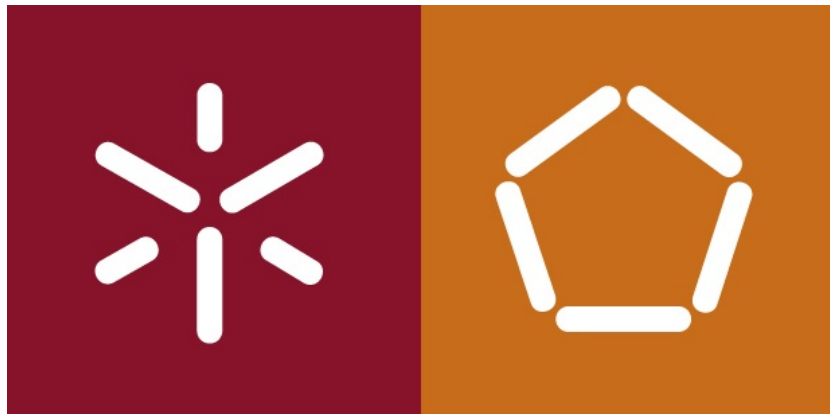


UNIVERSIDADE DO MINHO
MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA



Comunicações por Computador - Serviços de
Resolução de Nomes (DNS TP3)

PL3 GRUPO 1

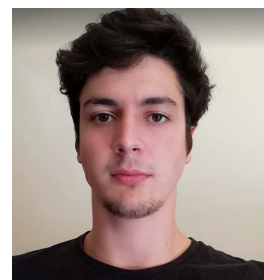
Trabalho realizado por:



A75119
Adriana Gonçalves



A74618
Bernardo Viseu



A75480
Marco Gonçalves

Braga, 24 de junho de 2021

Conteúdo

1	Introdução	2
2	Parte I	2
2.1	a) Qual o conteúdo do ficheiro <code>/etc/resolv.conf</code> e para que serve essa informação?	2
2.2	b) Os servidores <code>www.uminho.pt.</code> e <code>www.ubuntu.com.</code> têm endereços IPv6? Se sim, quais?	2
2.3	c) Quais os servidores de nomes definidos para os domínios: “ <code>sapo.pt.</code> ”, “ <code>pt.</code> ” e “ <code>.”</code> ?	3
2.3.1	Servidores para o domínio <code>www.sapo.pt</code>	4
2.3.2	Servidores para o domínio <code>.pt</code>	4
2.3.3	Servidores para o domínio “ <code>.”</code>	4
2.4	d) Existe o domínio <code>open.money.</code> ? Será que <code>open.money.</code> é um host ou um domínio?	5
2.5	e) Qual é o servidor DNS primário definido para o domínio <code>un.org.</code> ? Este servidor primário (master) aceita queries recursivas? Porquê?	5
2.6	f) Obtenha uma resposta “autoritativa” para a questão anterior.	5
2.7	g) Onde são entregues as mensagens de correio eletrónico dirigidas a <code>presidency@eu.eu</code> ou <code>presidencia@2021portugal.eu</code> ?	6
2.8	h) Que informação é possível obter, via DNS, acerca de <code>gov.pt</code> ?	7
2.9	i) Consegue interrogar o DNS sobre o endereço IPv6 <code>2001:690:2080:8005::38</code> 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?	7
2.10	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: <code>di.uminho.pt</code> ou o domínio <code>cc.pt</code> que vai ser criado na topologia virtual).	7
3	Parte II	9
3.1	Objetivos	9
3.2	Pré-Requisitos	9
3.3	Primário	9
3.4	Secundário	11
3.5	Querys	11
4	Conclusão	13

1 *Introdução*

Para a realização deste trabalho utilizamos a máquina virtual disponibilizada pelos docentes desta UC. Este trabalho prático está dividido em 2 partes, a parte I refere-se ao uso da camada de transporte por parte das aplicações onde nos é pedido para fazer uma análise ao tráfego quando usamos o browser, ftp, tftp, telnet, ssh, nslookup e traceroute. Já a parte II refere-se á instalação, configuração e utilização de serviços de transferência de ficheiros onde nos é pedido que utilizando a topologia disponibilizada pelos docentes seja transferido o mesmo ficheiro usando 4 serviços diferentes SFTP, FTP, TFTP e HTTP.

2 Parte I

2.1 a) Qual o conteúdo do ficheiro `/etc/resolv.conf` e para que serve essa informação?

Ficheiro de configuração do DNS resolver. Contém informação para regular os parâmetros operacionais e nameservers para que o DNS Resolver possa traduzir domain names para ip addresses.

2.2 b) Os servidores `www.uminho.pt` e `www.ubuntu.com` têm endereços IPv6? Se sim, quais?

```
core@core-VirtualBox:~$ nslookup www.uminho.pt
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.uminho.pt
Address: 193.137.9.114

core@core-VirtualBox:~$ nslookup www.ubuntu.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.ubuntu.com
Address: 91.189.88.181
Name:   www.ubuntu.com
Address: 91.189.88.180
Name:   www.ubuntu.com
Address: 2001:67c:1360:8001::2b
Name:   www.ubuntu.com
Address: 2001:67c:1360:8001::2c
```

nslookup `www.uminho.pt` e `www.ubuntu.com`

- `www.uminho.pt` - Não apenas tem o endereço IPv4 193.137.9.114
- `www.ubuntu.com` - Sim 2001:67c:1360:8001::2b e 2001:67c:1360:8001::2c

2.3 c) Quais os servidores de nomes definidos para os domínios: “sapo.pt.”, “pt.” e “.”?

```
core@core-VirtualBox:~$ nslookup
> set type=NS
> sapo.pt
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
sapo.pt nameserver = ns.sapo.pt.
sapo.pt nameserver = dns01.sapo.pt.
sapo.pt nameserver = ns2.sapo.pt.
sapo.pt nameserver = dns02.sapo.pt.

Authoritative answers can be found from:
> pt.
Server:      127.0.0.53
Address:     127.0.0.53#53

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

Authoritative answers can be found from:
> .
Server:      127.0.0.53
Address:     127.0.0.53#53

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

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

nslookup sapo.pt .pt .

2.3.1 Servidores para o domínio www.sapo.pt

- ns.sapo.pt.
- dns01.sapo.pt.
- ns2.sapo.pt.
- dns02.sapo.pt.

2.3.2 Servidores para o domínio .pt

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

2.3.3 Servidores para o domínio "."

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

2.4 d) Existe o domínio open.money.? Será que open.money. é um host ou um domínio?

```
core@core-VirtualBox:~$ nslookup
> set type=SOA
> open.money
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
open.money
    origin = jason.ns.cloudflare.com
    mail addr = dns.cloudflare.com
    serial = 2037127681
    refresh = 10000
    retry = 2400
    expire = 604800
    minimum = 3600
```

nslookup open.money

"open.money" é um domínio.

2.5 e) Qual é o servidor DNS primário definido para o domínio un.org.? Este servidor primário (master) aceita queries recursivas? Porquê?

```
core@core-VirtualBox:~$ dig un.org.

;<<>> DiG 9.16.1-Ubuntu <<>> un.org.
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 64612
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;un.org.
                IN      A

;; ANSWER SECTION:
un.org.         300    IN      A      157.150.185.49

;; Query time: 1064 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: ter mai 04 10:19:44 WEST 2021
;; MSG SIZE rcvd: 51
```

dig un.org.

O servidor primário é "un.org.". Este servidor como podemos verificar na figura, no campo flags encontramos a presença de "ra"(recursion available) que indica a possibilidade de de aceitar queries recursivas.

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

Não foi possível obter uma resposta autoritativa.

```

core@core-VirtualBox:~$ nslookup -type=soa un.org.
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
un.org
    origin = ns1.un.org
    mail addr = root.un.org
    serial = 2021042900
    refresh = 1200
    retry = 3600
    expire = 1209600
    minimum = 300

Authoritative answers can be found from:

core@core-VirtualBox:~$

```

nslookup -type=soa un.org.

2.7 g) Onde são entregues as mensagens de correio eletrónico dirigidas a presidency@eu.eu ou presidencia@2021portugal.eu?

```

> set type=MX
> eu.eu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
eu.eu mail exchanger = 20 smtp02.level27.be.
eu.eu mail exchanger = 10 smtp01.level27.be.

Authoritative answers can be found from:
> 2021portugal.eu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
2021portugal.eu mail exchanger = 10 mxg.eu.mpssec.net.

Authoritative answers can be found from:
>

```

nslookup type=MX eu.eu 2021portugal.eu

Quanto mais pequeno o numero melhor é o servidor para ser utilizado para a troca de emails. Como podemos verificar o emails que vão para ****@eu.eu vão preferencialmente para smtp01.level27.be e os que vão para ****@2021portugal.eu vão para mxg.eu.mpssec.net

- 2.8 h) Que informação é possível obter, via DNS, acerca de gov.pt?
- 2.9 i) Consegue interrogar o DNS sobre o endereço IPv6 2001:690:2080:8005::38 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?

```
% Information related to '2001:690:2080::/48'
% Abuse contact for '2001:690:2080::/48' is 'report@cert.rcts.pt'

inet6num:       2001:690:2080::/48
netname:        FCCN-v6-1
descr:          Fundacao para a Computacao Cientifica Nacional
country:        PT
geoloc:         38.759170 -9.142212
admin-c:        RCF19-RIPE
tech-c:         RCF19-RIPE
status:         ASSIGNED
org:            ORG-FPAC2-RIPE
remarks:        SERVIP-FCCN
mnt-by:         AS1930-MNT
mnt-lower:      AS1930-MNT
created:        2016-10-30T19:56:39Z
last-modified:  2017-03-05T00:04:02Z
source:         RIPE

organisation:   ORG-FPAC2-RIPE
org-name:       Fundacao para a Ciencia e a Tecnologia - Polo FCCN
org-type:       OTHER
address:        FCCN
address:        Av. do Brasil, 101
address:        1700-066 Lisboa
address:        PORTUGAL
phone:          +351 218440100
fax-no:         +351 218472167
admin-c:        RCF19-RIPE
tech-c:         RCF19-RIPE
tech-c:         FST8-RIPE
mnt-by:         AS1930-MNT
mnt-ref:        AS1930-MNT
abuse-c:        FST8-RIPE
created:        2014-01-20T17:38:32Z
last-modified:  2018-05-08T10:45:32Z
source:         RIPE # Filtered

role:           RCTS Contacts FCCN
address:        Fundacao para a Ciencia e a Tecnologia - Polo FCCN
address:        Av. do Brasil, 101
address:        1700-066 Lisboa
address:        PORTUGAL
admin-c:        JNF1-RIPE
tech-c:         JPP36-RIPE
tech-c:         AR7382-RIPE
tech-c:         JRG178-RIPE
mnt-by:         AS1930-MNT
nic-hdl:        RCF19-RIPE
created:        2015-05-08T23:23:52Z
last-modified:  2015-11-05T15:43:08Z
source:         RIPE # Filtered

% Information related to '2001:690::/32AS1930'
```

whois 2001:690:2080:8005::38

Através do comando whois conseguimos obter informações acerca da morada e até mesmo o contacto telefónico do responsável pelo endereço.

- 2.10 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).

A transferência de zona caracteriza-se por ser uma transacção de DNS entre um cliente e um servidor, usando o protocolo TCP. Este é usado por admins para replicar as bases de dados.

- **Serial** Representa o número de série da zona. Caso o servidor secundário que lhe está

associado notar o decrescimo do valor da zona, ele associa que esta está desatualizada e aí faz uma alteração da zona.

- **Refresh** Representa os segundos a esperar para que o servidor secundário comunique com o servidor primário e atualizar caso repare que há alterações na zona.
- **Retry** Representa os segundos para efetuar uma segunda tentativa de contacto com o servidor primário, caso a primeira tentativa tenha falhado.
- **Expire** Representa os segundos ao qual o servidor secundário deve para de pedir resposta ao primário depois de não obter qualquer resposta.

3 Parte II

3.1 Objetivos

Nesta segunda parte pretende-se que se crie um dominio CC.PT para o topologia de rede que estamos a usar nas aulas praticas (CC-Topo-2021.iml), de modo a que se possam usar os nomes em vez dos endereços IP. No final deve, por exemplo, poder fazer "ping Marte.cc.pt" ou mesmo apenas "ping Marte" ou "ping Marte.cc.pt." em vez de "ping 10.2.2.1".

3.2 Pré-Requisitos

Antes de começar certifique-se que o software BIND9 está instalado (sudo apt-get install bind9). Este pacote vem já pré-configurado de base (ficheiro em /etc/bind) pelo que o número de alterações a efetuar é mínimo.

3.3 Primário

```
$TTL      604800
@         IN      SOA      ns.cc.pt. PL03G01.cc.pt. (
                        3      ; serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL

;List Nameservers
@         IN      NS       ns.cc.pt.
@         IN      NS       ns2.cc.pt.

; PTR Records
1         IN      PTR      Server1.cc.pt. ; 10.1.1.1
2         IN      PTR      Server2.cc.pt.
3         IN      PTR      Server3.cc.pt.
```

db.1-1-10

```
$TTL      604800
@         IN      SOA      ns2.cc.pt. PL3G01.cc.pt. (
                        3      ; serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL

;List Nameservers
@         IN      NS       ns.cc.pt.
@         IN      NS       ns2.cc.pt.

; PTR Records
1         IN      PTR      Mercurio.cc.pt.
2         IN      PTR      Marte.cc.pt.
3         IN      PTR      Venus.cc.pt.
```

db.2-2-10

```

$TTL      604800
@         IN      SOA      ns.cc.pt. PL03G01.cc.pt. (
                        3      ; serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL

```

```

;List Nameservers
@         IN      NS       ns
@         IN      NS       ns2

```

```

;LAN 1

```

```

Server1 IN      A      10.1.1.1
ns      IN      A      10.1.1.1

```

```

;Mail,www

```

```

Server2 IN      A      10.1.1.2
www      IN      A      10.1.1.2
mail     IN      A      10.1.1.2
@        IN      MX 10  mail.cc.pt.

```

```

;imap,pop,mail2

```

```

Server3 IN      A      10.1.1.3
pop      IN      CNAME  Server3
imap     IN      CNAME  Server3
@        IN      MX 20  mail.cc.pt.

```

```

; LAN 2

```

```

Mercurio      IN      A      10.2.2.2
ns2           IN      A      10.2.2.2

```

```

Marte  IN      A      10.2.2.1

```

```

Venus  IN      A      10.2.2.3

```

```

;LAN

```

```

Pico   IN      A      10.3.3.1
Faial  IN      A      10.3.3.2
Corvo  IN      A      10.3.3.3

```

```

;LAN 4

```

```

Laptop1 IN      A      10.4.4.1
g01      IN      CNAME  Laptop1

```

```

Laptop2      IN      A      10.4.4.2

```

```

Laptop3      IN      A      10.4.4.3

```

db.cc.pt

```

zone "cc.pt"{
    type master;
    file "/home/core/primario/db.cc.pt";
    allow-transfer{ 10.2.2.2; };
};

zone "1.1.10.in-addr.arpa"{
    type master;
    file "/home/core/primario/db.1-1-10.rev";
    allow-transfer{ 10.2.2.2; };
};

zone "2.2.10.in-addr.arpa"{
    type master;
    file "/home/core/primario/db.2-2-10.rev";
    allow-transfer{ 10.2.2.2; };
};

```

named.conf.local

3.4 Secundário

```

zone "cc.pt"{
    type slave;
    file "/var/cache/bind/db.cc.pt";
    masters{ 10.1.1.1; };
};

zone "1.1.10.in-addr.arpa"{
    type slave;
    file "/var/cache/bind/db.1-1-10.rev";
    masters{ 10.1.1.1; };
};

zone "2.2.10.in-addr.arpa"{
    type slave;
    file "/var/cache/bind/db.2-2-10.rev";
    masters{ 10.1.1.1; };
};

```

named.conf.local

3.5 Querys

```

core@core-VirtualBox:~/primario$ /usr/sbin/named-checkconf -z /home/core/primario/named.conf
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
zone cc.pt/IN: loaded serial 3
zone 1.1.10.in-addr.arpa/IN: loaded serial 3
zone 2.2.10.in-addr.arpa/IN: loaded serial 3

```

named-checkconf

```
core@core-VirtualBox:~/primario$ /usr/sbin/named-checkzone cc.pt /home/core/primario/db.cc.pt
zone cc.pt/IN: loaded serial 3
OK
```

named-checkzone

```
core@core-VirtualBox:~/primario$ /usr/sbin/named-checkzone 1.1.10.in-addr.arpa /home/core/primario/db.1-1-10.rev
zone 1.1.10.in-addr.arpa/IN: loaded serial 3
OK
core@core-VirtualBox:~/primario$ /usr/sbin/named-checkzone 2.2.10.in-addr.arpa /home/core/primario/db.2-2-10.rev
zone 2.2.10.in-addr.arpa/IN: loaded serial 3
OK
```

named.conf.local

```
root@Laptop1:/tmp/pycore.42177/Laptop1.conf# nslookup - 10.2.2.2
> www.cc.pt
Server:      10.2.2.2
Address:     10.2.2.2#53

Name:   www.cc.pt
Address: 10.1.1.2
> █
```

named.conf.local

```
core@core-VirtualBox:~/secundario$ /usr/sbin/named-checkconf -z /home/core/secundario/named.conf
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
```

named.conf.local

```
vcmd
root@Laptop1:/tmp/pycore.40183/Laptop1.conf# nslookup - 10.1.1.1
> www.cc.pt
Server:      10.1.1.1
Address:     10.1.1.1#53

Name: www.cc.pt
Address: 10.1.1.2
> []

vcmd
07-May-2021 17:00:45.387 none:100: 'max-cache-size 90%' - setting to 1788MB (out
of 1987MB)
07-May-2021 17:00:45.395 configuring command channel from '/etc/bind/rndc.key'
07-May-2021 17:00:45.395 open: /etc/bind/rndc.key: permission denied
07-May-2021 17:00:45.395 couldn't add command channel 127.0.0.1#953: permission
denied
07-May-2021 17:00:45.395 configuring command channel from '/etc/bind/rndc.key'
07-May-2021 17:00:45.395 open: /etc/bind/rndc.key: permission denied
07-May-2021 17:00:45.395 couldn't add command channel ::1#953: permission denied
07-May-2021 17:00:45.395 not using config file logging statement for logging due
to -g option
07-May-2021 17:00:45.407 managed-keys-zone: loaded serial 15
07-May-2021 17:00:45.407 zone 2.2.10.in-addr.arpa/IN: loaded serial 3
07-May-2021 17:00:45.407 zone 0.in-addr.arpa/IN: loaded serial 1
07-May-2021 17:00:45.407 zone 1.1.10.in-addr.arpa/IN: loaded serial 3
07-May-2021 17:00:45.423 zone localhost/IN: loaded serial 2
07-May-2021 17:00:45.427 zone cc.pt/IN: loaded serial 3
07-May-2021 17:00:45.427 zone 127.in-addr.arpa/IN: loaded serial 1
07-May-2021 17:00:45.431 zone 255.in-addr.arpa/IN: loaded serial 1
07-May-2021 17:00:45.431 all zones loaded
07-May-2021 17:00:45.435 running
07-May-2021 17:00:45.439 zone 2.2.10.in-addr.arpa/IN: sending notifies (serial 3
)
07-May-2021 17:00:45.439 zone 1.1.10.in-addr.arpa/IN: sending notifies (serial 3
)
07-May-2021 17:00:45.439 zone cc.pt/IN: sending notifies (serial 3)
07-May-2021 17:00:46.639 timed out resolving './DNSKEY/IN': 193.136.19.1#53
07-May-2021 17:00:47.843 timed out resolving './DNSKEY/IN': 193.136.9.240#53
07-May-2021 17:00:55.435 managed-keys-zone: Unable to fetch DNSKEY set '.': time
d out
07-May-2021 17:00:55.435 managed-keys.bind.jnl: open: permission denied
07-May-2021 17:00:55.435 managed-keys-zone: keyfetch_done;dns_journal_open -> un
expected error
07-May-2021 17:00:55.435 managed-keys-zone: error during managed-keys processing
(unexpected error): DNSSEC validation may be at risk
07-May-2021 17:00:55.439 resolver priming query complete
```

named.conf.local

4 Conclusão

Durante a elaboração desta terceira fase do trabalho prático da unidade curricular de Comunicação por Computador, foram vários os desafios com que nos deparamos na tentativa de obter um resultado final o mais fidedigno e consistente possível.

Para obter estes resultados, tentamos seguir os ensinamentos lecionados nas aulas teóricas e práticas, tendo estes permitido uma maior consolidação de conhecimentos no que diz respeito às várias utilizações das camadas de transporte e o comportamento dos diferentes protocolos. Ficou assim demonstrado o nosso conhecimento em relação aos temas abordados.

Assim, concluímos que o nosso desempenho ao longo deste trabalho foi positivo, visto que conseguimos encontrar forma de ultrapassar os desafios apresentados durante o desenvolvimento do mesmo.