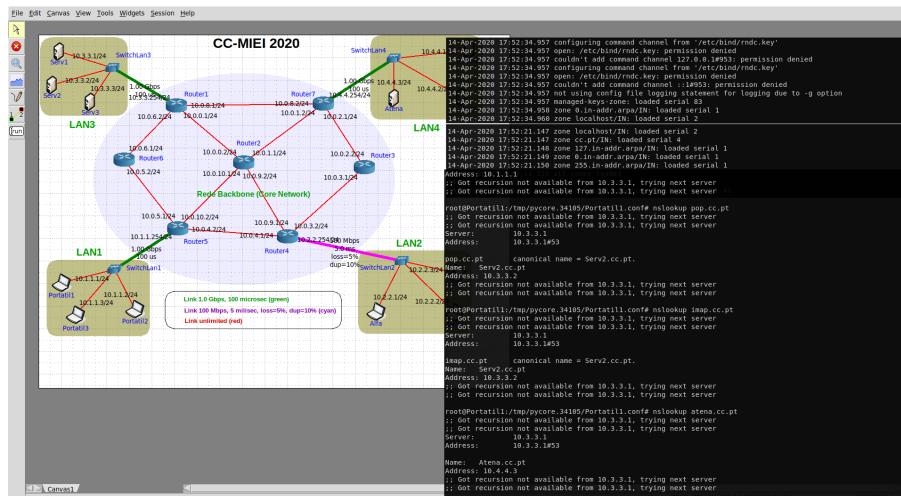


Figura 25: Queries aos servidores DNS

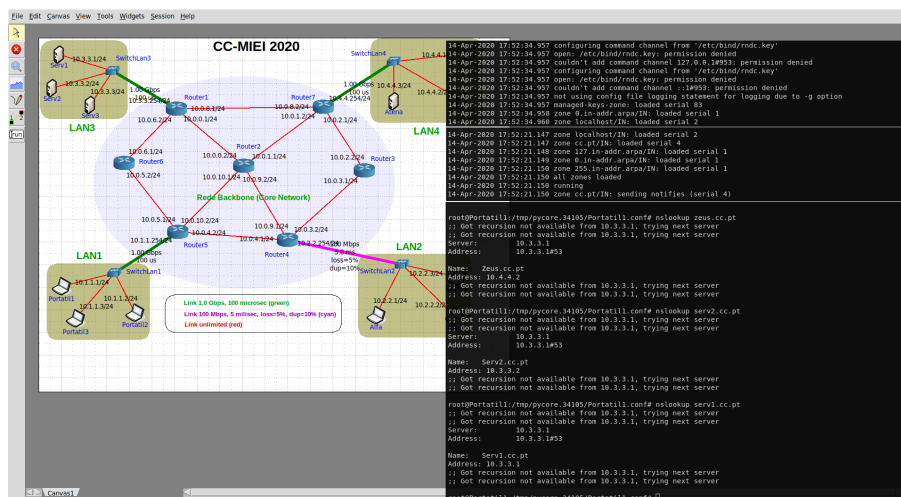


Figura 26: Queries aos servidores DNS

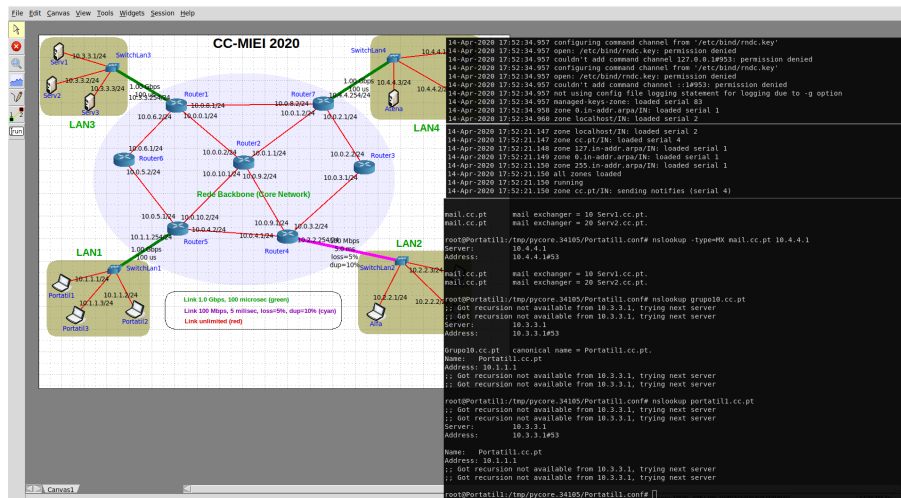


Figura 27: Queries aos servidores DNS

3 Conclusões

A elaboração deste trabalho prático relativo ao DNS - Serviço de resolução de nomes teve, entre muitos objetivos, um complemento às aulas teóricas e a consolidação dos temas abordados nas mesmas. Com a sua realização obtivemos conhecimentos acerca deste sistema de gestão de nomes hierárquico e distribuído.

Na primeira parte deste trabalho, relativa às questões e respostas, abordamos diferentes maneiras de interrogar o DNS utilizando diferentes comandos. São exemplo disso, **nslookup**, **dig**, **host**, entre outros, assim como vários tipos de queries que nos permitem obter diferentes informações.

Relativamente à segunda parte do trabalho, foi efetuada a instalação, configuração e verificação do domínio **CC.PT**. Para isso foi feita a configuração de um servidor primário e outro secundário assim como a utilização da ferramenta CORE.