



UNIVERSIDADE DO MINHO

DEPARTAMENTO DE INFORMÁTICA

Comunicações por Computador
TP3-Serviço de Resolução de Nomes (DNS)
Grupo N^o 03

Gonçalo Almeida (A84610)

Emanuel Rodrigues (A84776)

Lázaro Pinheiro (A86788)

15 de Abril de 2020

Conteúdo

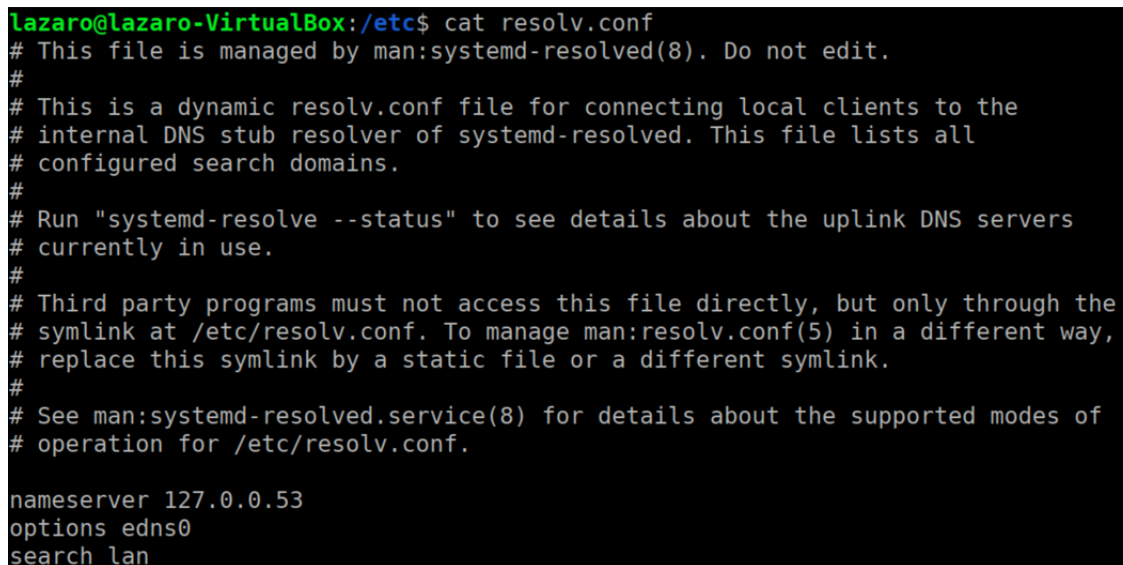
1	Questões e Respostas	3
1.1	Parte I: Consultas ao serviço de nomes DNS	3
1.2	Parte II: Instalação, configuração e teste de um domínio CC.PT	12
2	Conclusão	16

Capítulo 1

Questões e Respostas

1.1 Parte I: Consultas ao serviço de nomes DNS

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

A terminal window with a black background and green text. The prompt is 'lazaro@lazaro-VirtualBox:/etc\$'. The command 'cat resolv.conf' has been executed, displaying the following content: '# 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', 'search lan'.

```
lazaro@lazaro-VirtualBox:/etc$ cat 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
search lan
```

Figura 1.1: Conteúdo do ficheiro `/etc/resolv.conf`.

O ficheiro `/etc/resolv.conf` possui a informação relativa às configurações por omissão do sistema, nomeadamente os servidores de nome e o domínio em que nos encontramos, utilizados para aceder ao serviço de DNS.

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

```

lazaro@lazaro-VirtualBox:/etc$ 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
lazaro@lazaro-VirtualBox:/etc$ 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 87.248.98.8
atsv2-fp-shed.wg1.b.yahoo.com has address 87.248.98.7
atsv2-fp-shed.wg1.b.yahoo.com has IPv6 address 2a00:1288:110:1c::3
atsv2-fp-shed.wg1.b.yahoo.com has IPv6 address 2a00:1288:110:1c::4

```

Figura 1.2: Endereços IPv6 dos servidores www.sapo.pt. www.yahoo.com.

Os dois servidores indicados possuem os seguintes endereços IPv6:

1. www.sapo.pt.
2001:8a0:2102:c:213:13:146:142
2. www.yahoo.com.
2a00:1288:110:1c::3
2a00:1288:110:1c::4

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

Os servidores de nome definidos para “uminho.pt.” são ns02.fccn.pt., dns3.uminho.pt., dns2.uminho.pt., dns.uminho.pt. como se observa na Figura 3.

```

nslookup
> set q=NS
> uminho.pt.
Server:          127.0.0.53
Address:         127.0.0.53#53

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

```

Figura 1.3: Servidores de nome para o domínio “uminho.pt.”

Os servidores de nome definidos para “pt.” são os 10 nameservers apresentados na figura 4.

```
> pt.  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
pt      nameserver = d.dns.pt.  
pt      nameserver = e.dns.pt.  
pt      nameserver = b.dns.pt.  
pt      nameserver = ns2.nic.fr.  
pt      nameserver = h.dns.pt.  
pt      nameserver = a.dns.pt.  
pt      nameserver = c.dns.pt.  
pt      nameserver = g.dns.pt.  
pt      nameserver = ns.dns.br.  
pt      nameserver = f.dns.pt.
```

Figura 1.4: Servidores de nome para o domínio “pt.”

Os servidores de nome definidos para “.” são todos os nameserver apresentados na Figura 5.

```
> .
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 = a.root-servers.net.
.               nameserver = f.root-servers.net.
.               nameserver = c.root-servers.net.
.               nameserver = d.root-servers.net.
.               nameserver = m.root-servers.net.
.               nameserver = i.root-servers.net.
.               nameserver = l.root-servers.net.
.               nameserver = e.root-servers.net.
.               nameserver = k.root-servers.net.
.               nameserver = h.root-servers.net.
.               nameserver = b.root-servers.net.
```

Figura 1.5: Servidores de nome para o domínio “.”

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

Pode-se concluir que o domínio nice.software. existe, pois quando questionado acerca dos seus servidores de nome este responde com 3 nameserver's.

```

nslookup
> set q=NS
> nice.software.
Server:      127.0.0.53
Address:     127.0.0.53#53

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

Authoritative answers can be found from:

```

Figura 1.6: Query que permite determinar se nice.software. existe

Constatou-se que nice.software. é um host, dado que quando questionado com uma query com vista a obter o endereço de IP, este responde com um endereço.

```

> 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 1.7: Query que permite determinar o endereço IP de nice.software.

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

Com a finalidade de se obter o DNS primário definido para o domínio msf.org., elaborou-se uma query com o comando SOA. A partir da resposta desta à query verifica-se, partindo do campo origin na secção Non-authoritative answer, que DNS primário é o ns1.dds.nl.

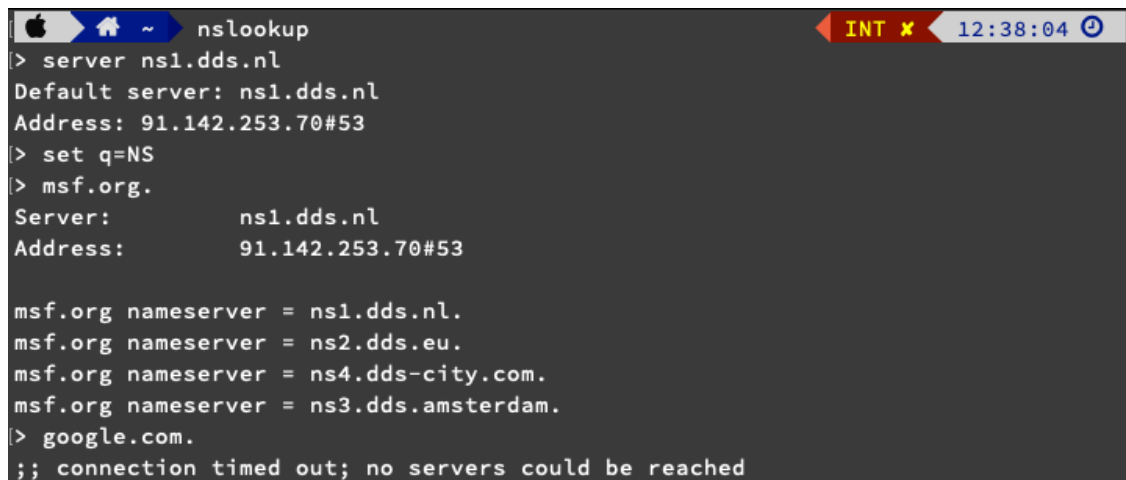
```
nslookup
> set q=SOA
> msf.org.
Server:          127.0.0.53
Address:         127.0.0.53#53

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:
```

Figura 1.8: Query do tipo SOA enviada para msf.org.

De modo a verificar se o servidor primário aceita queries recursivas alterou-se o servidor para o servidor primário (obtido anteriormente). Verificou-se que para o domínio msf.org. obtemos resposta, dado que a informação se encontra nativamente. Posteriormente, testou-se com um novo domínio (ex. - google.com.) e percebeu-se que não foi possível (no servers could be reached), concluindo-se assim que este não é recursivo.

A terminal window titled 'nslookup' with a status bar showing 'INT x' and '12:38:04'. The user enters the command 'server ns1.dds.nl', which sets the default server to ns1.dds.nl with address 91.142.253.70#53. Then, the user enters 'set q=NS' and 'msf.org.'. The terminal displays the server information for ns1.dds.nl and then lists four authoritative name servers for msf.org: ns1.dds.nl, ns2.dds.eu, ns4.dds-city.com, and ns3.dds.amsterdam. Finally, the user enters 'google.com.', and the terminal returns the message ';; connection timed out; no servers could be reached'.

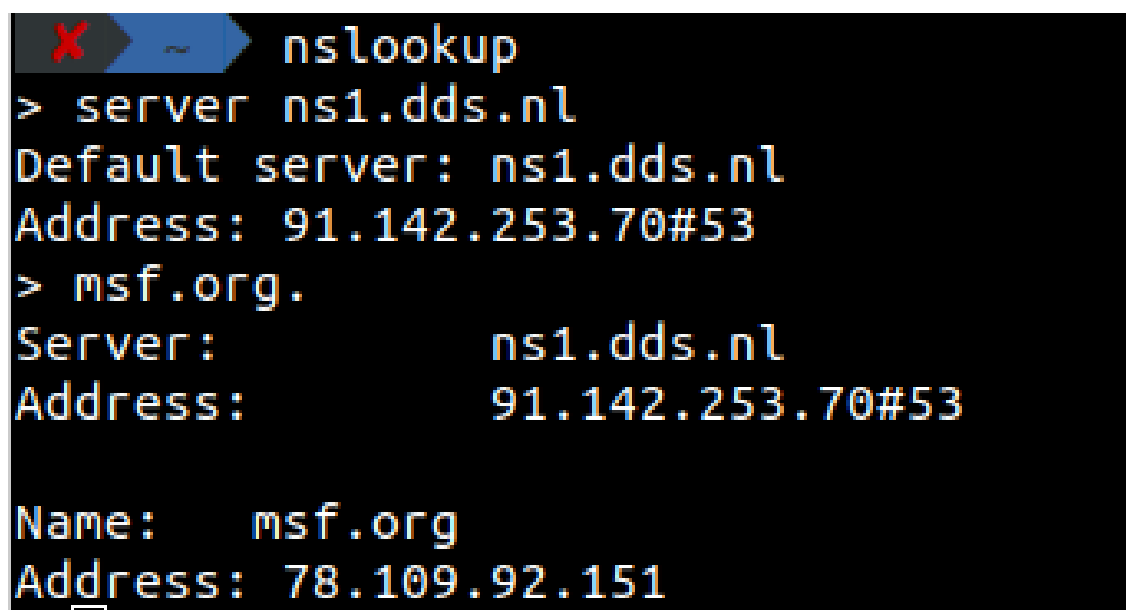
```
nslookup
> server ns1.dds.nl
Default server: ns1.dds.nl
Address: 91.142.253.70#53
> set q=NS
> msf.org.
Server:          ns1.dds.nl
Address:         91.142.253.70#53

msf.org nameserver = ns1.dds.nl.
msf.org nameserver = ns2.dds.eu.
msf.org nameserver = ns4.dds-city.com.
msf.org nameserver = ns3.dds.amsterdam.
> google.com.
;; connection timed out; no servers could be reached
```

Figura 1.9: Query ao novo servidor.

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

Por forma a obtermos uma resposta autoritativa, definiu-se como servidor default o ns1.dds.nl (servidor primário do domínio msf.org.), assim é possível realizar novamente a query.

A terminal window titled 'nslookup' with a status bar showing a red 'X' icon. The user enters the command 'server ns1.dds.nl', which sets the default server to ns1.dds.nl with address 91.142.253.70#53. Then, the user enters 'msf.org.'. The terminal displays the server information for ns1.dds.nl and then provides the authoritative response for msf.org, showing its name and address: 78.109.92.151.

```
nslookup
> server ns1.dds.nl
Default server: ns1.dds.nl
Address: 91.142.253.70#53
> msf.org.
Server:          ns1.dds.nl
Address:         91.142.253.70#53

Name:   msf.org
Address: 78.109.92.151
```

Figura 1.10: Exemplo de resposta autoritativa

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

```

goncalo@RC:~$ nslookup
> set q=MX
> presidencia.pt
Server:      127.0.0.53
Address:     127.0.0.53#53

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

Authoritative answers can be found from:

```

Figura 1.11: Query a marcelo@presidencia.pt

```

goncalo@RC:~$ nslookup
> set q=MX
> casacivil.gov.br
Server:      127.0.0.53
Address:     127.0.0.53#53

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

Authoritative answers can be found from:

```

Figura 1.12: Query a bolsonaro@casacivil.gov.br

Através de uma query do tipo MX ao domínio presidencia.pt podemos ver que as mensagens de correio dirigidas ao presidente marcelo@presidencia.pt são entregues a mail2.presidencia.pt, sendo que tem prioridade (mail exchanger = 10) e o mail1.presidencia.pt tem prioridade (mail exchanger = 50). Isto porque quanto menor este número, maior a prioridade.

Realizando o mesmo processo para o bolsonaro@casacivil.gov.br, verificamos que as mensagens de correio são entregues a esa01.presidencia.gov.br. pelo mesmo motivo do anterior.

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

```

goncalo@RC:~$ nslookup
> set q=A
> www.whitehouse.gov
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.whitehouse.gov      canonical name = wilddcard.whitehouse.gov.edgekey.net.
wilddcard.whitehouse.gov.edgekey.net canonical name = e4036.dscb.akamaiedge.net.
Name:   e4036.dscb.akamaiedge.net
Address: 184.25.43.191

```

Figura 1.13: Query a whitehouse.gov

Observando a figura 13, verificamos que o domínio whitehouse.gov é um alias do wilddcard.whitehouse.gov.edgekey.net. Por sua vez, o wilddcard.whitehouse.gov.edgekey.net é um alias do e4036.dscb.akamaiedge.net. No campo Address encontramos o IPv4 associado, sendo este 184.25.43.191.

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?

```

goncalo@RC:~$ nslookup
> set q=PTR
> 2001:690:a00:1036:1113::247
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
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:
>
>
> set q=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 1.14: Query ao IPv6 2001:690:a00:1036:1113::247

Como demonstrado na figura, é possível interrogar o DNS sobre o endereço pedido através do nslookup. Deste modo foi possível, através de uma query do tipo PTR, obter informações dos nameservers. De seguida, através de uma query do tipo SOA ao domínio fccn.pt., podemos observar no campo origin que o contacto responsável por esse IPv6 é o ns01.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).

```
goncalo@RC:~$ nslookup
> set q=SOA
> di.uminho.pt
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
di.uminho.pt
      origin = dns.di.uminho.pt
      mail addr = dnsadmin.di.uminho.pt
      serial = 2020033003
      refresh = 28800
      retry = 7200
      expire = 28800
      minimum = 43200

Authoritative answers can be found from:
```

Figura 1.15: Query a di.uminho.pt

O mecanismo “Transferência de zona” permite um servidor secundário (slave server) replicar a base de dados do servidor principal (main server), sendo que deve pedir ao servidor primário primeiro. Através de uma query do tipo SOA ao domínio di.uminho.pt obtivemos os campos demonstrados na figura. Podemos concluir que o servidor secundário tem acesso ao serial number da base de dados e a campos temporais que permitem a sua atualização. Caso o serial number seja o mesmo é porque não houve alterações, caso contrário o servidor secundário deve replicar novamente a base de dados. Caso este procedimento falhe e observando o campo retry, deve ser realizada uma nova tentativa após 7200 segundos.

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

O ficheiro primário/named.conf inclui cinco zonas do tipo master, uma vez que estamos perante um servidor primário. Dado que a topologia fornecida possui quatro redes LAN, tornou-se impreterível

a existência de uma zona para cada uma destas. Acrescentou-se ainda, uma cláusula que possibilita a transferência de dados para o servidor secundário através de allow-transfer 10.4.4.1; .

```
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/emanuel/primario/db.cc.pt";
    allow-transfer{10.4.4.1;};
};

zone "1.1.10.in-addr.arpa" {
    type master;
    file "/home/emanuel/primario/db.1-1-10.rev";
    allow-transfer{ 10.4.4.1; };
};

zone "2.2.10.in-addr.arpa" {
    type master;
    file "/home/emanuel/primario/db.2-2-10.rev";
    allow-transfer{ 10.4.4.1; };
};

zone "3.3.10.in-addr.arpa" {
    type master;
    file "/home/emanuel/primario/db.3-3-10.rev";
    allow-transfer{10.4.4.1;};
};

zone "4.4.10.in-addr.arpa" {
    type master;
    file "/home/emanuel/primario/db.4-4-10.rev";
    allow-transfer{ 10.4.4.1; };
};
```

Figura 1.16: Ficheiro primario/named.conf

Posteriormente procedeu-se à criação e configuração do ficheiro primário/db.cc.pt. Neste estabeleceu-se o servidor principal, o servidor dns.cc.pt e o grupo03.cc.pt como administrador. Os nameservers são o dns.cc.pt e o dns2.cc.pt e os servidores de email. Note-se ainda que o Serv3.cc.pt possui prioridade 10 e o Serv2.cc. prioridade 20.

Por fim, para cada nó da topologia de rede estabeleceu-se uma associação entre o nome e o endereço IP.

```

$TTL 604800
@ IN SOA Serv1.cc.pt. grupo03@cc.pt. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS Serv1.cc.pt.
@ IN NS Hermes.cc.pt.
;
dns IN CNAME Serv1.cc.pt.
dns2 IN CNAME Hermes.cc.pt.
www IN CNAME Serv3.cc.pt.
mail IN CNAME Serv3.cc.pt.
pop IN CNAME Serv2.cc.pt.
imap IN CNAME Serv2.cc.pt.
Grupo03 IN CNAME Portatil1.cc.pt.
;
@ IN MX 10 Serv3
@ IN MX 20 Serv2
;
Portatil1 IN A 10.1.1.1
Portatil2 IN A 10.1.1.2
Portatil3 IN A 10.1.1.3
Alfa IN A 10.2.2.1
Delta IN A 10.2.2.2
Omega IN A 10.2.2.3
Serv1 IN A 10.3.3.1
Serv2 IN A 10.3.3.2
Serv3 IN A 10.3.3.3
Hermes IN A 10.4.4.1
Zeus IN A 10.4.4.2
Atena IN A 10.4.4.3

```

No final, criaram-se os ficheiros de domínios reverse.

```

$TTL 604800
@ IN SOA Serv1.cc.pt. grupo03@cc.pt. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS Serv1.
@ IN NS Hermes.
1 IN PTR Serv1.cc.pt.
2 IN PTR Serv2.cc.pt.
3 IN PTR Serv3.cc.pt.

```

Figura 1.17: Ficheiro primario/db.3-3-10.rev

Capítulo 2

Conclusão

A realização deste trabalho prático permitiu-nos a melhor compreensão sobre o serviço de resolução de Nomes (DNS). Numa primeira fase tiramos proveito do comando `nslookup` que nos permitiu realizar queries a endereços e domínios. Numa segunda fase desenvolvemos servidores primário e secundário de forma a serem implementados na topologia core fornecida no início do semestre. Consideramos que este trabalho foi bem sucedido da nossa parte tendo em conta que atingimos todos os objetivos solicitados.