



UNIVERSIDADE DO MINHO

**Trabalho Prático N.º.3–
Serviço de Resolução de Nomes (DNS)**

PL3 Grupo 7

Mestrado Integrado em Engenharia Informática

Comunicações por Computador

A89983
Paulo Lima

A81931
Luís Duarte

A84010
Ulisses Araújo

14 de abril de 2020

Questões e Respostas

Parte 1

1.

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

R: O ficheiro contém o servidor de DNS por defeito, estipulado pelo administrador da rede para a resolução de domain names e IP's. Através do uso do comando "cat" obteve-se esta informação, sendo apresentada de seguida:

```
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 192.168.1.254
search lan
core@XubunCORE:~$
```

Figura 1- Conteúdo do ficheiro "resolve.conf"

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

R: Ambos os servidores contêm endereços IPv6. Estes foram obtidos, como apresentado de seguida, através do uso do comando "nslookup" com especificação do tipo sendo "AAAA".

Os endereços são apresentados de seguida:

`www.sapo.pt`: 2001:8a0:2102:c:213:13:146:142

`www.yahoo.com`: 2a00:1288:110:1c::4 / 2a00:1288:110:1c::3

```
core@XubunCORE:~$ nslookup -query=AAAA www.sapo.pt.
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
www.sapo.pt  has AAAA address 2001:8a0:2102:c:213:13:146:142

Authoritative answers can be found from:
sapo.pt nameserver = ns.sapo.pt.
sapo.pt nameserver = ns2.sapo.pt.
sapo.pt nameserver = dns01.sapo.pt.
sapo.pt nameserver = dns02.sapo.pt.
ns.sapo.pt  internet address = 212.55.154.202
ns2.sapo.pt internet address = 212.55.154.194
dns01.sapo.pt internet address = 213.13.28.116
dns01.sapo.pt has AAAA address 2001:8a0:2106:4:213:13:28:116
dns02.sapo.pt internet address = 213.13.30.116
dns02.sapo.pt has AAAA address 2001:8a0:2206:4:213:13:30:116
```

Figura 2- Ipv6 de `www.sapo.pt`.

```
core@XubunCORE:~$ nslookup -query=AAAA www.yahoo.com.
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
www.yahoo.com canonical name = atsv2-fp-shed.wg1.b.yahoo.com.
atsv2-fp-shed.wg1.b.yahoo.com has AAAA address 2a00:1288:110:1c::4
atsv2-fp-shed.wg1.b.yahoo.com has AAAA address 2a00:1288:110:1c::3

Authoritative answers can be found from:
```

Figura 3- IPv6 de `www.yahoo.com`.

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

R: O servidor de nome definido para um domínio pode ser obtido usando o comando “nslookup” com a interrogação “Name Server”. Usando esta estratégia para cada um dos domínios pretendidos é possível então conhecer os seus servidores de nome, e os resultados são apresentados de seguida:

```
> set type=NS
> uminho.pt.
Server:          192.168.1.254
Address:         192.168.1.254#53

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

Authoritative answers can be found from:
```

Figura 4- Nomes para domínio "uminho.pt."

```
core@XubunCORE:~$ nslookup
> set q=NS
> pt.
Server:          192.168.1.254
Address:         192.168.1.254#53

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

Authoritative answers can be found from:
```

Figura 5- Nomes para domínio "pt."

```

core@XubunCORE:~$ nslookup
> set q=NS
> .
Server:      192.168.1.254
Address:     192.168.1.254#53

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

Authoritative answers can be found from:
>

```

Figura 6- Nomes para o domínio "."

- d) **Existe o domínio nice.software. ? Será que nice.software. é um host ou um domínio?**
 Usando o comando "host" conseguimos encontrar o endereço IP, o que prova que o domínio nice.software. não só existe, como ainda que se trata de um host.

```

core@XubunCORE:~$ host nice.software.
nice.software has address 213.212.81.71

```

Figura 7- Consulta do domínio "nice.software."

- e) **Qual é o servidor DNS primário definido para o domínio msf.org.? Este servidor primário (master) aceita queries recursivas? Porquê?**
 Usando o comando "nslookup" com o tipo "Start of Authority" é possível conhecer o DNS primário para o domínio que se pretende sendo este igual a postmaster.msf.org. De seguida, usando o comando "dig" para o DNS descoberto anteriormente, é possível ver que nas flags está presente "ra" que significa "recursion available" e, por conseguinte, mostra que a opção de recursividade está ativa sendo aceite queries recursivas. Estas operações são demonstradas de seguida:

```

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:
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.

```

Figura 8- Consulta do DNS primário

```

core@XubunCORE:~$ dig postmaster.msf.org

; <<>> DiG 9.8.1-P1 <<>> postmaster.msf.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16715
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;postmaster.msf.org.          IN      A

;; ANSWER SECTION:
postmaster.msf.org.         3600    IN      A      188.226.238.13

;; Query time: 136 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Tue Mar 24 13:12:53 2020
;; MSG SIZE rcvd: 52

```

Figura 9- Verificação de aceitação de queries recursivas

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

R: De forma a obter uma resposta autoritativa usamos o tipo “Service Locator”, sendo isto apresentado de seguida:

```

Authoritative answers can be found from:
> set type=SRV
> msf.org.
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
*** Can't find msf.org.: No answer

Authoritative answers can be found from:
msf.org
  origin = ns1.dds.nl
  mail addr = postmaster.msf.org
  serial = 1407464621
  refresh = 16384
  retry = 2048
  expire = 1048576
  minimum = 2560

```

Figura 10- Resposta autoritativa

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

R: Usando o comando “host” com o type “Mail Exchanger” é possível saber os servidores de email para determinado domínio. Assim, usando esta estratégia, apresentada de seguida, obteve-se os seguintes resultados:

- marcelo@presidencia.pt: As mensagens são entregues nos servidores mail2.presidencia.pt. e mail1.presidencia.pt., sendo preferencialmente entregues em mail2.presidencia.pt devido ao grau de preferência maior.
- bolsonaro@casacivil.gov.br: As mensagens são entregues nos servidores esa02.presidencia.gov.br. e esa01.presidencia.gov.br., sendo preferencialmente entregues em esa02.presidencia.gov.br. devido ao grau de preferência maior.


```

core@XubunCORE:~$ nslookup
> set query=MX
> presidencia.pt.
Server:          192.168.1.254
Address:         192.168.1.254#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- Mail Exchanger de "presidencia.pt"

```

core@XubunCORE:~$ nslookup
> set q=MX
> casacivil.gov.br.
Server:          192.168.1.254
Address:         192.168.1.254#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 12- Mail Exchanger de "gov.br"

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

Usando o comando “dig” é possível obter bastante informação, sendo esta a identificação dos servidores de nomes, algumas estatísticas como o tempo que demorou a query, e ainda as flags associadas, que representam opções como “recursive available” e “recursive desirable” ativas. O endereço IPv4 associado é 69.192.66.35. Toda esta informação é apresentada de seguida:

```

core@XubunCORE:~$ dig whitehouse.gov

;; <<>> DiG 9.8.1-P1 <<>> whitehouse.gov
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41161
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;whitehouse.gov.                IN      A

;; ANSWER SECTION:
whitehouse.gov.                20      IN      A      69.192.66.35

;; Query time: 65 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Tue Mar 24 15:02:12 2020
;; MSG SIZE rcvd: 48

```

Figura 13- dig de whitehouse.gov

- 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?**

R: Sim, é possível interrogar o DNS sobre o endereço IPv6, e tal é mostrado na Figura 14. É possível obter o nome do domínio associado, sendo este `www.fccn.pt`. No entanto a resposta não teve origem autoritativa, sendo para isso necessário usar novamente o comando “`nslookup`”, mas agora com o tipo “Start of Authority”, para o nome do domínio obtido anteriormente. Na resposta autoritativa temos ainda o endereço de email associado ao endereço IPv6 fornecido, como se pode ver na figura 15.

```
> ^Ccore@XubunCORE:~$ nslookup
> 2001:690:a00:1036:1113::247
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
7.4.2.0.0.0.0.0.0.0.0.0.3.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa    n
ame = www.fccn.pt.
```

Figura 14- Interrogação com endereço IPv6

```
core@XubunCORE:~$ nslookup
> set q=SOA
> www.fccn.pt.
Server:      192.168.1.254
Address:     192.168.1.254#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 = 2020032305
    refresh = 21600
    retry = 7200
    expire = 1209600
    minimum = 14400
>
```

Figura 15- Resposta autoritativa para “`www.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 é uma query DNS do tipo AXFR usada com o objetivo de replicação de uma porção ou totalidade da base de dados do servidor que a atende. Normalmente é uma query usada para servidores secundários pedirem a informação mais recente ao servidor

primário para efeitos de sincronização. Por esta razão, é acompanhada por um número de serie que verifica se a informação do servidor secundária se encontra atualizada, porque se sim, a transferência é cancelada e apenas caso contrário prossegue, por questões de eficiência. Esta transferência é feita através de uma ligação TCP.

Parte 2

Criação de um domínio de nomes

```
$TTL      604800
@         IN      SOA      dns.cc.pt. grupo7.cc.pt. (
                        2      ; 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
Portatil1      IN      A        10.1.1.1
Grupo7         IN      CNAME    Portatil1

Portatil2      IN      A        10.1.1.2
Portatil3      IN      A        10.1.1.3

; SWITCH LAN 2
Alfa           IN      A        10.2.2.1
Delta          IN      A        10.2.2.2
Omega          IN      A        10.2.2.3

; SWITCH LAN 3
Serv1          IN      A        10.3.3.1
dns            IN      A        10.3.3.1

Serv3          IN      A        10.3.3.3
www            IN      CNAME    Serv3
mail           IN      MX       20      Serv3

Serv2          IN      A        10.3.3.2
pop            IN      CNAME    Serv2
imap           IN      CNAME    Serv2
mail           IN      MX       10      Serv3

; SWITCH LAN 4
Hermes         IN      A        10.4.4.1
dns2           IN      A        10.4.4.1

Zeus           IN      A        10.4.4.2
Atena          IN      A        10.4.4.3
```

Figura 16- primario/db.cc.pt


```

zone "cc.pt" {
    type master;
    file "/home/core/primario/db.cc.pt";
    allow-transfer {10.4.4.1; };
};

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

```

Figura 17- primario/named.conf.local

```

$TTL      604800
@          IN      SOA      cc.pt. admin.cc.pt. (
                        1          ; 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.      ; 10.3.3.1
2.2.10      IN      PTR      dns2.cc.pt.     ; 10.4.4.1

```

Figura 18- primario/db.3-3-10.rev

```

zone "cc.pt" {
    type slave;
    file "/home/core/secundario/db.cc.pt";
    masters {10.3.3.1; };
};

zone "3.3.10.in-addr.arpa." {
    type slave;
    file "/home/core/secundario/db.3-3-10.rev";
    masters {10.3.3.1; };
};

```

Figura 19-secundario/named.conf.local

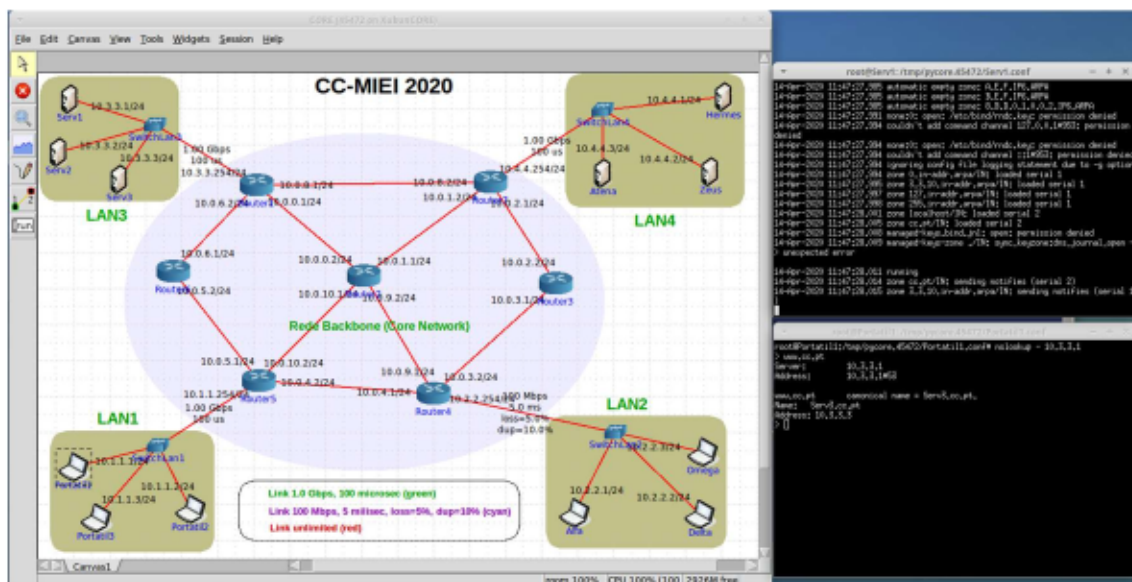


Figura 20-Teste à configuração primária (query ao Serv1)

```
> ^Croot@Portatil1:/tmp/pycore.45472/Portatil1.conf# dig www.cc.pt

: <<> DiG 9.8.1-P1 <<> www.cc.pt
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 42371
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.cc.pt.                IN      A

;; ANSWER SECTION:
www.cc.pt.                6048000 IN      CNAME   Serv3.cc.pt.
Serv3.cc.pt.              6048000 IN      A       10.3.3.3

;; AUTHORITY SECTION:
cc.pt.                    6048000 IN      NS      dns2.cc.pt.
cc.pt.                    6048000 IN      NS      dns.cc.pt.

;; ADDITIONAL SECTION:
dns.cc.pt.                6048000 IN      A       10.3.3.1
dns2.cc.pt.               6048000 IN      A       10.4.4.1

;; Query time: 13 msec
;; SERVER: 10.3.3.1#53(10.3.3.1)
;; WHEN: Tue Apr 14 11:53:18 2020
;; MSG SIZE rcvd: 132
```

Figura 21- Dig de "www.cc.pt"

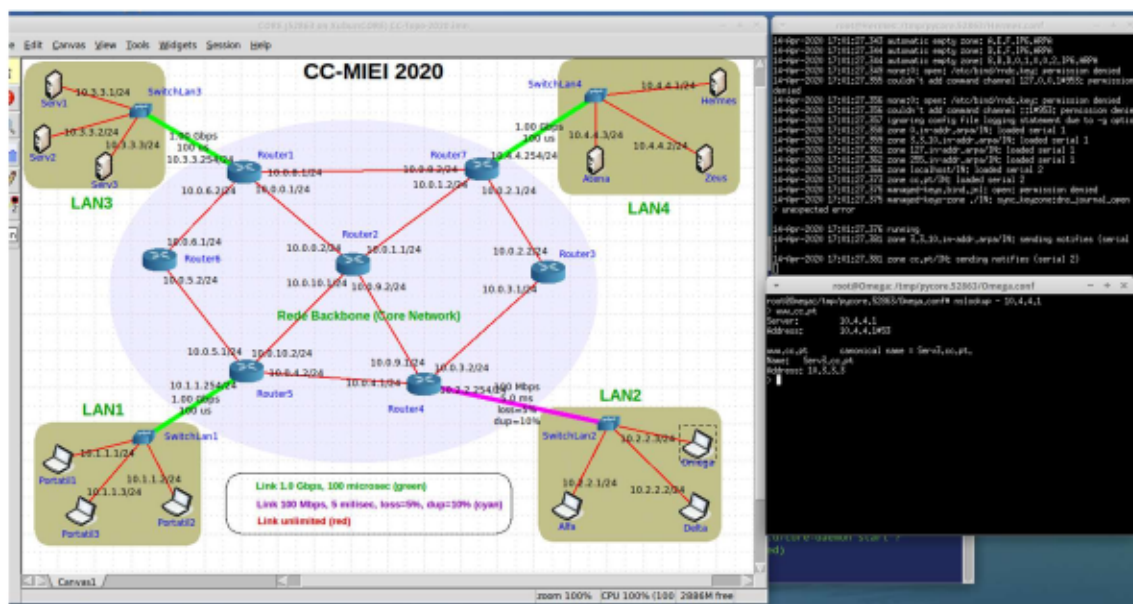


Figura 22- Teste à configuração secundária (query ao Hermes)

Conclusões

O presente trabalho prático serviu de reforço ao que já foi lecionada nas aulas teóricas, e ajudou a consolidar e praticar o conhecimento adquirido sobre o serviço DNS, desde como este funciona a como está organizado para permitir a resolução de nomes.

Na primeira parte do trabalho praticamos diferentes formas de interrogar o DNS e usamos vários comandos diferentes cada um com o seu respetivo objetivo. Estas diferentes formas de interrogar tem origem na necessidade do diferente tipo de informação eu podemos queres obter, que pode ser por exemplo obter endereços IPv6, registos com os name servers do domínio, registos com os servidores de email ou ainda a informação administrativa de uma área.

A segunda parte do trabalho foi a mais desafiadora, sendo que procedemos à instalação e configuração de um domínio. Para isso, primeiramente parámos o servidor DNS pré-instalado e de seguida configuramos o servidor primário e secundário. No final testamos ambos.

Por fim, consideramos que atingimos todos os objetivos propostos.