

TP3: Serviço de Resolução de Nomes (DNS)

Catarina Machado - a81047 Gonçalo Faria - a86264
João Vilaça - a82339

4 de Abril de 2019

Resumo

Consultas ao serviço de nomes DNS.

Instalação, configuração e teste de um domínio CC.PT.

Keywords: DNS, XubunCORE Host

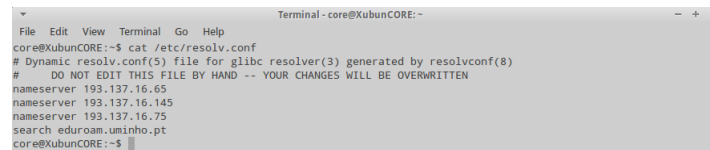
Questões e Respostas

1

1.1 a)

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

R: Contém os servidores de DNS por defeito, estipulados pelo administrador de rede, para resolução de domain names e IPs.

A terminal window titled 'Terminal - core@XubunCORE: ~' showing the output of the command 'cat /etc/resolv.conf'. The output is as follows:

```
core@XubunCORE:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 193.137.16.65
nameserver 193.137.16.145
nameserver 193.137.16.75
search eduroam.uminho.pt
core@XubunCORE:~$
```

Figura 1: Conteúdo do resolv.conf

1.2 b)

Os servidores `www.google.pt` e `www.google.com` têm endereços IPv6? Se sim, quais?

R: Sim, têm endereços IPv6. Estes foram obtidos através da especificação do *record store* DNS como sendo AAAA.

Os endereços obtidos são os seguintes:

`www.google.pt`: 2a00:1450:4003:80a::2003

`www.google.com`: 2a00:1450:4003:803::2004

```

+ nslookup -query=AAAA www.google.pt.
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
www.google.pt has AAAA address 2a00:1450:4003:80a::2003

Authoritative answers can be found from:
google.pt      nameserver = ns3.google.com.
google.pt      nameserver = ns1.google.com.
google.pt      nameserver = ns2.google.com.
google.pt      nameserver = ns4.google.com.
ns1.google.com internet address = 216.239.32.10
ns4.google.com internet address = 216.239.38.10
ns3.google.com internet address = 216.239.36.10
ns2.google.com internet address = 216.239.34.10
ns1.google.com has AAAA address 2001:4860:4802:32::a
ns4.google.com has AAAA address 2001:4860:4802:38::a
ns3.google.com has AAAA address 2001:4860:4802:36::a
ns2.google.com has AAAA address 2001:4860:4802:34::a

~

+ nslookup -query=AAAA www.google.com.
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
www.google.com has AAAA address 2a00:1450:4003:803::2004

Authoritative answers can be found from:
google.com     nameserver = ns2.google.com.
google.com     nameserver = ns4.google.com.
google.com     nameserver = ns1.google.com.
google.com     nameserver = ns3.google.com.
ns2.google.com internet address = 216.239.34.10
ns1.google.com internet address = 216.239.32.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10
ns2.google.com has AAAA address 2001:4860:4802:34::a
ns1.google.com has AAAA address 2001:4860:4802:32::a
ns3.google.com has AAAA address 2001:4860:4802:36::a
ns4.google.com has AAAA address 2001:4860:4802:38::a

```

Figura 2: IPv6 de www.google.pt e www.google.com

1.3 c)

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

- ccg.pt

Embora seja uma resposta não autoritativa, é possível verificar através do uso do comando nslookup com a interrogação do tipo NS que os servidores de nome são os representados na figura seguinte.

```

+ nslookup
> set q=NS
> ccg.pt.
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
ccg.pt nameserver = ns3.ccg.pt.
ccg.pt nameserver = ns1.ccg.pt.

Authoritative answers can be found from:
ns1.ccg.pt internet address = 193.136.11.201
ns3.ccg.pt internet address = 193.136.11.203

```

Figura 3: dig ccg.pt

- pt.

Embora seja uma resposta não autoritativa, é possível verificar através do uso do comando nslookup com a interrogação do tipo NS que os servidores de nome são os representados na figura seguinte.

```

+ nslookup
> set q=NS
> pt.
Server:      193.137.16.65
Address:     193.137.16.65#53

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

Authoritative answers can be found from:
d.dns.pt    internet address = 185.39.210.1
e.dns.pt    internet address = 193.136.192.64
f.dns.pt    internet address = 162.88.45.1
c.dns.pt    internet address = 204.61.216.105
b.dns.pt    internet address = 194.0.25.23
a.dns.pt    internet address = 185.39.208.1
g.dns.pt    internet address = 193.136.2.226
sns-pb.isc.org internet address = 192.5.4.1
ns2.nic.fr  internet address = 192.93.0.4
ns.dns.br   internet address = 200.160.0.5
d.dns.pt    has AAAA address 2a04:6d82::1
e.dns.pt    has AAAA address 2001:690:a00:4001::64
f.dns.pt    has AAAA address 2600:2000:3009::1
c.dns.pt    has AAAA address 2001:500:14:6105:ad::1
b.dns.pt    has AAAA address 2001:678:20::23

```

Figura 4: dig pt.

• .

Embora seja uma resposta não autoritativa, é possível verificar através do uso do comando nslookup com a interrogação do tipo NS que os servidores de nome são os representados na figura seguinte.

```

+ nslookup
> set q=NS
> .
Server:      193.137.16.65
Address:     193.137.16.65#53

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

Authoritative answers can be found from:
a.root-servers.net internet address = 198.41.0.4
b.root-servers.net internet address = 199.9.14.201
c.root-servers.net internet address = 192.33.4.12
d.root-servers.net internet address = 199.7.91.13
e.root-servers.net internet address = 192.203.230.10
f.root-servers.net internet address = 192.5.5.241
g.root-servers.net internet address = 192.112.36.4
h.root-servers.net internet address = 198.97.190.53
i.root-servers.net internet address = 192.36.148.17
a.root-servers.net has AAAA address 2001:503:ba3e::2:30
b.root-servers.net has AAAA address 2001:500:200::b
c.root-servers.net has AAAA address 2001:500:2::c
d.root-servers.net has AAAA address 2001:500:2d::d
e.root-servers.net has AAAA address 2001:500:a8::e

```

Figura 5: dig .

1.4 d)

Existe o domínio eureka.software.? Será que eureka.software. é um host?

Sim, existe um domínio eureka.software. e é um host uma vez que tem um endereço IP associado, tal como se pode ver na figura seguinte.

```
core@XubunCORE:~$ host eureka.software.  
eureka.software has address 34.214.90.141  
eureka.software mail is handled by 5 alt2.aspmx.l.google.com.  
eureka.software mail is handled by 10 aspmx3.googlemail.com.  
eureka.software mail is handled by 10 aspmx2.googlemail.com.  
eureka.software mail is handled by 1 aspmx.l.google.com.  
eureka.software mail is handled by 5 alt1.aspmx.l.google.com.  
core@XubunCORE:~$
```

Figura 6: Consulta do domínio eureka.software.

1.5 e)

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

DNS primário: ns1.dot2web.com.

O servidor primário (master) aceita queries recursivas. Nas flags da resposta ao comando 'dig ns1.dot2web.com.' está presente "ra" que significa "recursion available", Figura 8.

```
core@XubunCORE:~$ host -t soa ami.pt.  
ami.pt has SOA record ns1.dot2web.com. dc.dot2web.pt. 2019021301 3600 7200 1209600 86400
```

Figura 7: Consulta do DNS primário.

```
core@XubunCORE:~$ dig ns1.dot2web.com.  
  
; <<> DiG 9.8.1-P1 <<> ns1.dot2web.com.  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15434  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1  
  
;; QUESTION SECTION:  
;ns1.dot2web.com. IN A  
  
;; ANSWER SECTION:  
ns1.dot2web.com. 3034 IN A 80.172.230.28  
  
;; AUTHORITY SECTION:  
dot2web.com. 3023 IN NS ns2.dot2web.com.  
dot2web.com. 3023 IN NS ns1.dot2web.com.  
  
;; ADDITIONAL SECTION:  
ns2.dot2web.com. 2509 IN A 5.199.172.41  
  
;; Query time: 4 msec  
;; SERVER: 193.137.16.65#53(193.137.16.65)  
;; WHEN: Tue Mar 19 12:00:25 2019  
;; MSG SIZE rcvd: 97  
  
core@XubunCORE:~$
```

Figura 8: Verificação de aceitação de queries recursivas.

1.6 f)

Obtenha uma resposta “autoritativa” para a questão anterior.

Não foi possível obter uma resposta autoritativa. Nós, partindo do conhecimento obtido nas unidades curriculares de Redes de Computadores e Comunicação por Computador, supomos que isto é devido a estarmos a usar a rede uminho, na qual temos apenas um endereço IP privado. Ou seja, não há conectividade direta para o servidor primário ou secundário de ami.pt.

```
+ nslookup
> set q=NS
> ami.pt.
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
ami.pt  nameserver = ns2.dot2web.com.
ami.pt  nameserver = ns1.dot2web.com.

Authoritative answers can be found from:
ns1.dot2web.com internet address = 80.172.230.28
ns2.dot2web.com internet address = 54.36.137.213
> server 80.172.230.28
Default server: 80.172.230.28
Address: 80.172.230.28#53
> set q=SOA
> ami.pt.
;; connection timed out; no servers could be reached
> server 54.36.137.213
Default server: 54.36.137.213
Address: 54.36.137.213#53
> ami.pt.
;; connection timed out; no servers could be reached
```

Figura 9: Tentativa de resposta autorativa de ami.pt.

1.7 g)

Onde são entregues as mensagens dirigidas a marcelo@presidencia.pt ? E a guteres@onu.org?

Através de queries do tipo MX (Mail Exchanger) obtemos as seguintes respostas.

- presidencia.pt. :

As mensagens são entregues nos servidores mail2.presidencia.pt e mail1.presidencia.pt. Preferencialmente, são entregues em mail1.presidencia.pt pois o grau de preferência é superior.

```
+ nslookup
> set query=MX
> presidencia.pt.
Server:      193.137.16.65
Address:     193.137.16.65#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:
presidencia.pt nameserver = ns02.fccn.pt.
presidencia.pt nameserver = ns1.presidencia.pt.
presidencia.pt nameserver = ns2.presidencia.pt.
ns1.presidencia.pt internet address = 192.162.17.5
ns2.presidencia.pt internet address = 192.162.17.6
ns02.fccn.pt internet address = 193.136.2.228
ns02.fccn.pt has AAAA address 2001:690:a80:4001::200
```

Figura 10: Mail Exchanger presidencia.pt

- onu.org :

As mensagens são entregues no servidor mail.onu.org.

```
→ nslookup
> set query=MX
> onu.org.
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
onu.org mail exchanger = 10 mail.onu.org.

Authoritative answers can be found from:
onu.org nameserver = cp.semillasl.com.
onu.org nameserver = ns01.semillasl.com.
ns01.semillasl.com internet address = 178.33.85.8
```

Figura 11: Mail Exchanger onu.org.

1.8 h)

Que informação é possível obter acerca de www.whitehouse.gov? Qual é o endereço IPv4 associado?

Para além da identificação dos servidores de nomes, é possível consultar alguns dos pseudónimos deste domínio e também que as opções *recursive available* e *recursive desirable* estão ativas.

O endereço IPv4 associado é 23.10.65.110.

É possível obter também, através do comando dig, as informações que se encontram na figura seguinte.

```
+ dig www.whitehouse.gov.

; <<> DiG 9.10.6 <<> www.whitehouse.gov.
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 37257
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 8, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.whitehouse.gov.      IN      A

;; ANSWER SECTION:
www.whitehouse.gov.      300     IN      CNAME   wildcard.whitehouse.gov.edgekey.net.
wildcard.whitehouse.gov.edgekey.net. 499     IN      CNAME   e4036.dscb.akamaiedge.net.
e4036.dscb.akamaiedge.net. 20      IN      A       23.10.65.110

;; AUTHORITY SECTION:
dscb.akamaiedge.net.    2567    IN      NS       n0dscb.akamaiedge.net.
dscb.akamaiedge.net.    2567    IN      NS       n6dscb.akamaiedge.net.
dscb.akamaiedge.net.    2567    IN      NS       n4dscb.akamaiedge.net.
dscb.akamaiedge.net.    2567    IN      NS       n3dscb.akamaiedge.net.
dscb.akamaiedge.net.    2567    IN      NS       n7dscb.akamaiedge.net.
dscb.akamaiedge.net.    2567    IN      NS       n2dscb.akamaiedge.net.
dscb.akamaiedge.net.    2567    IN      NS       n5dscb.akamaiedge.net.
dscb.akamaiedge.net.    2567    IN      NS       n1dscb.akamaiedge.net.

;; ADDITIONAL SECTION:
n5dscb.akamaiedge.net.  2567    IN      A       88.221.90.165
n0dscb.akamaiedge.net.  2567    IN      A       88.221.81.192
n3dscb.akamaiedge.net.  2567    IN      A       2.16.65.213
n2dscb.akamaiedge.net.  2567    IN      A       2.16.65.212
n7dscb.akamaiedge.net.  2567    IN      A       104.86.111.37
n6dscb.akamaiedge.net.  2567    IN      A       2.16.65.205
n1dscb.akamaiedge.net.  2567    IN      A       2.16.65.207
n4dscb.akamaiedge.net.  2567    IN      A       2.16.65.214
n0dscb.akamaiedge.net.  2567    IN      AAAA    2600:1480:e800::c0

;; Query time: 49 msec
;; SERVER: 193.137.16.65#53(193.137.16.65)
;; WHEN: Tue Mar 26 12:33:12 WET 2019
;; MSG SIZE rcvd: 472
```

Figura 12: dig www.whitehouse.gov.

1.9 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?

Sim, é possível interrogar o DNS sobre o endereço IPv6, tal como se pode comprovar através da Figura 13. É possível obter o nome de domínio, neste caso `www.fccn.pt.`, associado ao endereço de IPv6 indicado assim como os seus servidores. No entanto, a informação obtida não teve origem numa resposta autoritativa. O responsável por este IPv6 têm o endereço de e-mail `hostmaster.fccn.pt.`

```
→ nslookup
> 2001:690:a00:1036:1113::247
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
7.4.2.0.0.0.0.0.0.0.3.1.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      name = www.fccn.pt.

Authoritative answers can be found from:
0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns01.fccn.pt.
0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns03.fccn.pt.
0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns02.fccn.pt.
ns03.fccn.pt      internet address = 138.246.255.249
ns02.fccn.pt      internet address = 193.136.2.228
ns01.fccn.pt      internet address = 193.136.192.40
ns03.fccn.pt      has AAAA address 2001:4ca0:106::250:56ff:fea9:3fd
ns02.fccn.pt      has AAAA address 2001:690:a00:4001::200
ns01.fccn.pt      has AAAA address 2001:690:a00:4001::200
```

Figura 13: Interrogação nslookup com endereço IPv6

```
→ nslookup
> set query=SOA
> www.fccn.pt.
Server:      193.137.16.145
Address:     193.137.16.145#53

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

Authoritative answers can be found from:
fccn.pt
  origin = ns01.fccn.pt
  mail addr = hostmaster.fccn.pt
  serial = 2019032801
  refresh = 21600
  retry = 7200
  expire = 1209600
  minimum = 14400
```

Figura 14

1.10 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)

Transferência de zona DNS é uma query DNS do tipo IXFR ou AXFR. Esta query é usada para replicar uma porção contígua (zona) ou a totalidade da base de dados DNS do servidor que a recebe. A transferência é feita, através de uma ligação TCP, começando pela verificação do preâmbulo que contém um número de série. Esta verificação determina se a transferência tem de facto de ocorrer pois, se o número de série for igual ou inferior ao do servidor que envia o pedido

de transferência de zona, a transferência não ocorre dado que este contém uma versão da base de dados igual ou mais recente.

Criação de um domínio de nomes CC.PT

```
zone "cc.pt" {  
    type master;  
    file "/home/core/primario/db.cc.pt";  
    allow-transfer { 10.2.2.3; };  
};  
  
zone "1.1.10.in-addr.arpa." {  
    type master;  
    file "/home/core/primario/db.1-1-10.rev";  
    allow-transfer { 10.2.2.3; };  
};
```

Figura 15: primario/named.conf.local

```
$TTL      604800  
@         IN      SOA      dns.cc.pt. grupo24.cc.pt. (  
            3          ; Serial  
            604800     ; Refresh  
            86400      ; Retry  
            2419200    ; Expire  
            604800 )    ; Negative Cache TTL  
;  
; name servers - NS records  
            IN      NS      dns.cc.pt.  
            IN      NS      dns2.cc.pt.  
;  
; SWITCH LAN 1  
Servidor1  IN      A        10.1.1.1  
dns        IN      A        10.1.1.1  
  
Servidor3  IN      A        10.1.1.3  
www        IN      CNAME    Servidor3  
mail       IN      MX       20      Servidor3  
  
Servidor2  IN      A        10.1.1.2  
pop        IN      CNAME    Servidor2  
imap       IN      CNAME    Servidor2  
mail       IN      MX       10      Servidor3  
  
; SWITCH LAN 2  
Plutao     IN      A        10.2.2.1  
Neptuno    IN      A        10.2.2.2  
Urano      IN      A        10.2.2.3  
dns2       IN      A        10.2.2.3  
  
; SWITCH LAN 3  
Alfa       IN      A        10.3.3.1  
Beta       IN      A        10.3.3.2  
Gama       IN      A        10.3.3.3  
  
; SWITCH LAN 4  
Cliente1   IN      A        10.4.4.1  
Grupo24    IN      CNAME    Cliente1  
  
Cliente2   IN      A        10.4.4.2  
Cliente3   IN      A        10.4.4.3
```

Figura 16: primario/db.cc.pt

```

$TTL 604800
@ IN SOA cc.pt. admin.cc.pt. (
                               3      ; Serial
                               604800  ; Refresh
                               86400   ; Retry
                               2419200 ; Expire
                               604800 ) ; Negative Cache TTL

; name servers
IN NS dns.cc.pt.
IN NS dns2.cc.pt.

; PTR Records
1.1.10 IN PTR dns.cc.pt. ; 10.1.1.1
2.2.10 IN PTR dns2.cc.pt. ; 10.2.2.3

```

Figura 17: primario/db.1-1-10.rev

```

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

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

```

Figura 18: secundario/named.conf.local

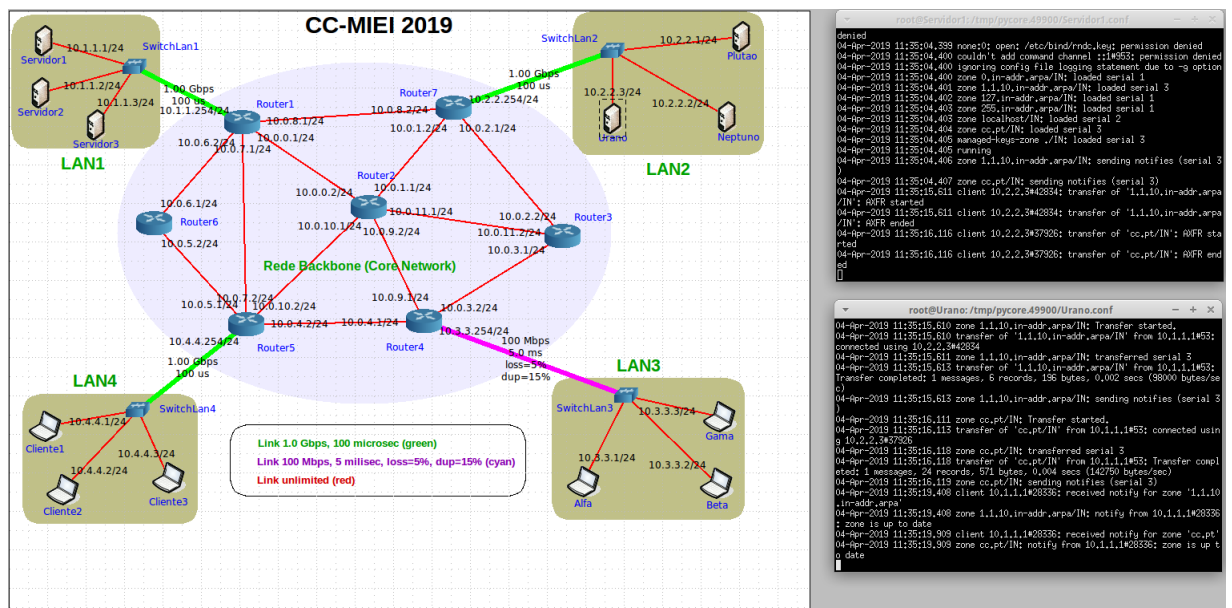


Figura 19: Transferência da base de dados de master para o slave

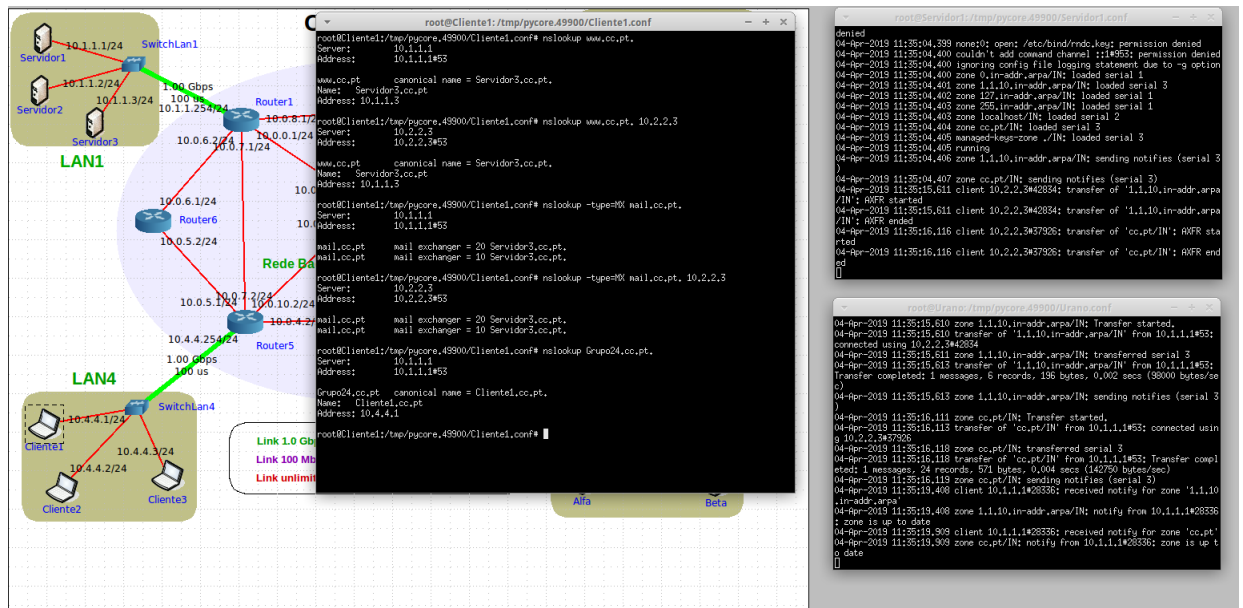


Figura 20: Queries aos servidores de DNS

Conclusões

Este trabalho prático serviu de complemento às aulas teóricas e ajudou a consolidar a matéria lecionada nas mesmas.

Depois de finalizado o trabalho prático número 3, relativo ao DNS, Serviço de Resolução de Nomes, obtivemos mais conhecimentos sobre este sistema de gestão de nomes hierárquico e distribuído.

Durante a primeira parte da resolução deste trabalho prático, Questões e Respostas, praticamos diferentes formas de interrogar o DNS. Começamos por analisar o ficheiro que contém os servidores de DNS por defeito, `resolv.conf` e, ao longo das questões, fomos utilizando o comando `nslookup`. O **nslookup** tem várias funcionalidades que permitem construir interrogações específicas a servidores DNS, em particular criamos interrogações que requeriam registos em particular, como por exemplo o registo **AAAA**, indicado para obter endereços IPv6, o registo **NS** com os name servers do domínio, o registo **MX** com os servidores de e-mail e o registo **SOA** que contém a informação administrativa de uma zona.

Na segunda parte do presente trabalho prático, procedemos à instalação, configuração e teste de um domínio CC.PT. Inicialmente, começamos por preparar o ambiente CORE, replicando os ficheiros de configuração, parando o servidor de DNS pré-instalado e, por fim, reconfigurando o `apparmor`. Em seguida, configuramos o servidor primário, o cliente, o teste do servidor primário e, por último, configuramos o servidor secundário.