



Universidade do Minho
Escola de Engenharia

Comunicações e Redes

TP7: DNS



João Miguel da Silva Alves (83624)

Paulo Jorge Alves (84480)

MESTRADO INTEGRADO EM ENGENHARIA BIOMÉDICA
INFORMÁTICA MÉDICA 2020/2021

Com a utilização dos protocolos TCP/IP, os computadores passaram a identificar-se uns aos outros através de endereços numéricos. Porém, é difícil memorizar diversos endereços numéricos correspondentes a diferentes computadores.

Foi então necessário estabelecer um sistema de mapeamento entre os nomes dos computadores e os respetivos endereços numéricos, o DNS – Domain Name System. É este sistema que traduz nomes de computadores no respetivo endereço numérico IP (sejam eles IPV4 ou IPV6), sendo uma das principais ferramentas para o funcionamento da Internet.

Esta ferramenta, memoriza um conjunto de dados implementado e gerido de forma hierárquica e distribuída, de modo a aumentar a probabilidade de se obter resposta.

Existem três classes de servidores, os servidores de nomes raiz, os servidores de domínio de alto nível – TDL, e os servidores com autoridade.

Relativamente aos primeiros, são 13 e encontram-se espalhados pelo Mundo. Cada um é um aglomerado de servidores replicados por razões de segurança e confiabilidade. Estes servidores são cruciais, pois constituem o primeiro passo para a tradução de nomes em IPs.

Os TDL encontram-se no segundo nível hierárquico e são responsáveis por domínios de alto nível como por exemplo: .pt, .com, .org, entre outros.

Por fim, os servidores com autoridade abrigam os registos DNS que são acessíveis ao público e mapeiam os nomes dos hosts em endereços IP.

Além de poderem deixar a navegação mais rápida, muitos servidores DNS oferecem deteção de sites falsos ou infetados e até oferecem um sistema de proteção parental para bloquear sites de conteúdo adulto, por exemplo. ^{[1][3]}

De seguida, responder-se-ão às questões propostas no enunciado.

Usar “Nslookup” ou “dig” para explorar os fundamentos do DNS.

Ao longo do trabalho foi utilizado o comando *nslookup*.

Este comando é utilizado para questionar servidores de nomes de domínios Internet (Internet domain name servers). O nome ou endereço Internet é fornecido como primeiro parâmetro. O segundo parâmetro é opcional e corresponde ao nome ou endereço de um servidor de nomes de domínios (name server).^[2]

1. Identifique os nomes dos servidores e endereços IP para os seguintes domínios:

“di.uminho.pt.” / “uminho.pt.” / “google.com.”

```
paulojorge@PAULOJ-PC:/mnt/c/Users/paulo$ nslookup di.uminho.pt.  
Server:      172.22.144.1  
Address:     172.22.144.1#53  
  
Non-authoritative answer:  
Name:   di.uminho.pt  
Address: 193.136.19.38
```

Figura 1 - nslookup: di.uminho.pt

```
paulojorge@PAULOJ-PC:/mnt/c/Users/paulo$ nslookup uminho.pt.  
Server:      172.22.144.1  
Address:     172.22.144.1#53  
  
Non-authoritative answer:  
*** Can't find uminho.pt: No answer
```

Figura 2 - nslookup: uminho.pt

```
paulojorge@PAULOJ-PC:/mnt/c/Users/paulo$ nslookup google.com.  
Server:      172.22.144.1  
Address:     172.22.144.1#53  
  
Non-authoritative answer:  
Name:   google.com  
Address: 172.217.17.14  
Name:   google.com  
Address: 2a00:1450:4003:800::200e
```

Figura 3 - nslookup: google.com

Os nomes dos servidores e os respetivos endereços IP encontram-se nas fotos acima.

Pela análise dos resultados do output é possível verificar apenas a existência de respostas não autoritativas nos servidores di.uminho.pt. e google.com., ou seja, não existem respostas autoritativas.

Uma resposta “autoritativa” é obtida quando questionamos um servidor de nomes “autoritativo”, ou seja, quando o servidor responsável por aquele registo de domínio é que devolve a resposta. Uma resposta não “autoritativa” é obtida quando obtemos resposta para o registo pretendido vindo de um servidor que não é responsável por aquele domínio.

Relativamente ao servidor uminho.pt não foram encontrados resultados pois este é o nome do domínio e como tal não possui endereço.

A existência de respostas não autoritativas pressupõe que foi realizada uma consulta externa aos servidores do domínio especificado, o que significa que o servidor DNS utilizado não responde através deste domínio. No entanto, um servidor não autoritativo detém a informação necessária para responder aos comandos executados pois terá inquirido um servidor autoritativo anteriormente e guardado a sua resposta em Cache.

2. Tente obter uma resposta confiável para os endereços IP (v4) de:

SOA para "sapo.pt." / "yahoo.com." / "publico.pt."

Registo MX para "di.uminho.pt." / "up.pt."

Numa primeira parte deste exercício pretendeu-se obter as respostas autoritativas de um servidor SOA (Start Of Authority Record) para os vários servidores apresentados no enunciado. Para tal, no *nslookup*, foi utilizado o seguinte comando: *set querytype=soa*.

```
paulojorge@PAULOJ-PC:/mnt/c/Users/paulo$ nslookup
> set querytype=soa
> sapo.pt.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
sapo.pt
  origin = ns.sapo.pt
  mail addr = root.sapo.pt
  serial = 1608290558
  refresh = 3600
  retry = 7200
  expire = 360000
  minimum = 300

Authoritative answers can be found from:
>
> set querytype=soa
> yahoo.com.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
yahoo.com
  origin = ns1.yahoo.com
  mail addr = hostmaster.yahoo-inc.com
  serial = 2020121900
  refresh = 3600
  retry = 300
  expire = 1814400
  minimum = 600

Authoritative answers can be found from:
>
> set querytype=soa
> publico.pt.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
publico.pt
  origin = dns.publico.pt
  mail addr = it.publico.pt
  serial = 2020120301
  refresh = 1800
  retry = 600
  expire = 604800
  minimum = 900

Authoritative answers can be found from:
>
```

Figura 4 - SOA para "sapo.pt." / "yahoo.com." / "publico.pt."

Ao utilizar a ferramenta *nslookup*, por defeito estamos a questionar o servidor *dns default*. Dessa forma, quando se questiona ao *dns default* pelos domínios *sapo.pt*, *yahoo.com* ou *publico.pt*, as respostas que obtém são não autoritativas, uma vez que ele não é o responsável por aquele domínio.

No entanto é fornecida a indicação dos servidores onde este tipo de resposta pode ser encontrado.

Repetindo o procedimento anterior utilizando os servidores descritos anteriormente (enunciados nas respostas não “autoritativas”), é possível obter uma resposta autoritativa, como se pode observar pelo exemplo representado na figura 5 (verifica-se a não existência de respostas não autoritativas).

```
paulojorge@PAULOJ-PC:/mnt/c/Users/paulo$ nslookup
>
> set querytype=soa
> ns.sapo.pt.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
*** Can't find ns.sapo.pt.: No answer

Authoritative answers can be found from:
sapo.pt
    origin = ns.sapo.pt
    mail addr = root.sapo.pt
    serial = 1608290558
    refresh = 3600
    retry = 7200
    expire = 3600000
    minimum = 300
>
> set querytype=soa
> ns1.yahoo.com
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
*** Can't find ns1.yahoo.com: No answer

Authoritative answers can be found from:
yahoo.com
    origin = ns1.yahoo.com
    mail addr = hostmaster.yahoo-inc.com
    serial = 2020121900
    refresh = 3600
    retry = 300
    expire = 1814400
    minimum = 600
>
> set querytype=soa
> dns.publico.pt
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
*** Can't find dns.publico.pt: No answer

Authoritative answers can be found from:
publico.pt
    origin = dns.publico.pt
    mail addr = it.publico.pt
    serial = 2020120301
    refresh = 1800
    retry = 600
    expire = 604800
    minimum = 900
>
```

Figura 5 - SOA para “ns.sapo.pt.” / “ns1.yahoo.com.” / “dns.publico.pt.”

Na segunda parte deste exercício, pretendeu-se uma vez mais obter respostas autoritativas, desta vez a partir de um registo MX (Mail Exchange Record) o que implica que a única alteração no procedimento anterior seja apenas a substituição do tipo por: *type=mx*.

Os resultados do output destes comandos estão representados na figura 6. É possível verificar que à semelhança do caso anterior, inicialmente, também não foram obtidas respostas "autoritativas".

Depois, na figura 7, repetindo o procedimento anterior, utilizando os servidores enunciados nas respostas não “autoritativas”, é possível obter uma resposta autoritativa.

```
paulojorge@PAULOJ-PC:/mnt/c/Users/paulo$ nslookup
>
> set querytype=mx
> di.uminho.pt.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
di.uminho.pt mail exchanger = 10 mx2.uminho.pt.
di.uminho.pt mail exchanger = 0 mx.uminho.pt.

Authoritative answers can be found from:
>
> set querytype=mx
> up.pt.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
up.pt mail exchanger = 10 mx04.up.pt.
up.pt mail exchanger = 10 mx03.up.pt.
up.pt mail exchanger = 10 mx06.up.pt.
up.pt mail exchanger = 10 mx05.up.pt.
up.pt mail exchanger = 10 mx02.up.pt.
up.pt mail exchanger = 10 mx01.up.pt.

Authoritative answers can be found from:
>
```

Figura 6 - MX para "di.uminho.pt." / "up.pt."

```
paulojorge@PAULOJ-PC:/mnt/c/Users/paulo$ nslookup
>
> set querytype=mx
> mx2.uminho.pt.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
*** Can't find mx2.uminho.pt.: No answer

Authoritative answers can be found from:
uminho.pt
    origin = dns.uminho.pt
    mail addr = servicos.scom.uminho.pt
    serial = 2020121712
    refresh = 14400
    retry = 7200
    expire = 1209600
    minimum = 300
>
> set querytype=mx
> mx04.up.pt.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
*** Can't find mx04.up.pt.: No answer

Authoritative answers can be found from:
up.pt
    origin = ns1.up.pt
    mail addr = it.up.pt
    serial = 1608288214
    refresh = 28800
    retry = 7200
    expire = 72000
    minimum = 86400
>
```

Figura 7 - MX para "mx2.uminho.pt." / "mx04.up.pt."

3. Tente obter os endereços IPv6 de:

SOA para "sapo.pt." / "yahoo.com." / "publico.pt."

Registo MX para "di.uminho.pt." / "up.pt."

No que diz respeito à primeira parte do exercício, a qual é necessário usar os comandos "set querytype = soa e set q =AAAA" para encontrar os endereços IPv6. No entanto, não foi possível encontrar os endereços IPv6 para os domínios "sapo.pt" e "publico.pt". No caso do domínio "yahoo.com" foi possível encontrar endereços IPv6, os quais correspondem aos primeiros seis a contar de cima, em que os valores desses endereços encontram-se separados por ":". [5]

```

joao_alves@LAPTOP-COE5NP4J:~$ nslookup
> set querytype=soa
*** Invalid option: querytype=soa
> set querytype=soa
> set q=AAAA
> sapo.pt
Server:          172.17.25.81
Address:         172.17.25.81#53

Non-authoritative answer:
*** Can't find sapo.pt: No answer
> set querytype=soa
> set q=AAAA
> yahoo.com
Server:          172.17.25.81
Address:         172.17.25.81#53

Non-authoritative answer:
Name:   yahoo.com
Address: 2001:4998:124:1507::f001
Name:   yahoo.com
Address: 2001:4998:24:120d::1:1
Name:   yahoo.com
Address: 2001:4998:44:3507::8000
Name:   yahoo.com
Address: 2001:4998:124:1507::f000
Name:   yahoo.com
Address: 2001:4998:24:120d::1:0
Name:   yahoo.com
Address: 2001:4998:44:3507::8001
Name:   ns3.yahoo.com
Address: 2406:2000:f03f:1f8::1003
Name:   ns2.yahoo.com
Address: 2001:4998:140::1002
Name:   ns5.yahoo.com
Address: 2406:2000:ff60::53
Name:   ns1.yahoo.com
Address: 2001:4998:130::1001
Name:   ns3.yahoo.com
Address: 27.123.42.42
Name:   ns2.yahoo.com
Address: 68.142.255.16
Name:   ns5.yahoo.com
Address: 202.165.97.53
Name:   ns1.yahoo.com
Address: 68.180.131.16
Name:   ns4.yahoo.com
Address: 98.138.11.157

```

Figura 8 - SOA para "sapo.pt" / "Yahoo.com"

```

joao_alves@LAPTOP-COE5NP4J:~$ nslookup
> set querytype=soa
> set q=AAAA
> publico.pt
Server:          172.17.25.81
Address:         172.17.25.81#53

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

```

Figura 9 - SOA para "publico.pt"

Na parte dois da alínea três era necessário descobrir os endereços IPv6 para os record MX dos domínios "di.uminho.pt" e "up.pt". No entanto, nenhum resultado foi obtido, evidenciando que para nestes domínios para este tipo de record apenas existem endereços IPv4.

```

joao_alves@LAPTOP-COE5NP4J:~$ nslookup
> set querytype=mx
> set q=AAAA
> di.uminho.pt
Server:          172.17.25.81
Address:         172.17.25.81#53

Non-authoritative answer:
*** Can't find di.uminho.pt: No answer
>
>
> set querytype=mx
> set q=AAAA
> up.pt
Server:          172.17.25.81
Address:         172.17.25.81#53

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

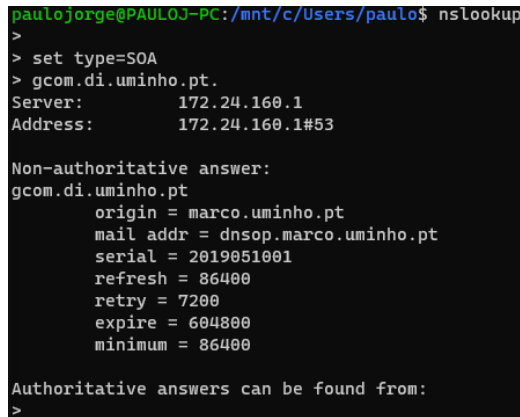
```

Figura 10 - MX para "di.uminho.pt." / "up.pt."

4. Identifique os parâmetros temporais para o domínio “gcom.di.uminho.pt.”

De forma a obter a identificação dos parâmetros temporais para os servidores fornecidos, foi novamente utilizado o comando nslookup e de forma especificar a query a utilizar foi executado o seguinte comando: *Set type=soa*.

Os resultados obtidos encontram-se representados na figura seguinte.



```
paulojorge@PAULOJ-PC:/mnt/c/Users/paulo$ nslookup
>
> set type=SOA
> gcom.di.uminho.pt.
Server:      172.24.160.1
Address:     172.24.160.1#53

Non-authoritative answer:
gcom.di.uminho.pt
    origin = marco.uminho.pt
    mail addr = dnsop.marco.uminho.pt
    serial = 2019051001
    refresh = 86400
    retry = 7200
    expire = 604800
    minimum = 86400

Authoritative answers can be found from:
>
```

Figura 11 – SOA para “gcom.di.uminho.pt.”

Através da figura anterior, é possível verificar os valores obtidos para os parâmetros temporais que correspondem aos valores apresentados em refresh, retry, expire e minimum.

O valor serial = 2019051001 corresponde ao número de série, que por norma diz respeito à data da última modificação.

- Refresh = 86400 seg, que corresponde à frequência com que os servidores secundários devem questionar o servidor primário quanto à ocorrência de atualizações para que estes possam efetuar as mesmas.
- Retry = 7200 seg, que indica o tempo de espera de um servidor secundário para que este questione o servidor primário quanto a alterações no número de série.
- Expire = 604800, que permite obter o tempo de utilização dos dados atualmente disponíveis pelos servidores secundários.
- Minimum = 86400, que diz respeito ao tempo em que um recurso é considerado válido.

5. Usando o WHOIS RIPE DB (<http://whois.domaintools.com/>), identifique completamente (incluindo nome de domínio, endereço de e-mail, endereço de superfície, número de telefone) um invasor hipotético combatendo de:

193.136.19.190, 193.136.60.146, 193.137.33.45

De forma a obter informações administrativas de supostos atacantes recorreremos às funcionalidades disponíveis pelo DomainTools, que é uma plataforma de investigação que combina o domínio de nível empresarial e inteligência baseada em DNS com uma interface web intuitiva.^[4]

193.136.19.190

IP Information for 193.136.19.190	
— Quick Stats	
IP Location	 Portugal Braga Fundacao Para A Ciencia E A Tecnologia I.p.
ASN	 AS1930 RCCN Fundacao para a Ciencia e a Tecnologia, I.P., PT (registered Sep 01, 1993)
Resolve Host	ce.grid.prociiv.pt
Whois Server	whois.ripe.net
IP Address	193.136.19.190
organisation:	ORG-UDM20-RIPE
org-name:	Universidade do Minho
org-type:	OTHER
address:	Campus de Gualtar
address:	4710-057 Braga
address:	PORTUGAL
phone:	+351 253604020
fax-no:	+351 253604021
e-mail:	servicedesk@scm.uminho.pt
admin-c:	RCUD2-RIPE
tech-c:	RCUD2-RIPE
mnt-by:	AS1930-MNT
mnt-ref:	AS1930-MNT
abuse-c:	CUDM3-RIPE
created:	2014-01-20T18:29:59Z
last-modified:	2017-10-30T14:46:28Z
source:	RIPE

Figura 12 – IP: “193.136.19.190”

- **Nome de Domínio:** “ce.grid.prociiv.pt.”
- **Endereço de e-mail:** servicedesk@scm.uminho.pt
- **Endereço de superfície:** Universidade do Minho, Campus de Gualtar, 4710-057, Braga, Portugal
- **Telefone:** +351 253604020

193.136.60.146

IP Information for 193.136.60.146	
— Quick Stats	
IP Location	 Portugal Porto Fundacao Para A Ciencia E A Tecnologia I.p.
ASN	 AS1930 RCCN Fundacao para a Ciencia e a Tecnologia, I.P., PT (registered Sep 01, 1993)
Resolve Host	jaguar.dem.isep.ipp.pt
Whois Server	whois.ripe.net
IP Address	193.136.60.146
organisation:	ORG-IPDP1-RIPE
org-name:	Instituto Politecnico do Porto
org-type:	OTHER
address:	Rua Dr. Roberto Frias, 712
address:	4200-465 Porto
address:	PORTUGAL
phone:	+351 225571000
e-mail:	noc@sc.ipp.pt
admin-c:	RCIP12-RIPE
tech-c:	RCIP12-RIPE
mnt-by:	AS1930-MNT
mnt-ref:	AS1930-MNT
abuse-c:	FST8-RIPE
created:	2014-02-07T16:34:05Z
last-modified:	2017-10-30T14:50:12Z
source:	RIPE

Figura 13 – IP: “193.136.60.146”

- **Nome de Domínio:** “jaguar.dem.isep.ipp.pt”
- **Endereço de e-mail:** noc@sc.ipp.pt
- **Endereço de superfície:** Instituto Politécnico do Porto, Rua Dr. Roberto Frias, 4200-465, Porto, Portugal
- **Telefone:** +351 225571000

193.137.33.45

IP Information for 193.137.33.45

— Quick Stats

IP Location	Portugal Pedroucos Fundacao Para A Ciencia E A Tecnologia I.p.
ASN	AS1930 RCCN Fundacao para a Ciencia e a Tecnologia, I.P., PT (registered Sep 01, 1993)
Whois Server	whois.ripe.net
IP Address	193.137.33.45

organisation:	ORG-UDP5-RIPE
org-name:	Universidade do Porto
org-type:	OTHER
address:	Universidade do Porto - Reitoria
address:	Praca Gomes Teixeira
address:	4099-002 Porto
address:	PORTUGAL
phone:	+351 220408000
fax-no:	+351 220408186
e-mail:	noc@up.pt
admin-c:	RCUD3-RIPE
tech-c:	RCUD3-RIPE
mnt-by:	AS1930-MNT
mnt-ref:	AS1930-MNT
abuse-c:	CUUP1-RIPE
created:	2014-01-20T18:29:59Z
last-modified:	2017-10-30T14:39:11Z
source:	RIPE

Figura 14 – IP: “193.137.33.45”

- **Nome de Domínio:** “whois.ripe.net”
- **Endereço de e-mail:** noc@up.pt
- **Endereço de superfície:** Universidade do Porto - Reitoria, Praça Gomes Teixeira, 4099-002, Porto, Portugal
- **Telefone:** +351 220408000

Bibliografia:

- [1] <https://canaltech.com.br/internet/o-que-e-dns/>
- [2] <https://paginas.fe.up.pt/~mgi97018/nslookup.html>
- [3] <https://paginas.fe.up.pt/~mgi97018/dns.html>
- [4] <https://whois.domaintools.com/>
- [5] <https://docs.oracle.com/cd/E19253-01/816-4554/ipv6-config-tasks-116/index.html>