



Universidade do Minho

LICENCIATURA EM CIÊNCIAS DA COMPUTAÇÃO
SISTEMAS DE COMUNICAÇÕES E REDES

Ensaio Escrito
Aplicações e Camada de Transporte

Grupo 28

Davide Santos (A102938)

Edgar Araújo (A102946)

Pedro Augusto Camargo (A102504)

Novembro 2023

Contents

1	Nível aplicacional	3
1.1	Identifique o endereço IP da estação que formulou a query DNS e o tipo de query realizada.	3
1.2	Localize a trama com a resposta à query DNS formulada. Identifique nesta trama o endereço IP do servidor web. Identifique também o servidor de nomes que forneceu a resposta, através do seu IP e nome	3
1.3	Aplique o filtro aos protocolos http // tcp. Identifique os endereços IP do cliente e do servidor HTTP	3
1.4	Identifique os segmentos TCP correspondentes ao estabelecimento da ligação entre o cliente e o servidor HTTP. Qual o o tamanho máximo de segmento (MSS) que o servidor aceita receber?	3
1.5	Identifique a resposta HTTP do servidor respeitante ao primeiro pedido GET efetuado pelo cliente. Quantos bytes de dados aplicacionais contém essa resposta HTTP?	4
1.6	A resposta HTTP identificada na alínea anterior foi transmitida em quantos segmentos TCP? Apresente também uma estimativa teórica para essa quantidade.	4
1.7	A partir da informação contida nos cabeçalhos dos protocolos IP e TCP, determine o número de bytes de dados enviados no primeiro e no último segmento TCP respeitantes à resposta HTTP.	4
1.8	Observe a informação apresentada no campo host do cabeçalho do pedido HTTP e diga qual o seu interesse?	4
1.9	Com base na sequência de dados trocados entre o cliente e o servidor diga, justificando, se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.	5
1.10	Aceda a https://www.uminho.pt, ao mesmo tempo que captura o tráfego desse acesso com o Wireshark. Porque razão o tráfego HTTP não é identificado como tal no Wireshark? Apesar disso, pode detetar-se qual o protocolo aplicacional. Como é que o Wireshark sabe que se trata duma ligação http-over-tls?	5
1.11	Diga, justificando, quais dos seguintes elementos uma comunicação HTTPS permite manter ocultos dum atacante: i) o endereço IP do cliente, ii) o endereço IP do servidor web, iii) o nome do servidor web, iv) o tamanho da mensagem trocada entre o cliente o servidor, v) a identificação da página acedida no servidor web, vi) a frequência das conexões estabelecidas entre o cliente e o servidor, vii) os dados da aplicação trocados entre o servidor e o cliente	5
2	Parte 2	5
3	Consultas ao serviço de resolução de nomes DNS	6
3.1	Usando os registos do tipo A, identifique os endereços IPv4 dos servidores mail.uminho.pt e www.ualg.pt? Qual o servidor de nomes que a sua máquina está a usar?	6
3.2	Usando os registos do tipo PTR, efetue uma query para 143.9.137.193.in-addr.arpa. O que permitiu identificar esta query?	7
3.3	Certas aplicações fazem uso do reverse DNS, como, por exemplo, o traceroute. Experimente fazer traceroute (tracert no Windows) para router-di.uminho.pt, ao mesmo tempo que captura o tráfego gerado com o Wireshark. Comente a diferença observada, em termos de tráfego DNS gerado, entre usar a opção com e sem resolução de nomes (-n no Linux, -d no Windows). Perante o observado, diga qual a utilidade que o reverse DNS oferece ao traceroute?	7
3.4	Usando o registo NS:	8
3.4.1	Identifique os servidores de nomes definidos para os domínios: “tecnico.ulisboa.pt.”, “ulisboa.pt.”, “pt.” e “.” (root).	9
3.4.2	Perante a informação obtida, diga, justificando, se os servidores de nomes de diferentes domínios podem coexistir numa mesma máquina física.	10
3.4.3	Encontra domínios geridos por servidores de nomes localizados em redes IP distintas? Se sim, apresente esses domínios e diga qual a vantagem resultante desse procedimento?	10
3.5	Usando o registo SOA:	11
3.5.1	Identifique o servidor DNS primário definido para os domínios: “tecnico.ulisboa.pt.”, “ulisboa.pt.”, “pt.” e “.” (root).	11

3.5.2	Quais são os servidores secundários dos domínios “tecnico.ulisboa.pt.” e “ulisboa.pt.”? Justifique.	11
3.5.3	Em que difere o servidor primário de um servidor secundário? Qual o significado dos parâmetros temporais associados ao servidor primário?	11
3.6	Usando o registo MX	13
3.6.1	Quais são os servidores de email do domínio “tecnico.ulisboa.pt.”?	13
3.6.2	A que sistema são preferencialmente entregues as mensagens dirigidas a geral@tecnico.ulisboa.pt?	13
3.7	A resposta obtida a uma query pode ser classificada como autoritativa ou não-autoritativa.	13
3.7.1	Qual a diferença fundamental entre ambos os tipos de resposta?	13
3.7.2	Usando o seu default DNS server, que tipos de resposta obtém se efetuar queries aos registos MX para identificar os servidores de email dos domínios “ulisboa.pt.” e “uminho.pt.”? Experimente e justifique os tipos de respostas obtidos.	13

1 Nível aplicacional

1.1 Identifique o endereço IP da estação que formulou a query DNS e o tipo de query realizada.

14	10.033359221	172.26.57.176	193.137.16.65	DNS	78 Standard query 0x7b03 A www.scom.uminho.pt
15	10.033386202	172.26.57.176	193.137.16.65	DNS	78 Standard query 0xda1c AAAA www.scom.uminho.pt
16	10.057275198	193.137.16.65	172.26.57.176	DNS	94 Standard query response 0x7b03 A www.scom.uminho.pt A 193.137.9.174
17	10.057275910	193.137.16.65	172.26.57.176	DNS	106 Standard query response 0xda1c AAAA www.scom.uminho.pt AAAA 2001:690:2280:1::105
18	10.058089977	172.26.57.176	193.137.9.174	TCP	74 38734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595496 TSecr=0 WS=128
19	10.060328175	193.137.9.174	172.26.57.176	TCP	78 80 → 38734 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM

O endereço IP da estação que formulou a query DNS: 172.26.57.176 (O meu computador) Foram enviadas 2 queries dns, uma do tipo A (endereço IPv4) e outra do tipo AAAA (endereço IPv6)

1.2 Localize a trama com a resposta à query DNS formulada. Identifique nesta trama o endereço IP do servidor web. Identifique também o servidor de nomes que forneceu a resposta, através do seu IP e nome

14	10.033359221	172.26.57.176	193.137.16.65	DNS	78 Standard query 0x7b03 A www.scom.uminho.pt
15	10.033386202	172.26.57.176	193.137.16.65	DNS	78 Standard query 0xda1c AAAA www.scom.uminho.pt
16	10.057275198	193.137.16.65	172.26.57.176	DNS	94 Standard query response 0x7b03 A www.scom.uminho.pt A 193.137.9.174
17	10.057275910	193.137.16.65	172.26.57.176	DNS	106 Standard query response 0xda1c AAAA www.scom.uminho.pt AAAA 2001:690:2280:1::105
18	10.058089977	172.26.57.176	193.137.9.174	TCP	74 38734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595496 TSecr=0 WS=128
19	10.060328175	193.137.9.174	172.26.57.176	TCP	78 80 → 38734 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM

O endereço IP do servidor web que respondeu a query DNS: 193.137.16.65 De forma a identificar o servidor de nomes que forneceu a resposta, poderia ter sido usado o utilitário nslookup, como também o serviço WEB <https://whatismyipaddress.com/ip/<ip>>, para o ip anterior:

IP Details For: 193.137.16.65	
Decimal:	3246985281
Hostname:	dns3.uminho.pt
ASN:	1930
ISP:	Fundacao Para a Ciencia e a Tecnologia I.P.
Services:	None detected
Assignment:	Likely Static IP
Country:	Portugal
State/Region:	Braga
City:	Braga
Latitude:	41.5500 (41° 32' 59.83" N)
Longitude:	-8.4199 (8° 25' 11.52" W)

Obtemos que o servidor DNS que forneceu a resposta, tem por hostname: dns3.uminho.pt

1.3 Aplique o filtro aos protocolos http // tcp. Identifique os endereços IP do cliente e do servidor HTTP

21	10.060450003	172.26.57.176	193.137.9.174	HTTP	439 GET / HTTP/1.1
22	10.120634426	193.137.9.174	172.26.57.176	TCP	2542 80 → 38734 [ACK] Seq=1 Ack=374 Win=65162 Len=2476 TSval=381818 TSecr=1449595498 [TCP
23	10.120710338	172.26.57.176	193.137.9.174	TCP	66 38734 → 80 [ACK] Seq=374 Ack=2477 Win=63360 Len=0 TSval=1449595558 TSecr=381818
24	10.124781915	193.137.9.174	172.26.57.176	TCP	3780 80 → 38734 [ACK] Seq=2477 Ack=374 Win=65162 Len=3714 TSval=381818 TSecr=1449595558 [
25	10.124795390	172.26.57.176	193.137.9.174	TCP	66 38734 → 80 [ACK] Seq=374 Ack=6191 Win=62336 Len=0 TSval=1449595562 TSecr=381818

- Temos o endereço IP do cliente, vindo do HTTP GET Request: 172.26.57.176
- Que tem como destino o IP do servidor: 193.137.9.174

1.4 Identifique os segmentos TCP correspondentes ao estabelecimento da ligação entre o cliente e o servidor HTTP. Qual o o tamanho máximo de segmento (MSS) que o servidor aceita receber?

18	10.058089977	172.26.57.176	193.137.9.174	TCP	74 38734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595496 TSecr=0 WS=128
19	10.060328175	193.137.9.174	172.26.57.176	TCP	78 80 → 38734 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
20	10.060351849	172.26.57.176	193.137.9.174	TCP	66 38734 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1449595498 TSecr=0
21	10.060450003	172.26.57.176	193.137.9.174	HTTP	439 GET / HTTP/1.1

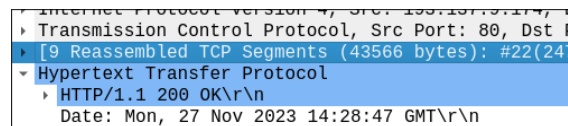
Tal como mostra a imagem, os pacotes 18 e 19 correspondem aos pacotes SYN do cliente e SYN-ACK do servidor, respetivamente. Logo ambos tem oportunidade nestes pacotes de solicitar um MSS, que no caso do servidor é de 1250 bytes.

- 1.5 Identifique a resposta HTTP do servidor respeitante ao primeiro pedido GET efetuado pelo cliente. Quantos bytes de dados aplicacionais contém essa resposta HTTP?



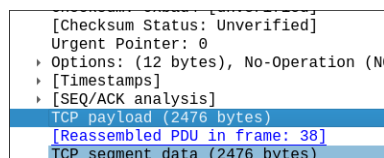
A resposta HTTP do servidor é do tipo 200 OK, e contém 43275 bytes de dados aplicacionais, tal como indica o campo Content-Length.

- 1.6 A resposta HTTP identificada na alínea anterior foi transmitida em quantos segmentos TCP? Apresente também uma estimativa teórica para essa quantidade.

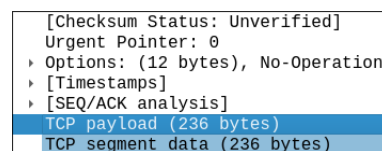


A resposta HTTP foi transmitida em 9 segmentos. A estimativa teórica para essa quantidade é de $43566/1460 = 29.8$, ou seja, 30 segmentos.

- 1.7 A partir da informação contida nos cabeçalhos dos protocolos IP e TCP, determine o número de bytes de dados enviados no primeiro e no último segmento TCP respeitantes à resposta HTTP.



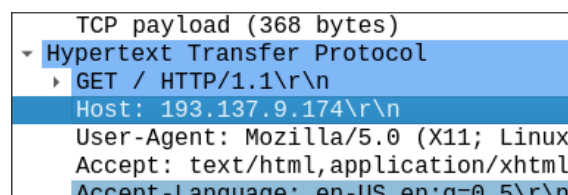
(a) Primeiro Segmento



(b) Último Segmento

No primeiro segmento TCP, o número de bytes de dados enviados é de 2476 bytes. No último segmento TCP, o número de bytes de dados enviados é de 236 bytes.

- 1.8 Observe a informação apresentada no campo host do cabeçalho do pedido HTTP e diga qual o seu interesse?



O campo host do cabeçalho do pedido HTTP indica o nome colocado no url do browser, que serve para identificar o website que se pretende aceder, em caso de um servidor conter vários websites diferentes.

1.9 Com base na sequência de dados trocados entre o cliente e o servidor diga, justificando, se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.

38	10	142171341	193.137.9.174	172.26.57.176	HTTP	382 HTTP/1.1 200 OK (text/html)
39	10	142199363	172.26.57.176	193.137.9.174	TCP	66 38734 → 80 [ACK] Seq=374 Ack=43567 Win=64128 Len=0 TSval=1449595580 TSecr=381818
40	10	274559560	172.26.57.176	193.137.9.174	HTTP	441 GET /portal.css HTTP/1.1
41	10	276000913	172.26.57.176	193.137.9.174	TCP	74 38744 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595714 TSecr=0 WS=128
42	10	276148730	172.26.57.176	193.137.9.174	TCP	74 38756 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1449595714 TSecr=0 WS=128
43	10	279664384	193.137.9.174	172.26.57.176	TCP	78 80 → 38744 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
44	10	279665146	193.137.9.174	172.26.57.176	TCP	78 80 → 38756 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1250 WS=1 TSval=0 TSecr=0 SACK_PERM
45	10	279785101	172.26.57.176	193.137.9.174	TCP	66 38744 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1449595717 TSecr=0
46	10	279888154	172.26.57.176	193.137.9.174	TCP	66 38756 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1449595717 TSecr=0

O servidor HTTP está a funcionar em modo de conexão persistente, pois nenhum dos segmentos TCP tem a flag FIN ativa, entre GET Requests.

1.10 Aceda a <https://www.uminho.pt>, ao mesmo tempo que captura o tráfego desse acesso com o Wireshark. Porque razão o tráfego HTTP não é identificado como tal no Wireshark? Apesar disso, pode detetar-se qual o protocolo aplicacional. Como é que o Wireshark sabe que se trata duma ligação http-over-tls?

A razão pela qual o tráfego HTTP não é identificado como tal no Wireshark, é porque o tráfego HTTP está a ser feito sobre o protocolo TLS, que é um protocolo de segurança que encripta o tráfego HTTP, de forma a que este não seja visível a terceiros. O Wireshark sabe que se trata de uma ligação http-over-tls, porque o protocolo TLS é identificado no campo Protocol do pacote.

1.11 Diga, justificando, quais dos seguintes elementos uma comunicação HTTPS permite manter ocultos dum atacante: i) o endereço IP do cliente, ii) o endereço IP do servidor web, iii) o nome do servidor web, iv) o tamanho da mensagem trocada entre o cliente o servidor, v) a identificação da página acedida no servidor web, vi) a frequência das conexões estabelecidas entre o cliente e o servidor, vii) os dados da aplicação trocados entre o servidor e o cliente

- i) O endereço IP do cliente não é oculto, pois é necessário para que o servidor saiba para onde enviar a resposta.
- ii) O endereço IP do servidor web não é oculto, pois é necessário para que o cliente saiba para onde enviar o pedido.
- iii) O nome do servidor web não é oculto, pois é necessário para que o servidor saiba para que website enviar o pedido.
- iv) O tamanho da mensagem trocada entre o cliente e o servidor não é oculto, pois é necessário para que o cliente saiba se recebeu a mensagem completa.
- v) A identificação da página acedida no servidor web não é oculto. O caminho do URL é parte da solicitação HTTP e, embora a comunicação seja criptografada, a estrutura básica da solicitação permanece visível.
- vi) A frequência das conexões estabelecidas entre o cliente e o servidor não é oculto, pois é necessário para que o servidor saiba se o cliente está a tentar fazer um ataque de negação de serviço.
- vii) Os dados da aplicação trocados entre o servidor e o cliente SÃO ocultos, isso garante que o conteúdo da mensagem, incluindo informações sensíveis, não seja visível para um atacante que possa interceptar a comunicação.

2 Parte 2

3 Consultas ao serviço de resolução de nomes DNS

3.1 Usando os registos do tipo A, identifique os endereços IPv4 dos servidores *mail.uminho.pt* e *www.ualg.pt*? Qual o servidor de nomes que a sua máquina está a usar?

```
; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> A mail.uminho.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20585
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
mail.uminho.pt.                0       IN      A      193.137.9.143

;; Query time: 32 msec
;; SERVER: 172.24.128.1#53(172.24.128.1) (UDP)
;; WHEN: Mon Dec 04 16:34:16 WET 2023
;; MSG SIZE rcvd: 62
```

Figure 1: Output do comando *dig A mail.uminho.pt*

```
; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> A www.ualg.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55362
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
www.ualg.pt.                   0       IN      A      193.136.224.33

;; Query time: 10 msec
;; SERVER: 172.24.128.1#53(172.24.128.1) (UDP)
;; WHEN: Mon Dec 04 16:34:22 WET 2023
;; MSG SIZE rcvd: 56
```

Figure 2: Output do comando *dig A www.ualg.pt*

```
# This file was automatically generated by WSL. To stop automatic generation of this file, add the following entry to /etc/wsl.conf:
# [network]
# generateResolvConf = false
nameserver 172.24.128.1
```

Figure 3: Output do comando *cat /etc/resolv.conf*

- O endereço IPv4 do servidor *mail.uminho.pt* é *193.137.9.143*.
- O endereço IPv4 do servidor *www.ualg.pt* é *193.136.224.33*.
- O servidor de nomes utilizado pela sua máquina é *172.24.128.1*.

O servidor de nomes utilizado pela máquina é, na verdade, uma *bridge* para a minha máquina principal, uma vez que estou a usar wsl2. O servidor de nomes utilizado pela máquina principal é: 193.137.16.65, 193.137.16.145 e 193.137.16.75

IPv4 address:	172.26.91.193
IPv4 DNS servers:	193.137.16.65 (Unencrypted) 193.137.16.145 (Unencrypted) 193.137.16.75 (Unencrypted)
Primary DNS suffix:	eduroam.uminho.pt

Figure 4: IPv4 DNS do servidor de nomes da máquina principal

3.2 Usando os registos do tipo PTR, efetue uma query para 143.9.137.193.in-addr.arpa. O que permitiu identificar esta query?

```
; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> -x 143.9.137.193
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16703
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 55f9f0e4952ad37a01000000656e407ff1fab904f4bf12cd (good)
; QUESTION SECTION:
; 193.137.9.143.in-addr.arpa.      IN      PTR
; AUTHORITY SECTION:
9.143.in-addr.arpa.      3599    IN      SOA     ns2.savvis.net. dns-admin.centurylink.com. 2191106000 10800 3600 604800
3600
; Query time: 1657 msec
; SERVER: 172.24.128.1#53(172.24.128.1) (UDP)
; WHEN: Mon Dec 04 20:15:34 WET 2023
; MSG SIZE rcvd: 176
```

Figure 5
Output do comando *dig -x 143.9.137.193*

A consulta PTR para 143.9.137.193.in-addr.arpa resultou em um status de NXDOMAIN (não encontrado), indicando que não há um registro PTR associado a esse endereço IP. A resposta também inclui informações sobre a autoridade, mostrando que o domínio 9.143.in-addr.arpa tem um registro SOA associado.

3.3 Certas aplicações fazem uso do reverse DNS, como, por exemplo, o traceroute. Experimente fazer traceroute (tracert no Windows) para router-di.uminho.pt, ao mesmo tempo que captura o tráfego gerado com o Wireshark. Comente a diferença observada, em termos de tráfego DNS gerado, entre usar a opção com e sem resolução de nomes (-n no Linux, -d no Windows). Perante o observado, diga qual a utilidade que o reverse DNS oferece ao traceroute?

O comando `traceroute` foi executado para o destino `router-di.uminho.pt` com o endereço IP 193.136.9.254. Os resultados mostram o tempo de resposta (em milissegundos) para cada salto no caminho até o destino. No quarto salto, houve uma perda de pacotes indicada pelo asterisco (*).

1. Primeiro Salto (172.24.128.1):

- Tempo de resposta: 0.650ms, 0.282ms, 0.328ms.

2. Segundo Salto (172.26.254.254):


```
tracert to router-di.uminho.pt (193.136.9.254), 64 hops max
 1  172.24.128.1  0.650ms  0.282ms  0.328ms
 2  172.26.254.254 10.189ms  3.837ms  2.250ms
 3  172.16.2.1  2.029ms  1.619ms  1.358ms
 4  172.16.115.252 2.174ms  *  2.290ms
```

Figure 6
Output do comando *tracert router-di.uminho.pt*

- Tempo de resposta: 10.189ms, 3.837ms, 2.250ms.
3. **Terceiro Salto (172.16.2.1):**
- Tempo de resposta: 2.029ms, 1.619ms, 1.358ms.
4. **Quarto Salto (172.16.115.252):**
- Tempo de resposta: 2.174ms, * (perda de pacotes), 2.290ms.

A perda de pacotes no quarto salto pode indicar uma interrupção temporária na comunicação ou congestionamento na rede nesse ponto específico. O aumento no tempo de resposta nos saltos subsequentes pode ser causado por várias razões, como a distância física, congestão de rede ou configuração específica dos *routers*.

3.4 Usando o registo NS:

- Para o domínio "tecnico.ulisboa.pt." (tamanho do pacote de resposta: 381 bytes):

tecnico.ulisboa.pt.	0	IN	NS	ns2.tecnico.ulisboa.pt.
tecnico.ulisboa.pt.	0	IN	NS	a.ul.pt.
tecnico.ulisboa.pt.	0	IN	NS	ns1.tecnico.ulisboa.pt.
a.ul.pt.	0	IN	A	194.117.0.150
ns1.tecnico.ulisboa.pt.	0	IN	A	193.136.128.1
ns2.tecnico.ulisboa.pt.	0	IN	A	193.136.128.2
a.ul.pt.	0	IN	AAAA	2001:690:21c0:a::150
ns1.tecnico.ulisboa.pt.	0	IN	AAAA	2001:690:2100:1::53:1
ns2.tecnico.ulisboa.pt.	0	IN	AAAA	2001:690:2100:1::2

- Para o domínio "ulisboa.pt." (tamanho do pacote de resposta: 444 bytes):

ulisboa.pt.	0	IN	NS	ns1.tecnico.ulisboa.pt.
ulisboa.pt.	0	IN	NS	ns2.tecnico.ulisboa.pt.
ulisboa.pt.	0	IN	NS	a.ul.pt.
ulisboa.pt.	0	IN	NS	b.ul.pt.
a.ul.pt.	0	IN	A	194.117.0.150
b.ul.pt.	0	IN	A	194.117.1.150
ns1.tecnico.ulisboa.pt.	0	IN	A	193.136.128.1
ns2.tecnico.ulisboa.pt.	0	IN	A	193.136.128.2
a.ul.pt.	0	IN	AAAA	2001:690:21c0:a::150
b.ul.pt.	0	IN	AAAA	2001:690:21c0:b::150
ns1.tecnico.ulisboa.pt.	0	IN	AAAA	2001:690:2100:1::53:1
ns2.tecnico.ulisboa.pt.	0	IN	AAAA	2001:690:2100:1::2

- Para o domínio "pt." (tamanho do pacote de resposta: 658 bytes):

pt.	0	IN	NS	d.dns.pt.
pt.	0	IN	NS	ns.dns.br.
pt.	0	IN	NS	e.dns.pt.
pt.	0	IN	NS	a.dns.pt.
pt.	0	IN	NS	ns2.nic.fr.
pt.	0	IN	NS	b.dns.pt.

pt.	0	IN	NS	h.dns.pt.
pt.	0	IN	NS	g.dns.pt.
pt.	0	IN	NS	c.dns.pt.
a.dns.pt.	0	IN	A	185.39.208.1
b.dns.pt.	0	IN	A	194.0.25.23
c.dns.pt.	0	IN	A	204.61.216.105
d.dns.pt.	0	IN	A	185.39.210.1
e.dns.pt.	0	IN	A	193.136.192.64
g.dns.pt.	0	IN	A	193.136.2.226
h.dns.pt.	0	IN	A	194.146.106.138
ns.dns.br.	0	IN	A	200.160.0.5
ns2.nic.fr.	0	IN	A	192.93.0.4
a.dns.pt.	0	IN	AAAA	2a04:6d80::1
b.dns.pt.	0	IN	AAAA	2001:678:20::23
c.dns.pt.	0	IN	AAAA	2001:500:14:6105:ad::1
d.dns.pt.	0	IN	AAAA	2a04:6d82::1
e.dns.pt.	0	IN	AAAA	2001:690:a00:4001::64
g.dns.pt.	0	IN	AAAA	2001:690:a80:4001::100

- Para o domínio “.” (tamanho do pacote de resposta: 966 bytes):

.	0	IN	NS	e.root-servers.net.
.	0	IN	NS	d.root-servers.net.
.	0	IN	NS	a.root-servers.net.
.	0	IN	NS	l.root-servers.net.
.	0	IN	NS	g.root-servers.net.
.	0	IN	NS	b.root-servers.net.
.	0	IN	NS	h.root-servers.net.
.	0	IN	NS	j.root-servers.net.
.	0	IN	NS	f.root-servers.net.
.	0	IN	NS	i.root-servers.net.
.	0	IN	NS	m.root-servers.net.
.	0	IN	NS	c.root-servers.net.
.	0	IN	NS	k.root-servers.net.
a.root-servers.net.	0	IN	A	198.41.0.4
b.root-servers.net.	0	IN	A	170.247.170.2
c.root-servers.net.	0	IN	A	192.33.4.12
d.root-servers.net.	0	IN	A	199.7.91.13
e.root-servers.net.	0	IN	A	192.203.230.10
f.root-servers.net.	0	IN	A	192.5.5.241
g.root-servers.net.	0	IN	A	192.112.36.4
h.root-servers.net.	0	IN	A	198.97.190.53
i.root-servers.net.	0	IN	A	192.36.148.17
j.root-servers.net.	0	IN	A	192.58.128.30
k.root-servers.net.	0	IN	A	193.0.14.129
l.root-servers.net.	0	IN	A	199.7.83.42
m.root-servers.net.	0	IN	A	202.12.27.33
a.root-servers.net.	0	IN	AAAA	2001:503:ba3e::2:30
b.root-servers.net.	0	IN	AAAA	2801:1b8:10::b

3.4.1 Identifique os servidores de nomes definidos para os domínios: “tecnico.ulisboa.pt.”, “ulisboa.pt.”, “pt.” e “.” (root).

1. tecnico.ulisboa.pt.:

- ns2.tecnico.ulisboa.pt.
- a.ul.pt.
- ns1.tecnico.ulisboa.pt.

2. ulisboa.pt.:

- ns1.tecnico.ulisboa.pt.

- ns2.tecnico.ulisboa.pt.
- a.ul.pt.
- b.ul.pt.

3. pt.:

- d.dns.pt.
- ns.dns.br.
- e.dns.pt.
- a.dns.pt.
- ns2.nic.fr.
- b.dns.pt.
- h.dns.pt.
- g.dns.pt.
- c.dns.pt.

4. . (root):

- e.root-servers.net.
- d.root-servers.net.
- a.root-servers.net.
- l.root-servers.net.
- g.root-servers.net.
- b.root-servers.net.
- h.root-servers.net.
- j.root-servers.net.
- f.root-servers.net.
- i.root-servers.net.
- m.root-servers.net.
- c.root-servers.net.
- k.root-servers.net.

3.4.2 Perante a informação obtida, diga, justificando, se os servidores de nomes de diferentes domínios podem coexistir numa mesma máquina física.

Os resultados indicam que os servidores de nomes para diferentes domínios estão hospedados em máquinas distintas. No entanto, apenas com os registos NS, não podemos afirmar conclusivamente se estão em máquinas físicas separadas. Para uma conclusão mais precisa, seria necessário verificar informações adicionais, como endereços IP e configurações específicas.

3.4.3 Encontra domínios geridos por servidores de nomes localizados em redes IP distintas? Se sim, apresente esses domínios e diga qual a vantagem resultante desse procedimento?

Sim, é possível identificar domínios geridos por servidores de nomes localizados em redes IP distintas. Por exemplo, ao observar os servidores de nomes para o domínio "pt.", notamos que eles estão distribuídos em várias redes IP. Isso é uma prática comum para garantir redundância e maior robustez na infraestrutura de DNS. Alguns desses domínios são:

- d.dns.pt
- ns.dns.br
- e.dns.pt
- a.dns.pt
- ns2.nic.fr

- b.dns.pt
- h.dns.pt
- g.dns.pt
- c.dns.pt

A vantagem de ter servidores de nomes em redes IP distintas está na resiliência do sistema. Se uma rede ou servidor falhar, outros ainda podem responder às consultas DNS, garantindo a disponibilidade contínua dos serviços.

3.5 Usando o registo SOA:

3.5.1 Identifique o servidor DNS primário definido para os domínios: “tecnico.ulisboa.pt.”, “ulisboa.pt.”, “pt.” e “.” (root).

1. tecnico.ulisboa.pt.:

- ns2.tecnico.ulisboa.pt.

2. ulisboa.pt.:

- ns1.tecnico.ulisboa.pt.

3. pt.:

- d.dns.pt.

4. . (root):

- a.root-servers.net.

3.5.2 Quais são os servidores secundários dos domínios “tecnico.ulisboa.pt.” e “ulisboa.pt.”? Justifique.

1. tecnico.ulisboa.pt.:

- a.ul.pt.
- ns1.tecnico.ulisboa.pt.

2. ulisboa.pt.:

- ns2.tecnico.ulisboa.pt.

Servidores secundários são configurados para armazenar cópias de zonas DNS e fornecer redundância e resistência a falhas. No caso:

- Para “tecnico.ulisboa.pt.”, a.ul.pt. e ns1.tecnico.ulisboa.pt. atuam como servidores secundários.
- Para “ulisboa.pt.”, ns2.tecnico.ulisboa.pt. é o servidor secundário.

3.5.3 Em que difere o servidor primário de um servidor secundário? Qual o significado dos parâmetros temporais associados ao servidor primário?

Servidor Primário:

- Contém a cópia principal e autoritativa da zona DNS.
- Tem a autoridade final sobre a zona.
- Atualizações são feitas diretamente no servidor primário.

Servidor Secundário:

- Mantém uma cópia secundária (réplica) da zona DNS.
- Obtém atualizações do servidor primário periodicamente.

- Serve como backup e distribui a carga de consulta.

Parâmetros temporais associados ao servidor primário:

- **SOA (Start of Authority):**
 - 2191106000: Número de série da zona.
 - * Incrementa a cada modificação.
 - 10800: Tempo de espera padrão (3 horas) antes de tentar novamente uma transferência de zona falhada.
 - 3600: Tempo de espera entre tentativas de transferência de zona.
 - 604800: Tempo máximo que um servidor secundário espera por uma transferência de zona antes de expirar o registro SOA.
 - 3600: Tempo de vida padrão para registros negativos (1 hora).

3.6 Usando o registo MX

3.6.1 Quais são os servidores de email do domínio “tecnico.ulisboa.pt.”?

Utilizando o comando `dig MX tecnico.ulisboa.pt`, obtemos os seguintes servidores de email:

- 51 smtp1.tecnico.ulisboa.pt.
- 10 smtp.tecnico.ulisboa.pt.
- 61 smtp2.tecnico.ulisboa.pt.

3.6.2 A que sistema são preferencialmente entregues as mensagens dirigidas a `geral@tecnico.ulisboa.pt`?

As mensagens são preferencialmente entregues ao sistema de maior prioridade, isto é, os de menor número à esquerda do nome do servidor de email, logo as mensagens seriam entregues ao servidor `smtp.tecnico.ulisboa.pt`, no caso deste estar indisponível, a mensagem seria então entregue ao seguintes, por ordem, `smtp1.tecnico.ulisboa.pt` e por fim `smtp2.tecnico.ulisboa.pt`.

3.7 A resposta obtida a uma query pode ser classificada como autoritativa ou não-autoritativa.

3.7.1 Qual a diferença fundamental entre ambos os tipos de resposta?

A diferença fundamental entre ambos os tipos de resposta é que uma resposta autoritativa é uma resposta que vem diretamente do servidor DNS que contém a informação sobre o domínio, enquanto que uma resposta não-autoritativa é uma resposta que vem de um servidor DNS que não contém a informação sobre o domínio, mas que obteve essa informação de um servidor DNS autoritativo. Logo enquanto a resposta não autoritativa pode conter informação desatualizada, a resposta autoritativa contém sempre a informação mais atualizada.

3.7.2 Usando o seu default DNS server, que tipos de resposta obtém se efetuar queries aos registos MX para identificar os servidores de email dos domínios “ulisboa.pt.” e “uminho.pt.”? Experimente e justifique os tipos de respostas obtidos.

```
~$ dig MX ulisboa.pt
<<>> Dig 9.16.22 <<>> MX ulisboa.pt
; global options: +cmd
; Got answer:
;->HEADER: opcode: QUERY, status: NOERROR, id: 329
; flags: qr rd ra ud; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: 0, udp: 1232
; COOKIE: 8a7c79a4e4a2a78100000095ee1da967add35036b2ab1 (good)
; QUESTION SECTION:
; ulisboa.pt.                IN      MX

; ANSWER SECTION:
ulisboa.pt.        600    IN      MX      100 mx11.ulisboa.pt.
ulisboa.pt.        600    IN      MX      500 mx05.ulisboa.pt.
ulisboa.pt.        600    IN      MX      50 mx14.ulisboa.pt.
ulisboa.pt.        600    IN      MX      50 mx13.ulisboa.pt.
ulisboa.pt.        600    IN      MX      100 mx12.ulisboa.pt.

; Query time: 19 msec
; SERVER: 193.137.16.65#53(193.137.16.65)
; WHEN: Mon Dec 04 18:45:00 WET 2023
; MSG SIZE rcvd: 172
```

(a) ULisboa

```
~$ dig MX uminho.pt
<<>> Dig 9.16.22 <<>> MX uminho.pt
; global options: +cmd
; Got answer:
;->HEADER: opcode: QUERY, status: NOERROR, id: 30304
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: 0, udp: 1232
; COOKIE: 8a7c79a4e4a2a78100000095ee1da967add35036b2ab1 (good)
; QUESTION SECTION:
; uminho.pt.                IN      MX

; ANSWER SECTION:
uminho.pt.         14400  IN      MX      0 uminho-pt.mail.protection.outlook.com.

; Query time: 23 msec
; SERVER: 193.137.16.65#53(193.137.16.65)
; WHEN: Mon Dec 04 18:46:19 WET 2023
; MSG SIZE rcvd: 119
```

(b) UMinho