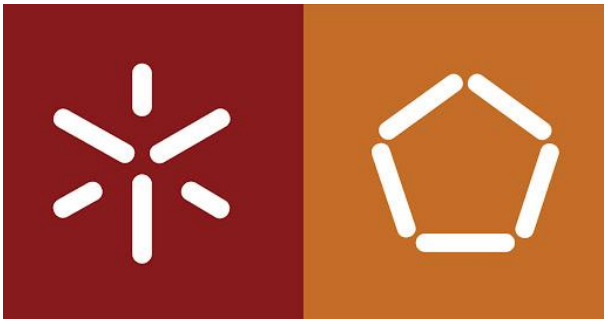


Universidade do Minho
Departamento de Informática
Licenciatura em Engenharia Informática

Comunicações por Computador

Trabalho Prático 3

Grupo Nº 53

Rui Monteiro (A93179)
Diogo Barbosa (A93184)
Joaquim Roque (A93310)

20 de novembro de 2021

Parte I

Questão a)

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

Resposta:

O ficheiro *resolv.conf* contém a informação necessária, organizada em diretivas, para conectar os clientes locais aos servidores DNS, nomeadamente o(s) ***nameserver(s)*** por omissão para resolução de nomes, e ***search***, que define um ou mais *search domains* por omissão para completar um determinado endereço numa *query*, de modo a obter um *fully qualified domain name*, quando não há um sufixo especificado.

```
core@xubuncore:~$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search eduroam.uminho.pt
```

1. Conteúdo do ficheiro resolv.conf

Questão b)

Os servidores "**www.di.uminho.pt.**" e "**www.europa.eu.**" têm endereços IPv6? Se sim, quais?

Resposta:

O servidor "**www.di.uminho.pt.**" não possui endereços IPv6, como é possível constatar na imagem anexada.

O servidor "**www.europa.eu.**" tem os endereços IPv6 "**2a01:7080:24:100::666:25**" e "**2a01:7080:14:100::666:25**".

```
core@xubuncore:~$ dig www.di.uminho.pt. AAAA

; <<>> DiG 9.16.1-Ubuntu <<>> www.di.uminho.pt. AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59953
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.di.uminho.pt.              IN      AAAA

;; ANSWER SECTION:
www.di.uminho.pt.       7793    IN      CNAME   www5.di.uminho.pt.
```

2. Query IPv6 para o endereço "www.di.uminho.pt."

```
core@xubuncore:~$ dig www.europa.eu. AAAA

; <<>> DiG 9.16.1-Ubuntu <<>> www.europa.eu. AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64383
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.europa.eu.                 IN      AAAA

;; ANSWER SECTION:
www.europa.eu.          600     IN      CNAME   ip-europa.ec.europa.eu.
ip-europa.ec.europa.eu. 299     IN      AAAA    2a01:7080:24:100::666:25
ip-europa.ec.europa.eu. 299     IN      AAAA    2a01:7080:14:100::666:25
```

3. Query IPv6 para o endereço "www.europa.eu."

Questão c)

Quais os servidores de nomes definidos para os domínios: "**gov.pt.**" e "**.**"?

Resposta:

Para "**gov.pt.**", os servidores são os seguintes:

```
core@xubuncore:~$ dig gov.pt. NS

; <<>> DiG 9.16.1-Ubuntu <<>> gov.pt. NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4745
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gov.pt.                                IN      NS

;; ANSWER SECTION:
gov.pt.                 151     IN      NS      nsp.dnsnode.net.
gov.pt.                 151     IN      NS      ns02.fccn.pt.
gov.pt.                 151     IN      NS      dns1.gov.pt.
gov.pt.                 151     IN      NS      europe1.dnsnode.net.
gov.pt.                 151     IN      NS      a.dns.pt.
```

4. Query NS para o endereço "gov.pt."

Já para "**.**" temos os seguintes servidores:

```
core@xubuncore:~$ dig . NS

; <<>> DiG 9.16.1-Ubuntu <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44912
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       20113   IN      NS      b.root-servers.net.
.                       20113   IN      NS      h.root-servers.net.
.                       20113   IN      NS      i.root-servers.net.
.                       20113   IN      NS      c.root-servers.net.
.                       20113   IN      NS      g.root-servers.net.
.                       20113   IN      NS      f.root-servers.net.
.                       20113   IN      NS      e.root-servers.net.
.                       20113   IN      NS      j.root-servers.net.
.                       20113   IN      NS      m.root-servers.net.
.                       20113   IN      NS      l.root-servers.net.
.                       20113   IN      NS      k.root-servers.net.
.                       20113   IN      NS      d.root-servers.net.
.                       20113   IN      NS      a.root-servers.net.
```

5. Query NS para o endereço "."

Questão d)

Existe o domínio "**efiko.academy.**"? Com base na informação obtida do DNS, nomeadamente os registos associados a esse nome, diga se o considera um *host* ou um domínio de nomes.

Resposta:

Trata-se de um *host* de endereço "**5.134.7.2**". O tipo *A* indica que se trata de um endereço IPv4.

```
core@xubuncore:~$ dig efiko.academy.

; <<>> DiG 9.16.1-Ubuntu <<>> efiko.academy.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41796
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
efiko.academy.          3600    IN      A       5.134.7.2
```

6. Query para o endereço "efiko.academy."

Questão e)

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

Resposta:

Analisando o resultado de *nslookup* com o *type* definido como *SOA (Start of Authority)*, o servidor DNS primário definido para o domínio "**gov.pt.**" é "**dnssec.gov.pt.**".

```
core@xubuncore:~$ nslookup
> set type=SOA
> gov.pt.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
gov.pt
        origin = dnssec.gov.pt
        mail addr = dns.ceger.gov.pt
        serial = 2019072064
        refresh = 18000
```

7. Query SOA para o endereço "gov.pt."

No entanto, este servidor não consta da lista dos *nameservers* do domínio (figura 4). Isto indica um potencial erro de configuração do mesmo. Dessa forma, qualquer *query* para este mesmo servidor inevitavelmente falha. Consideremos, então, um dos servidores DNS que obtivemos na figura 4 para o teste da recursividade (arbitrariamente, "**a.dns.pt.**").

Como se pode observar, o comando *dig* deixa tal bem explícito, onde um *WARNING* indica que a recursividade não está disponível no servidor em questão. Tal era expectável, uma vez que o uso de recursividade acarreta todos os problemas de um serviço DNS centralizado, em particular o elevado volume de tráfego.

```
core@xubuncore:~$ dig @dnssec.gov.pt. gov.pt. NS
dig: couldn't get address for 'dnssec.gov.pt.': not found
core@xubuncore:~$ dig @a.dns.pt gov.pt NS

; <<>> DiG 9.16.1-Ubuntu <<>> @a.dns.pt gov.pt NS
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9938
;; flags: qr aa rd; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 339770d48bd16d35df8d1c9b6196a82f428d0edcd8c02de9 (good)
;; QUESTION SECTION:
;gov.pt.                        IN      NS

;; ANSWER SECTION:
gov.pt.                 600     IN      NS      dns1.gov.pt.
gov.pt.                 600     IN      NS      europe1.dnsnode.net.
gov.pt.                 600     IN      NS      a.dns.pt.
gov.pt.                 600     IN      NS      ns02.fccn.pt.
gov.pt.                 600     IN      NS      nsp.dnsnode.net.

;; ADDITIONAL SECTION:
dns1.gov.pt.            600     IN      A       193.47.185.3
```

8. Query NS para "gov.pt." interrogando o servidor primário e um dos servidores secundários

Questão f)

Obtenha uma resposta "autoritativa" para a questão anterior.

Resposta:

Uma vez que contactamos diretamente um *nameserver* do domínio em questão, a resposta obtida já é autoritativa - de salientar a *flag aa* (*authoritative answer*) na figura 8.

Questão g)

Onde são entregues as mensagens de correio eletrónico dirigidas a "**marcelo@presidencia.pt**"?

Resposta:

As mensagens dirigidas a "**marcelo@presidencia.pt**" são entregues nos endereços "**mail1.presidencia.pt.**" e "**mail2.presidencia.pt.**". Este último é o endereço preferencial de entrega, uma vez que o seu valor de preferência é menor.[1]

```
core@xubuncore:~$ dig presidencia.pt. MX

; <<>> DiG 9.16.1-Ubuntu <<>> presidencia.pt. MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56250
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;presidencia.pt.                        IN      MX

;; ANSWER SECTION:
presidencia.pt.         86400   IN      MX      50 mail1.presidencia.pt.
presidencia.pt.         86400   IN      MX      10 mail2.presidencia.pt.
```

9. Query MX para o endereço "presidencia.pt."

[1] https://www.linux.com/training-tutorials/check-your-dns-records-dig/

Questão h)

Que informação é possível obter, via DNS, acerca de "**gov.pt.**"?

Resposta:

Usando o comando *dig* com a opção ANY podemos extrair toda a informação relativa ao domínio, da qual se destacam os *resource records* dos tipos *SOA (Start of Authority)*, que indicam o servidor DNS primário (*master*), bem como informação necessária para a atualização dos servidores secundários (*slaves*), e *NS* – a lista de *nameservers* do domínio.

```
core@xubuncore:~$ dig gov.pt. ANY| cut -c -100

; <<>> DiG 9.16.1-Ubuntu <<>> gov.pt. ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53806
;; flags: qr rd ra; QUERY: 1, ANSWER: 18, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gov.pt.                                IN      ANY

;; ANSWER SECTION:
gov.pt.                 3582    IN      RRSIG   NSEC3PARAM 10 2 3600 20211126192850 20211112192850 57803 gov.pt. G13nTcpTEb9
gov.pt.                 3582    IN      NSEC3PARAM 1 0 1 A1019A7DA7ACAEF4
gov.pt.                 582     IN      RRSIG   TXT 10 2 600 20211126192850 20211112192850 57803 gov.pt. Z4TtqzJ3boKMzGPmw94J
gov.pt.                 582     IN      TXT     "v=spf1 mx ip4:193.47.185.0/24 ip4:185.32.36.9 -all"
gov.pt.                 582     IN      RRSIG   SOA 10 2 600 20211126192850 20211112192850 57803 gov.pt. WKW3pgMNfjKyMJEFWVp9
gov.pt.                 582     IN      SOA     dnssec.gov.pt. dns.ceger.gov.pt. 2019072064 18000 7200 2419200 86400
gov.pt.                 3582    IN      RRSIG   DNSKEY 10 2 86400 20211126192850 20211112192850 51381 gov.pt. B97oIKrJZ98v43
gov.pt.                 3582    IN      RRSIG   DNSKEY 10 2 86400 20211126192850 20211112192850 57803 gov.pt. Sx5gvcwuxlyKBZ
gov.pt.                 3582    IN      DNSKEY  256 3 10 AwEAActlSXtgSNqOzROrlBlZiK6nFcXJNTEd6oattqkPyldfslXdzakm LKG5orO1T
gov.pt.                 3582    IN      DNSKEY  257 3 10 AwEAAYp1GwX/VzsfDmYynbtblgGMNAjluTjKa7AaxlwGoElxeXZCMcZx cFNmz8y7x
gov.pt.                 2629    IN      RRSIG   DS 13 2 7200 20211124211930 20211114211930 30640 pt. ilVQrFtNEhu3gjpK4I7e0MQ
gov.pt.                 2629    IN      DS      51381 10 2 3804088045D4F3A870C13A8E45329862D997D1CFB6E6EF94777B195A E0DC95D0
gov.pt.                 582     IN      RRSIG   NS 10 2 600 20211126192850 20211112192850 57803 gov.pt. dyszxqpb0zzSV0jihgvY+
gov.pt.                 582     IN      NS      europe1.dnsnode.net.
gov.pt.                 582     IN      NS      ns02.fccn.pt.
gov.pt.                 582     IN      NS      nsp.dnsnode.net.
gov.pt.                 582     IN      NS      a.dns.pt.
gov.pt.                 582     IN      NS      dns1.gov.pt.
```

10. Query ANY para o endereço "gov.pt."

Questão 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?

Resposta:

Usando *nslookup* e definindo o tipo para *AAAA*, obtemos o endereço "**smtp01.fccn.pt.**".

```
core@xubuncore:~$ nslookup
> set type=AAAA
> 2001:690:2080:8005::38
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
8.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.8.0.8.0.2.0.9.6.0.1.0.0.2.ip6.arpa      name = smtp01.fccn.pt.

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

11. Query para o endereço IPv6 "2001:690:2080:8005::38"

Questão 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: "**uminho.pt.**").

Resposta:

O *resource record* do tipo *SOA* contém (além do endereço do servidor primário) vários parâmetros usados pelos servidores secundários para se atualizarem.[2]

```
core@xubuncore:~/Desktop$ nslookup
> set TYPE=SOA
> uminho.pt.
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
uminho.pt
        origin = dns.uminho.pt
        mail addr = servicos.scom.uminho.pt
        serial = 2021111501
        refresh = 14400
        retry = 7200
        expire = 1209600
        minimum = 300

Authoritative answers can be found from:
```

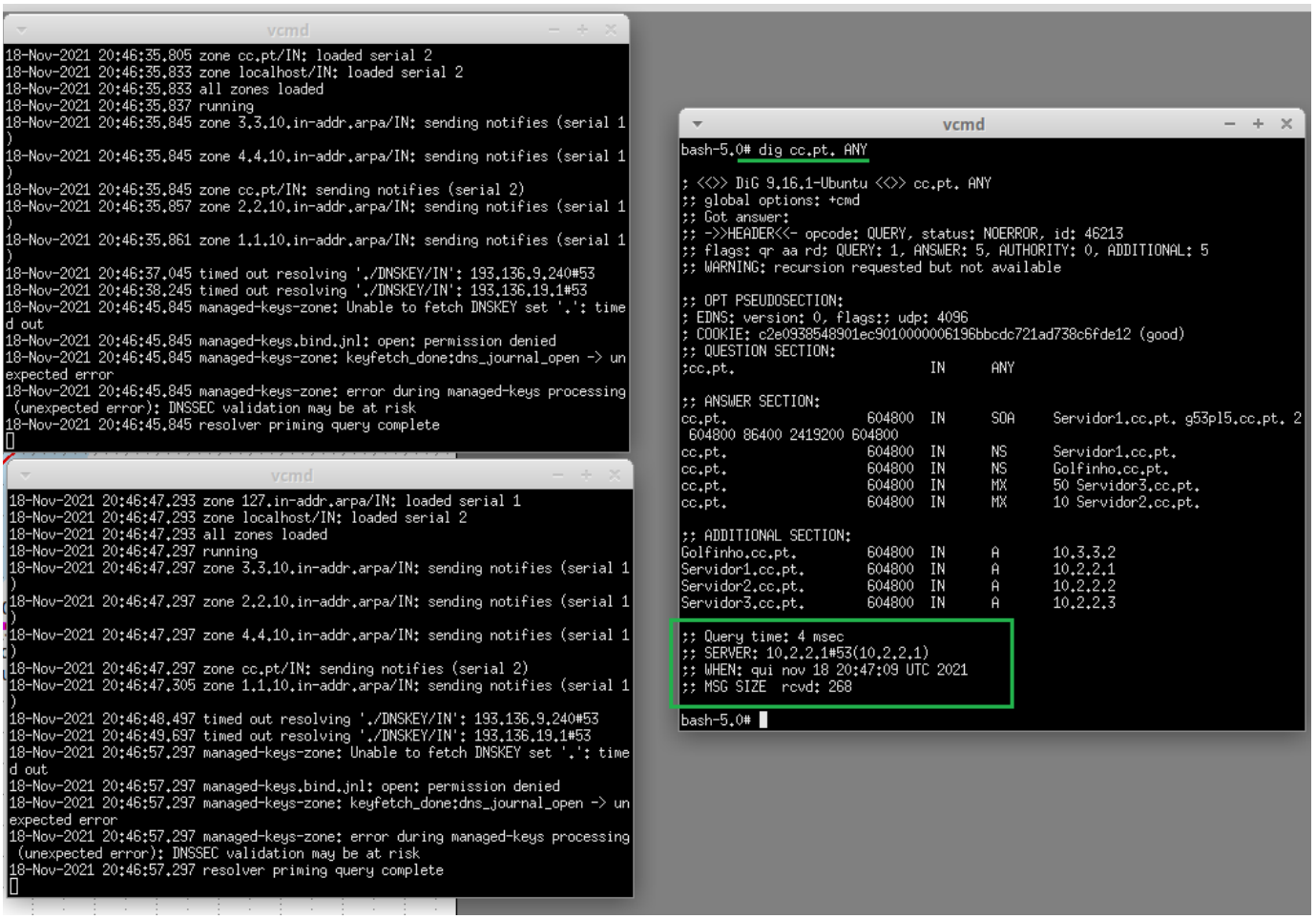
12. Query SOA para o endereço "uminho.pt."

[2] https://www.ionos.com/digitalguide/hosting/technical-matters/soa-record/

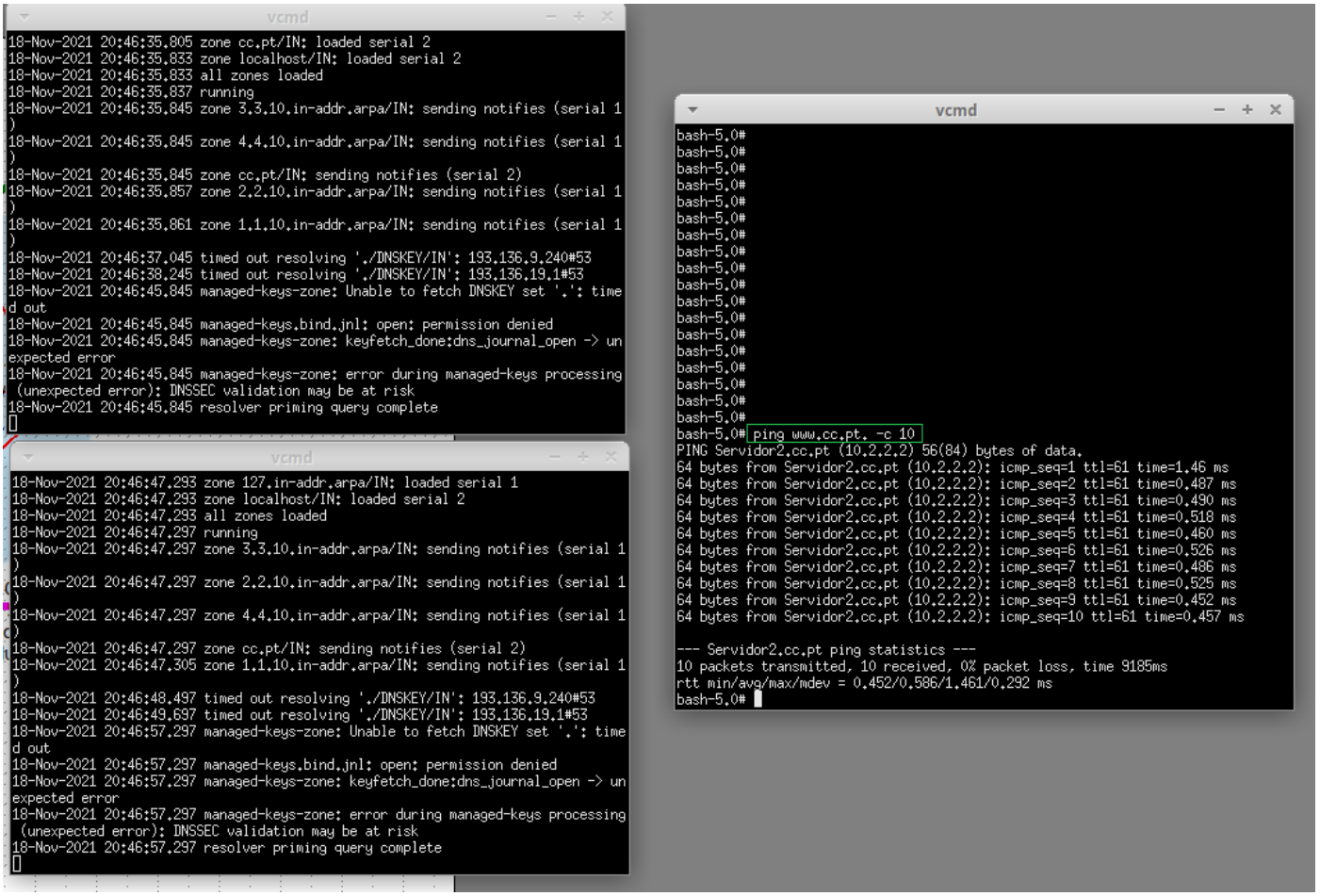
- *serial* - este valor é incrementado com cada alteração aos dados do servidor. Permite, assim, aos servidores secundários "saber" se estão ou não atualizados.
- *refresh* - tempo, em segundos, que indica quando deve um *slave* pedir informação atualizada ao *master* (neste caso, 4 horas).
- *retry* - *timeout* para um novo pedido de *refresh*, no caso deste falhar (neste caso, 2 horas).
- *expire* - durante quanto tempo um *slave* pode continuar em atividade com uma base de dados desatualizada (neste caso, 14 dias).
- *minimum* - *time to live* dos dados em *cache* de um cliente, até ser necessário interrogar novamente o servidor (neste caso, 5 minutos).

Parte II

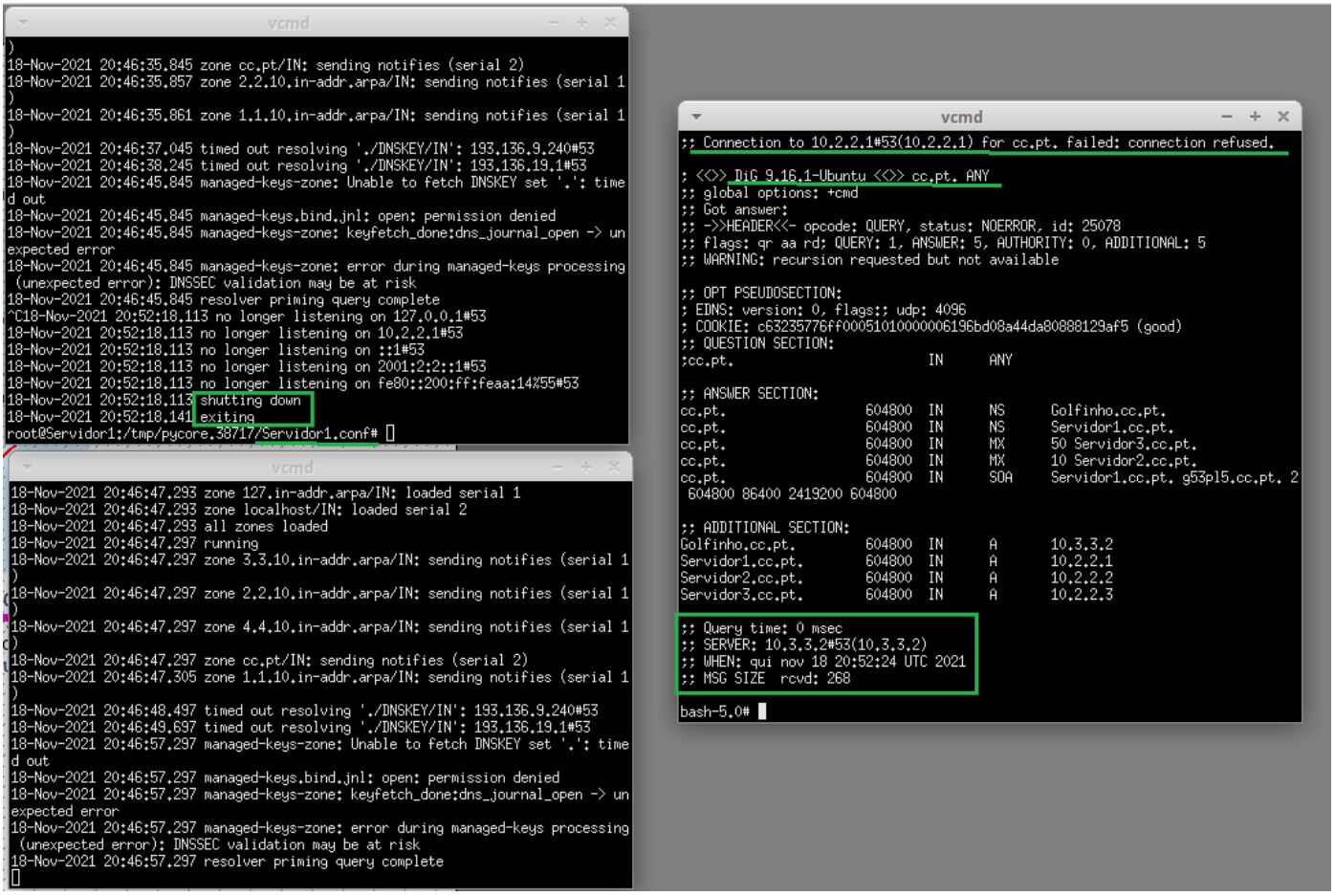
Nesta secção, apresentam-se as demonstrações necessárias aos testes que nos foram exigidos, fazendo uso da topologia de rede fornecida. De notar que esta foi alterada de modo a que os *nameservers* fossem de encontro ao contexto da topologia, isto é, o *Servidor1* e o *Golfinho*. Para tal, em cada nodo que representa um cliente, alterou-se o *scrupt* de configuração do ficheiro *resolv.conf* adequadamente, como nos foi instruído. Os testes foram executados no *Portatil2*, mas seriam igualmente válidos em qualquer outro nodo cliente.



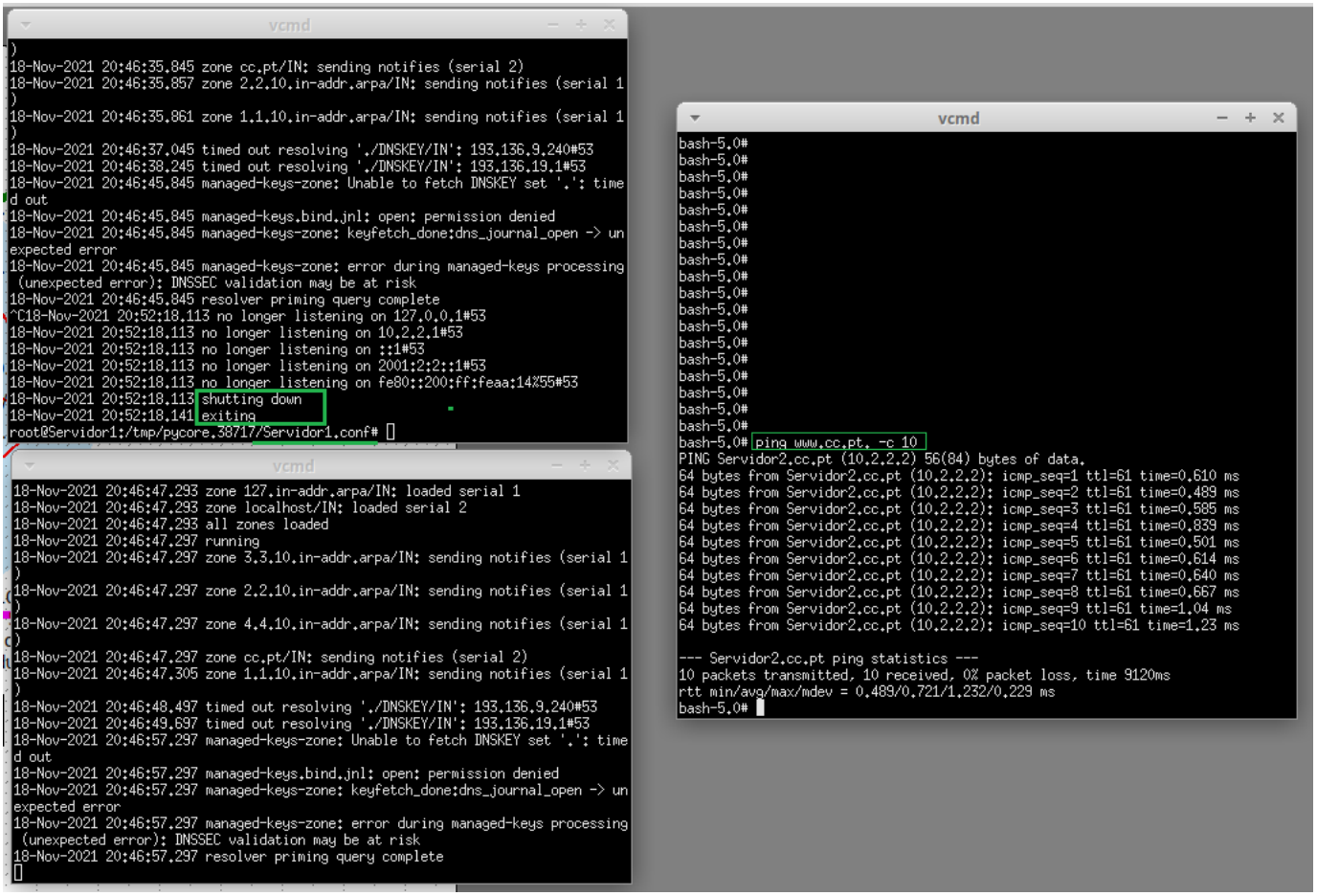
13. Dig para o domínio "cc.pt." com ambos os servidores a correr



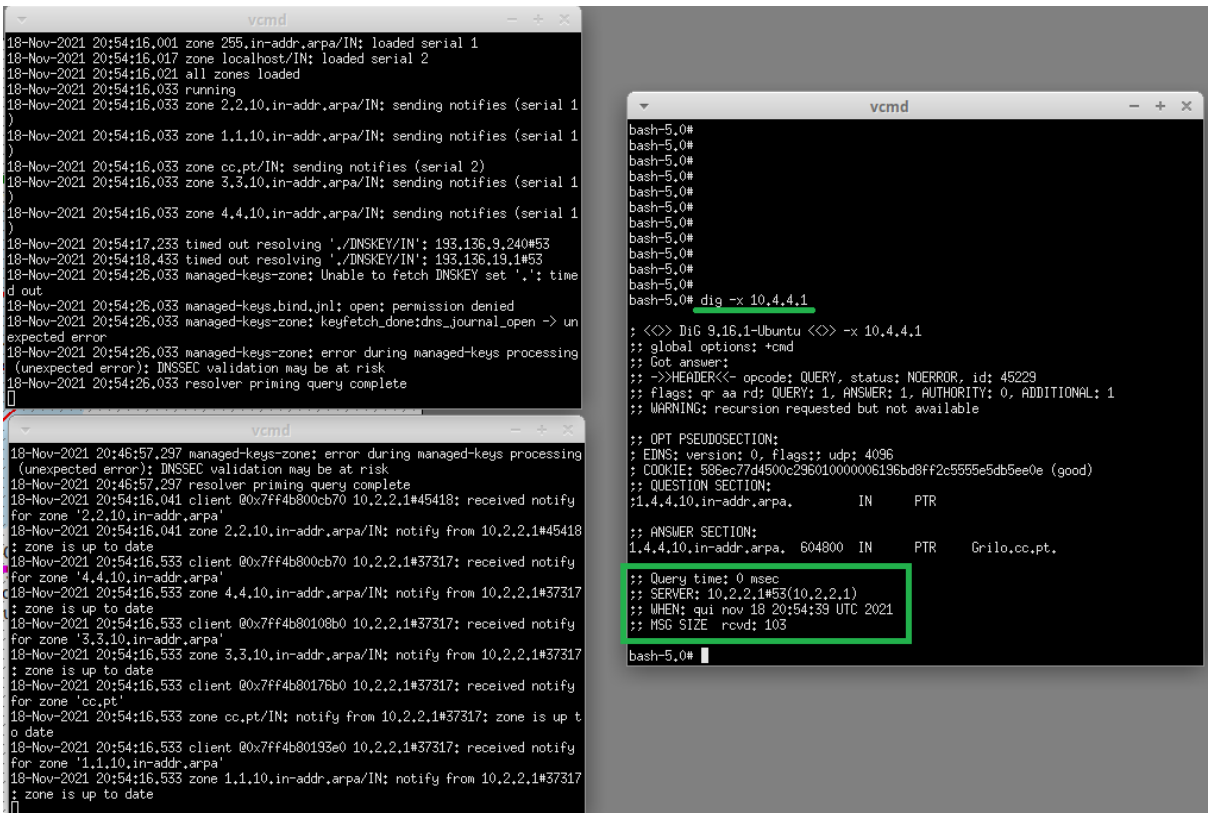
14. Ping para "www.cc.pt." com ambos os servidores a correr



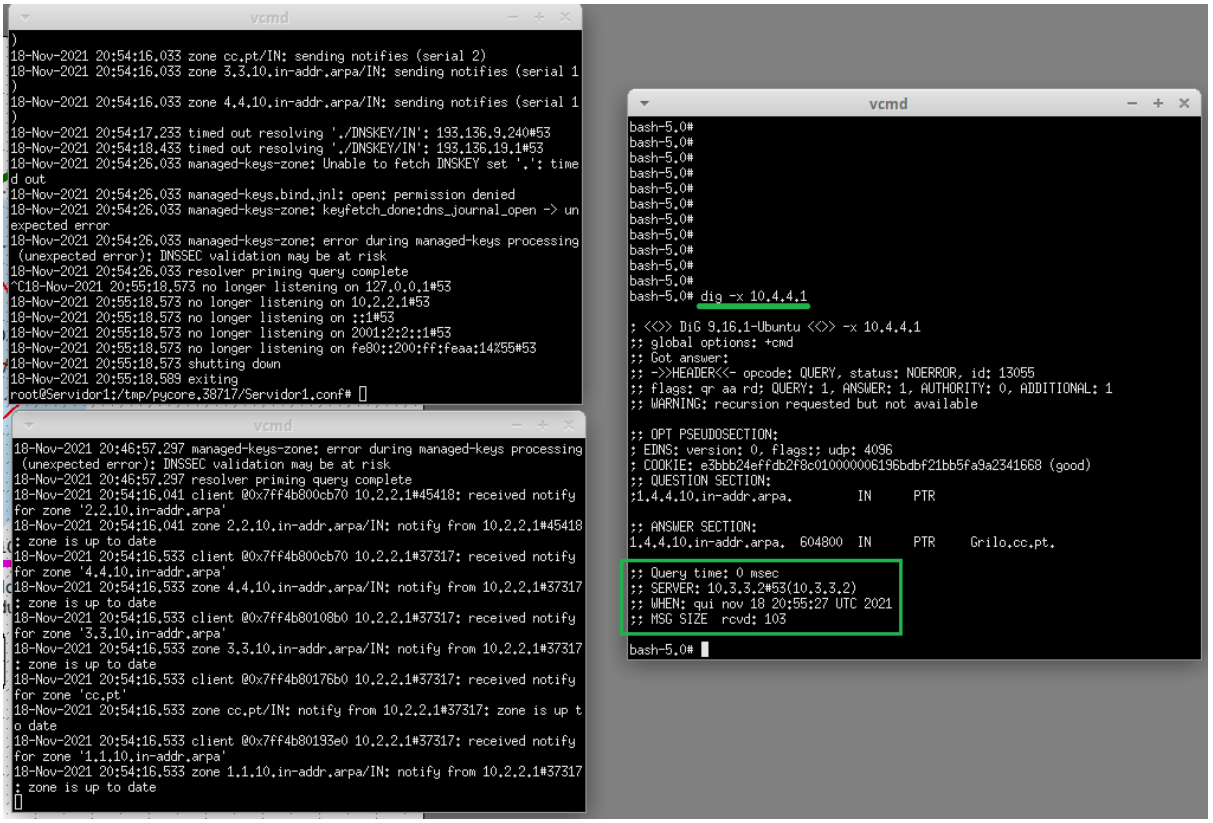
15. Dig para o domínio "cc.pt." com apenas o servidor secundário a correr



16. Ping para "www.cc.pt." apenas o servidor secundário a correr



17. Query inversa para um endereço da topologia com ambos os servidores a correr



18. Query inversa para um endereço da topologia com apenas o servidor secundário a correr

Parte III

Conclusão

O serviço de resolução de nomes (DNS) é essencial para o normal funcionamento da *world wide web*. Demonstra-se como sendo um serviço complexo e minucioso, pois requer uma série de configurações de modo a garantir a sua total operabilidade. Dado por concluído, este trabalho permite-nos agora compreender os conceitos de *nameserver*, *host*, domínio, servidores primários e secundários, TLD (*top level domains*), entre outros, bem como visualizar a árvore de resolução de nomes.