UNIVERSIDADE D
COIMBRA

Trabalho 1

Configuração de DHCP e DNS

Duarte Manuel Bento Dias 2018293526
André Pinto Dias 2020209083

Índice

Motivação

O presente trabalho, realizado no âmbito da cadeira de Gestão de Infraestruturas e Serviços na Internet tem como objetivo a configuração dos serviços DHCP e DNS Protocolo DHCP.

Introdução teórica

DHCP

O *Dynamic Host Configuration Protocol* (DHCP) é um protocolo cliente/servidor que fornece automaticamente um conjunto de configurações (ip, dns, gateways, máscara de sub-rede, etc). Sem a existência de DHCP, um novo computador na rede teria de configurar o seu IP manualmente, correndo ainda o risco de existir um "choque" com outro dispositivo (se ambos tivessem o mesmo IP).
Este protocolo permite assim ter uma mais facilitada gestão dos endereços de rede. Para executar a atribuição automática das configurações, o DHCP segue a metodologia presente tanto abaixo como na Figura 1.

1. O cliente envia uma mensagem de broadcast, para a rede, solicitando um endereço IP.
2. O servidor presente na rede envia uma mensagem indicando o IP disponível (se existente).
3. O cliente aceita (ou não) o IP atribuído.
4. O servidor dhcp confirma o novo IP atribuído ao cliente.

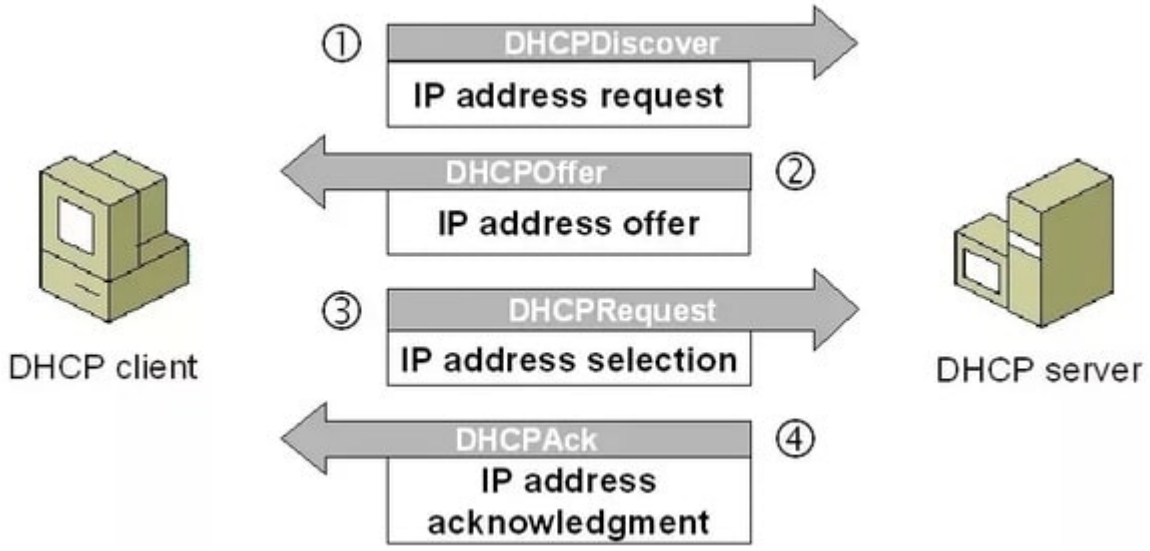

Fig. 1 Exemplo de um DHCP "Handshake"

Protocolo DNS

O Protocolo *Domain Name System* (DNS) serve como uma espécie de "páginas amarelas" da Internet. Assim sendo, o protocolo tem como função traduzir nomes (www.google.pt) em endereços IP (142.250.184.3).
De forma a tornar o DNS eficiente e resistente a ataques, o protocolo é baseado num sistema de delegação "loosely-coupled", no qual os diversos servidores, delegam informação aos ramos mais abaixo na árvore, de modo chegar a um determinado endereço. Esta informação é depois transmitida ao cliente.

O protocolo DNS é vital para o funcionamento da internet dado que o ser humano tem uma maior facilidade a recordar-se de nomes ao invés de sequências de números.

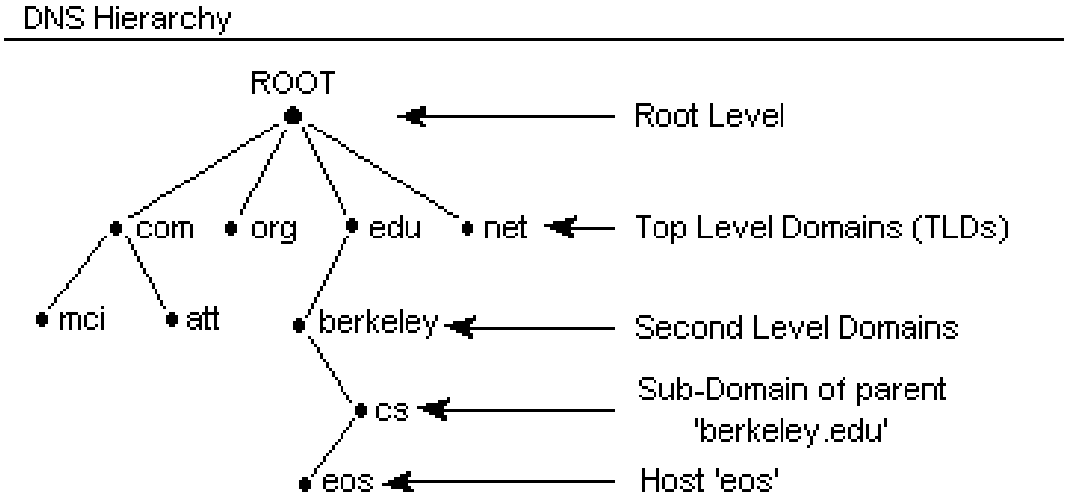

Fig. 2 Hierarquia de DNS

Topologia de rede

Para a realização deste trabalho prático, foi usada a topologia, apresentada na figura abaixo.

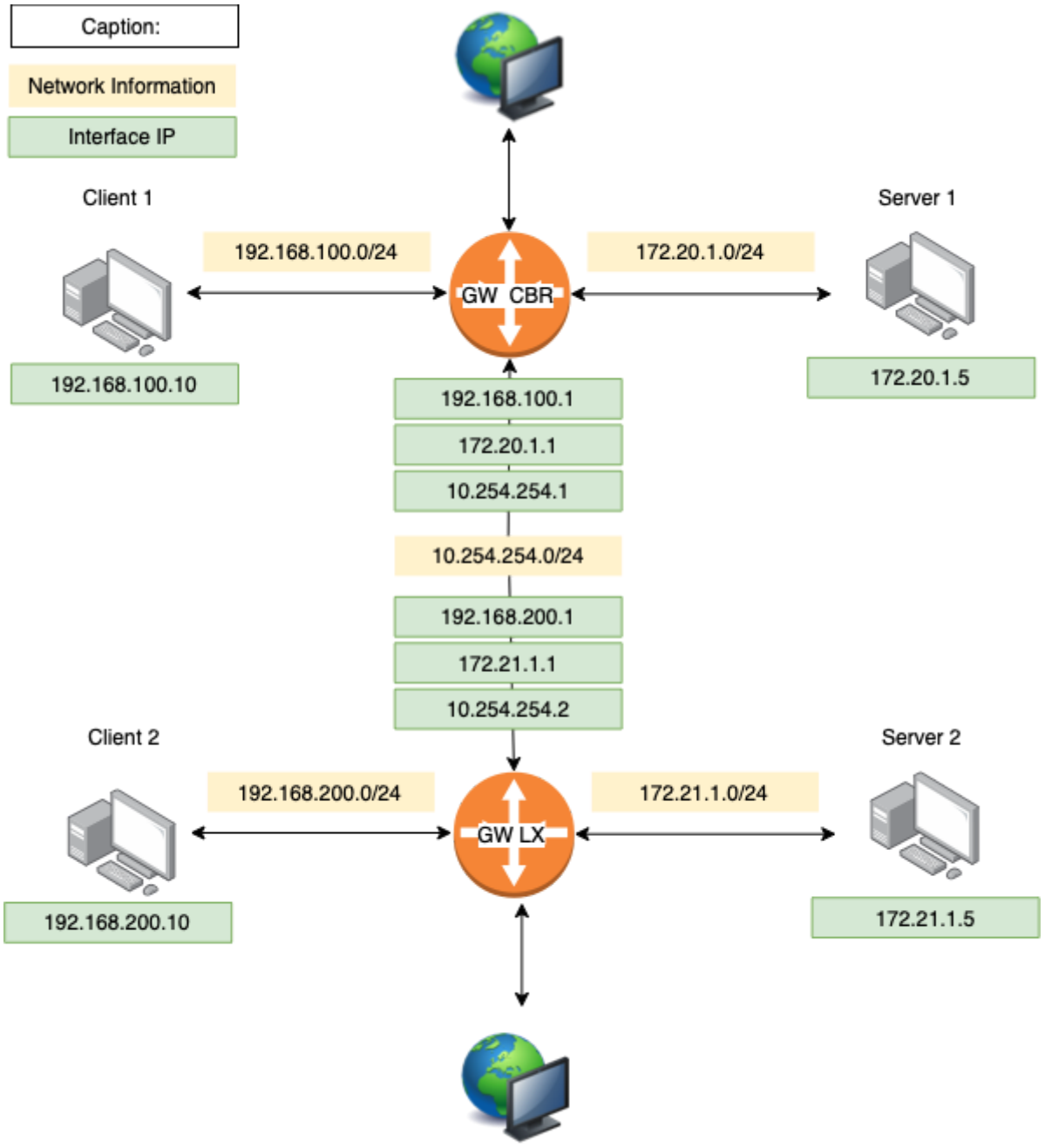

Fig. 3 Topologia de Rede

Configuração de Encaminhamento

O primeiro passo na montagem do sistema é garantir que existe comunicação entre entre quaisquer 2 pontos da rede interna. Neste caso, basta garantir que existem rotas nos 2 gateways principais (GW CBR, GW LX).
Dado que o sistema operativo, por defeito, não deixa fazer o forwarding dos pacotes de rede, ativa-se essa opção, usando o seguinte comando:

```
sysctl -w net.ipv4.ip_forward=1
```

Snip. 1 Encaminhamento

Após esta alteração é necessário configurar as rotas. De forma a tornar estas rotas permanentes, procedeu-se à alteração do ficheiro /etc/network/interfaces:

```
# File /etc/network/interfaces in machine - GW CGR
The primary network interface
allow-hotplug ens160
auto ens160
iface ens160 inet dhcp
        # NAT for all networks (MASQUERADE)
        post-up iptables -t nat -A POSTROUTING -o ens160 -j
MASQUERADE

auto ens193
iface ens193 inet static
        address 10.254.254.1
        netmask 255.255.255.0
        # Route 192.168.200.0/24 network via GW2
        up route add -net 192.168.200.0 netmask 255.255.255.0 gw
10.254.254.2
        # Route 172.21.1.0/24 network via GW2
        up route add -net 172.21.1.0 netmask 255.255.255.0 gw
10.254.254.2
```

Snip. 2 Interface Config

Podemos ver 2 comandos principais, o “post-up (...)” presente na interface ens160, que garante a chegada dos pacotes externos à rede à internet.
O segundo comando, up “route (...)”, estabelece as rotas para os pacotes da rede direcionados à rede de Lisboa usando a interface de rede do gateway de Lisboa.
A configuração para o gateway de Lisboa é análoga, sendo apenas feitas as mudanças necessárias para garantir o routing Lisboa - Coimbra.
Na Figura 4 e Figura 5 podemos visualizar as comunicações entre os clientes de Coimbra e de Lisboa.

```
tldart@client1:~$ traceroute 172.21.1.5
traceroute to 172.21.1.5 (172.21.1.5), 30 hops max, 60 byte packets
 1  192.168.100.1 (192.168.100.1)  2.155 ms  2.031 ms  1.976 ms
 2  10.254.254.2 (10.254.254.2)  7.150 ms  7.095 ms  6.996 ms
 3  mx.lx.gisi.pt (172.21.1.5)  10.484 ms  10.381 ms  10.304 ms
```

Fig. 4 Rota Client CBR - Server LX

```
tldart@client2:~$ traceroute 172.20.1.5
traceroute to 172.20.1.5 (172.20.1.5), 30 hops max, 60 byte packets
 1  192.168.200.1 (192.168.200.1)  4.736 ms  4.678 ms  4.641 ms
 2  10.254.254.1 (10.254.254.1)  10.812 ms  10.778 ms  10.616 ms
 3  mx.cbr.gisi.pt (172.20.1.5)  14.699 ms  14.641 ms  14.401 ms
```

Fig. 5 Rota Client LX - Server CBR

Configuração do DHCP

Havendo uma rota estática presente, trata-se agora da atribuição de IPs.
Em ambas as redes existe uma componente estática e uma componente dinâmica.
Um exemplo de configuração fica abaixo:

```
# File /etc/dhcpd/dhcpd.conf in machine - GW CGR
option domain-name "cbr.gisi.pt";
option domain-name-servers 10.254.254.1, 10.254.254.2;

default-lease-time 21600; # 6Hrs
max-lease-time 21600;
min-lease-time 21600;

ddns-update-style none;

subnet 192.168.100.0 netmask 255.255.255.0 {
        option dhcp-renewal-time 14400; # 4Hrs
        option routers 192.168.100.1;
        option subnet-mask 255.255.255.0;
        range 192.168.100.10 192.168.100.100;
}

subnet 172.20.1.0 netmask 255.255.255.0 {
        option dhcp-renewal-time 14400;
        option routers 172.20.1.1;
        option subnet-mask 255.255.255.0;
        range 172.20.1.10 172.20.1.100;
}
```

```
host mail-server{
        option host-name "mail-server.cbr.gisi.pt"; #static ip for
the mail server
        option routers 172.20.1.1;
        hardware ethernet 00:0c:29:8c:8d:52;
        fixed-address 172.20.1.5;
}
```

Snip. 3 DHCP config

Denote-se que a lease time definida foi escolhida com os parâmetros do enunciado (validade 6 horas, renovação 4 horas). A escolha do IPs de name server escolheu-se por convenção já qualquer NIC daquela máquina serviria.

Analogamente existe uma configuração, usando as redes apropriadas, para a sub-rede LX.

Na Figura 6 e Figura 7 podemos ver o processo de atribuição de IP´s, para as diferentes redes, como inicialmente explicado na Figura 1.

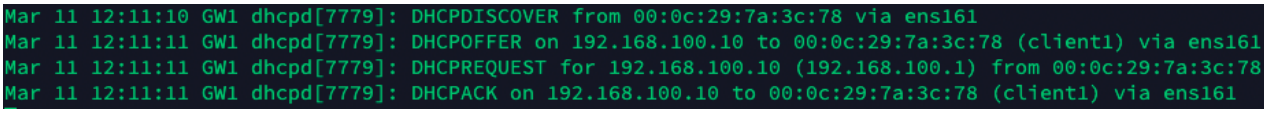

Fig. 6 DHCP Client CBR

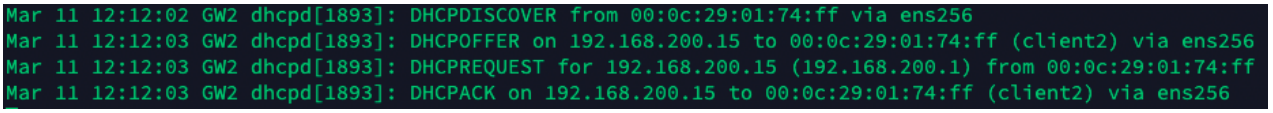

Fig. 7 DHCP Client LX

Autenticação segura sem Password

De forma a fazer a ligação às outras máquinas da rede sem necessidade de password, fez uso da tecnologia *secure passwordless authentication.* É apenas necessário gerar um par de chaves no host (que no nosso caso é o servidor de coimbra) e depois fazer passar essa chave para as restantes máquinas.

```
ssh-keygen -t rsa
```

Snip. 4 Criação de chave privada

Depois de gerada a chave, esta foi enviada para a(s) respectiva(s) maquinas destino.

```
ssh-copy-id tldart@10.254.254.2
```

Snip. 5 Envio de chave por SSH

Após isso, ao estabelecermos uma sessão SSH às máquinas já não é necessário introduzir a password.

```
tldart@GW1:~$ ssh tldart@10.254.254.2
Linux GW2 5.10.0-11-arm64 #1 SMP Debian 5.10.92-1 (2022-01-18) aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 11 11:42:13 2022 from 172.16.121.1
```

Fig. 8 SSH Passwordless Authentication

Configuração do DNS

Por fim, configurou-se o DNS. O enunciado refere a criação de zonas de DNS, gisi.pt, cbr.gisi.pt e lx.gisi.pt. Assim sendo utilizou-se o utilitário bind9 e procedeu-se à configuração das seguintes zonas:

```
# File /etc/bind9/named.local.conf in machine - GW CGR
zone "gisi.pt" IN {
        type master;
        file "/etc/bind/gisi.db";
        allow-transfer {10.254.254.2;};
```

```
};

zone "cbr.gisi.pt" IN{
        type master;
        file "/etc/bind/gisi_cbr.db";
        allow-transfer {10.254.254.2;};
};

zone "lx.gisi.pt" IN{
        type master;
        file "/etc/bind/gisi_lx.db";
        allow-transfer {10.254.254.2;};
};

zone "1.20.172.in-addr.arpa." IN{
        type master;
        file "/etc/bind/cbr1_rev.db";
        allow-transfer {10.254.254.2;};
};

zone "100.168.192.in-addr.arpa." IN{
        type master;
        file "/etc/bind/cbr2_rev.db";
        allow-transfer {10.254.254.2;};
};

zone "1.21.172.in-addr.arpa." IN{
        type master;
        file "/etc/bind/lx1_rev.db";
        allow-transfer {10.254.254.2;};
};

zone "200.168.192.in-addr.arpa." IN{
        type master;
        file "/etc/bind/lx2_rev.db";
        allow-transfer {10.254.254.2;};
};
```

Snip. 6 Configuração de zonas

De entre as configurações aplicadas denote-se:

- Existe um balanceamento de carga entre os servidores de email, denotado pelo mesmo valor de prioridade. (Snip. 7)

- São aplicados vários CNAME records quando necessário (ao invés de repetir definições).(Snip. 7)
- Como de momento as maquinas mail.lx.gisi.pt e mail.cbr.gisi.pt nao existem, estas foram configuradas com IPs "*dummy*", para não coexistirem com os respectivos IPs de mx.lx.gisi.pt e mx.cbr.gisi.pt. (Snip. 7)
- Atribuíram-se 3 IPs na gama de rede DHCP sendo estes limitados pela atribuição dinâmica de IPs do DHCP (Snip. 8)

```
# File /etc/bind/gisi.db in machine - GW CGR (ONLY PART OF THE
FILE)
$TTL    604800
@       IN      SOA     dns1.gisi.pt. webmaster.gisi.pt. (
                         2022031100     ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
                IN      NS      dns1
                IN      MX      10      mx.cbr
                IN      MX      10      mx.lx


dns1            IN      A       10.254.254.1
ssh             IN      CNAME   dns1

web             IN      CNAME   web.lx
ftp             IN      CNAME   web.lx
web.lx          IN      A       8.8.8.8 #Dummy IP
```

Snip. 7 Ficheiro DNS da zona gisi.pt

```
# File /etc/bind/cbr1_rev.db in machine - GW CGR (ONLY PART OF THE
FILE)
10      IN      PTR      dhcp4.cbr.gisi.pt.
11      IN      PTR      dhcp5.cbr.gisi.pt.
12      IN      PTR      dhcp6.cbr.gisi.pt.
```

Snip. 8 Ficheiro DNS da zona cbr.gisi.pt

```
tldart@client1:~$ nslookup mx.lx.gisi.pt
Server:         10.254.254.1
Address:        10.254.254.1#53

Name:   mx.lx.gisi.pt
Address: 172.21.1.5
```

Fig. 9 Funcionamento do DNS

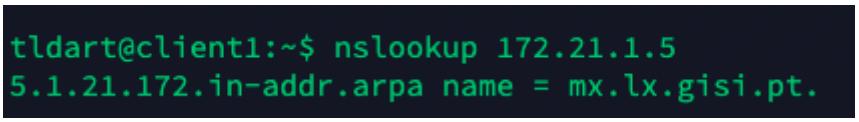

Fig. 10 Funcionamento do DNS reverso

Fig. 11 Query do servidor email

O slave foi ainda configurado de forma a permitir transferências de zona.

Fig. 9 Exemplo de transferência de zona

Referências

[1] R. Saive, “How to Setup SSH Passwordless Login in Linux [3 Easy Steps],” 16 setembro 2021. [Online]. Available: https://www.tecmint.com/ssh-passwordless-login-using-ssh-keygen-in-5-easy-steps/. [Acedido em 9 março 2022].

[2] “Practical class #2,” 2022.

[3] “Practical class #3,” 2022.