

Trabalho Prático Nº.3 – Serviço de Resolução de Nomes (DNS) Comunicações por Computador

Grupo:

João Nuno Abreu

Hugo Matias

Data de entrega: April 15, 2020

N: A84802

N: A85370

Problem 1

Consultas ao serviço de nomes DNS

- a) Qual o conteúdo do ficheiro `/etc/resolv.conf` e para que serve essa informação?
- b) Os servidores `www.sapo.pt.` e `www.yahoo.com.` têm endereços IPv6? Se sim, quais?
- c) Quais os servidores de nomes definidos para os domínios: `“uminho.pt.”`, `“pt.”` e `“.”`?
- d) Existe o domínio `nice.software.`? Será que `nice.software.` é um host ou um domínio?
- e) Qual é o servidor DNS primário definido para o domínio `msf.org.`? Este servidor primário (master) aceita queries recursivas? Porquê?
- f) Obtenha uma resposta “autoritativa” para a questão anterior.
- g) Onde são entregues as mensagens de correio eletrónico dirigidas aos presidentes `marcelo@presidencia.pt` e `bolsonaro@casacivil.gov.br`?
- h) Que informação é possível obter, via DNS, acerca 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?
- 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).

Solution:

- a) O ficheiro `resolv.conf` é usado para configurar o resolver do DNS do sistema. É um ficheiro de texto sem formatação normalmente criado pelo administrador da rede ou por aplicações capazes de gerir as tarefas de configuração do sistema.

```

> cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
domain lan
nameserver 192.168.1.254
nameserver 192.168.1.254
~
> |

```

Figure 1: Conteúdo do ficheiro /etc/resolv.conf

b) Sim, têm endereços IPv6. Estes foram obtidos através do commando nslookup com a query AAAA, para informarmos que apenas queremos conexões IPv6. Os endereços obtidos são os seguintes:

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

```

> 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

~
> 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::3
atsv2-fp-shed.wg1.b.yahoo.com has AAAA address 2a00:1288:110:1c::4

Authoritative answers can be found from:

~
> |

```

Figure 2: Endereços IPv6 de sapo.pt e yahoo.com

c) Embora sejam respostas não autoritativas, 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:

```
joaonunoabreu: nslookup
> nslookup
> set q=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 = dns3.uminho.pt.
uminho.pt    nameserver = dns2.uminho.pt.
uminho.pt    nameserver = dns.uminho.pt.

Authoritative answers can be found from:
>
|
```

Figure 3: Dig uminho.pt.

```
joaonunoabreu: nslookup
> nslookup
> set q=NS
> pt.
Server:      192.168.1.254
Address:     192.168.1.254#53

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

Authoritative answers can be found from:
>
|
```

Figure 4: Dig pt.

```
joaonunoabreu: nslookup
> nslookup
> set q=NS
> .
Server:      192.168.1.254
Address:     192.168.1.254#53

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

Authoritative answers can be found from:
>
|
```

Figure 5: Dig root.

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

```
joaonunoabreu: ~
> host nice.software
nice.software has address 213.212.81.71

~
> |
```

Figure 6: Consulta de domínio de nice.software.

- e) DNS primário: ns1.dds.nl. O servidor primário (master) aceita queries recursivas. Nas flags da resposta ao comando 'dig ns1.dds.nl.' está presente "ra" que significa "recursion available".

```

> host -t soa msf.org.
msf.org has SOA record ns1.dds.nl. postmaster.msf.org. 1407464621 16384 2048 1048576 2560
~
> |

```

Figure 7: Consulta do DNS primário.

```

> dig ns1.dds.nl.
<<>> DiG 9.10.6 <<>> ns1.dds.nl.
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 18600
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ns1.dds.nl.                IN      A
;; ANSWER SECTION:
ns1.dds.nl.                82503   IN      A      91.142.253.70
;; AUTHORITY SECTION:
dds.nl.                    184599  IN      NS      ns1.dds.nl.
dds.nl.                    184599  IN      NS      ns2.dds.eu.
dds.nl.                    184599  IN      NS      ns4.dds-city.com.
dds.nl.                    184599  IN      NS      ns3.dds.amsterdam.
;; Query time: 48 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Wed Apr 01 10:39:06 WEST 2020
;; MSG SIZE rcvd: 154
~
> |

```

Figure 8: Verificação da aceitação de queries recursivas.

- f) Consultando um dos nameservers de msf.org seguido do comando "server" para este conseguimos obter a resposta autoritativa.

```

joaonunoabreu: nslookup
> nslookup
> set q=NS
> msf.org.
Server:          192.168.1.254
Address:         192.168.1.254#53

Non-authoritative answer:
msf.org nameserver = ns2.dds.eu.
msf.org nameserver = ns4.dds-city.com.
msf.org nameserver = ns3.dds.amsterdam.
msf.org nameserver = ns1.dds.nl.

Authoritative answers can be found from:
> server ns1.dds.nl.
Default server: ns1.dds.nl.
Address: 91.142.253.70#53
> set q=SOA
> msf.org.
Server:          ns1.dds.nl.
Address:         91.142.253.70#53

msf.org
origin = ns1.dds.nl
mail addr = postmaster.msf.org
serial = 1407464621
refresh = 16384
retry = 2048
expire = 1048576
minimum = 2560
>

```

Figure 9: Resposta autoritativa de msf.org.

- g) Com recurso ao comando nslookup com a query Mail Exchanger(MX) foram obtidas as seguintes respostas:

```

core@XubunCORE:~/Desktop$ 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:
presidencia.pt nameserver = ns1.presidencia.pt.
presidencia.pt nameserver = ns2.presidencia.pt.
presidencia.pt nameserver = ns02.fccn.pt.
mail2.presidencia.pt internet address = 192.162.17.32
mail1.presidencia.pt internet address = 192.162.17.31
ns1.presidencia.pt internet address = 192.162.17.5
ns2.presidencia.pt internet address = 192.162.17.6
>

```

Figure 10: MX de presidencia.pt.

```

core@XubunCORE:~/Desktop$ nslookup
> set query=MX
> casacivil.gov.br
Server:      192.168.1.254
Address:     192.168.1.254#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:
casacivil.gov.br nameserver = alpha2.planalto.gov.br.
casacivil.gov.br nameserver = alpha.planalto.gov.br.
>

```

Figure 11: MX de casacivil.gov.br.

- h) A partir do comando dig é possível obter a informação que se encontra na seguinte figura, nomeadamente o endereço IPV4 associado 23.207.177.41:

```

core@XubunCORE:~/Desktop$ dig whitehouse.gov

;; <<>> DiG 9.8.1-P1 <<>> whitehouse.gov
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 45362
;; 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      23.207.177.41

;; Query time: 62 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Wed Apr 1 12:01:52 2020
;; MSG SIZE rcvd: 48

```

Figure 12: whitehouse.gov.

- i) É possível interrogar o o DNS sobre o endereço IPv6, assim como se pode ver na figura 13. Obte-mos o nome de domínio(www.fccn.pt) e os seus servidores. O contacto responsável encontra-se na figura 14 e tem o endereço de email hostmaster.fccn.pt.

```

core@XubunCORE:~/Desktop$ 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      name = www.fccn.pt.

Authoritative answers can be found from:
6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns02.fccn.pt.
6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns01.fccn.pt.
> █

```

Figure 13: nslookup de endereço IPv6.

```

core@XubunCORE:~/Desktop$ 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      name = www.fccn.pt.

Authoritative answers can be found from:
6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns02.fccn.pt.
6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns01.fccn.pt.
> █

```

Figure 14: nslookup de WWW.fccn.pt.

- j) Transferência de zona é uma query que é usada para replicar a base de dados DNS de um servidor que a recebe. Esta transferência começa pela verificação do preâmbulo que contém um número de série.

Este número de séries determina se a transferência deve ocorrer ou não. A transferência só ocorre se o número de série for superior ao do servidor.

Problem 2

Demonstração

- a) Transferência efetuada
- b) Queries

Solution:

- a) Transferência efetuada

```
root@Serv1: /tmp/pycore.32798/Serv1.conf
15-Apr-2020 12:40:33.251 zone 127.in-addr.arpa/IN: loaded serial 1
15-Apr-2020 12:40:33.252 zone 255.in-addr.arpa/IN: loaded serial 1
15-Apr-2020 12:40:33.254 zone localhost/IN: loaded serial 2
15-Apr-2020 12:40:33.255 zone cc.pt/IN: loaded serial 4
15-Apr-2020 12:40:33.255 managed-keys-zone ./IN: loaded serial 37
15-Apr-2020 12:40:33.256 running
15-Apr-2020 12:40:33.257 zone cc.pt/IN: sending notifies (serial 4)
15-Apr-2020 12:40:33.257 zone 3.3.10.in-addr.arpa/IN: sending notifies (serial 4)
15-Apr-2020 12:40:48.262 client 10.4.4.1#50684: transfer of 'cc.pt/IN': AXFR-style IXFR started
15-Apr-2020 12:40:48.263 client 10.4.4.1#50684: transfer of 'cc.pt/IN': AXFR-style IXFR ended
15-Apr-2020 12:40:48.761 client 10.4.4.1#60344: transfer of '3.3.10.in-addr.arpa/IN': AXFR-style IXFR started
15-Apr-2020 12:40:48.762 client 10.4.4.1#60344: transfer of '3.3.10.in-addr.arpa/IN': AXFR-style IXFR ended
15-Apr-2020 12:40:54.071 managed-keys-zone ./IN: Unable to fetch DNSKEY set '.': SERVFAIL
15-Apr-2020 12:40:54.071 managed-keys.bind.jnl: open: permission denied
15-Apr-2020 12:40:54.071 managed-keys-zone ./IN: keyfetch_done: dns_journal_open -> unexpected error
```

Figure 15: Output do primário

```
root@Hermes: /tmp/pycore.32798/Hermes.conf
15-Apr-2020 12:40:48.262 transfer of 'cc.pt/IN' from 10.3.3.1#53: connected using 10.4.4.1#50684
15-Apr-2020 12:40:48.264 zone cc.pt/IN: transferred serial 4
15-Apr-2020 12:40:48.264 transfer of 'cc.pt/IN' from 10.3.3.1#53: Transfer completed: 1 messages, 24 records, 573 bytes, 0.002 secs (286500 bytes/sec)
15-Apr-2020 12:40:48.264 zone cc.pt/IN: sending notifies (serial 4)
15-Apr-2020 12:40:48.758 client 10.3.3.1#34145: received notify for zone '3.3.10.in-addr.arpa'
15-Apr-2020 12:40:48.760 zone 3.3.10.in-addr.arpa/IN: Transfer started.
15-Apr-2020 12:40:48.760 transfer of '3.3.10.in-addr.arpa/IN' from 10.3.3.1#53: connected using 10.4.4.1#60344
15-Apr-2020 12:40:48.762 zone 3.3.10.in-addr.arpa/IN: transferred serial 4
15-Apr-2020 12:40:48.762 transfer of '3.3.10.in-addr.arpa/IN' from 10.3.3.1#53: Transfer completed: 1 messages, 24 records, 601 bytes, 0.002 secs (300500 bytes/sec)
15-Apr-2020 12:40:48.762 zone 3.3.10.in-addr.arpa/IN: sending notifies (serial 4)
15-Apr-2020 12:40:56.635 managed-keys-zone ./IN: Unable to fetch DNSKEY set '.': SERVFAIL
15-Apr-2020 12:40:56.635 managed-keys.bind.jnl: open: permission denied
15-Apr-2020 12:40:56.635 managed-keys-zone ./IN: keyfetch_done: dns_journal_open -> unexpected error
```

Figure 16: Output do secundário

b) Queries

```

root@Portatil1:/tmp/pycore.32798/Portatil1.conf# nslookup - 10.4.4.1
> Servidor1.cc.pt
Server:      10.4.4.1
Address:     10.4.4.1#53

Name:  Servidor1.cc.pt
Address: 10.3.3.1
> www.cc.pt
Server:      10.4.4.1
Address:     10.4.4.1#53

www.cc.pt      canonical name = Servidor3.cc.pt.
Name:  Servidor3.cc.pt
Address: 10.3.3.3
> $

```

Figure 17: Output do nslookup

```

root@Portatil1:/tmp/pycore.32798/Portatil1.conf
root@Portatil1:/tmp/pycore.32798/Portatil1.conf# !type
bash: !type: event not found
root@Portatil1:/tmp/pycore.32798/Portatil1.conf# nslookup -type=MX mail.cc.pt 10
.4.4.1
Server:      10.4.4.1
Address:     10.4.4.1#53

mail.cc.pt    mail exchanger = 10 Servidor3.cc.pt.
mail.cc.pt    mail exchanger = 20 Servidor2.cc.pt.

root@Portatil1:/tmp/pycore.32798/Portatil1.conf# nslookup - 10.4.4.1

```

Figure 18: Output do nslookup para o mail