Comunicações e Redes

“Queries DNS”

Grupo 1

07/11/2011

1. Use the command "dig @193.136.9.240 www.google.pt A" and try to identify all the servers IP addresses

```
; <<>> DiG 9.6.0-APPLE-P2 <<>> @193.236.9.240 www.google.pt A
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

- Usando o comando “dig @193.136.9.240 www.google.pt A” a conecção fez time out pois nesse momento não se teve acesso ao servidor DNS do marco.uminho.pt (cujo IP é 193.136.9.240), devido à falta de conectividade da máquina utilizada.
- Seguidamente usou-se o comando *“dig”* mas sem o servidor DNS onde interrogar i.e: “dig www.google.pt A” o resultado foi o seguinte:

```
; <<>> DiG 9.7.3 <<>> www.google.pt A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64528
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 4, ADDITIONAL: 4

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

;; ANSWER SECTION:
www.google.pt.          230049  IN      CNAME   www.google.com.
www.google.com.         56689   IN      CNAME   www.l.google.com.
www.l.google.com.       183     IN      A       209.85.227.147
www.l.google.com.       183     IN      A       209.85.227.99
www.l.google.com.       183     IN      A       209.85.227.103
www.l.google.com.       183     IN      A       209.85.227.104
www.l.google.com.       183     IN      A       209.85.227.105
www.l.google.com.       183     IN      A       209.85.227.106

;; AUTHORITY SECTION:
google.com.             69635   IN      NS      ns2.google.com.
google.com.             69635   IN      NS      ns3.google.com.
google.com.             69635   IN      NS      ns4.google.com.
google.com.             69635   IN      NS      ns1.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         229361  IN      A       216.239.32.10
ns2.google.com.         229361  IN      A       216.239.34.10
ns3.google.com.         229361  IN      A       216.239.36.10
ns4.google.com.         229361  IN      A       216.239.38.10

;; Query time: 11 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Nov  7 17:15:26 2011
;; MSG SIZE  rcvd: 311
```

- Como se pode verificar pela informação obtida a secção não autoritativa concedeu 8 respostas, das quais 2 são do tipo CNAM (nome canónico) e 6 do tipo A (IP). Na secção autoritativa obteve-se 4 respostas do tipo NS (name server) indicando o servidor DNS que pode responder a essa questão, sendo ainda dada a informação adicional sobre o IP desses mesmo servidores DNS.
- Com esta informação podemos identificar todos os endereços de IP associados a www.google.pt (apresentados a laranja). No entanto não se pode ter certeza absoluta sobre os IP dos servidores porque esta resposta está em cache nestes servidores não-

autoritativos. Não foi possível ligar aos servidores autoritativos na realização deste exercício.

2. Using the command "nslookup" and try to get similar results for a query on the IP address (query=A) of "www.google.pt"

```
Server:         192.168.2.1
Address:    192.168.2.1#

Non-authoritative answer:
www.google.pt    canonical name = www.google.com.
www.google.com   canonical name = www.l.google.com.
Name:   www.l.google.com
Address: 209.85.227.105
Name:   www.l.google.com
Address: 209.85.227.104
Name:   www.l.google.com
Address: 209.85.227.103
Name:   www.l.google.com
Address: 209.85.227.99
Name:   www.l.google.com
Address: 209.85.227.147
Name:   www.l.google.com
Address: 209.85.227.106
```

- Ao utilizar-se o comando *nslookup* foi possivel identificar a localização do servidor e também da porta (#53) que disponibiliza o serviço, além disso tal como tinha acontecido com o comando "*dig"* é-nos também fornecida a informação referente as respostas não autoritativas onde é possível verificar as duas do tipo CNAM, onde podemos observar que o verdadeiro nome de "www.google.pt" é "www.google.com" e que o verdadeiro nome de "www.google.com" é "www.l.google.com.", sendo as restantes respostas referentes à localização dos servidores em cache de "www.l.google.com" que podem responder a esta questão. Como se pode verificar as respostas são iguais às do exercício anterior (faltando apenas as localizações dos servidores de DNS autoritativos).

3. Using both of the above commands determine which are the Name Servers and IP addresses for "di.uminho.pt.", "uminho.pt.", "google.com."

di.uminho.pt.:

nslookup di.uminho.pt.

```
Server:         192.168.2.1
Address:    192.168.2.1#53

Non-authoritative answer:
Name:       di.uminho.pt
Address: 193.136.19.20
```

dig di.uminho.pt A

```
; <<>> DiG 9.7.3-P3 <<>> di.uminho.pt. A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60058
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;di.uminho.pt.                  IN      A
```

```
;; ANSWER SECTION:
di.uminho.pt.           9305    IN      A       193.136.19.20

;; Query time: 4 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Nov  7 17:21:29 2011
;; MSG SIZE  rcvd: 46
```

- Fazendo o *nslookup* e o "*dig"* de "di.uminho.pt" verifica-se que o verdadeiro nome do servidor é de facto "di.uminho.pt" e o seu endereço de IP é 193.136.19.20.

dig uminho.pt. A

```
; <<>> DiG 9.7.3-P3 <<>> uminho.pt. A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26748
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;uminho.pt.                     IN      A

;; AUTHORITY SECTION:
uminho.pt.              282     IN      SOA     dns.uminho.pt. servicos.scom.uminho.pt.
2011100300 21600 7200 604800 14400

;; Query time: 13 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Nov  7 17:21:51 2011
;; MSG SIZE  rcvd: 81
```

nslookup uminho.pt.

```
Server:         192.168.2.1
Address:        192.168.2.1#53

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

- Como podemos observar pelo obtido acima, através do comando "*dig"*, não se obteve nenhuma resposta não autoritativa, o que foi comprovado em seguida pelo *nslookup*. Contudo é-nos fornecida a informação do melhor local (dns.uminho.pt.servicos.scom.uminho.pt.) onde podemos obter a resposta à nossa questão através da resposta autoritativa obtida no comando *dig*.
  Tendo em conta que não foi possível obter uma resposta é possível afirmar que a entidade não existe em cache.

dig google.pt

```
 ; <<>> DiG 9.6.0-APPLE-P2 <<>> google.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14980
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
```

```
;google.pt.                    IN      A

;; ANSWER SECTION:
google.pt.          284     IN      A       209.85.227.104
google.pt.          284     IN      A       209.85.227.103
google.pt.          284     IN      A       209.85.227.99
google.pt.          284     IN      A       209.85.227.147
google.pt.          284     IN      A       209.85.227.106
google.pt.          284     IN      A       209.85.227.105

;; Query time: 11 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Nov  7 18:42:25 2011
;; MSG SIZE  rcvd: 123
```

nslookup google.pt

```
Server:             192.168.2.1
Address:    192.168.2.1#53

Non-authoritative answer:
Name:       google.pt
Address: 209.85.227.99
Name:       google.pt
Address: 209.85.227.103
Name:       google.pt
Address: 209.85.227.104
Name:       google.pt
Address: 209.85.227.105
Name:       google.pt
Address: 209.85.227.106
Name:       google.pt
Address: 209.85.227.147
```

- Apresentados os dados obtidos pelos comandos *dig* e *nslookup* para google.pt podemos afirmar que o nome do servidor é google.pt e que tem 6 endereços de IP associados.

4. Now try to get Authoritative Answers for the IP address of:

4.a) SOA server for sapo.pt., yahoo.com., publico.pt.

```
$ nslookup
> set query=soa
> sapo.pt.
Server:             192.168.2.1
Address:    192.168.2.1#53

Non-authoritative answer:
sapo.pt
        origin = ns.sapo.pt
        mail addr = root.sapo.pt
        serial = 1320686536
        refresh = 3600
        retry = 7200
        expire = 360000
        minimum = 18000
```

```
Authoritative answers can be found from:
pt      nameserver = sns-pb.isc.org.
pt      nameserver = auth200.ns.uu.net.
pt      nameserver = auth210.ns.uu.net.
pt      nameserver = ns.dns.br.
pt      nameserver = ns.dns.pt.
pt      nameserver = ns2.dns.pt.
pt      nameserver = ns2.nic.fr.
pt      nameserver = ns-pt.nlnetlabs.nl.
ns.dns.br       internet address = 200.160.0.5
ns.dns.pt       internet address = 193.136.0.1
ns.dns.pt       has AAAA address 2001:690:a00:1016:905::1
ns2.dns.pt      internet address = 193.136.2.226
ns2.dns.pt      has AAAA address 2001:690:a80:4001::100
ns2.nic.fr      internet address = 192.93.0.4
ns2.nic.fr      has AAAA address 2001:660:3005:1::1:2
ns-pt.nlnetlabs.nl      internet address = 213.154.224.141
ns-pt.nlnetlabs.nl      has AAAA address 2001:7b8:206:1::4:141
sns-pb.isc.org internet address = 192.5.4.1
sns-pb.isc.org has AAAA address 2001:500:2e::1
```

- O servidor SOA do sapo.pt. é ns.sapo.pt (resposta não autoritativa)

```
$ nslookup
> set query=soa
> yahoo.com
Server:         192.168.2.1
Address:        192.168.2.1#53

Non-authoritative answer:
yahoo.com
        origin = ns1.yahoo.com
        mail addr = hostmaster.yahoo-inc.com
        serial = 2011110701
        refresh = 3600
        retry = 300
        expire = 1814400
        minimum = 600

Authoritative answers can be found from:
yahoo.com       nameserver = ns2.yahoo.com.
yahoo.com       nameserver = ns3.yahoo.com.
yahoo.com       nameserver = ns4.yahoo.com.
yahoo.com       nameserver = ns5.yahoo.com.
yahoo.com       nameserver = ns6.yahoo.com.
yahoo.com       nameserver = ns8.yahoo.com.
yahoo.com       nameserver = ns1.yahoo.com.
ns1.yahoo.com           internet address = 68.180.131.16
ns2.yahoo.com           internet address = 68.142.255.16
ns3.yahoo.com           internet address = 121.101.152.99
ns4.yahoo.com           internet address = 68.142.196.63
ns5.yahoo.com           internet address = 119.160.247.124
ns6.yahoo.com           internet address = 202.43.223.170
ns8.yahoo.com           internet address = 202.165.104.22
```

- O servidor SOA do yahoo.com. é ns1.yahoo.com (resposta não autoritativa)

```
$ nslookup
> set query=soa
> publico.pt.
Server:         192.168.2.1
Address:        192.168.2.1#53

Non-authoritative answer:
publico.pt
        origin = ns1.novis.pt
        mail addr = dns-admin.isp.novis.pt
        serial = 2011100701
        refresh = 1800
        retry = 600
        expire = 604800
        minimum = 900

Authoritative answers can be found from:
publico.pt      nameserver = ns1.novis.pt.
publico.pt      nameserver = ns2.novis.pt.
ns1.novis.pt    internet address = 194.79.69.129
ns1.novis.pt    has AAAA address 2001:1588:4001:8::1
ns2.novis.pt    internet address = 194.79.69.131
ns2.novis.pt    has AAAA address 2001:1588:4001:9::1
```

- O servidor SOA do publico.pt. é ns1.novis.pt (resposta não autoritativa)

4.b) MX record for domains di.uminho.pt., up.pt.

dig di.uminho.pt. MX

```
; <<>> DiG 9.7.3-P3 <<>> di.uminho.pt MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57626
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 9, ADDITIONAL: 13

;; QUESTION SECTION:
;di.uminho.pt.                  IN      MX

;; ANSWER SECTION:
di.uminho.pt.           9348    IN      MX      20 imss2.di.uminho.pt.
di.uminho.pt.           9348    IN      MX      20 imss1.di.uminho.pt.
;; AUTHORITY SECTION:
di.uminho.pt.           13888   IN      NS      ns1.eurotux.com.
di.uminho.pt.           13888   IN      NS      ns3.eurotux.com.
di.uminho.pt.           13888   IN      NS      alfa.di.uminho.pt.
di.uminho.pt.           13888   IN      NS      dns2.di.uminho.pt.
di.uminho.pt.           13888   IN      NS      dns2.uminho.pt.
di.uminho.pt.           13888   IN      NS      dns3.uminho.pt.
di.uminho.pt.           13888   IN      NS      marco.uminho.pt.
di.uminho.pt.           13888   IN      NS      dns.di.uminho.pt.
di.uminho.pt.           13888   IN      NS      dns.uminho.pt.

;; ADDITIONAL SECTION:
imss1.di.uminho.pt.     9348    IN      A       193.136.19.251
imss2.di.uminho.pt.     9348    IN      A       193.136.19.252
dns.di.uminho.pt.       13888   IN      A       193.136.19.1
dns.di.uminho.pt.       13888   IN      AAAA    2001:690:2280:28::1
dns.uminho.pt.          8832    IN      A       193.137.16.75
```

```
dns.uminho.pt.          16147   IN      AAAA    2001:690:2280:1::75
ns1.eurotux.com. 53079  IN      A       194.107.127.1
ns3.eurotux.com. 53077  IN      A       216.75.63.6
alfa.di.uminho.pt. 13888 IN     A       193.136.19.3
dns2.di.uminho.pt.      13888   IN      A       193.136.19.2
dns2.di.uminho.pt.      13888   IN      AAAA    2001:690:2280:28::2
dns2.uminho.pt.         8832    IN      A       193.137.16.145
dns2.uminho.pt.         16147   IN      AAAA    2001:690:2280:801::145

;; Query time: 7 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Nov  7 19:17:41 2011
;; MSG SIZE  rcvd: 509
```

- O mail exchanger do di.uminho.pt. é “20 imss2.di.uminho.pt.” ou “20 imss1.di.uminho.pt.” (Resposta não-autoritativa)

```
    dig up.pt. MX
; <<>> DiG 9.7.3-P3 <<>> up.pt. MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64592
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 12

;; QUESTION SECTION:
;up.pt.                         IN      MX

;; ANSWER SECTION:
up.pt.                  81149   IN      MX      20 relay2.up.pt.
up.pt.                  81149   IN      MX      10 relay1.up.pt.

;; AUTHORITY SECTION:
up.pt.                  50570   IN      NS      dns4.up.pt.
up.pt.                  50570   IN      NS      dns1.up.pt.
up.pt.                  50570   IN      NS      dns2.up.pt.
up.pt.                  50570   IN      NS      dns3.up.pt.

;; ADDITIONAL SECTION:
relay1.up.pt.           81149   IN      A       193.137.55.26
relay1.up.pt.           81149   IN      AAAA    2001:690:2200:a10::26
relay2.up.pt.           81149   IN      A       193.137.55.27
relay2.up.pt.           81149   IN      AAAA    2001:690:2200:a10::27
dns1.up.pt.             8228    IN      A       193.137.55.20
dns1.up.pt.             8228    IN      AAAA    2001:690:2200:a10::20
dns2.up.pt.             8228    IN      A       193.137.55.21
dns2.up.pt.             8228    IN      AAAA    2001:690:2200:a10::21
dns3.up.pt.             8229    IN      A       193.137.35.100
dns3.up.pt.             8229    IN      AAAA    2001:690:2200:b10::100
dns4.up.pt.             8229    IN      A       193.136.37.10
dns4.up.pt.             8229    IN      AAAA    2001:690:2200:910::10

;; Query time: 7 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Mon Nov  7 19:23:39 2011
;; MSG SIZE  rcvd: 409
```

- O mail exchanger do up.pt é “20 relay2.up.pt.” ou “10 relay1.up.pt.” (Resposta não-autoritativa)

4.c) AAAA address of marco.ip6.uminho.pt

```
> set query=AAAA
> marco.ip6.uminho.pt.
Server:                 192.168.2.1
Address:        192.168.2.1#53

Non-authoritative answer:
marco.ip6.uminho.pt     has AAAA address 2001:690:2280:20:206:2bff:fe02:f202

Authoritative answers can be found from:
ip6.uminho.pt  nameserver = dns3.uminho.pt.
ip6.uminho.pt  nameserver = marco.ip6.uminho.pt.
ip6.uminho.pt  nameserver = marco.uminho.pt.
ip6.uminho.pt  nameserver = dns.uminho.pt.
ip6.uminho.pt  nameserver = dns2.uminho.pt.
dns.uminho.pt internet address = 193.137.16.75
dns.uminho.pt has AAAA address 2001:690:2280:1::75
dns2.uminho.pt          internet address = 193.137.16.145
dns2.uminho.pt          has AAAA address 2001:690:2280:801::145
dns3.uminho.pt          internet address = 193.137.16.65
dns3.uminho.pt          has AAAA address 2001:690:2280:1::65
marco.ip6.uminho.pt     internet address = 193.136.9.240
```

- Usando o comando nslookup, é possível chgar à conclusão que o endereço IPv6 do marco.ip6.uminho.pt é 2001:690:2280:20:206:2bff:fe02:f202.

5. Using the above tools and a browser access to "http://www.ripe.net":

5.a) identify completely (including domain name, email address, surface address, telephone #) an hypothetical attacker comming from:

IP 193.136.19.190,

Nome completo incluindo o domínio: ce.grid.prociv.pt.
Entidade: Universidade do Minho, Centro de Informatica
Morada: Campus de Gualtar, Braga, Portugal
Não existem contactos da instituição é apresentado só a titulo de exemplo o contacto de uma pessoa da instituição:
Telefone: +351 253604474
E-mail: alex@di.uminho.pt

Entidade Fornecedora do Serviço:
Morada: Avenida do Brasil 101, 1700-066 Lisboa, Portugal
Telefone: +351 21 8440177
E-mail: report@cert.pt

IP 193.137.89.146,

Nome completo incluindo o domínio: endpub146.bio-glt.uminho.pt.
Entidade: Universidade do Minho, Centro de Comunicações
Morada: Campus de Gualtar, Braga, Portugal
Mais uma vez não existem contactos da instituição.

Entidade Fornecedora do Serviço:
Morada: Avenida do Brasil 101, 1700-066 Lisboa, Portugal
Telefone: +351 21 8440177
E-mail: report@cert.pt

193.137.90.45,

Nome completo incluindo o domínio:endpub045.civil-glt.uminho.pt.
Entidade: Universidade do Minho, Centro de Comunicações
Morada: Campus de Gualtar, Braga, Portugal
Mais uma vez não existem contactos da instituição.

Entidade Fornecedora do Serviço:
Morada: Avenida do Brasil 101, 1700-066 Lisboa, Portugal
Telefone: +351 21 8440177
E-mail: report@cert.pt

5.b) identify temporal parameters established for the DNS (sub)domain “gcom.di.uminho.pt”

```
nslookup
> set type=soa
> gcom.di.uminho.pt
Server:         192.168.2.1
Address:  192.168.2.1#53

Non-authoritative answer:
gcom.di.uminho.pt
        origin = marco.uminho.pt
        mail addr = dnsop.marco.uminho.pt
        serial = 2011051201
        refresh = 86400
        retry = 7200
        expire = 604800
        minimum = 86400
```

- Pela informação obtida acima podemos retirar os dados referentes aos parâmetros temporais estabelecidos. Podemos então verificar, a data da última actualização a partir da serial 2011051201, ou seja dia 12 do mês cinco de 2011, o seu tempo de refresh 86400 segundos, 1 dia, que corresponde ao tempo que um servidor secundário demora para verificar se foi feita ou não alguma alteração no servidor, o tempo de retry, 7200 segundos, que é o tempo que o servidor deve aguardar até realizar uma nova tentativa de refresh caso a primeira tenha falhado, o tempo de expire, de 604800, 7 dias, que é o tempo que um servidor secundário pode conter uma informação oriunda do servidor antes de ser descartada, e ainda o tempo minimum de 86400 segundos, 1 dia, que é o tempo mínimo de ttl (time to live) dos registros.