

Comunicações por Computador

MIEI - 3º ANO - 2º SEMESTRE
UNIVERSIDADE DO MINHO

TP3 - SERVIÇO DE RESOLUÇÃO DE NOMES (DNS)

Grupo 13:

João Vieira, A76516
João Leal, A75569
Manuel Monteiro, A74036

April 3, 2019

1 Introdução

O DNS (Sistema de Nome de Domínio) é um sistema distribuído de gestão de nomes de domínio para computadores, serviços ou qualquer outro tipo de máquina conectada à Internet ou a uma rede Privada, fazendo a associação de várias informações atribuídas a nomes de domínios a cada uma das entidades participantes.

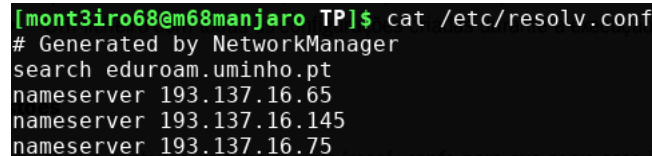
De forma a explorar mais sobre este sistema e sobre os domínios em si e que tipos de registos estes têm em sua posse, ao longo deste relatório usaremos as ferramentas *dig* e *nslookup*.

2 Questões e Respostas

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

Tradicionalmente, à determinação do endereço de IP a partir de um nome de domínio dá-se o nome de **resolver**.

Posto isto, o ficheiro */etc/resolv.conf* tipicamente contém directivas que especificam os domínios de pesquisa pré-definidos, os IP's utilizados para resolver os nomes de domínio.

A terminal window with a black background and green text. The prompt is [mont3iro68@m68manjaro TP]\$ and the command is cat /etc/resolv.conf. The output shows configuration for NetworkManager, a search domain, and three nameservers.

```
[mont3iro68@m68manjaro TP]$ cat /etc/resolv.conf
# Generated by NetworkManager
search eduroam.uminho.pt
nameserver 193.137.16.65
nameserver 193.137.16.145
nameserver 193.137.16.75
```

Figure 1: Exemplo do ficheiro */etc/resolv.conf*

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

Os servidores mencionados na questão possuem endereços IPv6, sendo estes apresentados nos prints que se seguem:

```

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

Non-authoritative answer:
Name:   www.google.pt
Address: 2a00:1450:4003:804::2003

```

Figure 2: Output do comando *nslookup* para *www.google.pt*

```

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

Non-authoritative answer:
Name:   www.google.com
Address: 2a00:1450:4003:802::2004

```

Figure 3: Output do comando *nslookup* para *www.google.com*

Foi usada a flag **-query=AAAA** de forma a mudar o tipo da informação da query, forçando a que esta corresponda aos registos de endereços IPv6 (do tipo AAAA).

- IPv6 (*google.pt*) = 2a00:1450:4003:803::2003
- IPv6 (*google.com*) = 2a00:1450:4003:802::2004

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

Usufruindo do comando *dig*, conseguimos obter os nameservers dos domínios referidos (*ccg.pt.*, *pt.* e *.*), que se encontram na secção “**ANSWER SECTION**”, na coluna mais à direita.

```

→ ~ dig ccg.pt NS +noadditional

; <<>> DiG 9.13.7 <<>> ccg.pt NS +noadditional
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6411
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: bbaba67f569ae08835e37dfd5c98c4bb55e5d122d11a4d69 (good)
;; QUESTION SECTION:
;ccg.pt.                                IN      NS

;; ANSWER SECTION:
ccg.pt.                360      IN      NS      ns3.ccg.pt.
ccg.pt.                360      IN      NS      ns1.ccg.pt.

;; Query time: 11 msec
;; SERVER: 193.137.16.65#53(193.137.16.65)
;; WHEN: seg mar 25 12:08:39 WET 2019
;; MSG SIZE rcvd: 131

```

Figure 4: Output do comando *dig ccg.pt NS +noadditional*

```

→ ~ dig pt. NS +noadditional

; <<>> DiG 9.13.7 <<>> pt. NS +noadditional
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30476
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 10, AUTHORITY: 0, ADDITIONAL: 21

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7fcf6d9f00ac10eead199ba35c98c4d7d157ec81462e3d19 (good)
;; QUESTION SECTION:
;pt.                                IN      NS

;; ANSWER SECTION:
pt.                2674     IN      NS      d.dns.pt.
pt.                2674     IN      NS      ns.dns.br.
pt.                2674     IN      NS      a.dns.pt.
pt.                2674     IN      NS      e.dns.pt.
pt.                2674     IN      NS      c.dns.pt.
pt.                2674     IN      NS      ns2.nic.fr.
pt.                2674     IN      NS      sns-pb.isc.org.
pt.                2674     IN      NS      b.dns.pt.
pt.                2674     IN      NS      g.dns.pt.
pt.                2674     IN      NS      f.dns.pt.

;; Query time: 5 msec
;; SERVER: 193.137.16.65#53(193.137.16.65)
;; WHEN: seg mar 25 12:09:07 WET 2019
;; MSG SIZE rcvd: 690

```

Figure 5: Output do comando *dig pt. NS +noadditional* em pt.

```

→ ~ dig . NS +noadditional

; <<>> DiG 9.13.7 <<>> . NS +noadditional
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 3194
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: ad8497ec2929d9f36df8f4cc5c98c4db6075e2f4686a1cf3 (good)
;; QUESTION SECTION:
;.                               IN      NS

;; ANSWER SECTION:
.                               3600    IN      NS      m.root-servers.net.
.                               3600    IN      NS      b.root-servers.net.
.                               3600    IN      NS      c.root-servers.net.
.                               3600    IN      NS      h.root-servers.net.
.                               3600    IN      NS      f.root-servers.net.
.                               3600    IN      NS      e.root-servers.net.
.                               3600    IN      NS      g.root-servers.net.
.                               3600    IN      NS      k.root-servers.net.
.                               3600    IN      NS      j.root-servers.net.
.                               3600    IN      NS      d.root-servers.net.
.                               3600    IN      NS      l.root-servers.net.
.                               3600    IN      NS      a.root-servers.net.
.                               3600    IN      NS      i.root-servers.net.

;; Query time: 55 msec
;; SERVER: 193.137.16.65#53(193.137.16.65)
;; WHEN: seg mar 25 12:09:11 WET 2019
;; MSG SIZE rcvd: 839

```

Figure 6: Output do comando `dig . NS +noadditional`

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

Através do comando `nslookup` conseguimos ver que existe o domínio *eureka.software*, uma vez que encontramos nameservers definidos para este. Ao mesmo tempo, conseguimos verificar que este é um host, uma vez que tem endereço IP.

```

→ ~ nslookup -querytype=NS eureka.software
Server:          193.137.16.65
Address:         193.137.16.65#53

Non-authoritative answer:
eureka.software nameserver = ns-957.awsdns-55.net.
eureka.software nameserver = ns-312.awsdns-39.com.
eureka.software nameserver = ns-1624.awsdns-11.co.uk.
eureka.software nameserver = ns-1241.awsdns-27.org.

Authoritative answers can be found from:
ns-312.awsdns-39.com    internet address = 205.251.193.56

```

Figure 7: Output do comando `nslookup -querytype=NS` em *eureka.software*

```

→ ~ nslookup -querytype=A eureka.software
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
Name:   eureka.software
Address: 34.214.90.141

```

Figure 8: Output do comando `nslookup -querytype=A` em `eureka.software`

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

Através dos comandos `dig` e `nslookup` conseguimos verificar que o servidor DNS primário é "`ns1.dot2web.com.`".

```

→ ~ dig ami.pt NS +noadditional

; <<>> DiG 9.13.7 <<>> ami.pt NS +noadditional
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54666
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 4096
; COOKIE: 0a689ac81fc79bd81e5c46275ca1ecc4b5d40009d0bd116a (good)
;; QUESTION SECTION:
;ami.pt.                                IN      NS

;; ANSWER SECTION:
ami.pt.      1433    IN      NS      ns2.dot2web.com.
ami.pt.      1433    IN      NS      ns1.dot2web.com.

;; Query time: 5 msec
;; SERVER: 193.137.16.65#53(193.137.16.65)
;; WHEN: seg abr 01 11:49:56 WEST 2019
;; MSG SIZE rcvd: 142

```

Figure 9: Output do comando `dig ami.pt NS +noadditional`

Usando o comando `nslookup` para executar uma query ao servidor primário, verificamos que este não consegue chegar a outros domínios, logo não aceita queries recursivas.

```

→ ~ nslookup
> server ns1.dot2web.com
Default server: ns1.dot2web.com
Address: 80.172.230.28#53
>
> google.pt
;; connection timed out; no servers could be reached
>

```

Figure 10: Output do comando *nslookup*

- 2.6 Obtenha uma resposta “autoritativa” para a questão anterior.

```

→ ~ nslookup -querytype=SOA ami.pt
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
ami.pt
      origin = ns1.dot2web.com
      mail addr = dc.dot2web.pt
      serial = 2019021301
      refresh = 3600
      retry = 7200
      expire = 1209600
      minimum = 86400

Authoritative answers can be found from:
ami.pt nameserver = ns1.dot2web.com.
ami.pt nameserver = ns2.dot2web.com.
ns2.dot2web.com internet address = 5.199.172.41
ns1.dot2web.com internet address = 80.172.230.28

```

Figure 11: Output do comando *nslookup -querytype= SOA ami.pt*

- 2.7 Onde são entregues as mensagens dirigidas a *marcelo@presidencia.pt*?
E a *guterres@onu.org*?

Recorrendo ao comando *nslookup* e, usando a flag *-querytype=MX*, conseguimos saber onde estas mensagens são entregues, apresentadas na secção “*Non-authoritative answer*”.

```

→ ~ nslookup -querytype=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 = ns2.presidencia.pt.
presidencia.pt nameserver = ns02.fccn.pt.
presidencia.pt nameserver = ns1.presidencia.pt.
ns02.fccn.pt   internet address = 193.136.2.228
ns02.fccn.pt   has AAAA address 2001:690:a80:4001::200

```

Figure 12: Output do comando `nslookup -querytype=MX presidencia.pt`

```

→ ~ nslookup -querytype=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 = ns01.semillasl.com.
onu.org nameserver = cp.semillasl.com.
ns01.semillasl.com internet address = 178.33.85.8

```

Figure 13: Output do comando `nslookup -querytype=MX onu.org`

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

Interrogando o domínio *www.whitehouse.gov* de forma a obter um Registo SOA (Start of Authority), conseguimos obter as seguintes informações;

- Servidor DNS primário definido para o domínio (**Origin**);
- Endereço de email da administração do domínio (**Mail addr**);
- O Serial Number da Zona (**Serial**);
- O tempo em segundos após o qual os servidores DNS secundários devem interrogar novamente o primário de forma a verificar mudanças na Zona (**Refresh**);

- O tempo em segundos após o qual os servidores DNS secundários devem interograr o servidor primário de forma a obter o Serial da Zona, se este não tiver respondido ao pedido (**Retry**);
- O tempo em segundos após o qual os servidores DNS secundários devem parar de interogar o servidor DNS primário caso este não responda (**Expire**);
- O TTL (**Minimum**);

```

→ ~ nslookup -querytype=SOA www.whitehouse.gov
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
www.whitehouse.gov      canonical name = wildcard.whitehouse.gov.edgekey.net.
wildcard.whitehouse.gov.edgekey.net canonical name = e4036.dscb.akamaiedge.net.

Authoritative answers can be found from:
dscb.akamaiedge.net
    origin = n0dscb.akamaiedge.net
    mail addr = hostmaster.akamai.com
    serial = 1554116111
    refresh = 1000
    retry = 1000
    expire = 1000
    minimum = 1800

```

Figure 14: Output do comando `nslookup -querytype=SOA www.whitehouse.gov`

```

→ ~ nslookup -querytype=A www.whitehouse.gov
Server:      193.137.16.65
Address:     193.137.16.65#53

Non-authoritative answer:
www.whitehouse.gov      canonical name = wildcard.whitehouse.gov.edgekey.net.
wildcard.whitehouse.gov.edgekey.net canonical name = e4036.dscb.akamaiedge.net.
Name:   e4036.dscb.akamaiedge.net
Address: 2.19.159.149

```

Figure 15: Output do comando `nslookup -querytype=A www.whitehouse.gov`

2.9 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*?

Conseguimos e, através desta interrogação, conseguimos obter os nameservers associados ao domínio, assim como os respetivos endereços IPv4 e IPv6.

```
➔ ~ nslookup 2001:690:a00:1036:1113::247
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:
0.9.6.0.1.0.0.2.ip6.arpa      nameserver = ns02.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 = ns01.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 2001:4ca0:106:0:250:56ff:fea9:3fd
ns02.fccn.pt      has AAAA address 2001:690:a80:4001::200
ns01.fccn.pt      has AAAA address 2001:690:a00:4001::200
```

Figure 16: Output do comando *nslookup* ao endereço IPv6 apresentado

O responsável pelo IPv6 é o domínio fccn.pt.

2.10 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” é um dos mecanismos disponíveis para a replicação de Bases de Dados DNS num conjunto de servidores DNS, sendo baseado numa comunicação Cliente-Servidor, usando TCP para o transporte de informação, onde uma ”Zona” representa uma porção da Base de Dados que será replicada. Quando são feitas alterações à ”Zona” do servidor DNS primário, estas têm de ser partilhadas pelos servidores DNS secundários de forma a estes se manterem atualizados.

Neste mecanismo, o cliente que requisita uma ”Transferência de Zona” é denominado de ”slave” (servidor secundário) e o servidor que aceita esta mesma transferência e possui a informação a ser replicada é denominado de ”master” (servidor primário).

Esta transferência consiste, em primeiro lugar, numa pesquisa ao registo "Start of Authority" (SOA) do DNS namespace que se encontra no topo da "Zona", onde o registo "Serial Number" determinará se a transferência irá ocorrer ou não. Assim sendo, o Cliente compara o "Serial Number" desse registo, com o da última cópia do registo que este tem em sua posse.

Caso o "Serial Number" do registo a ser transferido seja igual, a informação contida na "Zona" é igual à que o "slave" tem em sua posse, podendo este continuar a usá-la. Caso seja maior, a informação que o "slave" tem em sua posse não está atualizada e, portanto, este inicia um pedido de "Transferência de Zona" ao "master", de forma a poder usar informação atualizada.

De forma a manter-se atualizado, os servidores secundários verificam periodicamente se é necessária o uso deste mecanismo. Esta periodicidade é controlada pelos campos "refresh", "retry" e "expire".

O Servidor secundário aguarda o intervalo de tempo "Refresh" antes de verificar com o servidor primário para um novo "Serial Number". Caso esta verificação não possa ser concluída, novas verificações são feitas a cada intervalo de tempo "Retry". Caso seja impossível a realização de uma verificação dentro do intervalo de tempo "Expire", a "Zona" será descartada.

```
→ CC nslookup -query=SOA di.uminho.pt
Server:      193.137.16.65
Address:     193.137.16.65#53

di.uminho.pt
    origin = dns.di.uminho.pt
    mail addr = dnsadmin.di.uminho.pt
    serial = 2019032901
    refresh = 28800
    retry = 7200
    expire = 28800
    minimum = 43200
```

Figure 17:

3 Demonstração do domínio cc.pt

```
root@Cliente1:/tmp/pycore.43289/Cliente1.conf# ping -c1 servidor1.cc.pt
PING servidor1.cc.pt (10.1.1.1) 56(84) bytes of data:
64 bytes from Servidor1 (10.1.1.1): icmp_req=1 ttl=62 time=4.67 ms

--- servidor1.cc.pt ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.678/4.678/4.678/0.000 ms
```

Figure 18: Output de *ping* ao Servidor1

```

root@Cliente1:/tmp/pycore.43289/Cliente1.conf# ping -c1 urano.cc.pt
PING urano.cc.pt (10.2.2.3) 56(84) bytes of data.
64 bytes from Urano (10.2.2.3): icmp_req=1 ttl=61 time=4.73 ms

--- urano.cc.pt ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.736/4.736/4.736/0.000 ms
root@Cliente1:/tmp/pycore.43289/Cliente1.conf# █

```

Figure 19: Output de *ping* ao Urano (secundário)

```

root@Cliente1:/tmp/pycore.43289/Cliente1.conf# nslookup www.cc.pt
Server:      10.1.1.1
Address:     10.1.1.1#53

Name:   www.cc.pt
Address: 10.1.1.3

root@Cliente1:/tmp/pycore.43289/Cliente1.conf# █

```

Figure 20: Output de *nslookup* a *www.cc.pt*

```

root@Cliente1:/tmp/pycore.43289/Cliente1.conf# nslookup www.cc.pt 10.2.2.3
Server:      10.2.2.3
Address:     10.2.2.3#53

Name:   www.cc.pt
Address: 10.1.1.3

```

Figure 21: Output de *nslookup* a *www.cc.pt* através do Urano

4 Conclusão

Com este Trabalho, ficamos a saber que o DNS apresenta uma hierarquia cliente-servidor, podendo a resposta de uma consulta envolver vários servidores DNS. Tivemos também a oportunidade de observar que tipos de registos a Base de Dados DNS armazena, como por exemplo Start of Authority (**SOA**), IP Adresses (**A** e **AAAA**), Name Servers (**NS**) e Mail Exchanger (**MX**), assim como a informação que cada um destes nos oferece. Além disso, conseguimos observar a hierarquia deste sistema, tendo um servidor DNS primário ("master") e servidores DNS secundários ("slaves"), que funcionam como uma cópia de segurança do primeiro.

Concluimos portanto que o DNS (Sistema de Nome de Domínio) funciona como um livro de "Páginas Amarelas" para a Internet, traduzindo nomes de

domínio fáceis de entender pelos utilizadores (user-friendly) em endereços IP, servindo como um componente essencial à Internet.