

Comunicações por Computador

Trabalho Prático Nº. 3 - Serviço de Resolução de Nomes (DNS)

Eduardo Coelho, Henrique Neto, Júlio Alves
e-mail: {a89616,a89618,a89468}@alunos.uminho.pt

7 de maio de 2021

1 Consultas ao serviço de nomes DNS

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

Conteúdo do ficheiro `/etc/resolv.conf`

Contém os servidores de DNS por defeito, estipulados pelo administrador de rede, para resolução de nomes domínios e IP's.

```
# 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 eduroam.uminho.pt
```

1.b Os servidores `www.uminho.pt.` e `www.ubuntu.com.` têm endereços IPv6? Se sim, quais?

Como podemos ver pela imagem que se segue, `www.uminho.pt.` não possui endereço IPv6 e `www.ubuntu.com.` possui, sendo eles `2001:67c:1360:8001::2c` e `2001:67c:1360:8001::2b`

```
Terminal - core@core-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help

core@core-VirtualBox:~/Desktop$ nslookup -q=AAAA www.uminho.pt.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
*** Can't find www.uminho.pt.: No answer

core@core-VirtualBox:~/Desktop$ nslookup -q=AAAA www.ubuntu.com.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.ubuntu.com
Address: 2001:67c:1360:8001::2c
Name:   www.ubuntu.com
Address: 2001:67c:1360:8001::2b
```

Figura 1: Endereços IPv6 www.uminho.pt e www.ubuntu.com

1.c Quais os servidores de nomes definidos para os domínios: “sapo.pt.”, “pt.” e “.”?

Os servidores de nomes definidos para os domínios *sapo.pt.*, *pt.* e *.* são os apresentados na imagem seguinte.

```
core@core-VirtualBox:/etc$ nslookup -q=NS sapo.pt.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
sapo.pt nameserver = dns02.sapo.pt.
sapo.pt nameserver = ns.sapo.pt.
sapo.pt nameserver = ns2.sapo.pt.
sapo.pt nameserver = dns01.sapo.pt.

Authoritative answers can be found from:

core@core-VirtualBox:/etc$ nslookup -q=NS pt.
Server:      127.0.0.53
Address:     127.0.0.53#53

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

Authoritative answers can be found from:

core@core-VirtualBox:/etc$ nslookup -q=NS .
Server:      127.0.0.53
Address:     127.0.0.53#53

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

Authoritative answers can be found from:

core@core-VirtualBox:/etc$
```

Figura 2: Servidores nomes para os domínios em questão

1.d Existe o domínio open.money.? Será que open.money. é um host ou um domínio?

Existe o domínio open.money. :

```
core@core-VirtualBox:/etc$ nslookup open.money.  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
Name:   open.money  
Address: 35.154.208.116
```

Figura 3: Domínio open.money.

e é um host pois tem um endereço IP associado:

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

Figura 4: Host open.money.

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

O servidor DNS primário definido para o domínio un.org. é ns1.un.org. . Como as flags rd e ra são igual a 1 significa que este servidor aceita queries recursivas.

```
Terminal - core@core-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help
core@core-VirtualBox:~/Desktop$ host -t soa un.org.
un.org has SOA record ns1.un.org. root.un.org. 2021042900 1200 3600 1209600 300
core@core-VirtualBox:~/Desktop$ dig dig ns1.un.org.

; <<>> DiG 9.16.1-Ubuntu <<>> dig ns1.un.org.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 10177
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui mai 06 22:25:23 WEST 2021
;; MSG SIZE rcvd: 32

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16146
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ns1.un.org.         IN      A

;; ANSWER SECTION:
ns1.un.org.         300     IN      A      157.150.185.28

;; Query time: 52 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qui mai 06 22:25:23 WEST 2021
;; MSG SIZE rcvd: 55
core@core-VirtualBox:~/Desktop$
```

Figura 5: DNS Primário

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

Não foi possível obter uma resposta autoritativa como demonstrado pela imagem seguinte.

```
core@core-VirtualBox:~/Desktop$ nslookup -q=ns un.org.
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
un.org  nameserver = ns1.un.org.
un.org  nameserver = ns3.un.org.
un.org  nameserver = ns2.un.org.

Authoritative answers can be found from:

core@core-VirtualBox:~/Desktop$
```

Figura 6: Autoritativa

1.g Onde são entregues as mensagens de correio eletrónico dirigidas a *presidency@eu.eu* ou *presidencia@2021portugal.eu*?

No caso de *presidencia@2021portugal.eu* as mensagens são entregues em *mxg.eu.mpssec.net*. No caso de *presidency@eu.eu* as mensagens podem ser entregues em *smtp01.level27.be* e

smtp02.level27.be, uma vez que é dada maior prioridade em smtp02.level27.be, as mensagens são preferencialmente entregues neste.

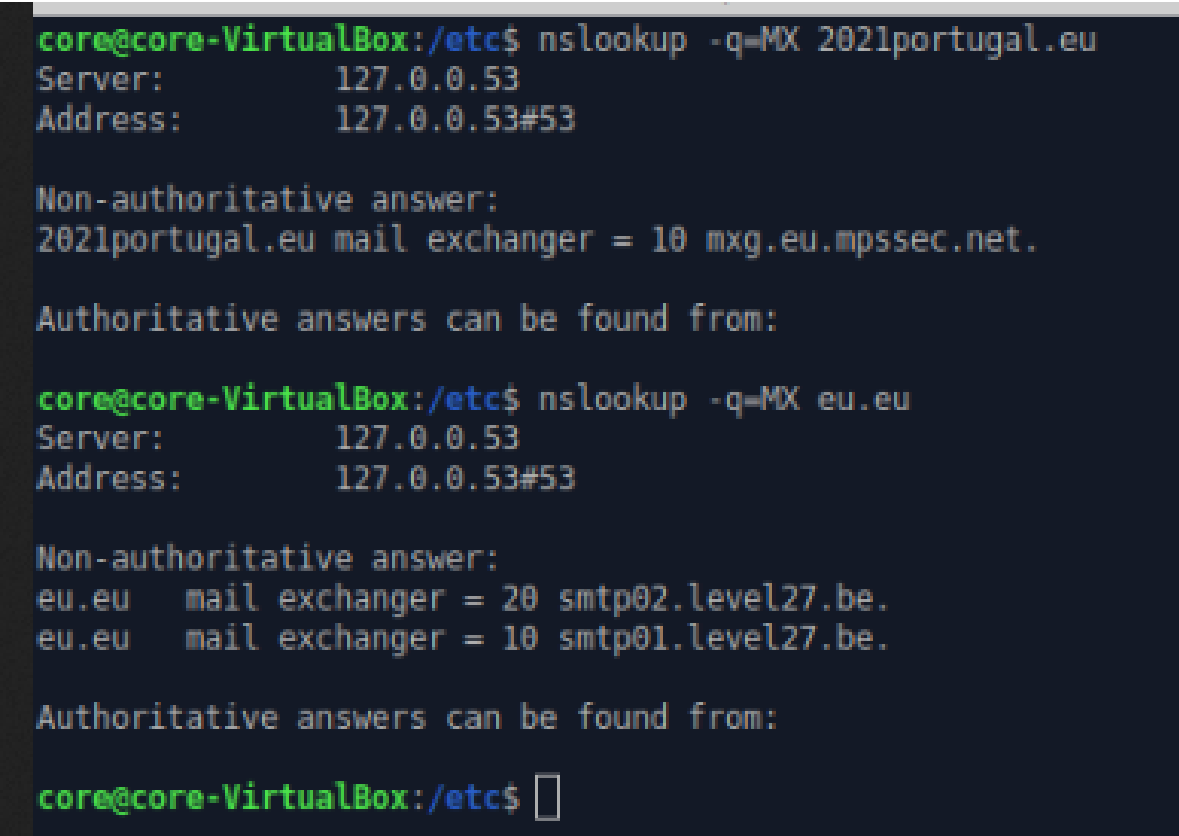


Figura 7: Correio eletrónico

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

Para além da identificação dos servidores de nome, podemos ver o endereço IP associado 127.0.0.53, o endereço de email dns.ceger.gov.pt, bem como os parâmetros do domínio tais como a serial, os tempos de refresh, retry e expire.

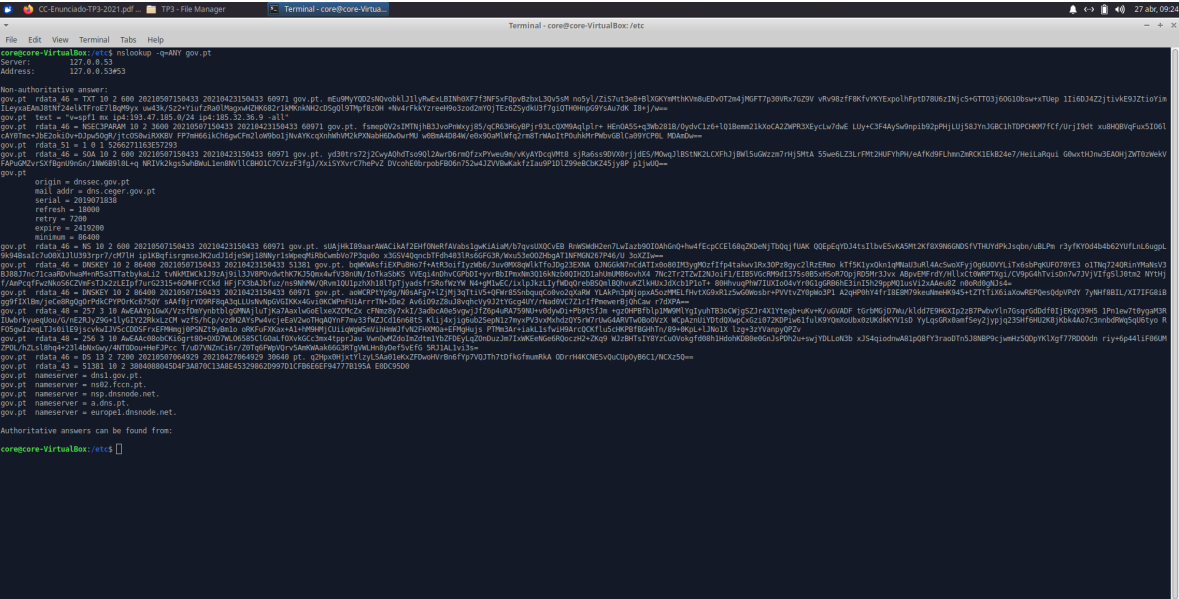


Figura 8: DNS gov.pt

Com o comando dig, ainda é possível verificar que as flags recursive available e recurse desirable estão ativas e mais algumas informações:

```

^Ccore@xubuncore:~$ dig gov.pt

;<> DiG 9.11.3-1ubuntu1.10-Ubuntu <> gov.pt
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30952
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

; Query time: 10 msec
; SERVER: 127.0.0.53#53(127.0.0.53)
; WHEN: Fri May 07 15:14:12 WEST 2021
; MSG SIZE rcvd: 35

```

Figura 9: Dig

- 1.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. Como podemos ver pela figura seguinte, o nome de domínio associado smtp01.fcn.pt. Ao interrogar o DNS sobre o nome de domínio fcn.pt. conseguimos obter o contacto de email do responsável: hostmaster.fcn.pt

```
Terminal - core@core-VirtualBox: ~
File Edit View Terminal Tabs Help

core@core-VirtualBox:~$ nslookup
> set query=SOA
> 2001:690:2080:8005::38
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
8.3.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.8.0.8.0.2.0.9.6.0.1.0.0.2.ip6.arpa    n
ame = smtp01.fccn.pt.

Authoritative answers can be found from:
> 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 = 2021050701
      refresh = 21600
      retry = 7200
      expire = 1209600
      minimum = 300

Authoritative answers can be found from:
> 
```

Figura 10: nslookup com IPv6

- 1.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).**

A "Transferência de zona" é uma query DNS do tipo AXFR que permite aos secundários ter acesso a uma zona de uma base de dados ou a uma base de dados inteira replicada dos primários, sendo que isto só acontece se o secundário o requisitar ao primário. Esta utiliza TCP para o transporte e assume a forma de cliente-servidor. Ao iniciar a transferência da base de dados replicada, verifica-se o número de série existente no preâmbulo que nos diz se a versão da base de dados que vamos replicar é mais recente do que aquela que o secundário já possui. Caso seja, a transferência é iniciada e pelo outro lado, se a versão que o secundário possui é igual ou mais recente do que aquela que estamos a pedir para transferir, esta não é efetuada visto não haver essa necessidade.

2 Parte II: Instalação, configuração e teste de um domínio CC.PT

2.0.1 Ficheiro /etc/hosts

```
127.0.0.1      localhost
127.0.1.1      xubuncore
10.1.1.1 Server1 ns.cc.pt
10.2.2.2 Mercurio ns2.cc.pt
# The following lines are desirable for IPv6 capable hosts
::1           ip6-localhost ip6-loopback
fe00::0       ip6-localnet
ff00::0       ip6-mcastprefix
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

2.1 Servidor Primário

2.1.1 Ficheiro primario/named.conf.options

```
options {
    directory "/home/core/primario";

    forwarders {
        193.136.9.240;
        193.136.19.1;
    };

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
```

2.1.2 Ficheiro primario/named.conf

```
include "/home/core/primario/named.conf.options";
include "/home/core/primario/named.conf.local";
include "/home/core/primario/named.conf.default-zones";

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

zone "1.1.10.in-addr.arpa"{
    type master;
    file "db.1-1-10.rev";
    allow-transfer { 10.2.2.2; };
};

zone "2.2.10.in-addr.arpa"{
    type master;
    file "db.2-2-10.rev";
    allow-transfer { 10.2.2.2; };
};

zone "4.4.10.in-addr.arpa"{
    type master;
    file "db.4-4-10.rev";
    allow-transfer { 10.2.2.2; };
};
```


};

2.1.3 Ficheiro primario/db.cc.pt

```
$TTL 604800

@      IN      SOA      Server1.cc.pt. PL05G03.cc.pt.(
                                2      ;Serial
                                604800 ;Refresh
                                86400  ;Retry
                                2419200 ;Expire
                                604800) ;Negative Cache TTL

@      IN NS     Server1.cc.pt.
@      IN NS     Mercurio.cc.pt.
@      IN MX     10 Server2.cc.pt.
@      IN MX     20 Server3.cc.pt.

Server1 IN A 10.1.1.1
ns      IN CNAME Server1

Mercurio IN A 10.2.2.2
ns2     IN CNAME Mercurio

Server2 IN A 10.1.1.2
www     IN CNAME Server2
mail    IN CNAME Server2

Server3 IN A 10.1.1.3
pop     IN CNAME Server3
imap    IN CNAME Server3

g03     IN A 10.4.4.1
Laptop1 IN CNAME g03

Marte   IN A 10.2.2.1

Venus   IN A 10.2.2.3
```

2.1.4 Ficheiro primario/db.1-1-10.rev

```
$TTL 86400

@      IN      SOA      cc.pt. PL05G03.cc.pt. (
                                1521262 ;Serial
                                28800   ;Refresh -24 hours
                                7200    ;Retry - 2hours
                                604800  ;Expire -7days
                                86400)  ;Minimum TTL - 1days

      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.
```

2.1.5 Ficheiro primario/db.2-2-10.rev

```
$TTL 86400

@      IN      SOA      cc.pt  PL05G03.cc.pt. (
                                1521262
                                28800
                                7200
                                604800
                                86400)

      IN      NS      Server1.cc.pt.
      IN      NS      Mercurio.cc.pt.

1     IN PTR  Marte.cc.pt.
2     IN PTR  Mercurio.cc.pt.
3     IN PTR  Venus.cc.pt.
```

2.1.6 Ficheiro primario/db.4-4-10.rev

```
$TTL 86400
@      IN      SOA      cc.pt.  PL05G03.cc.pt. (
                                1521262
                                28800
                                7200
                                604800
                                86400)

      IN      NS      Server1.cc.pt.
      IN      NS      Mercurio.cc.pt.

1      IN      PTR     Laptop1.cc.pt.
```

2.2 Servidor Secundário

2.2.1 Ficheiro secundario/named.conf.options

```
options {
    directory "/var/cache/bind";

    forwarders {
        193.136.9.240;
        193.136.19.1;
    };

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    auth-nxdomain no;      # conform to RFC1035
    listen-on-v6 { any; };
};
```

2.2.2 Ficheiro secundario/named.conf

```
include "/home/core/secundario/named.conf.options";
include "/home/core/secundario/named.conf.local";
include "/home/core/secundario/named.conf.default-zones";

zone "cc.pt"{
    type slave;
    masters {10.1.1.1; };
    file "db.cc.pt";
};

zone "1.1.10.in-addr.arpa"{
    type slave;
    masters {10.1.1.1; };
    file "db.1-1-10.rev";
};

zone "2.2.10.in-addr.arpa"{
    type slave;
    masters {10.1.1.1; };
    file "db.2-2-10.rev";
};

zone "4.4.10.in-addr.arpa"{
    type slave;
    masters {10.1.1.1; };
    file "db.4-4-10.rev";
};
```

2.3 Demonstração do domínio CC.PT

2.3.1 Inicialização dos servidores

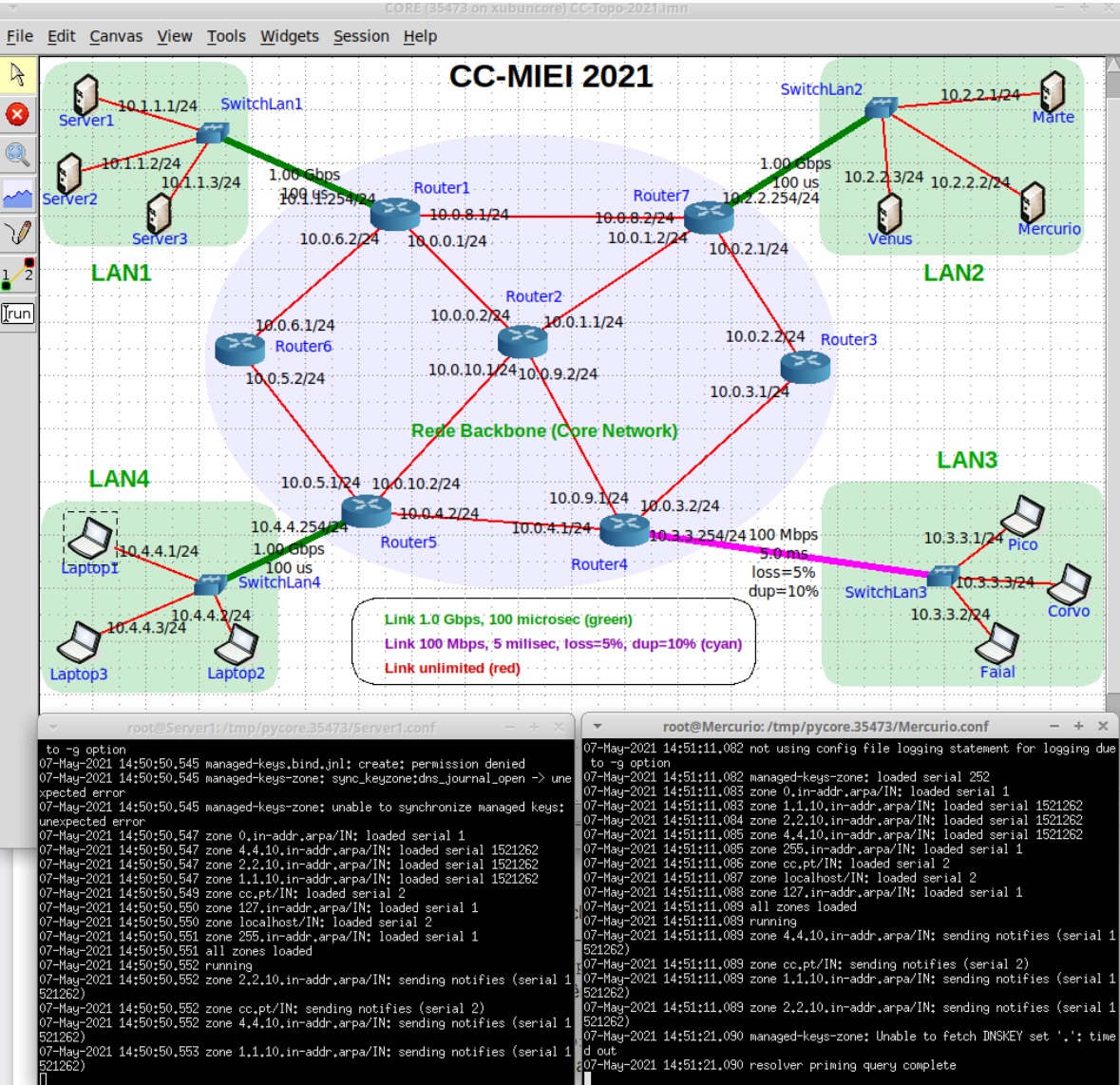


Figura 11: Demonstração da inicialização de ambos os servidores

2.3.2 Servidor Primário

```
root@Laptop1: /tmp/pycore.35473/Laptop1.conf
root@Laptop1:/tmp/pycore.35473/Laptop1.conf# nslookup - 10.1.1.1
> www.cc.pt
Server:      10.1.1.1
Address:     10.1.1.1#53

www.cc.pt    canonical name = Server2.cc.pt.
Name:  Server2.cc.pt
Address: 10.1.1.2
> G03.cc.pt
Server:      10.1.1.1
Address:     10.1.1.1#53

Name:  g03.cc.pt
Address: 10.4.4.1
> 10.2.2.2
2.2.2.10.in-addr.arpa  name = Mercurio.cc.pt.
> 10.1.1.2
2.1.1.10.in-addr.arpa  name = Server2.cc.pt.
>
```

Figura 12: Demonstração do domínio CC.PT utilizando queries no servidor primário

2.3.3 Servidor Secundário

```
root@Laptop1: /tmp/pycore.35473/Laptop1.conf
root@Laptop1:/tmp/pycore.35473/Laptop1.conf# nslookup - 10.2.2.2
> www.cc.pt
Server:      10.2.2.2
Address:     10.2.2.2#53

www.cc.pt    canonical name = Server2.cc.pt.
Name:  Server2.cc.pt
Address: 10.1.1.2
> g03.cc.pt
Server:      10.2.2.2
Address:     10.2.2.2#53

Name:  g03.cc.pt
Address: 10.4.4.1
> 10.1.1.1
1.1.1.10.in-addr.arpa  name = Server1.cc.pt.
> 10.1.1.2
2.1.1.10.in-addr.arpa  name = Server2.cc.pt.
>
```

Figura 13: Demonstração do domínio CC.PT utilizando queries no servidor secundário