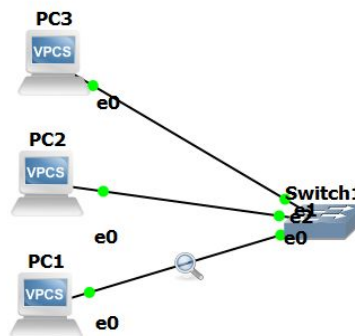


# Exercício das Camadas 1, 2, 3 de Redes

Gustavo Marangoni Rubo - 4584080

## Exercício 1 - Criação de uma Lan Básica

Primeiro criamos a topologia da rede, com três computadores virtuais e um switch:



Configuramos os IPs das três máquinas:

<pre>PC1&gt; show ip</pre> <table><tr><td>NAME</td><td>: PC1[1]</td></tr><tr><td>IP/MASK</td><td>: 192.168.180.1/24</td></tr><tr><td>GATEWAY</td><td>: 0.0.0.0</td></tr><tr><td>DNS</td><td>:</td></tr><tr><td>MAC</td><td>: 00:50:79:66:68:00</td></tr><tr><td>LPORT</td><td>: 20004</td></tr><tr><td>RHOST:PORT</td><td>: 127.0.0.1:20005</td></tr><tr><td>MTU:</td><td>: 1500</td></tr></table>	NAME	: PC1[1]	IP/MASK	: 192.168.180.1/24	GATEWAY	: 0.0.0.0	DNS	:	MAC	: 00:50:79:66:68:00	LPORT	: 20004	RHOST:PORT	: 127.0.0.1:20005	MTU:	: 1500	<pre>PC2&gt; show ip</pre> <table><tr><td>NAME</td><td>: PC2[1]</td></tr><tr><td>IP/MASK</td><td>: 192.168.180.2/24</td></tr><tr><td>GATEWAY</td><td>: 0.0.0.0</td></tr><tr><td>DNS</td><td>:</td></tr><tr><td>MAC</td><td>: 00:50:79:66:68:01</td></tr><tr><td>LPORT</td><td>: 20006</td></tr><tr><td>RHOST:PORT</td><td>: 127.0.0.1:20007</td></tr><tr><td>MTU:</td><td>: 1500</td></tr></table>	NAME	: PC2[1]	IP/MASK	: 192.168.180.2/24	GATEWAY	: 0.0.0.0	DNS	:	MAC	: 00:50:79:66:68:01	LPORT	: 20006	RHOST:PORT	: 127.0.0.1:20007	MTU:	: 1500	<pre>PC3&gt; show ip</pre> <table><tr><td>NAME</td><td>: PC3[1]</td></tr><tr><td>IP/MASK</td><td>: 192.168.180.3/24</td></tr><tr><td>GATEWAY</td><td>: 0.0.0.0</td></tr><tr><td>DNS</td><td>:</td></tr><tr><td>MAC</td><td>: 00:50:79:66:68:02</td></tr><tr><td>LPORT</td><td>: 20010</td></tr><tr><td>RHOST:PORT</td><td>: 127.0.0.1:20011</td></tr><tr><td>MTU:</td><td>: 1500</td></tr></table>	NAME	: PC3[1]	IP/MASK	: 192.168.180.3/24	GATEWAY	: 0.0.0.0	DNS	:	MAC	: 00:50:79:66:68:02	LPORT	: 20010	RHOST:PORT	: 127.0.0.1:20011	MTU:	: 1500
NAME	: PC1[1]																																																	
IP/MASK	: 192.168.180.1/24																																																	
GATEWAY	: 0.0.0.0																																																	
DNS	:																																																	
MAC	: 00:50:79:66:68:00																																																	
LPORT	: 20004																																																	
RHOST:PORT	: 127.0.0.1:20005																																																	
MTU:	: 1500																																																	
NAME	: PC2[1]																																																	
IP/MASK	: 192.168.180.2/24																																																	
GATEWAY	: 0.0.0.0																																																	
DNS	:																																																	
MAC	: 00:50:79:66:68:01																																																	
LPORT	: 20006																																																	
RHOST:PORT	: 127.0.0.1:20007																																																	
MTU:	: 1500																																																	
NAME	: PC3[1]																																																	
IP/MASK	: 192.168.180.3/24																																																	
GATEWAY	: 0.0.0.0																																																	
DNS	:																																																	
MAC	: 00:50:79:66:68:02																																																	
LPORT	: 20010																																																	
RHOST:PORT	: 127.0.0.1:20011																																																	
MTU:	: 1500																																																	

Fazemos um ping do PC1 para o PC2, que está sendo mostrado no console e na visão do wireshark (que está capturando pacotes da conexão entre PC1 e switch):

Wireshark - Capturing from [PC1 Ethernet0 to Switch1 Ethernet0]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.180.2? (00:50:79:66:68:00)
2	0.000001	Private_66:68:01	Private_66:68:00	ARP	64	192.168.180.2 is at 00:50:79:66:68:01
3	0.000059	192.168.180.1	192.168.180.2	ICMP	98	Echo (ping) request id=0
4	0.001008	192.168.180.2	192.168.180.1	ICMP	98	Echo (ping) reply id=0
5	1.002182	192.168.180.1	192.168.180.2	ICMP	98	Echo (ping) request id=0
6	1.002264	192.168.180.2	192.168.180.1	ICMP	98	Echo (ping) reply id=0
7	2.003629	192.168.180.1	192.168.180.2	ICMP	98	Echo (ping) request id=0
8	2.003701	192.168.180.2	192.168.180.1	ICMP	98	Echo (ping) reply id=0
9	3.005040	192.168.180.1	192.168.180.2	ICMP	98	Echo (ping) request id=0
10	3.005111	192.168.180.2	192.168.180.1	ICMP	98	Echo (ping) reply id=0
11	4.006708	192.168.180.1	192.168.180.2	ICMP	98	Echo (ping) request id=0

Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0  
> Ethernet II, Src: Private\_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)

Console do VPCS:

```
Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Dalling.
Build time: Apr  9 2014 11:00:00
Copyright (c) 2007-2014, Paul Heng (mirmashi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcslab.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC1> ip 192.168.180.1/24
Checking for duplicate address...
PC1: 192.168.180.1 255.255.255.0

PC1> ping 192.168.180.2
64 bytes from 192.168.180.2: icmp_seq=1 ttl=64 time=0.100 ms
64 bytes from 192.168.180.2: icmp_seq=2 ttl=64 time=0.172 ms
64 bytes from 192.168.180.2: icmp_seq=3 ttl=64 time=0.175 ms
64 bytes from 192.168.180.2: icmp_seq=4 ttl=64 time=0.159 ms
64 bytes from 192.168.180.2: icmp_seq=5 ttl=64 time=0.468 ms

PC1>
```

Escolhemos o primeiro pacote de request do ping e visualizamos o dump do wireshark para este pacote:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000091	Private_66:68:01	Private_66:68:00	ARP	64	192.168.180.2 is at 00:50:79:66:68:00
3	0.000959	192.168.180.1	192.168.180.2	ICMP	98	Echo (ping) request id=0
4	0.001008	192.168.180.2	192.168.180.1	ICMP	98	Echo (ping) reply id=0
5	1.002182	192.168.180.1	192.168.180.2	ICMP	98	Echo (ping) request id=0

> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0

> Ethernet II, Src: Private\_66:68:00 (00:50:79:66:68:00), Dst: Private\_66:68:01 (00:50:79:66:68:01)

▼ Internet Protocol Version 4, Src: 192.168.180.1, Dst: 192.168.180.2

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 84

Identification: 0x9560 (38240)

> Flags: 0x0000

Fragment offset: 0

Time to live: 64

Protocol: ICMP (1)

Header checksum: 0xfbf3 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.180.1

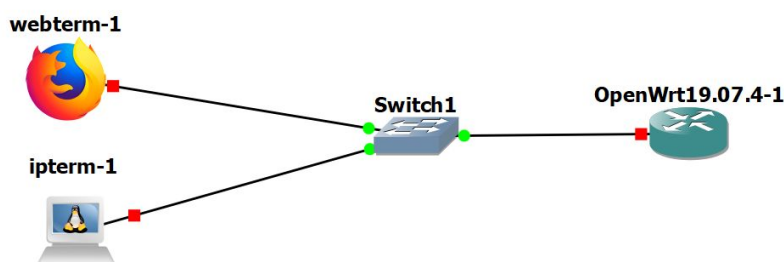
Destination: 192.168.180.2

> Internet Control Message Protocol

Os quatro primeiros bits do cabeçalho IP nos dizem qual é a versão que está sendo usada do protocolo. Neste caso, é a versão 4. A seção “Time to Live” (TTL) nos diz quantos pulos entre dispositivos essa mensagem ainda pode fazer antes de ser considerada perdida, ou em loop. O próximo campo nos diz qual é o tipo de protocolo da mensagem, que no caso é ICMP, pois a mensagem é parte de um ping. Ao final, temos duas das informações mais importantes do header, o endereço de origem e o endereço de destino da mensagem.

## Exercício 2 - Configuração de um roteador em DHCP

Topologia da rede:



O IP do roteador configurado de acordo com o enunciado:

```

root@OpenWrt:/# ifconfig br-lan
br-lan    Link encap:Ethernet  HWaddr 0C:AC:3F:D9:7C:00
          inet addr:192.168.180.1  Bcast:192.168.180.255  Mask:255.255.255.0
          inet6 addr: fe80::eac:3fff:fed9:7c00/64  Scope:Link
          inet6 addr: fd60:8cf5:e930::1/60  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:1964 (1.9 KiB)
  
```

Configuração do webTerm e do IPTerm, respectivamente:

```
#
# This is a sample network config uncomment lines to configure the network
#

# Static config for eth0
#auto eth0
#iface eth0 inet static
#       address 192.168.0.2
#       netmask 255.255.255.0
#       gateway 192.168.0.1
#       up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
#auto eth0
#iface eth0 inet dhcp
```

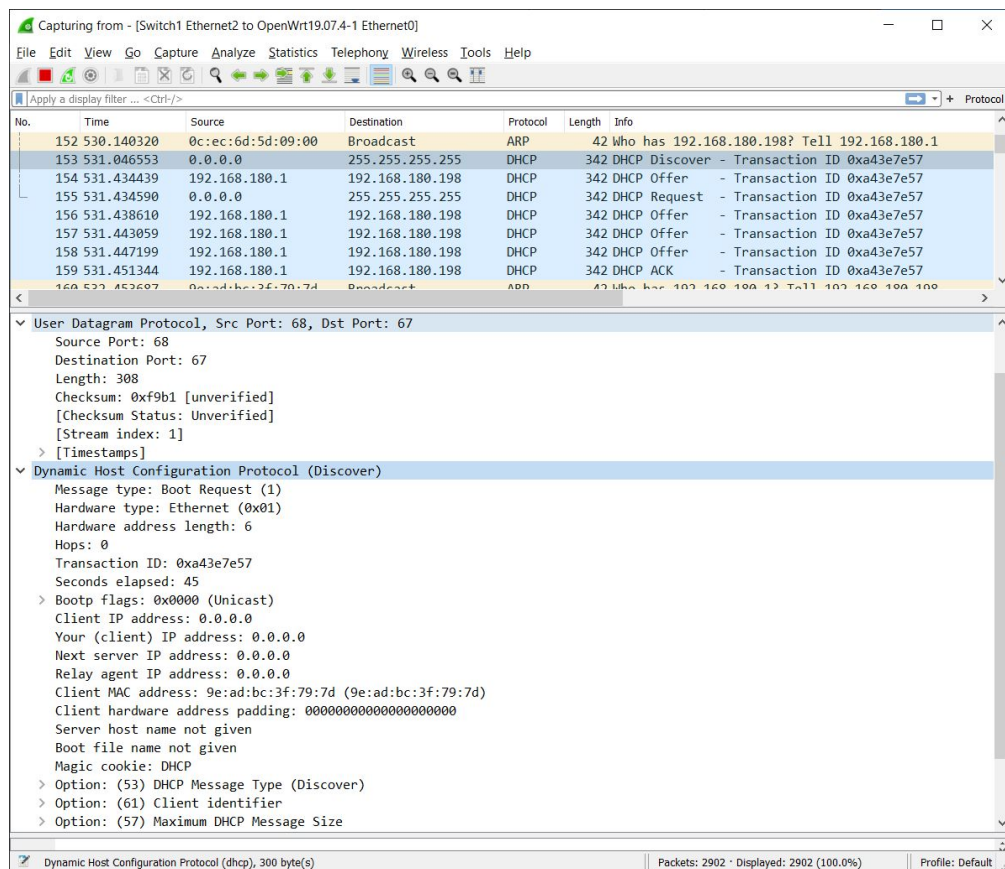
```
#
# This is a sample network config uncomment lines to configure the network
#

# Static config for eth0
auto eth0
iface eth0 inet static
       address 192.168.180.2
       netmask 255.255.255.0
       gateway 192.168.180.1
       up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
# auto eth0
# iface eth0 inet dhcp
```

Após a configuração, todos os nós foram desligados. O Wireshark foi iniciado entre o switch e o roteador, e então o roteador foi ligado, e em seguida o webterm também foi.

A seguir, mostramos os prints das mensagens de DORA, capturadas pelo wireshark:



Capturing from - [Switch1 Ethernet2 to OpenWrt19.07.4-1 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
152	530.140320	0c:ec:6d:5d:09:00	Broadcast	ARP	42	Who has 192.168.180.198? Tell 192.168.180.1
153	531.046553	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa43e7e57
154	531.434439	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
155	531.434590	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xa43e7e57
156	531.438610	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
157	531.443059	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
158	531.447199	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
159	531.451344	192.168.180.1	192.168.180.198	DHCP	342	DHCP ACK - Transaction ID 0xa43e7e57
160	532.452697	0e:ad:bc:3f:79:7d	Broadcast	ARP	42	Who has 192.168.180.1? Tell 192.168.180.198

User Datagram Protocol, Src Port: 67, Dst Port: 68

Source Port: 67  
Destination Port: 68  
Length: 308  
Checksum: 0xa467 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 3]  
> [Timestamps]

Dynamic Host Configuration Protocol (Offer)

Message type: Boot Reply (2)  
Hardware type: Ethernet (0x01)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0xa43e7e57  
Seconds elapsed: 42  
> Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 192.168.180.198  
Next server IP address: 192.168.180.1  
Relay agent IP address: 0.0.0.0  
Client MAC address: 9e:ad:bc:3f:79:7d (9e:ad:bc:3f:79:7d)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
> Option: (53) DHCP Message Type (Offer)  
> Option: (54) DHCP Server Identifier (192.168.180.1)  
> Option: (51) IP Address Lease Time

Dynamic Host Configuration Protocol (dhcp), 300 byte(s) | Packets: 2902 · Displayed: 2902 (100.0%) | Profile: Default

Capturing from - [Switch1 Ethernet2 to OpenWrt19.07.4-1 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
152	530.140320	0c:ec:6d:5d:09:00	Broadcast	ARP	42	Who has 192.168.180.198? Tell 192.168.180.1
153	531.046553	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa43e7e57
154	531.434439	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
155	531.434590	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xa43e7e57
156	531.438610	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
157	531.443059	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
158	531.447199	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
159	531.451344	192.168.180.1	192.168.180.198	DHCP	342	DHCP ACK - Transaction ID 0xa43e7e57
160	532.452697	0e:ad:bc:3f:79:7d	Broadcast	ARP	42	Who has 192.168.180.1? Tell 192.168.180.198

User Datagram Protocol, Src Port: 68, Dst Port: 67

Source Port: 68  
Destination Port: 67  
Length: 308  
Checksum: 0xa58e [unverified]  
[Checksum Status: Unverified]  
[Stream index: 1]  
> [Timestamps]

Dynamic Host Configuration Protocol (Request)

Message type: Boot Request (1)  
Hardware type: Ethernet (0x01)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0xa43e7e57  
Seconds elapsed: 46  
> Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 0.0.0.0  
Next server IP address: 0.0.0.0  
Relay agent IP address: 0.0.0.0  
Client MAC address: 9e:ad:bc:3f:79:7d (9e:ad:bc:3f:79:7d)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
> Option: (53) DHCP Message Type (Request)  
> Option: (61) Client identifier  
> Option: (50) Requested IP Address (192.168.180.198)

Dynamic Host Configuration Protocol (dhcp), 300 byte(s) | Packets: 2902 · Displayed: 2902 (100.0%) | Profile: Default



Capturing from - [Switch1 Ethernet2 to OpenWrt19.07.4-1 Ethernet0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
152	530.140320	0c:ec:6d:5d:09:00	Broadcast	ARP	42	Who has 192.168.180.198? Tell 192.168.180.1
153	531.046553	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa43e7e57
154	531.434439	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
155	531.434590	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xa43e7e57
156	531.438610	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
157	531.443059	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
158	531.447199	192.168.180.1	192.168.180.198	DHCP	342	DHCP Offer - Transaction ID 0xa43e7e57
159	531.451344	192.168.180.1	192.168.180.198	DHCP	342	DHCP ACK - Transaction ID 0xa43e7e57
160	532.452607	0c:ec:6d:5d:09:00	Broadcast	ARP	42	Who has 192.168.180.198? Tell 192.168.180.198

User Datagram Protocol, Src Port: 67, Dst Port: 68

Source Port: 67  
Destination Port: 68  
Length: 308  
Checksum: 0x4163 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 3]  
> [Timestamps]

Dynamic Host Configuration Protocol (ACK)

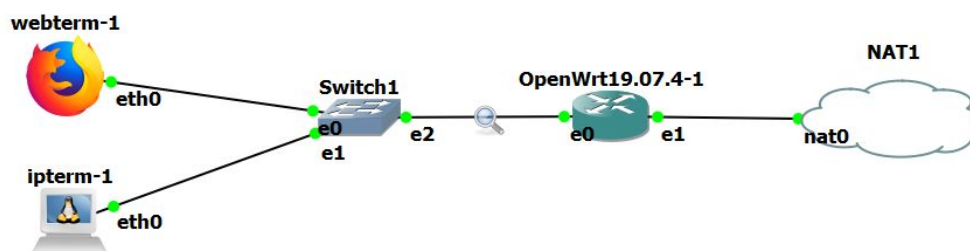
Message type: Boot Reply (2)  
Hardware type: Ethernet (0x01)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0xa43e7e57  
Seconds elapsed: 46  
> Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 192.168.180.198  
Next server IP address: 192.168.180.1  
Relay agent IP address: 0.0.0.0  
Client MAC address: 9e:ad:bc:3f:79:7d (9e:ad:bc:3f:79:7d)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
> Option: (53) DHCP Message Type (ACK)  
> Option: (54) DHCP Server Identifier (192.168.180.1)  
> Option: (51) IP Address Lease Time

Dynamic Host Configuration Protocol (dhcp), 300 byte(s) | Packets: 2902 · Displayed: 2902 (100.0%) | Profile: Default

A primeira mensagem de Discover é feita em broadcast, com o campo de endereço de remetente ainda em branco. A mensagem Offer já dá para o webterm um IP, que no caso é 192.168.180.198. A próxima mensagem, de Request, ainda tem o campo do remetente em branco, mas dessa vez tem um campo “Requested IP Address”, que está preenchido com o IP ofertado anteriormente. Por último, o roteador responde com uma mensagem ACK, com as informações repetidas da mensagem de Offer, mas agora confirmando o IP do webterm.

### Exercício 3 - Configuração de um NAT e acesso à internet

Topologia da rede:



Entrando na configuração do OpenWrt, vemos que a WAN está configurada como DHCP client:

## Interfaces

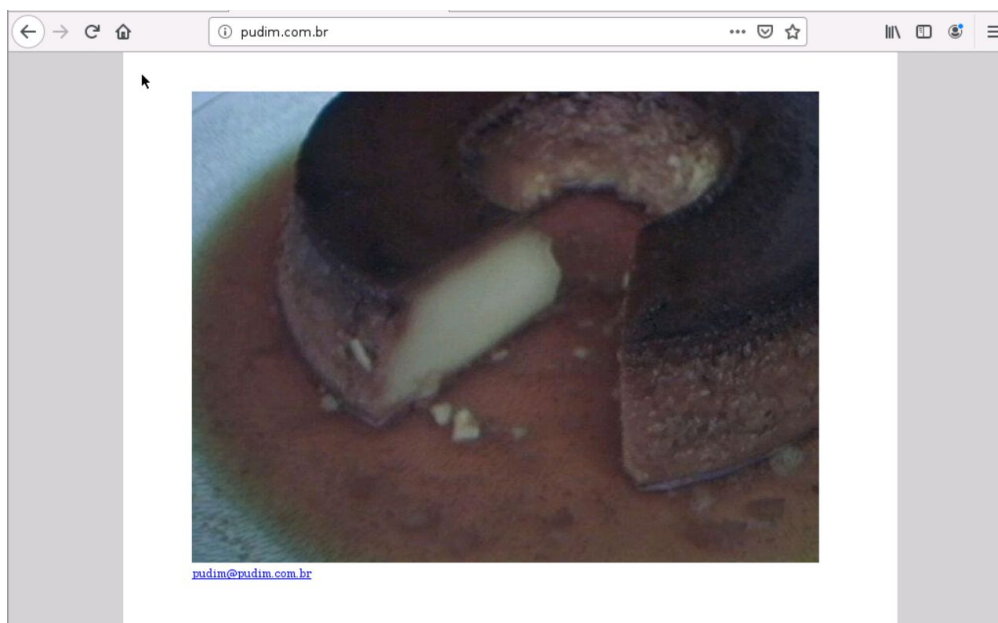
<b>LAN</b> br-lan	<b>Protocol:</b> Static address <b>Uptime:</b> 0h 9m 55s <b>MAC:</b> 0C:EC:6D:5D:09:00 <b>RX:</b> 330.88 KB (4825 Pkts.) <b>TX:</b> 7.08 MB (6840 Pkts.) <b>IPv4:</b> 192.168.180.1/24 <b>IPv6:</b> fd2a:7765:ae95::1/60	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>
<b>WAN</b> eth1	<b>Protocol:</b> DHCP client <b>Uptime:</b> 0h 9m 52s <b>MAC:</b> 0C:EC:6D:5D:09:01 <b>RX:</b> 6.26 MB (4968 Pkts.) <b>TX:</b> 204.59 KB (3101 Pkts.) <b>IPv4:</b> 192.168.122.218/24	<button>Restart</button> <button>Stop</button> <button>Edit</button> <button>Delete</button>

Podemos encontrar o endereço do webterm e do NAT monitorando as conexões de internet antes e depois do roteador. A seguir, mostramos o mesmo pacote lido entre o switch e o roteador, e quando lido entre o roteador e o NAT, respectivamente:

644	360.465247	192.168.180.126	179.235.24.73	HTTP	342 GET /success.txt HTTP/1.1
3373	2485.989801	192.168.122.218	179.235.24.73	HTTP	342 GET /success.txt HTTP/1.1

Vemos que o endereço do remetente foi substituído. O endereço 192.168.180.126 pertence ao webterm, e o endereço 192.168.122.218 pertence ao NAT.

Iremos agora acessar o site [pudim.com.br](http://pudim.com.br) e analisar os pacotes HTTP que trafegam entre o roteador e o NAT:



Mostramos a seguir um pacote HTTP da transmissão:

```

1304 919.176683 192.168.122.218 54.207.20.104 HTTP 401 GET /pudim.jpg HTTP/1.1
1305 919.176942 54.207.20.104 192.168.122.218 TCP 54 80 → 52464 [ACK] Seq=1 Ack=348 Win=65535 Len=0

> Internet Protocol Version 4, Src: 192.168.122.218, Dst: 54.207.20.104
> Transmission Control Protocol, Src Port: 52464, Dst Port: 80, Seq: 1, Ack: 1, Len: 347
  Hypertext Transfer Protocol
    > GET /pudim.jpg HTTP/1.1\r\n
      Host: pudim.com.br\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n
      Accept: image/webp,*/*\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Referer: http://pudim.com.br/\r\n
      Connection: keep-alive\r\n
    > Cookie: _ga=GA1.3.2114375503.1602969380; _gid=GA1.3.775878624.1602969380\r\n
      \r\n
    [Full request URI: http://pudim.com.br/pudim.jpg]
    [HTTP request 1/1]

```

Esse pacote foi responsável por puxar a foto de um pudim do servidor a partir de um “GET”.

O próximo pacote HTTP que veremos carrega as informações de css da página:

```

1308 919.201568 54.207.20.104 192.168.122.218 HTTP 810 HTTP/1.1 200 OK (text/css)

[Request URI: http://pudim.com.br/estilo.css]
File Data: 441 bytes
  Line-based text data: text/css (24 lines)
    body{\r\n
      background-color: #d0d0d0;\r\n
      margin: 0px;\r\n
      padding: 0px;\r\n
    }\r\n
    .container{\r\n
      width: 650px;\r\n
      background-color: #FFF;\r\n
      position: relative;\r\n
      padding: 40px 70px;\r\n
      position: absolute;\r\n
      top: 0px;\r\n

```

Analisando um desses pacotes, podemos ver sua origem e destino:

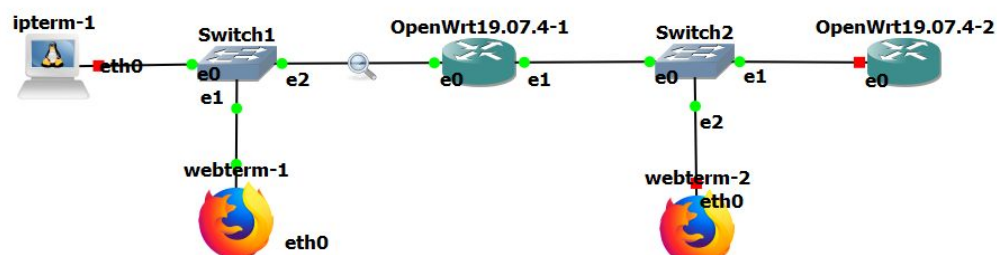
```

> Internet Protocol Version 4, Src: 192.168.122.218, Dst: 54.207.20.104
  Transmission Control Protocol, Src Port: 52462, Dst Port: 80, Seq: 1, Ack: 1, Len: 352

```

Os pacotes são enviados pelo webterm com um IP privado, mas ao chegarem no roteador, esses IPs são substituídos por IPs públicos pelo NAT, para que o servidor do outro lado (no nossa caso, pudim.com.br) possa mandar o pacote de volta através da rede pública.

Mudamos agora a topologia da nossa rede:



O webterm-2 foi configurado para obter seu IP via DHCP. O roteador R2 ficou com o gateway padrão.

Fizemos um ping do R1 para o R2, e confirmamos que há conexão entre eles:

```

root@OpenWrt:/# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=7.323 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.595 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=1.041 ms

```

Podemos ver também a transmissão dos pacotes de ping com o um wireshark que está entre o switch2 e o R2:

5	2.007244	192.168.1.156	192.168.1.1	ICMP	98 Echo (ping) request
6	2.007519	192.168.1.1	192.168.1.156	ICMP	98 Echo (ping) reply

Quando tentamos abrir a configuração em modo gráfico dos roteadores a partir do webterm-1, conseguimos acessar ambos R1 e R2. Porém, o webterm-2 não foi capaz de acessar o roteador R1. Com uma instância do wireshark capturando os pacotes entre o webterm-2 e o Switch2, podemos ver o pacote que foi enviado quando tentamos fazer a conexão ao R1:

670	85.289180	192.168.1.1	192.168.1.232	ICMP	102 Destination unreachable
-----	-----------	-------------	---------------	------	-----------------------------

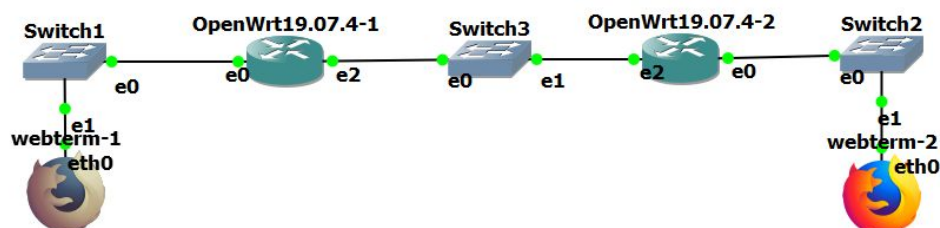
```

<
>
> Frame 670: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
> Ethernet II, Src: 0c:ec:6d:9b:26:00 (0c:ec:6d:9b:26:00), Dst: 5e:d7:48:ca:81:d4 (5e:d7:48:ca:81:d4)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.232
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 88
    Identification: 0x1de6 (7654)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xd7c5 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 192.168.1.232
  
```

Este pacote foi enviado do roteador R2 (ip 192.168.1.1) para o webterm-2 (ip 192.168.1.232). O webterm-2 manda inicialmente seus pacotes para o roteador R2, pois está na mesma subrede que ele. Quando o R2 tenta encontrar o endereço do roteador R1 (ip 192.168.180.1), ele procura em suas rotas registradas um caminho para a subrede 192.168.180.0/24. Porém, não existe caminho para essa subrede no roteador R2, então ele julga que o endereço é inalcançável.

## Exercício 4 - Roteamento estático entre duas redes LAN

Topologia da rede:



Configuramos os dois webterms para receberem seu endereço IP via DHCP. Configuramos o roteador R1 para ter o IP 192.168.180.1, e o roteador R2 para ter o IP 172.168.180.1, como está mostrado nas imagens abaixo do console dos roteadores:



```

root@OpenWrt:/# ifconfig br-lan
br-lan  Link encap:Ethernet  HWaddr 0C:41:B1:AC:8C:00
        inet addr:192.168.180.1  Bcast:192.168.180.255  Mask:255.255.255.0
        inet6 addr: fe80::e41:b1ff:feac:8c00/64 Scope:Link
        inet6 addr: fdd0:5448:89a3::1/60 Scope:Global
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:2016 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2141 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:208029 (203.1 KiB)  TX bytes:831722 (812.2 KiB)


root@OpenWrt:/# ifconfig br-lan
br-lan  Link encap:Ethernet  HWaddr 0C:41:B1:D9:A6:00
        inet addr:172.168.180.1  Bcast:172.168.180.255  Mask:255.255.255.0
        inet6 addr: fd8d:e453:4dcc::1/60 Scope:Global
        inet6 addr: fe80::e41:b1ff:fed9:a600/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1725 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1863 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:176963 (172.8 KiB)  TX bytes:748684 (731.1 KiB)

```

Cada um dos roteadores foi configurado através da interface gráfica de acordo com os dados do enunciado. A interface LAN2 do roteador R1 recebeu o endereço IP 10.0.1.1, como mostramos na imagem a seguir:

**Interfaces » LAN2**

[General Settings](#) [Advanced Settings](#) [Physical Settings](#) [Firewall Settings](#)

Status  **Device:** eth2  
**MAC:** 0C:41:B1:AC:8C:02  
**RX:** 0 B (0 Pkts.)  
**TX:** 0 B (0 Pkts.)


Protocol Static address

Bring up on boot ☒

IPv4 address  ...

IPv4 netmask 255.255.255.0

Ao final da configuração, a interface pode ser vista na lista:

<div>LAN2</div> <div> eth2</div>	<b>Protocol:</b> Static address <b>Uptime:</b> 0h 1m 16s <b>MAC:</b> 0C:41:B1:AC:8C:02 <b>RX:</b> 0 B (0 Pkts.) <b>TX:</b> 746 B (7 Pkts.) <b>IPv4:</b> 10.0.1.1/24
---	--

Em seguida, criamos rotas estáticas entre os roteadores R1 e R2. A configuração da rota estática do roteador R1 para o R2 pode ser vista na imagem abaixo:

Static IPv4 Routes			
Interface	Target	IPv4-Netmask	IPv4-Gateway
	Host-IP or Network	if target is a network	
LAN2: 	172.168.180.0	255.255.255.0	10.0.1.2

Agora podemos abrir o LXTerminal dentro de cada um dos webterms para conferir os IPs usando ifconfig:

```
LXTerminal
File Edit Tabs Help
root@webterm-1:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 2a:e8:94:cc:e4:fb
          inet addr:192.168.180.163  Bcast:192.168.180.255  Mask:255.255.255.0
          inet6 addr: fdd0:5448:89a3:0:28e8:94ff:fecc:e4fb/64  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9565 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9233 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3007662 (2.8 MiB)  TX bytes:998168 (974.7 KiB)

root@webterm-2:~# ifconfig br-lan
br-lan: error fetching interface information: Device not found
root@webterm-2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr a6:94:ef:69:d9:69
          inet addr:172.168.180.230  Bcast:172.168.180.255  Mask:255.255.255.0
          inet6 addr: fd8d:e453:4dcc:0:a494:efff:fe69:d969/64  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10871 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10441 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3581947 (3.4 MiB)  TX bytes:1178373 (1.1 MiB)
```

Agora faremos um ping do webterm1 para o webterm2:

```
root@webterm-1:~# ping 172.168.180.230
PING 172.168.180.230 (172.168.180.230) 56(84) bytes of data.
64 bytes from 172.168.180.230: icmp_seq=1 ttl=62 time=7.09 ms
64 bytes from 172.168.180.230: icmp_seq=2 ttl=62 time=1.30 ms
64 bytes from 172.168.180.230: icmp_seq=3 ttl=62 time=1.12 ms
64 bytes from 172.168.180.230: icmp_seq=4 ttl=62 time=1.12 ms
64 bytes from 172.168.180.230: icmp_seq=5 ttl=62 time=0.962 ms
64 bytes from 172.168.180.230: icmp_seq=6 ttl=62 time=1.23 ms
^C
--- 172.168.180.230 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5032ms
rtt min/avg/max/mdev = 0.962/2.140/7.096/2.219 ms
```

O ping foi bem sucedido. Podemos também ver os pacotes do ping através do wireshark:

→	18962	3341.243746	192.168.180.163	172.168.180.230	ICMP	98 Echo (ping) request
*←	18963	3341.250750	172.168.180.230	192.168.180.163	ICMP	98 Echo (ping) reply

Usaremos então um traceroute para determinar a rota entre webterm 1 e 2:

```
root@webterm-1:~# traceroute 172.168.180.230
traceroute to 172.168.180.230 (172.168.180.230), 30 hops max, 60 byte packets
 1 OpenWrt.lan (192.168.180.1)  10.440 ms  11.407 ms  11.654 ms
 2 10.0.1.2 (10.0.1.2)  22.386 ms  22.662 ms  22.763 ms
 3 172.168.180.230 (172.168.180.230)  22.860 ms  22.973 ms  23.075 ms
```

A seguir mostramos os pacotes capturados pelo wireshark (que está entre o webterm1 e o switch1). Podemos ver pelo histórico de Source e Destination qual é a rota entre os webterms. O pacote selecionado é o primeiro, que está partindo do roteador R1 com destino ao webterm1.

No.	Time	Source	Destination	Protocol	Length	Info
19174	3534.006660	192.168.180.1	192.168.180.163	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19176	3534.007661	192.168.180.1	192.168.180.163	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19177	3534.007916	192.168.180.1	192.168.180.163	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19182	3534.018655	10.0.1.2	192.168.180.163	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19184	3534.018939	10.0.1.2	192.168.180.163	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19185	3534.019047	10.0.1.2	192.168.180.163	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
19186	3534.019154	172.168.180.230	192.168.180.163	ICMP	102	Destination unreachable (Port unreachable)
19187	3534.019261	172.168.180.230	192.168.180.163	ICMP	102	Destination unreachable (Port unreachable)
19188	3534.019384	172.168.180.230	192.168.180.163	ICMP	102	Destination unreachable (Port unreachable)
19189	3534.019509	172.168.180.230	192.168.180.163	ICMP	102	Destination unreachable (Port unreachable)
19190	3534.019615	172.168.180.230	192.168.180.163	ICMP	102	Destination unreachable (Port unreachable)
19191	3534.019754	172.168.180.230	192.168.180.163	ICMP	102	Destination unreachable (Port unreachable)

> Ethernet II, Src: 0c:41:b1:ac:8c:00 (0c:41:b1:ac:8c:00), Dst: 2a:e8:94:cc:e4:fb (2a:e8:94:cc:e4:fb)	
▼	Internet Protocol Version 4, Src: 192.168.180.1, Dst: 192.168.180.163
0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT) Total Length: 88 Identification: 0x13a6 (5030) > Flags: 0x0000 Fragment offset: 0 Time to live: 64 Protocol: ICMP (1) Header checksum: 0x7c49 [validation disabled] [Header checksum status: Unverified] Source: 192.168.180.1 Destination: 192.168.180.163	

Vendo as informações dos pacotes, podemos determinar que a rota entre os webterms é:

- 192.168.180.1 - o gateway do roteador R1;
- 10.0.1.2 - a interface LAN2 do roteador R2;
- 172.168.180.230 - o webterm2.