

Universidade do Minho
Mestrado Integrado em Engenharia Informática
3ºano - 2º Semestre

Comunicações por Computador

Trabalho Prático Nº.3 – Serviço de Resolução de Nomes (DNS)

Grupo 1 - PL4



a83732 – Gonçalo Rodrigues Pinto
a84197 – João Pedro Araújo Parente
a84829 – José Nuno Martins da Costa

15 de Abril de 2020

Conteúdo

1	Introdução	3
2	Questões e Respostas	3
2.1	Consultas ao serviço de nomes DNS	3
2.2	Instalação, configuração e teste de um domínio CC.PT	9
2.2.1	Configuração do servidor primário	9
2.2.2	Configuração do cliente e teste do primário	11
2.2.3	Configuração do servidor secundário	13
3	Conclusão	14

Lista de Figuras

1	Endereço IPv6 dos servidores <code>www.sapo.pt</code>	3
2	Endereço IPv6 dos servidores <code>www.yahoo.com</code>	3
3	Servidores de nomes definidos para os diferentes domínios. . .	4
4	Verificação do domínio <code>nice.software</code>	5
5	Verificação servidor DNS primário definido para o domínio <code>msf.org</code>	5
6	Obtenção de uma resposta “autoritativa”.	6
7	Localização onde as mensagens de correio electrónico dirigidas aos presidentes são entregues.	6
8	Informações obtidas acerca de <code>whitehouse.gov</code>	7
9	Endereço IPv6 <code>2001:690:a00:1036:1113::247</code>	7
10	Ficheiro de dados do domínio de nomes: <code>primario/db.cc.pt</code> . .	10
11	Ficheiro de dados do(s) domínio(s) de reverse: <code>primario/db.3- 3-10.rev</code>	10
12	Teste simples com <code>nslookup</code> , fora do emulador.	11
13	Query ao servidor primário com o intuito de encontrar o en- dereço <code>www.cc.pt</code> , sem sucesso.	11
14	Query ao servidor primário com o intuito de encontrar o en- dereço <code>www.cc.pt</code> , após alterar o <code>/etc/resolv.conf</code>	12
15	Ficheiro <code>secundario/named.conf</code> com a indicação das zonas. . .	13
16	Query ao servidor secundário com o intuito de encontrar o endereço <code>www.cc.pt</code>	13

1 Introdução

O objectivo deste trabalho foi estudar o Serviço de Resolução de Nomes (DNS).

O objectivo do serviço de resolução de nomes é fazer a associação entre várias informações atribuídas a nomes de domínios e cada entidade participante. A sua utilização mais convencional associa nomes de domínios mais facilmente memorizáveis a endereços IP numéricos, necessários à localização e identificação de serviços e dispositivos, processo esse denominado por: resolução de nome.

2 Questões e Respostas

2.1 Consultas ao serviço de nomes DNS

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

R: O ficheiro */etc/resolv.conf* contém informação que determina os parâmetros operacionais dos servidores DNS. Estes servidores permitem que as aplicações que correm no sistema operativo traduzam nomes de domínios para endereços IP, que são necessários para aceder a recursos de uma área local ou Internet.

- (b) **Os servidores *www.sapo.pt.* e *www.yahoo.com.* têm endereços IPv6? Se sim, quais**

R: Os servidores *www.sapo.pt.* e *www.yahoo.com.* possuem endereços IPv6, os mesmos encontram-se presentes na figura 1 e 2, respectivamente.

```
goncalo@goncalo-K401UQK ~ $ nslookup
> set q=AAAA
> www.sapo.pt
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
www.sapo.pt  has AAAA address 2001:8a0:2102:c:213:13:146:142
```

Figura 1: Endereço IPv6 dos servidores *www.sapo.pt.*

```
goncalo@goncalo-K401UQK ~ $ nslookup
> set q=AAAA
> www.sapo.pt
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
www.sapo.pt  has AAAA address 2001:8a0:2102:c:213:13:146:142
```

Figura 2: Endereço IPv6 dos servidores *www.yahoo.com.*

- (c) Quais os servidores de nomes definidos para os domínios: “uminho.pt.”, “pt.” e “.”?

R: Os servidores de nomes definidos para os domínios ”uminho.pt” são ns02.fccn.pt., dns3.uminho.pt., dns.uminho.pt. e dns2.uminho.pt. Os servidores de nomes definidos para ”pt.” são a.dns.pt., b.dns.pt., c.dns.pt., d.dns.pt., e.dns.pt., f.dns.pt., g.dns.pt., h.dns.pt., ns.dns.br. e ns2.nic.fr.. Os servidores de nomes definidos para ”.” são a.root-servers.net., b.root-servers.net., c.root-servers.net., d.root-servers.net., e.root-servers.net., f.root-servers.net., g.root-servers.net., h.root-servers.net., i.root-servers.net., j.root-servers.net., k.root-servers.net., l.root-servers.net. e m.root-servers.net..

```
goncalo@goncalo-K401UQK ~ $ nslookup
> set q=NS
> uminho.pt
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
uminho.pt    nameserver = dns.uminho.pt.
uminho.pt    nameserver = dns3.uminho.pt.
uminho.pt    nameserver = ns02.fccn.pt.
uminho.pt    nameserver = dns2.uminho.pt.

Authoritative answers can be found from:
> pt.
Server:      127.0.1.1
Address:     127.0.1.1#53

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

Authoritative answers can be found from:
> .
Server:      127.0.1.1
Address:     127.0.1.1#53

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

Authoritative answers can be found from:
```

Figura 3: Servidores de nomes definidos para os diferentes domínios.

- (d) **Existe o domínio nice.software.? Será que nice.software. é um host ou um domínio?**

R: O domínio nice.software. existe porque têm name servers e este é um host porque possui um endereço IP. Chegou-se a esta conclusão usando nslookup estabelecendo querytypes para especificar um servidor de nomes DNS para a zona nomeada (set q=NS) e para especificar o endereço IP de um computador (set q=A).

```
goncalo@goncalo-K401UQK ~ $ nslookup
> set q=NS
> nice.software.
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
nice.software nameserver = nsqbr.comlaude.co.uk.
nice.software nameserver = nssui.comlaude.ch.
nice.software nameserver = nsusa.comlaude.net.

Authoritative answers can be found from:
> set q=A
> nice.software.
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
Name:   nice.software
Address: 213.212.81.71
```

Figura 4: Verificação do domínio nice.software.

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

R: O servidor DNS primário definido para o domínio msf.org é ns1.dds.nl. Este servidor primário (master) não consegue fazer queries recursivas pois não consegue alcançar outros domínios. Como se pode observar na figura abaixo onde obteve-se "Connection timed out".

```
goncalo@goncalo-K401UQK ~ $ nslookup
> set q=NS
> msf.org
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
msf.org nameserver = ns1.dds.nl.
msf.org nameserver = ns4.dds-city.com.
msf.org nameserver = ns2.dds.eu.
msf.org nameserver = ns3.dds.amsterdam.

Authoritative answers can be found from:
> server ns1.dds.nl.
Default server: ns1.dds.nl.
Address: 91.142.253.70#53
> uminho.pt
;; connection timed out; no servers could be reached
```

Figura 5: Verificação servidor DNS primário definido para o domínio msf.org..

- (f) **Obtenha uma resposta “autoritativa” para a questão anterior.**

R: Para simplificar, incluímos a imagem apresentada abaixo que ilustra de forma clara a resposta “autoritativa” obtida através nslookup estabelecendo querytype que permite especificar o início da autoridade para uma zona DNS (set q=SOA).

```
goncalo@goncalo-K401UQK ~ $ nslookup
> set q=SOA
> msf.org.
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
msf.org
  origin = ns1.dds.nl
  mail addr = postmaster.msf.org
  serial = 1407464621
  refresh = 16384
  retry = 2048
  expire = 1048576
  minimum = 2560

Authoritative answers can be found from:
```

Figura 6: Obtenção de uma resposta “autoritativa”.

- (g) **Onde são entregues as mensagens de correio electrónico dirigidas aos presidentes marcelo@presidencia.pt e bolsonaro@casacivil.gov.br?**

R: As mensagens de correio electrónico dirigidas para o presidente marcelo@presidencia.pt são enviadas para mail1.presidencia.pt. ou para mail2.presidencia.pt. enquanto as do presidente bolsonaro@casacivil.gov.br são enviadas para esa02.presidencia.gov.br. ou para esa01.presidencia.gov.br..

```
goncalo@goncalo-K401UQK ~ $ nslookup
> set q=MX
> presidencia.pt
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
presidencia.pt mail exchanger = 10 mail2.presidencia.pt.
presidencia.pt mail exchanger = 50 mail1.presidencia.pt.

Authoritative answers can be found from:
> casacivil.gov.br.
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
casacivil.gov.br mail exchanger = 10 esa02.presidencia.gov.br.
casacivil.gov.br mail exchanger = 5 esa01.presidencia.gov.br.

Authoritative answers can be found from:
```

Figura 7: Localização onde as mensagens de correio electrónico dirigidas aos presidentes são entregues.

- (h) **Que informação é possível obter, via DNS, acerca de whitehouse.gov?**

R: A informação obtida, via DNS, acerca de whitehouse.gov foi o endereço primário, os mail address e os nome de servidores.

```
goncalo@goncalo-K401U0K ~ $ nslookup
> set q=SOA
> whitehouse.gov
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
whitehouse.gov
  origin = 399e-adcs001.ede.pitc.gov
  mail addr = postmaster.whitehouse.gov
  serial = 2017022363
  refresh = 300
  retry = 300
  expire = 604800
  minimum = 300

Authoritative answers can be found from:
```

Figura 8: Informações obtidas acerca de whitehouse.gov..

- (i) **Consegue interrogar o DNS sobre o endereço IPv6 2001:690:a00:1036:1113::247 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?**

R: Utilizando algum dos clientes DNS foi possível interrogar o DNS sobre o endereço IPv6 2001:690:a00:1036:1113::247 desta forma foi possível obter algumas informações tal como o nome do domínio do qual este endereço encontra-se à responsabilidade, neste caso é fccn.pt o responsável. Supondo que existe problemas com esse endereço é possível obter contacto do responsável por esse IPv6 para obter tal executou-se o comando 'host' com a flag 'SOA' que pode ser observado na figura abaixo, onde concluímos que o contacto do responsável é hostmaster@fccn.pt tendo chegado a esta conclusão depois de observar a norma RFC 1035.

```
goncalo@goncalo-K401U0K ~ $ nslookup 2001:690:a00:1036:1113::247
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
7.4.2.0.0.0.0.0.0.0.0.0.3.1.1.6.3.0.1.0.0.a.0.0.9.6.0.1.0.0.2.ip6.arpa      name = www.fccn.pt.

Authoritative answers can be found from:

goncalo@goncalo-K401U0K ~ $ host -t SOA fccn.pt
fccn.pt has SOA record ns01.fccn.pt. hostmaster.fccn.pt. 2020040103 21600 7200 1209600 14400
```

Figura 9: Endereço IPv6 2001:690:a00:1036:1113::247

- (j) **Os secundários usam um mecanismo designado por “Transferência de zona” para se actualizarem automaticamente a partir do primário, usando os parâmetros definidos no Record do tipo SOA do domínio. Descrever sucintamente o mecanismo com base num exemplo concreto.**

R: Por exemplo, quando tentamos conectar ao site di.uminho.pt, o nosso sistema tenta primeiro converter a URL amigável introduzido num endereço IP no servidor DNS primário. Se este servidor falhar ou estiver em manutenção, ele vai tentar no DNS secundário. Se o secundário também não contiver o endereço IP do servidor do site que estamos a tentar aceder, então obtemos uma mensagem de erro no nosso navegador. Para evitar estas mensagens é necessário efectuar transferências de zonas para evitar estas falhas.

Numa forma resumida um servidor DNS primário possui a “cópia principal” de uma zona e os servidores DNS secundários mantêm cópias da zona para redundância. Quando são feitas alterações nos dados da zona no servidor DNS primário, essas alterações são distribuídas aos servidores DNS secundários da zona, isso é feito através de transferências de zona.

A maioria dos servidores primários DNS notificam automaticamente os servidores secundários sempre que ocorram alterações, estas são feitas por meio de uma solicitação NOTIFY, e a maioria dos servidores secundários DNS solicitam uma transferência de zona sempre que uma notificação é recebida. Contudo, os servidores secundários também verificam periodicamente as alterações consultando o servidor primário para o registo SOA da zona e verificam o número de série. Além de quaisquer outras alterações feitas numa zona e nos seus registos, o número de série do registo SOA deve ser sempre incrementado. A pesquisa periódica pelos servidores secundários é controlada pelos parâmetros de actualização, de novas tentativas e de finalização do registo SOA. O servidor secundário aguarda pelo intervalo de “actualização” antes de verificar com o primário um novo número de série. Se essa verificação não puder ser concluída, novas verificações serão iniciadas a cada intervalo de “novas tentativas”. Se o secundário achar impossível executar uma verificação sequencial dentro do intervalo “expirado”, ele descarta a zona. Quando a pesquisa mostra que a zona foi alterada, o servidor secundário executa uma nova cópia da zona por meio de uma solicitação de transferência de zona. Uma transferência de zona padrão (completa) transfere todos os registos da zona do servidor primário para o secundário.

2.2 Instalação, configuração e teste de um domínio CC.PT

Pretendeu-se criar um domínio CC.PT para a topologia de rede que estamos a usar nas aulas práticas, de modo a que se possam usar os nomes em vez dos endereços IP. No final desta fase o objectivo será, por exemplo, poder fazer-se “ping Serv1.cc.pt” ou mesmo apenas “ping Serv1” ou “ping Serv1.cc.pt.” em vez de “ping 10.3.3.1”. Para atingir esse fim, foi necessário executar alguns preparativos no ambiente CORE tais como replicar ficheiros de configuração, parar o servidor DNS pré-instalado e reconfigurar apparmor para permitir que /usr/sbin/named aceda a ficheiros noutros locais.

2.2.1 Configuração do servidor primário

As configurações executadas respeitaram algumas regras, como por exemplo os dados do domínio cc.pt devem ser editados/mantidos no ficheiro db.cc.pt, os dados do domínio reverse 3.3.10.in-addr.arpa. relativos à rede 10.3.3.0/24 devem ser editados/mantidos no ficheiro db.3-3-10.rev (aplicar sempre o mesmo critério de nomes a outros domínios reversos que decida incluir), entre outras. Após a edição de alguns ficheiros importantes para incluir os registos do primário e secundário para que os servidores DNS se identifiquem correctamente a si próprios, os servidores do DI como forwarders tal como a inclusão de novas zonas, criou-se o ficheiro de dados do domínio de nomes: primario/db.cc.pt como também o ficheiro de dados do(s) domínio(s) de reverse: primario/db.3-3-10.rev

```

$TTL 604800
@      IN      SOA      dns.cc.pt.      grupo01.cc.pt. (
                        2              ;Serial
                        604800         ;Refresh
                        86400          ;Retry
                        2419200        ;Expire
                        604800)        ;Negative Cache TTL

@      IN      NS      dns.cc.pt.
@      IN      NS      dns2.cc.pt.
@      IN      MX      10 mail.cc.pt.
@      IN      MX      10 mail2.cc.pt.

mail   IN      A      10.3.3.3
www    IN      A      10.3.3.3
dns2   IN      A      10.4.4.1
dns    IN      A      10.3.3.1
mail2  IN      A      10.3.3.2

```

Figura 10: Ficheiro de dados do domínio de nomes: primario/db.cc.pt

```

$TTL      604800
@      IN      SOA      dns1.example.com.  hostmaster.example.com. (
                        4555127         ; Serial
                        604800          ; Refresh
                        86400           ; Retry
                        2419200         ; Expire
                        604800)         ; Negative Cache TTL

@      IN      NS      dns1.cc.pt.

1      IN      PTR      dns.cc.pt.
2      IN      PTR      dns2.cc.pt.

3      IN      PTR      Portatil1.cc.pt.
4      IN      PTR      Hermes.cc.pt.
5      IN      PTR      Atena.cc.pt.
6      IN      PTR      Zeus.cc.pt

7      IN      PTR      Grupo01.cc.pt.

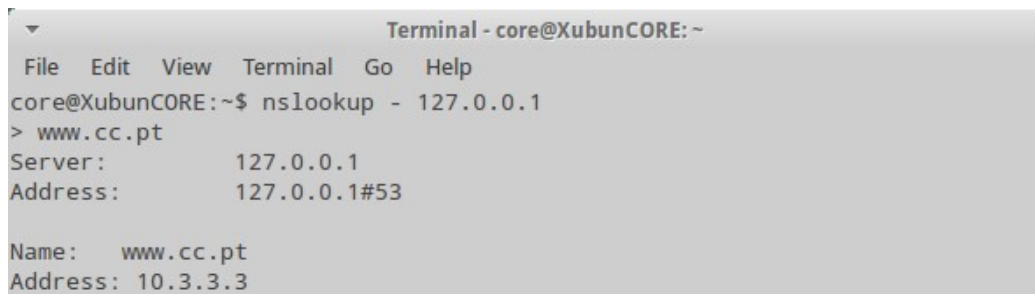
```

Figura 11: Ficheiro de dados do(s) domínio(s) de reverse: primario/db.3-3-10.rev

Por fim, testou-se as configurações e os ficheiros de dados com auxílio de algumas ferramentas e executou-se o servidor, na linha de comando.

2.2.2 Configuração do cliente e teste do primário

Após efectuar um teste simples com nslookup, fora do emulador CORE, repetiu-se os testes iniciando o CORE com a topologia **CC-Topo-2020.imn** após executar o comando fornecido (*sudo /usr/sbin/named -c /home/core/-primario/named.conf -g*) de arranque do servidor no nó "**Serv1**", abriu-se uma bash no nó "**Portatil1**" a testar uma query (*nslookup - 10.3.3.1*) ao servidor primário contudo não foi encontrar o endereço *www.cc.pt*, figura 13. De forma a resolver este problema foi sugerido modificar o */etc/resolv.conf* (editando fora do CORE) alterando/acrescentando informação (*nameserver 10.3.3.1 ; domain cc.pt ; search cc.pt*) e testar de novo com nslookup ou dig, obtendo o resultado presente na figura 14.



```
Terminal - core@XubunCORE: ~
File Edit View Terminal Go Help
core@XubunCORE:~$ nslookup - 127.0.0.1
> www.cc.pt
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   www.cc.pt
Address: 10.3.3.3
```

Figura 12: Teste simples com nslookup, fora do emulador.



```
> www.cc.pt
Server:          10.3.3.1
Address:         10.3.3.1#53

** server can't find www.cc.pt: NXDOMAIN
```

Figura 13: Query ao servidor primário com o intuito de encontrar o endereço *www.cc.pt*, sem sucesso.

```

> ^Croot@Portatil1:/tmp/pycore.57771/Portatil1.conf# nslookup www.cc.pt
Server:      10.3.3.1
Address:     10.3.3.1#53

Name:   www.cc.pt
Address: 10.3.3.3

root@Portatil1:/tmp/pycore.57771/Portatil1.conf# dig www.cc.pt

;; <>> DiG 9.8.1-P1 <>> www.cc.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11498
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
www.cc.pt.                 604800  IN      A      10.3.3.3

;; AUTHORITY SECTION:
cc.pt.                     604800  IN      NS      dns.cc.pt.
cc.pt.                     604800  IN      NS      dns2.cc.pt.

;; ADDITIONAL SECTION:
dns.cc.pt.                 604800  IN      A      10.3.3.1
dns2.cc.pt.                604800  IN      A      10.4.4.1

;; Query time: 7 msec
;; SERVER: 10.3.3.1#53(10.3.3.1)
;; WHEN: Thu Apr  9 16:32:25 2020
;; MSG SIZE  rcvd: 112

```

Figura 14: Query ao servidor primário com o intuito de encontrar o endereço www.cc.pt, após alterar o /etc/resolv.conf.

2.2.3 Configuração do servidor secundário

Por fim após editar o ficheiro *secundario/named.conf.options* por forma a incluir os servidores 193.136.9.240 e 193.136.19.1 (servidores do DI) como forwarders como também o ficheiro *secundario/named.conf* para incluir a indicação das novas zonas “cc.pt”, “3.3.10.inaddr.arpa” mas desta vez apenas como zonas do tipo “slave”.

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "cc.pt"{
    type slave;
    file "/var/cache/bind/db.cc.pt";
    masters { 10.3.3.1; };
};

zone "3.3.10.in-addr.arpa"{
    type slave;
    file "/var/cache/bind/db.3-3-10.rev";
    masters { 10.3.3.1; };
};
```

Figura 15: Ficheiro *secundario/named.conf* com a indicação das zonas.

Testou-se as configurações e os ficheiros de dados com auxílio de algumas ferramentas para verificar a configuração. Executando o core e abriu-se a bash no nó **Hermes**, executando o servidor, na linha de comando, fazendo: *sudo /usr/sbin/named -c /home/core/secundario/named.conf -g .* Consequentemente executou-se um teste simples com *nslookup* num nó arbitrário neste caso foi o Portátil 1.

```
root@Portatil1:/tmp/pycore.53281/Portatil1.conf# nslookup - 10.4.4.1
> www.cc.pt.
Server:      10.4.4.1
Address:     10.4.4.1#53

Name:   www.cc.pt
Address: 10.3.3.3
```

Figura 16: Query ao servidor secundário com o intuito de encontrar o endereço *www.cc.pt*.

3 Conclusão

O presente relatório descreveu, de forma sucinta, a resolução das questões propostas utilizando os softwares disponibilizados pelos docentes.

Após a realização deste trabalho, ficamos conscientes dos vários aspectos do Serviço de Resolução de Nomes (DNS).

Consideramos que os principais objectivos foram cumpridos.

Sentimos que a realização deste trabalho prático consolidou os nossos conhecimentos em relação ao Serviço de Resolução de Nomes (DNS).