

TP2

Protocolo IPv4 (802.11)

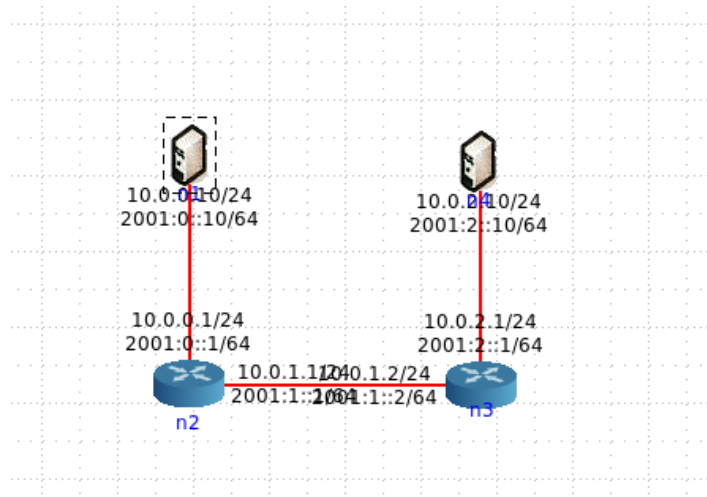
Daniel Vieira A73974

José Cunha A74702

João Palmeira A73864

PARTE 1

1.



- a. Active o *wireshark* ou o *tcpdump* no *host* n1. Numa *shell* de n1, execute o comando *traceroute -I* para o endereço IP do *host* n4.

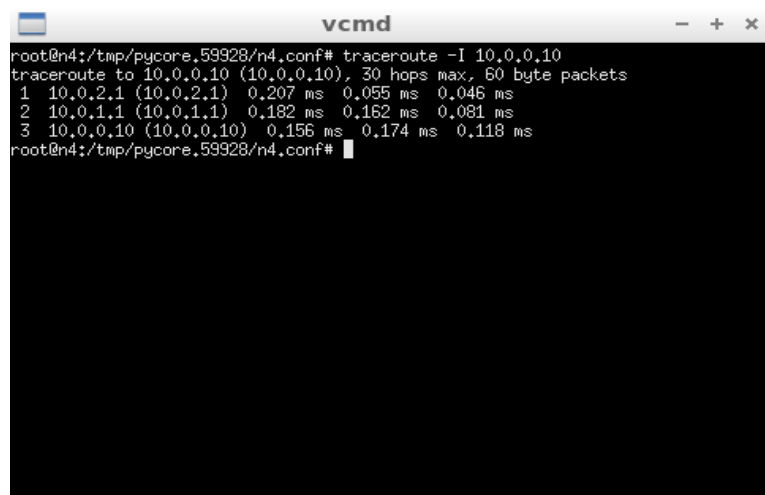
R:

```
vcmd
root@n1:/tmp/pycore.59928/n1.conf# traceroute -I 10.0.2.10
traceroute to 10.0.2.10 (10.0.2.10), 30 hops max, 60 byte packets
 1 10.0.0.1 (10.0.0.1)  0.116 ms  0.069 ms  0.089 ms
 2 10.0.1.2 (10.0.1.2)  0.132 ms  0.122 ms  0.118 ms
 3 10.0.2.10 (10.0.2.10)  0.179 ms  0.136 ms  0.212 ms
root@n1:/tmp/pycore.59928/n1.conf#
```

- b. Registe e analise o tráfego ICMP enviado por n1 e o tráfego ICMP recebido como resposta. Comente os resultados face ao comportamento esperado.

R: O tráfego ICMP enviado por n1 para 10.0.2.10 (n4) corresponde a 3 datagramas com o mesmo TTL de cada vez, pois não existe segurança na rede.

- c. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o destino n4? Verifique na prática que a sua resposta está correta.



```
vcmd
root@n4:/tmp/pycore.59928/n4.conf# traceroute -I 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 60 byte packets
 1 10.0.2.1 (10.0.2.1) 0.207 ms 0.055 ms 0.046 ms
 2 10.0.1.1 (10.0.1.1) 0.182 ms 0.162 ms 0.081 ms
 3 10.0.0.10 (10.0.0.10) 0.156 ms 0.174 ms 0.118 ms
root@n4:/tmp/pycore.59928/n4.conf#
```

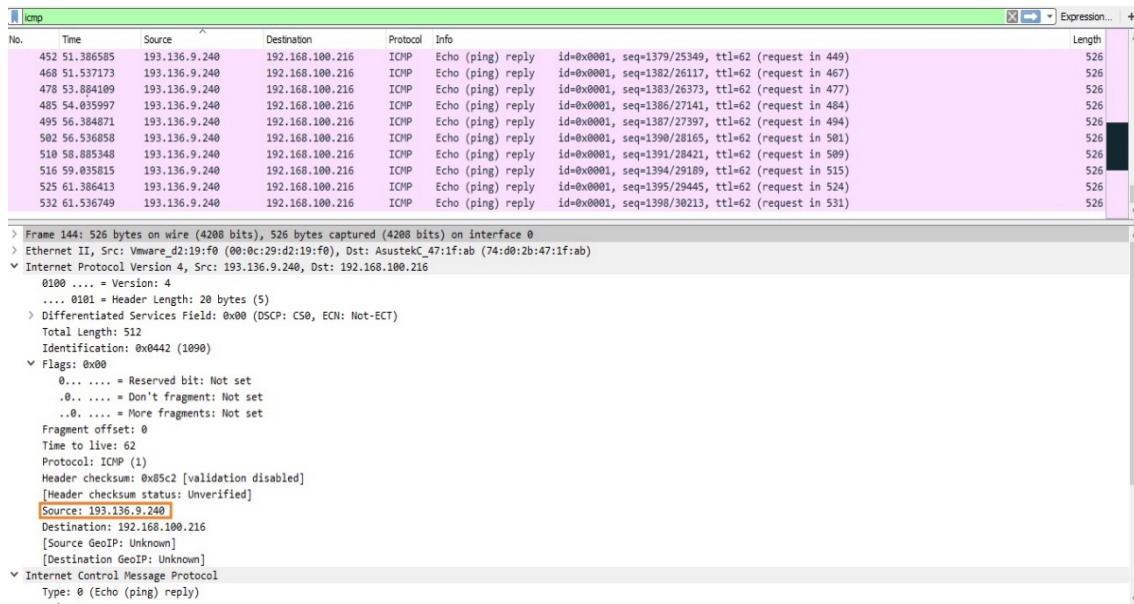
R: O tempo mínimo necessário para alcançar n4 é 3.

- d. Qual o valor médio do tempo de ida-e-volta (Round-Trip Time) obtido?

R: 1: $(0.207 + 0.055 + 0.046) / 3 = 0.102(6)$ ms
2: $(0.182 + 0.162 + 0.081) / 3 = 0.141(6)$ ms
3: $(0.156 + 0.174 + 0.118) / 3 = 0.149(3)$ ms

2.

a. Qual é o endereço IP da interface ativa do seu computador?

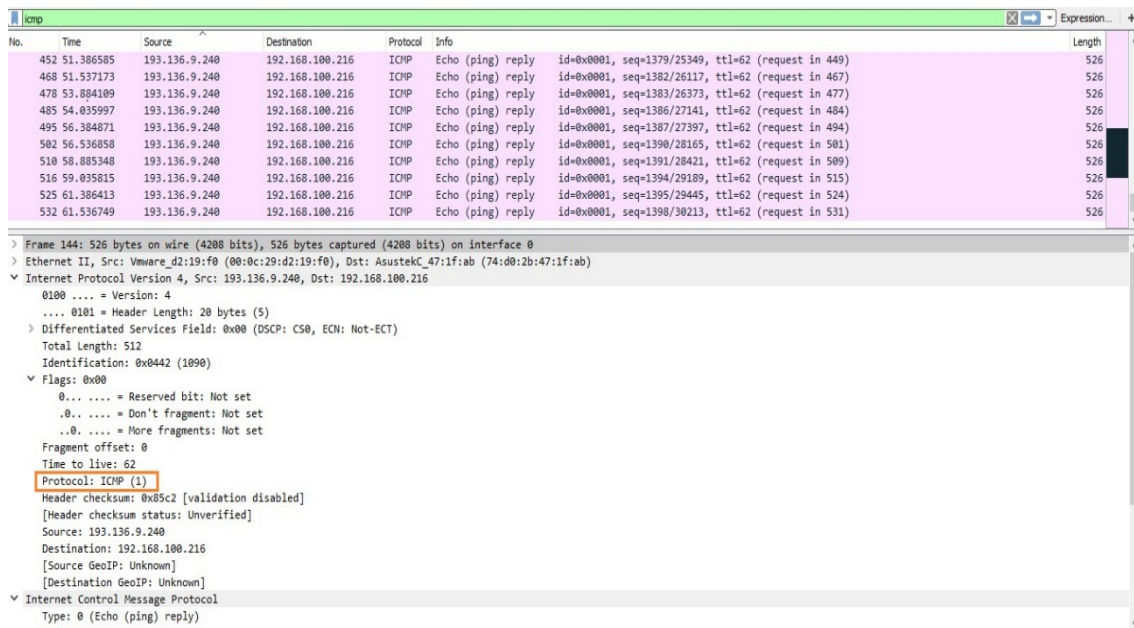


No.	Time	Source	Destination	Protocol	Info	Length
452	51.386585	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1379/25349, ttl=62 (request in 449)	526
468	51.537173	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1382/26117, ttl=62 (request in 467)	526
478	53.884109	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1383/26373, ttl=62 (request in 477)	526
485	54.835997	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1386/27141, ttl=62 (request in 484)	526
495	56.384871	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1387/27397, ttl=62 (request in 494)	526
502	56.536858	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1390/28165, ttl=62 (request in 501)	526
510	58.885348	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1391/28421, ttl=62 (request in 509)	526
516	59.835815	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1394/29189, ttl=62 (request in 515)	526
525	61.386413	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1395/29445, ttl=62 (request in 524)	526
532	61.536749	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1398/30213, ttl=62 (request in 531)	526

Frame 144: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: AsustekC_47:1f:ab (74:d0:2b:47:1f:ab)
Internet Protocol Version 4, Src: 193.136.9.240, Dst: 192.168.100.216
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 512
Identification: 0x0442 (1090)
Flags: 0x00
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0... = More fragments: Not set
Fragment offset: 0
Time to live: 62
Protocol: ICMP (1)
Header checksum: 0x85c2 [validation disabled]
[Header checksum status: Unverified]
Source: 193.136.9.240
Destination: 192.168.100.216
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)

R: O endereço IP da interface ativa do computador é o endereço “Source”, que tem o valor 193.136.9.248

b. Qual é o valor do campo protocolo? O que identifica?



No.	Time	Source	Destination	Protocol	Info	Length
452	51.386585	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1379/25349, ttl=62 (request in 449)	526
468	51.537173	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1382/26117, ttl=62 (request in 467)	526
478	53.884109	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1383/26373, ttl=62 (request in 477)	526
485	54.835997	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1386/27141, ttl=62 (request in 484)	526
495	56.384871	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1387/27397, ttl=62 (request in 494)	526
502	56.536858	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1390/28165, ttl=62 (request in 501)	526
510	58.885348	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1391/28421, ttl=62 (request in 509)	526
516	59.835815	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1394/29189, ttl=62 (request in 515)	526
525	61.386413	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1395/29445, ttl=62 (request in 524)	526
532	61.536749	193.136.9.240	192.168.100.216	ICMP	Echo (ping) reply id=0x0001, seq=1398/30213, ttl=62 (request in 531)	526

Frame 144: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: AsustekC_47:1f:ab (74:d0:2b:47:1f:ab)
Internet Protocol Version 4, Src: 193.136.9.240, Dst: 192.168.100.216
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 512
Identification: 0x0442 (1090)
Flags: 0x00
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0... = More fragments: Not set
Fragment offset: 0
Time to live: 62
Protocol: ICMP (1)
Header checksum: 0x85c2 [validation disabled]
[Header checksum status: Unverified]
Source: 193.136.9.240
Destination: 192.168.100.216
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)

R: O valor do campo protocolo é 1. Este campo identifica o tipo de protocolo e neste caso trata-se de ICMP.

- c. Quantos *bytes* tem o cabeçalho IP(v4)? Quantos *bytes* tem o campo de dados (*payload*) do datagrama? Como se calcula o tamanho do *payload*?

No.	Time	Source	Destination	Protocol	Length	Info
145	6.421297	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1308/7173, ttl=1 (no response found!)
143	6.370443	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1307/6917, ttl=255 (reply in 144)
→ 182	4.020134	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1306/6661, ttl=3 (reply in 103)
100	3.970220	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1305/6405, ttl=2 (no response found!)
98	3.920192	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1304/6149, ttl=1 (no response found!)
96	3.869999	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1303/5893, ttl=255 (reply in 97)
27	1.521008	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1302/5637, ttl=3 (reply in 28)
19	1.471068	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1301/5381, ttl=2 (no response found!)
16	1.420479	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1300/5125, ttl=1 (no response found!)
14	1.369593	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1299/4869, ttl=255 (reply in 15)

Frame 182: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
 Ethernet II, Src: AsustekC_47:1f:ab (74:d0:2b:47:1f:ab), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
 Internet Protocol Version 4, Src: 192.168.100.216, Dst: 193.136.9.240
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 512
 Identification: 0x1539 (5433)
 Flags: 0x00
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 Fragment offset: 0
 > Time to live: 3
 Protocol: ICMP (1)
 Header checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.100.216
 Destination: 193.136.9.240
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)

R: O cabeçalho IP(v4) tem 20 *bytes*. O tamanho do campo de dados é 512 e o número de *bytes* deste é $512 - 20 = 492$ *bytes*.

- d. O datagrama IP foi fragmentado? Justifique.

```

Flags: 0x00
0... .... = Reserved bit: Not set
.0... .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 0

```

R: O datagrama IP não foi fragmentado, a partir da análise da informação das flags da imagem acima apresentada (“More Fragments: Not set”). Além disso, o offset toma o valor 0.

- e. Ordene os pacotes capturados de acordo com o endereço IP fonte (e.g., selecionando o cabeçalho da coluna *Source*), e analise a sequência de tráfego ICMP gerado a partir do endereço IP atribuído à sua máquina. Para a sequência de mensagens ICMP enviadas pelo seu computador, indique que campos do cabeçalho IP variam de pacote para pacote.

No.	Time	Source	Destination	Protocol	Length	Info
14	1.369593	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1299/4869, ttl=255 (reply in 15)
15	1.370798	193.136.9.240	192.168.100.216	ICMP	526	Echo (ping) reply id=0x0001, seq=1299/4869, ttl=62 (request in 14)
16	1.420479	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1300/5125, ttl=1 (no response found!)
17	1.421161	192.168.100.254	192.168.100.216	ICMP	554	Time-to-live exceeded (Time to live exceeded in transit)
19	1.471068	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1301/5381, ttl=2 (no response found!)
20	1.472013	193.136.9.240	192.168.100.216	ICMP	526	Time-to-live exceeded (Time to live exceeded in transit)
27	1.521000	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1302/5637, ttl=3 (reply in 28)
28	1.522223	193.136.9.240	192.168.100.216	ICMP	526	Echo (ping) reply id=0x0001, seq=1302/5637, ttl=62 (request in 27)
96	3.869999	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1303/5893, ttl=255 (reply in 97)
97	3.871458	193.136.9.240	192.168.100.216	ICMP	526	Echo (ping) reply id=0x0001, seq=1303/5893, ttl=62 (request in 96)
98	3.878103	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1304/6149, ttl=1 (no response found!)
100	3.970220	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1305/6405, ttl=2 (no response found!)
102	4.020134	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1306/6661, ttl=3 (reply in 103)
143	6.370443	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1307/6917, ttl=255 (reply in 144)
145	6.421207	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1308/7173, ttl=1 (no response found!)
147	6.471386	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1309/7429, ttl=2 (no response found!)
149	6.521639	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1310/7685, ttl=3 (reply in 150)
152	8.870357	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1311/7941, ttl=255 (reply in 153)
154	8.921273	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1312/8197, ttl=1 (no response found!)

Total Length: 512
Identification: 0x1532 (5426)
Flags: 0x00
Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.100.216
Destination: 193.136.9.240
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]

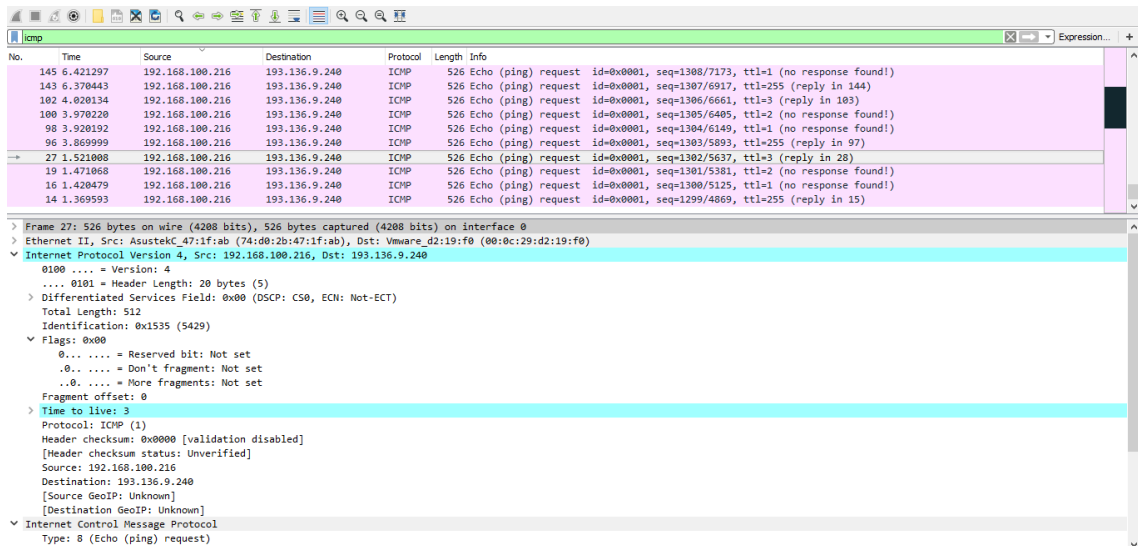
Frame 16: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
> Ethernet II, Src: AsustekC47:1f:ab (74:d0:2b:47:1f:ab), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
v Internet Protocol Version 4, Src: 192.168.100.216, Dst: 193.136.9.240
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 512
Identification: 0x1532 (5427)
Flags: 0x00
Fragment offset: 0
Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]

R: Os campos do cabeçalho IP que variam de pacote para pacote são o “Time to live” e o “Identification”.

- f. Observa algum padrão nos valores do campo de Identificação do datagrama IP e TTL?

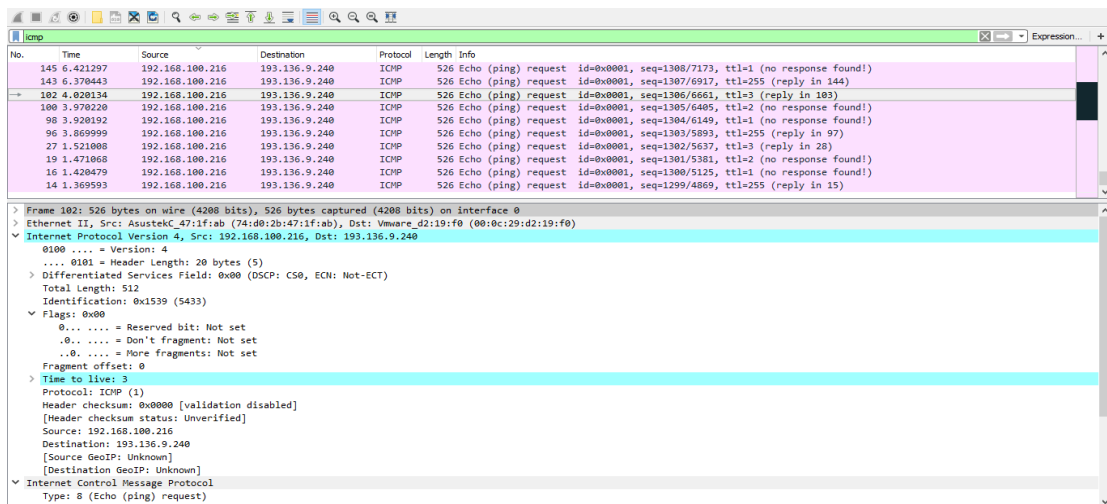
R: Os campos de identificação do datagrama IP estão sequenciados (como se pode ver no campo *Identification* que consta nas imagens acima, sendo os seus valores 0x3eee e 0x3eef). O TTL também segue um padrão: verifica-se que os valores dos pedidos são sempre 255 e 1.

- g. Ordene o tráfego capturado por endereço destino e encontre a série de respostas ICMP TTL *exceeded* enviadas ao seu computador. Qual é o valor do campo TTL? Esse valor permanece constante para todas as mensagens de resposta ICMP TTL *exceeded* enviados ao seu *host*? Porquê?



No.	Time	Source	Destination	Protocol	Length	Info
145	6.421297	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1308/7173, ttl=1 (no response found!)
143	6.370443	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1307/6917, ttl=255 (reply in 144)
102	4.020134	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1306/6661, ttl=3 (reply in 103)
100	3.970220	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1305/6405, ttl=2 (no response found!)
98	3.920192	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1304/6149, ttl=1 (no response found!)
96	3.869999	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1303/5893, ttl=255 (reply in 97)
27	1.521008	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1302/5637, ttl=3 (reply in 28)
19	1.471068	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1301/5381, ttl=2 (no response found!)
16	1.420479	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1300/5125, ttl=1 (no response found!)
14	1.369593	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1299/4869, ttl=255 (reply in 15)

Frame 27: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
> Ethernet II, Src: AsustekC_47:1f:ab (74:00:2b:47:1f:ab), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
Internet Protocol Version 4, Src: 192.168.100.216, Dst: 193.136.9.240
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 512
Identification: 0x1535 (5429)
Flags: 0x00
0... = Reserved bit: Not set
0... = Don't fragment: Not set
..0... = More fragments: Not set
Fragment offset: 0
> Time to live: 3
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.100.216
Destination: 193.136.9.240
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)



No.	Time	Source	Destination	Protocol	Length	Info
145	6.421297	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1308/7173, ttl=1 (no response found!)
143	6.370443	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1307/6917, ttl=255 (reply in 144)
102	4.020134	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1306/6661, ttl=3 (reply in 103)
100	3.970220	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1305/6405, ttl=2 (no response found!)
98	3.920192	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1304/6149, ttl=1 (no response found!)
96	3.869999	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1303/5893, ttl=255 (reply in 97)
27	1.521008	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1302/5637, ttl=3 (reply in 28)
19	1.471068	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1301/5381, ttl=2 (no response found!)
16	1.420479	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1300/5125, ttl=1 (no response found!)
14	1.369593	192.168.100.216	193.136.9.240	ICMP	526	Echo (ping) request id=0x0001, seq=1299/4869, ttl=255 (reply in 15)

Frame 102: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0
> Ethernet II, Src: AsustekC_47:1f:ab (74:00:2b:47:1f:ab), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
Internet Protocol Version 4, Src: 192.168.100.216, Dst: 193.136.9.240
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 512
Identification: 0x1539 (5433)
Flags: 0x00
0... = Reserved bit: Not set
0... = Don't fragment: Not set
..0... = More fragments: Not set
Fragment offset: 0
> Time to live: 3
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.100.216
Destination: 193.136.9.240
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)

R: O valor do campo TTL é 3. Permanece constante para todas as mensagens de resposta enviadas, pois trata-se de um *reply*. Este valor de tempo de vida serve para garantir que o *reply* chega ao destino independentemente dos saltos que possa vir a dar.

3.

- a. Localize a primeira mensagem ICMP. Porque é que houve necessidade de fragmentar o pacote inicial?

```
▼ [3 IPv4 Fragments (3003 bytes): #7(1480), #8(1480), #9(43)]
[Frame: 7, payload: 0-1479 (1480 bytes)]
[Frame: 8, payload: 1480-2959 (1480 bytes)]
[Frame: 9, payload: 2960-3002 (43 bytes)]
[Fragment count: 3]
[Reassembled IPv4 length: 3003]
[Reassembled IPv4 data: 0800f5f70001062b2020202020202020202020202020...]
```

R: Houve necessidade de fragmentar o pacote inicial, pois este era demasiado grande, tendo de se dividir, neste caso, em 3 fragmentos.

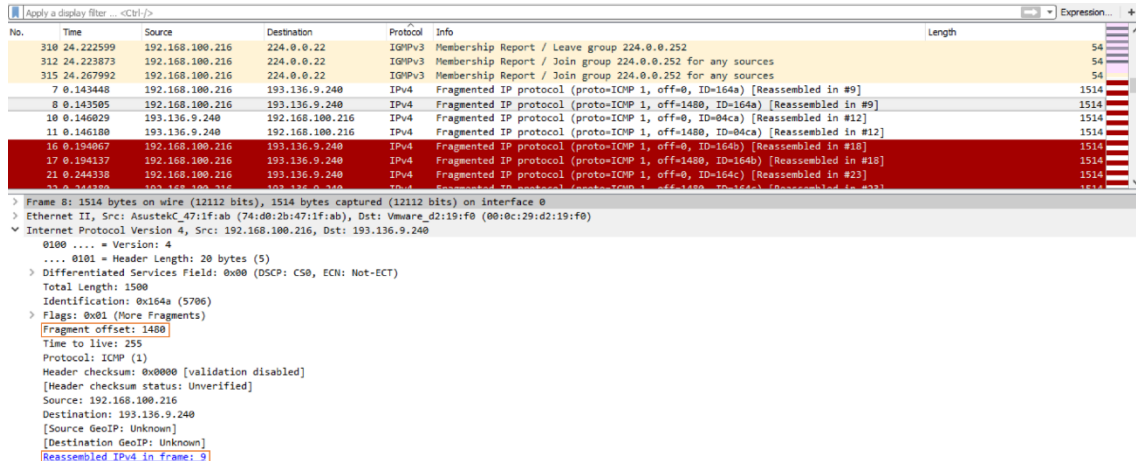
- b. Imprima o primeiro fragmento do datagrama IP segmentado. Que informação no cabeçalho indica que o datagrama foi fragmentado? Que informação no cabeçalho IP indica que se trata do primeiro fragmento? Qual é o tamanho deste datagrama IP?

No.	Time	Source	Destination	Protocol	Info	Length
310	24.222599	192.168.100.216	224.0.0.22	IGMPv3	Membership Report / Leave group 224.0.0.252	54
312	24.223873	192.168.100.216	224.0.0.22	IGMPv3	Membership Report / Join group 224.0.0.252 for any sources	54
315	24.267992	192.168.100.216	224.0.0.22	IGMPv3	Membership Report / Join group 224.0.0.252 for any sources	54
7	0.143448	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=0, ID=164a) [Reassembled in #9]	1514
8	0.143505	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=164a) [Reassembled in #9]	1514
10	0.146029	193.136.9.240	192.168.100.216	IPv4	Fragmented IP protocol (proto=ICMP 1, off=0, ID=04ca) [Reassembled in #12]	1514
11	0.146180	193.136.9.240	192.168.100.216	IPv4	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=04ca) [Reassembled in #12]	1514
13	0.150057	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=0, ID=164b) [Reassembled in #10]	1514
17	0.154137	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=164b) [Reassembled in #10]	1514
21	0.244338	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=0, ID=164c) [Reassembled in #23]	1514
33	0.344320	193.136.9.240	192.168.100.216	IPv4	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=164c) [Reassembled in #23]	1514

> Frame 7: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: AsustekC_47:1f:ab (74:d0:2b:47:1f:ab), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
> Internet Protocol Version 4, Src: 192.168.100.216, Dst: 193.136.9.240
0100 = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x164a (5706)
> Flags: 0x01 (More Fragments)
Fragment offset: 0
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.100.216
Destination: 193.136.9.240
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Reassembled IPv4 in frame: 9
> Data (1480 bytes)

R: “Reassembled IPv4 in frame: 9” indica-nos que é um fragmento que vai ser reconstruído na trama 9. “More Fragments: Set” (toma valor 1) indica que existem mais fragmentos para além deste. Trata-se do primeiro fragmento pois o offset é igual a 0. O segundo fragmento vai ter o offset igual a 1480. Em relação ao tamanho, temos 1480 de dados e 20 de header, logo, no total, 1500.

- c. Imprima o segundo fragmento do datagrama IP original. Que informação do cabeçalho IP indica que não se trata do 1º fragmento? Há mais fragmentos? O que nos permite afirmar isso?



No.	Time	Source	Destination	Protocol	Info	Length
310	24.222599	192.168.100.216	224.0.0.22	IGMPv3	Membership Report / Leave group 224.0.0.252	54
312	24.223873	192.168.100.216	224.0.0.22	IGMPv3	Membership Report / Join group 224.0.0.252 for any sources	54
315	24.267992	192.168.100.216	224.0.0.22	IGMPv3	Membership Report / Join group 224.0.0.252 for any sources	54
7	0.143448	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=0, ID=164a) [Reassembled in #9]	1514
8	0.143505	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=164a) [Reassembled in #9]	1514
10	0.146029	193.136.9.240	192.168.100.216	IPv4	Fragmented IP protocol (proto=ICMP 1, off=0, ID=84ca) [Reassembled in #12]	1514
11	0.146100	193.136.9.240	192.168.100.216	IPv4	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=84ca) [Reassembled in #12]	1514
16	0.194067	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=0, ID=164b) [Reassembled in #18]	1514
17	0.194137	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=164b) [Reassembled in #18]	1514
21	0.244338	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=0, ID=164c) [Reassembled in #23]	1514
23	0.244358	192.168.100.216	193.136.9.240	IPv4	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=164c) [Reassembled in #23]	1514

> Frame 8: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

> Ethernet II, Src: AsustekC_47:1f:ab (74:d0:2b:47:1f:ab), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)

> Internet Protocol Version 4, Src: 192.168.100.216, Dst: 193.136.9.240

0100 = Version: 4

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

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

Total Length: 1500

Identification: 0x164a (5706)

> Flags: 0x01 (More Fragments)

Fragment offset: 1480

Time to live: 255

Protocol: ICMP (1)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.100.216

Destination: 193.136.9.240

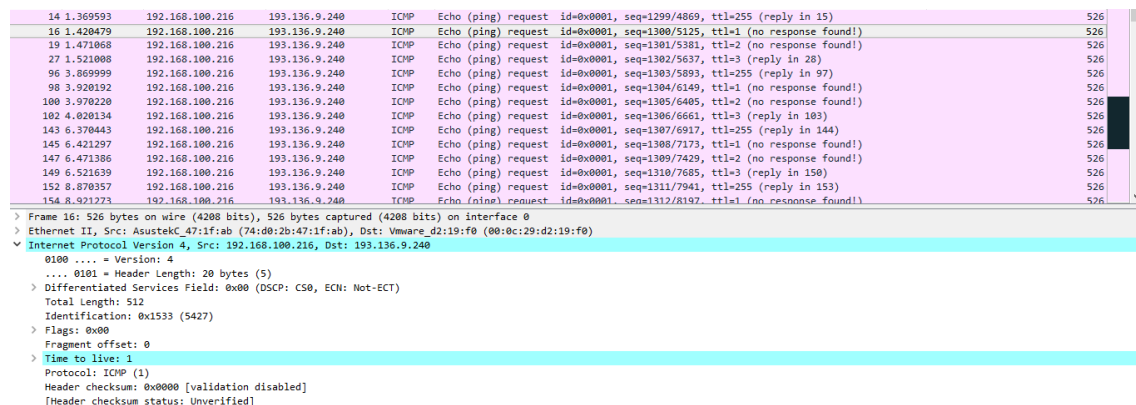
[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Reassembled IPv4 in frame: 9

R: O que indica que não se trata do 1º fragmento é o facto de o offset ter o valor 1480, ou seja, diferente de 0. Há mais fragmentos pois conseguimos ver na flag que “More Fragments : Set” (toma valor 1).

- d. Quantos fragmentos foram criados a partir do datagrama original? Como se deteta o último fragmento correspondente ao datagrama original?



No.	Time	Source	Destination	Protocol	Info	Length
14	1.369593	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1299/4869, ttl=255 (reply in 15)	526
16	1.420479	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1300/5125, ttl=1 (no response found!)	526
19	1.471068	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1301/5381, ttl=2 (no response found!)	526
27	1.521008	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1302/5637, ttl=3 (reply in 28)	526
96	3.869999	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1303/5893, ttl=255 (reply in 97)	526
98	3.920192	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1304/6149, ttl=1 (no response found!)	526
100	3.970220	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1305/6405, ttl=2 (no response found!)	526
102	4.020134	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1306/6661, ttl=3 (reply in 103)	526
143	6.370443	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1307/6917, ttl=255 (reply in 144)	526
145	6.421297	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1308/7173, ttl=1 (no response found!)	526
147	6.471386	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1309/7429, ttl=2 (no response found!)	526
149	6.521639	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1310/7685, ttl=3 (reply in 150)	526
152	8.870357	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1311/7941, ttl=255 (reply in 153)	526
154	8.921273	192.168.100.216	193.136.9.240	ICMP	Echo (ping) request id=0x0001, seq=1312/8197, ttl=1 (no response found!)	526

> Frame 16: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface 0

> Ethernet II, Src: AsustekC_47:1f:ab (74:d0:2b:47:1f:ab), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)

> Internet Protocol Version 4, Src: 192.168.100.216, Dst: 193.136.9.240

0100 = Version: 4

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

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

Total Length: 512

Identification: 0x1533 (5427)

> Flags: 0x00

Fragment offset: 0

> Time to live: 1

Protocol: ICMP (1)

Header checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

R: Foram criados 3 fragmentos a partir do datagrama original. Como estes 3 fragmentos vão ser reconstruídos na trama 9, a trama 9 corresponderá ao último fragmento do datagrama original. Através da flag “More Fragments: Not Set” (toma valor 0) sabemos que não há mais fragmentos, e através do offset igual a 0 verifica-se que não se trata do primeiro fragmento, pois é igual de 0, logo o fragmento em questão só pode ser o último.

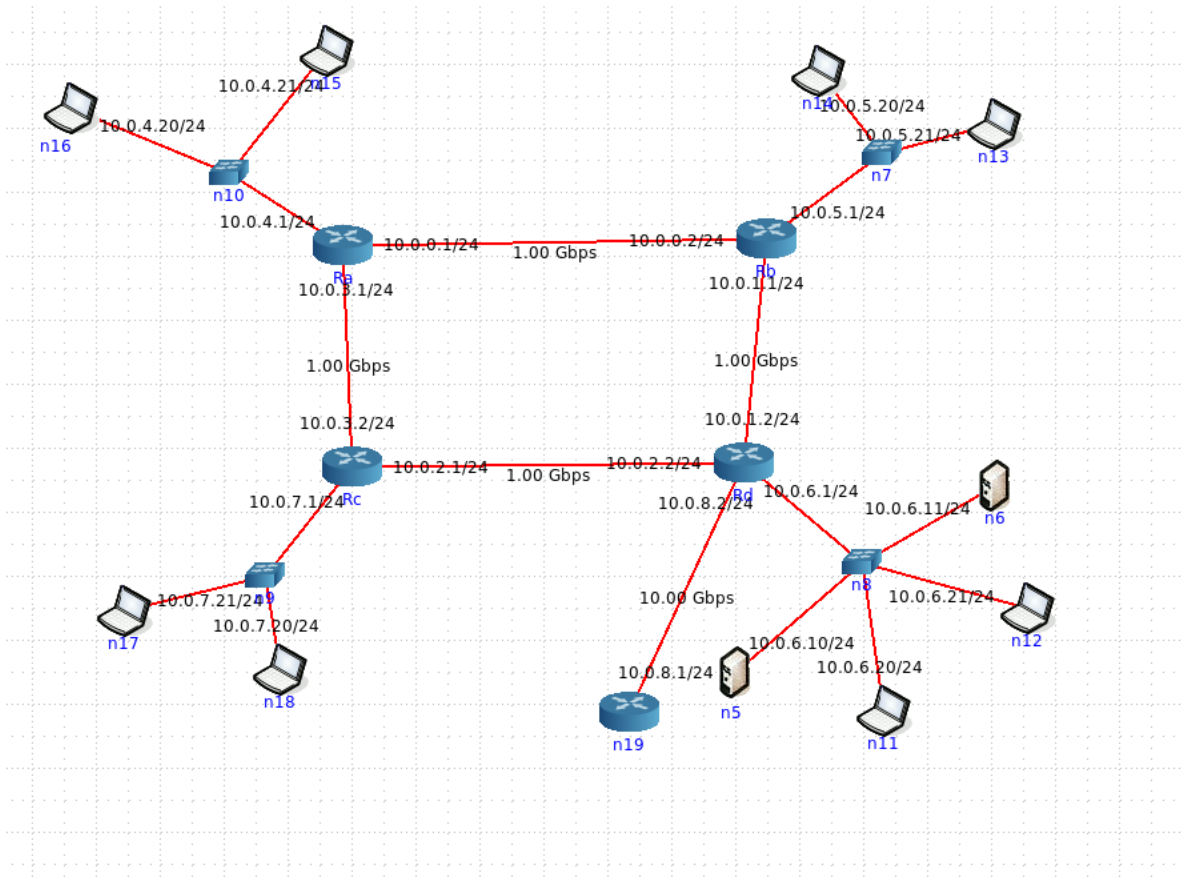
- e. Indique, resumindo, os campos que mudam no cabeçalho IP entre os diferentes fragmentos, e explique a forma como essa informação permite reconstruir o datagrama original.

R: Os campos que mudam no cabeçalho IP entre os diferentes fragmentos são o *offset* dos fragmentos, assim como a identificação de cada um destes. Através do *offset*, é possível reconstruir o datagrama, pois este fornece a posição de cada fragmento.

PARTE 2

1) Atenda aos endereços IP atribuídos automaticamente pelo CORE aos diversos equipamentos da topologia.

a) Indique que endereços IP e máscaras de rede foram atribuídos pelo CORE a cada equipamento. Para simplificar, pode incluir uma imagem que ilustre de forma clara a topologia e o endereçamento.



R: Atribuímos a seguinte máscara de rede pois temos /24 no endereço IP, o que significa que temos 24 bits identificadores da rede, logo corresponde ao endereço 255.255.255.0, visto que a máscara vai conter o limite máximo de valores decimais quando temos os primeiros 24 bits do endereço IP todos a 1.

Ra to Rb: ip=10.0.0.1	Mascara de rede= 255.255.255.0
Ra to Rc: ip=10.0.3.1	Mascara de rede= 255.255.255.0
Rc to Rd: ip=10.0.2.1	Mascara de rede= 255.255.255.0
Rc to Ra: ip= 10.0.3.2	Mascara de rede= 255.255.255.0
Rd to Rc: ip=10.0.2.2	Mascara de rede= 255.255.255.0
Rd to Rb: ip=10.0.1.2	Mascara de rede= 255.255.255.0
Rb to Ra: ip=10.0.0.2	Mascara de rede= 255.255.255.0
Rb to Rd: ip=10.0.1.1	Mascara de rede= 255.255.255.0
Rd to n19: ip=10.0.8.2	Mascara de rede= 255.255.255.0

N5: ip=10.0.6.10	Mascara de rede= 255.255.255.0
N6: ip= 10.0.6.11	Mascara de rede= 255.255.255.0
N11: ip=10.0.6.20	Mascara de rede= 255.255.255.0
N12: ip= 10.0.6.21	Mascara de rede= 255.255.255.0
N13: ip=10.0.5.21	Mascara de rede= 255.255.255.0
N14: ip=10.0.5.20	Mascara de rede= 255.255.255.0
N15: ip=10.0.4.21	Mascara de rede= 255.255.255.0
N16: ip=10.0.4.20	Mascara de rede= 255.255.255.0
N17: ip=10.0.7.21	Mascara de rede= 255.255.255.0
N18: ip=10.0.7.20	Mascara de rede= 255.255.255.0
N19 to Rd: ip=10.0.8.1	Mascara de rede= 255.255.255.0

b) Tratam-se de endereços públicos ou privados? Porquê?

R: Estes endereçamentos vão ser privados, visto que eles não têm acesso direto à internet.

c) Porque razão não é atribuído um endereço IP aos *switches*?

```
vcmd
root@n5:/tmp/pycore.37745/n5.conf# route delete
page: inet_route [-vF] del {-host|-net} Target[/prefix] [gw Gw] [metric M] [[de
] IF]
inet_route [-vF] add {-host|-net} Target[/prefix] [gw Gw] [metric M]
[netmask M] [tos Hs] [window W] [irtt I]
[mod] [dup] [reinstata] [[dev] IF]
inet_route [-vF] add {-host|-net} Target[/prefix] [metric M] reject
inet_route [-FC] Flush NOT supported
root@n5:/tmp/pycore.37745/n5.conf# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 10.0.6.1 0.0.0.0 UG 0 0 0 eth0
0.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
root@n5:/tmp/pycore.37745/n5.conf# route delete 0.0.0.0
OCDLRT: No such process
root@n5:/tmp/pycore.37745/n5.conf# route delete default
root@n5:/tmp/pycore.37745/n5.conf# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
root@n5:/tmp/pycore.37745/n5.conf#
```

R: Não é atribuído um endereço IP aos *switches* porque estes são usados em ligações de nível 2, e o endereço IP só irá ser atribuído em ligações de nível 3, nível de rede.

d) Usando o comando *ping* certifique-se que existe conectividade IP entre os laptops dos utilizadores e o servidor do departamento D (basta certificar a conectividade de um laptop por departamento).

```
vcmd
root@n18:/tmp/pycore.37777/n18.conf# ping 10.0.6.10
PING 10.0.6.10 (10.0.6.10) 56(84) bytes of data.
64 bytes from 10.0.6.10: icmp_req=1 ttl=62 time=0.323 ms
64 bytes from 10.0.6.10: icmp_req=2 ttl=62 time=0.273 ms
64 bytes from 10.0.6.10: icmp_req=3 ttl=62 time=0.281 ms
64 bytes from 10.0.6.10: icmp_req=4 ttl=62 time=0.247 ms
64 bytes from 10.0.6.10: icmp_req=5 ttl=62 time=0.300 ms
64 bytes from 10.0.6.10: icmp_req=6 ttl=62 time=0.245 ms
64 bytes from 10.0.6.10: icmp_req=7 ttl=62 time=0.244 ms
64 bytes from 10.0.6.10: icmp_req=8 ttl=62 time=0.194 ms
64 bytes from 10.0.6.10: icmp_req=9 ttl=62 time=0.245 ms
64 bytes from 10.0.6.10: icmp_req=10 ttl=62 time=0.267 ms
64 bytes from 10.0.6.10: icmp_req=11 ttl=62 time=0.239 ms
64 bytes from 10.0.6.10: icmp_req=12 ttl=62 time=0.233 ms
64 bytes from 10.0.6.10: icmp_req=13 ttl=62 time=0.246 ms
64 bytes from 10.0.6.10: icmp_req=14 ttl=62 time=0.266 ms
--- 10.0.6.10 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 12993ms
rtt min/avg/max/ndev = 0.194/0.257/0.323/0.032 ms
root@n18:/tmp/pycore.37777/n18.conf#

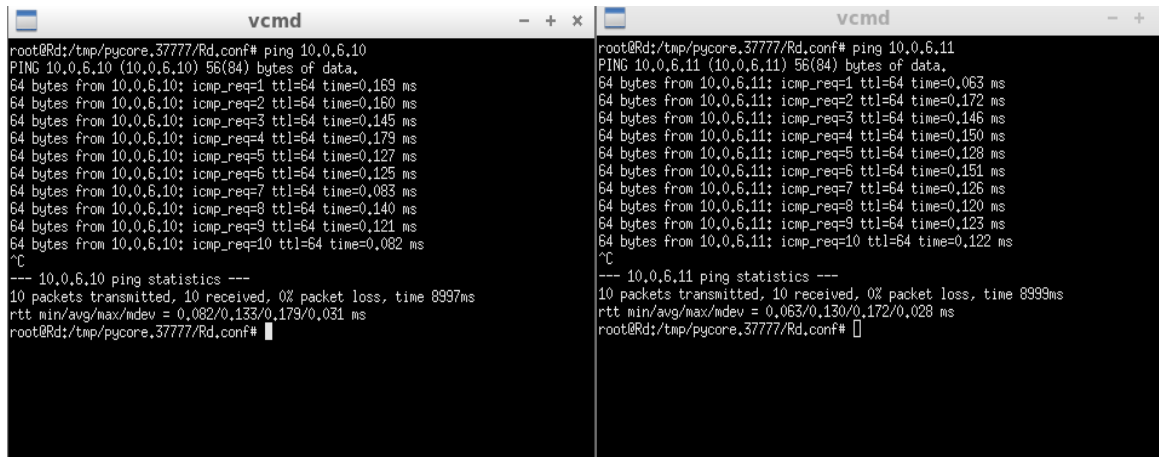
vcmd
root@n11:/tmp/pycore.37777/n11.conf# ping 10.0.6.10
PING 10.0.6.10 (10.0.6.10) 56(84) bytes of data.
64 bytes from 10.0.6.10: icmp_req=1 ttl=64 time=0.135 ms
64 bytes from 10.0.6.10: icmp_req=2 ttl=64 time=0.160 ms
64 bytes from 10.0.6.10: icmp_req=3 ttl=64 time=0.168 ms
64 bytes from 10.0.6.10: icmp_req=4 ttl=64 time=0.098 ms
64 bytes from 10.0.6.10: icmp_req=5 ttl=64 time=0.126 ms
64 bytes from 10.0.6.10: icmp_req=6 ttl=64 time=0.126 ms
64 bytes from 10.0.6.10: icmp_req=7 ttl=64 time=0.123 ms
64 bytes from 10.0.6.10: icmp_req=8 ttl=64 time=0.102 ms
64 bytes from 10.0.6.10: icmp_req=9 ttl=64 time=0.113 ms
64 bytes from 10.0.6.10: icmp_req=10 ttl=64 time=0.145 ms
64 bytes from 10.0.6.10: icmp_req=11 ttl=64 time=0.119 ms
64 bytes from 10.0.6.10: icmp_req=12 ttl=64 time=0.123 ms
64 bytes from 10.0.6.10: icmp_req=13 ttl=64 time=0.126 ms
--- 10.0.6.10 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12000ms
rtt min/avg/max/ndev = 0.098/0.128/0.168/0.021 ms
root@n11:/tmp/pycore.37777/n11.conf#

vcmd
root@n15:/tmp/pycore.37777/n15.conf# ping 10.0.6.10
PING 10.0.6.10 (10.0.6.10) 56(84) bytes of data.
64 bytes from 10.0.6.10: icmp_req=1 ttl=61 time=0.207 ms
64 bytes from 10.0.6.10: icmp_req=2 ttl=61 time=0.372 ms
64 bytes from 10.0.6.10: icmp_req=3 ttl=61 time=0.339 ms
64 bytes from 10.0.6.10: icmp_req=4 ttl=61 time=0.327 ms
64 bytes from 10.0.6.10: icmp_req=5 ttl=61 time=0.302 ms
64 bytes from 10.0.6.10: icmp_req=6 ttl=61 time=0.328 ms
64 bytes from 10.0.6.10: icmp_req=7 ttl=61 time=0.398 ms
64 bytes from 10.0.6.10: icmp_req=8 ttl=61 time=0.314 ms
64 bytes from 10.0.6.10: icmp_req=9 ttl=61 time=0.317 ms
64 bytes from 10.0.6.10: icmp_req=10 ttl=61 time=0.165 ms
64 bytes from 10.0.6.10: icmp_req=11 ttl=61 time=0.440 ms
64 bytes from 10.0.6.10: icmp_req=12 ttl=61 time=0.277 ms
--- 10.0.6.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 10997ms
rtt min/avg/max/ndev = 0.165/0.315/0.440/0.074 ms
root@n15:/tmp/pycore.37777/n15.conf#

vcmd
root@n13:/tmp/pycore.37777/n13.conf# ping 10.0.6.10
PING 10.0.6.10 (10.0.6.10) 56(84) bytes of data.
64 bytes from 10.0.6.10: icmp_req=1 ttl=62 time=0.202 ms
64 bytes from 10.0.6.10: icmp_req=2 ttl=62 time=0.254 ms
64 bytes from 10.0.6.10: icmp_req=3 ttl=62 time=0.263 ms
64 bytes from 10.0.6.10: icmp_req=4 ttl=62 time=0.263 ms
64 bytes from 10.0.6.10: icmp_req=5 ttl=62 time=0.364 ms
64 bytes from 10.0.6.10: icmp_req=6 ttl=62 time=0.298 ms
64 bytes from 10.0.6.10: icmp_req=7 ttl=62 time=0.382 ms
64 bytes from 10.0.6.10: icmp_req=8 ttl=62 time=0.214 ms
64 bytes from 10.0.6.10: icmp_req=9 ttl=62 time=0.275 ms
64 bytes from 10.0.6.10: icmp_req=10 ttl=62 time=0.242 ms
--- 10.0.6.10 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9000ms
rtt min/avg/max/ndev = 0.202/0.273/0.364/0.054 ms
root@n13:/tmp/pycore.37777/n13.conf#
```

R: Como se pode ver pela figura acima, existe conectividade entre um laptop de cada departamento e o servidor do departamento D, sendo n18 do departamento C, n15 do departamento A, n11 do departamento D, e n13 do departamento B e 10.0.6.10 o endereço IP do servidor do departamento D.

- e) Verifique se existe conectividade IP do router acesso aos servidores S1 e S2.



The image shows two side-by-side terminal windows, both titled 'vcmd'. The left window shows the output of a ping command from the router to the server at IP 10.0.6.10. It displays 10 successful ping requests with varying response times (e.g., 0.169 ms, 0.160 ms, etc.) and a summary at the bottom: '10 packets transmitted, 10 received, 0% packet loss, time 8997ms'. The right window shows the output of a ping command from the router to the server at IP 10.0.6.11. It also displays 10 successful ping requests with varying response times (e.g., 0.063 ms, 0.172 ms, etc.) and a summary at the bottom: '10 packets transmitted, 10 received, 0% packet loss, time 8999ms'.

Existe conectividade entre o router de acesso e os 2 servidores porque ao realizar o comando -ping existe transferência de dados entre o router e os 2 servidores.

- 2) Para o router e um laptop do departamento B:

- a) Execute o comando netstat -rn por forma a poder consultar a tabela de encaminhamento unicast (Ipv4). Inclua no seu relatório as tabelas de encaminhamento obtidas; interprete as várias entradas de cada tabela. Se necessário, consulte o manual respetivo (man netstat).

Router:

```
root@Ra:/tmp/pycore.37777/Ra.conf# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.0.1.0 10.0.0.2 255.255.255.0 UG 0 0 0 eth0
10.0.2.0 10.0.3.2 255.255.255.0 UG 0 0 0 eth1
10.0.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
10.0.4.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
10.0.5.0 10.0.0.2 255.255.255.0 UG 0 0 0 eth0
10.0.6.0 10.0.0.2 255.255.255.0 UG 0 0 0 eth0
10.0.7.0 10.0.3.2 255.255.255.0 UG 0 0 0 eth1
10.0.8.0 10.0.0.2 255.255.255.0 UG 0 0 0 eth0
root@Ra:/tmp/pycore.37777/Ra.conf#
```

Laptop:

```
root@n15:/tmp/pycore.37777/n15.conf# netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 10.0.4.1 0.0.0.0 UG 0 0 0 eth0
10.0.4.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
root@n15:/tmp/pycore.37777/n15.conf#
```

R: Relativamente ao router Ra:

A primeira entrada da tabela tem como rede destino a rede Ra (10.0.0.0) e o próximo salto vai corresponder ao próprio router Ra (10.0.0.1, sendo na tabela representado por 0.0.0.0), pois já estamos dentro dessa rede.

Para a segunda entrada, a rede destino é entre os routers Ra e Rb (10.0.0.2) e o próximo salto vai corresponder ao próprio router Rc (10.0.3.2, sendo na tabela representado por 0.0.0.0), pois já estamos dentro dessa rede.

Para a terceira entrada, o destino é a rede dos routers entre Ra e Rb (10.0.0.2) e o próximo salto vai corresponder ao router Rb (10.0.0.2) visto ser o caminho mais próximo de chegarmos a essa rede através do router Ra.

Para a quarta entrada, o destino é a rede dos routers entre Rd e Rc (10.0.3.2) e o próximo salto vai corresponder ao router Rd (10.0.1.2)

visto ser o caminho mais próximo de chegarmos a essa rede através do router Rc.

Para a quinta entrada, o destino é a rede dos routers entre Rd e Rb (10.0.3.2) e o próximo salto vai corresponder ao router Rd (10.0.1.2).

Relativamente ao laptop: Para a primeira entrada da tabela de encaminhamento, a rede destino é a rota por defeito (0.0.0.0) e o próximo salto vai corresponder ao *router* Ra (10.0.4.1).

Para a segunda entrada, a rede destino é a rede do departamento A (10.0.4.1) e o próximo salto vai corresponder ao próprio *host* (10.0.4.21, sendo que na tabela corresponde a 0.0.0.0).

- b) Diga, justificando, se está a ser usado encaminhamento estático ou dinâmico (sugestão: analise que processos estão a correr em cada sistema).

R: Está a ser usado encaminhamento estático nos três departamentos porque, além de ser uma rede de pequena dimensão, o endereçamento é baseado em rotas pré-definidas e estas rotas permanecem fixas. Entre os routers dos três departamentos o encaminhamento é dinâmico.

- c) Admita que, por questões administrativas, a rota por defeito (0.0.0.0 ou default) deve ser retirada definitivamente da tabela de encaminhamento do servidor S1 localizado no departamento D. Use o comando `route delete` para o efeito. Que implicações tem esta medida para os utilizadores da empresa que acedem ao servidor. Justifique.


```
vcmd
root@n5:/tmp/pycore.37745/n5.conf# route delete
Usage: inet_route [-vF] del {-host|-net} Target[/prefix] [gw Gw] [metric M] [[de
] If]
      inet_route [-vF] add {-host|-net} Target[/prefix] [gw Gw] [metric M]
      [netmask M] [mss Mss] [window W] [irtt I]
      [mod] [dyn] [reinststate] [[dev] If]
      inet_route [-vF] add {-host|-net} Target[/prefix] [metric M] reject
      inet_route [-FC] flush NOT supported
root@n5:/tmp/pycore.37745/n5.conf# netstat -rn
Kernel IP routing table
  Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
  0.0.0.0         10.0.6.1       0.0.0.0         Ug      0 0        0 eth0
  0.0.6.0         0.0.0.0       255.255.255.0   U        0 0        0 eth0
root@n5:/tmp/pycore.37745/n5.conf# route delete 0.0.0.0
OCDLRT: No such process
root@n5:/tmp/pycore.37745/n5.conf# route delete default
root@n5:/tmp/pycore.37745/n5.conf# netstat -rn
Kernel IP routing table
  Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
  0.0.6.0         0.0.0.0       255.255.255.0   U        0 0        0 eth0
root@n5:/tmp/pycore.37745/n5.conf#
```

R: A implementação desta medida não tem nenhuma implicação para os utilizadores que acedem ao servidor pois continua a existir a rota para a rede 10.0.6.0 a partir do servidor.

- d) Adicione as rotas estáticas necessárias para restaurar a conectividade para o servidor S1, por forma a contornar a restrição imposta em c). Utilize para o efeito o comando route add e registre os comandos que usou.

```
root@n5:/tmp/pycore.54265/n5.conf# route add -net 10.0.4.0 netmask 255.255.255.0 gw 10.0.6.1
root@n5:/tmp/pycore.54265/n5.conf# route add -net 10.0.5.0 netmask 255.255.255.0 gw 10.0.6.1
root@n5:/tmp/pycore.54265/n5.conf# route add -net 10.0.7.0 netmask 255.255.255.0 gw 10.0.6.1
```

R: Em que 10.0.4.0 corresponde a sub-rede do departamento A, 10.0.5.0 corresponde a B e a 10.0.7.0 corresponde a C.

- e) Teste a nova política de encaminhamento garantindo que o servidor está novamente acessível, utilizando para o efeito o comando ping. Registe a nova tabela de encaminhamento do servidor.

R: A nova tabela de encaminhamento é a seguinte:

```

root@n5:/tmp/pycore.54265/n5.conf# netstat -rn
Kernel IP routing table
Destination      Gateway         Genmask         Flags        MSS Window  irtt  Iface
10.0.4.0         10.0.6.1       255.255.255.0   UG           0 0        0     eth0
10.0.5.0         10.0.6.1       255.255.255.0   UG           0 0        0     eth0
10.0.6.0         0.0.0.0        255.255.255.0   U            0 0        0     eth0
10.0.7.0         10.0.6.1       255.255.255.0   UG           0 0        0     eth0

```

De seguida são novamente verificadas as ligações dos laptops com os departamentos:

```

ot@n5:/tmp/pycore.54265/n5.conf# ping 10.0.7.20
PING 10.0.7.20 (10.0.7.20) 56(84) bytes of data:
  bytes from 10.0.7.20: icmp_req=1 ttl=62 time=0.545 ms
  bytes from 10.0.7.20: icmp_req=2 ttl=62 time=0.374 ms
  bytes from 10.0.7.20: icmp_req=3 ttl=62 time=0.253 ms

- 10.0.7.20 ping statistics ---
packets transmitted, 3 received, 0% packet loss, time 2000ms
t min/avg/max/mdev = 0.253/0.390/0.545/0.121 ms
ot@n5:/tmp/pycore.54265/n5.conf# ping 10.0.4.20
PING 10.0.4.20 (10.0.4.20) 56(84) bytes of data:
  bytes from 10.0.4.20: icmp_req=1 ttl=61 time=0.273 ms
  bytes from 10.0.4.20: icmp_req=2 ttl=61 time=0.368 ms
  bytes from 10.0.4.20: icmp_req=3 ttl=61 time=0.358 ms

- 10.0.4.20 ping statistics ---
packets transmitted, 3 received, 0% packet loss, time 1998ms
t min/avg/max/mdev = 0.273/0.333/0.368/0.042 ms
ot@n5:/tmp/pycore.54265/n5.conf#

```

```

ot@n5:/tmp/pycore.54266/n5.conf# ping 10.0.5.20
PING 10.0.5.20 (10.0.5.20) 56(84) bytes of data:
  bytes from 10.0.5.20: icmp_req=1 ttl=62 time=0.338 ms
  bytes from 10.0.5.20: icmp_req=2 ttl=62 time=0.318 ms
  bytes from 10.0.5.20: icmp_req=3 ttl=62 time=0.269 ms
  bytes from 10.0.5.20: icmp_req=4 ttl=62 time=0.313 ms
  bytes from 10.0.5.20: icmp_req=5 ttl=62 time=0.346 ms
  bytes from 10.0.5.20: icmp_req=6 ttl=62 time=0.295 ms
  bytes from 10.0.5.20: icmp_req=7 ttl=62 time=0.263 ms

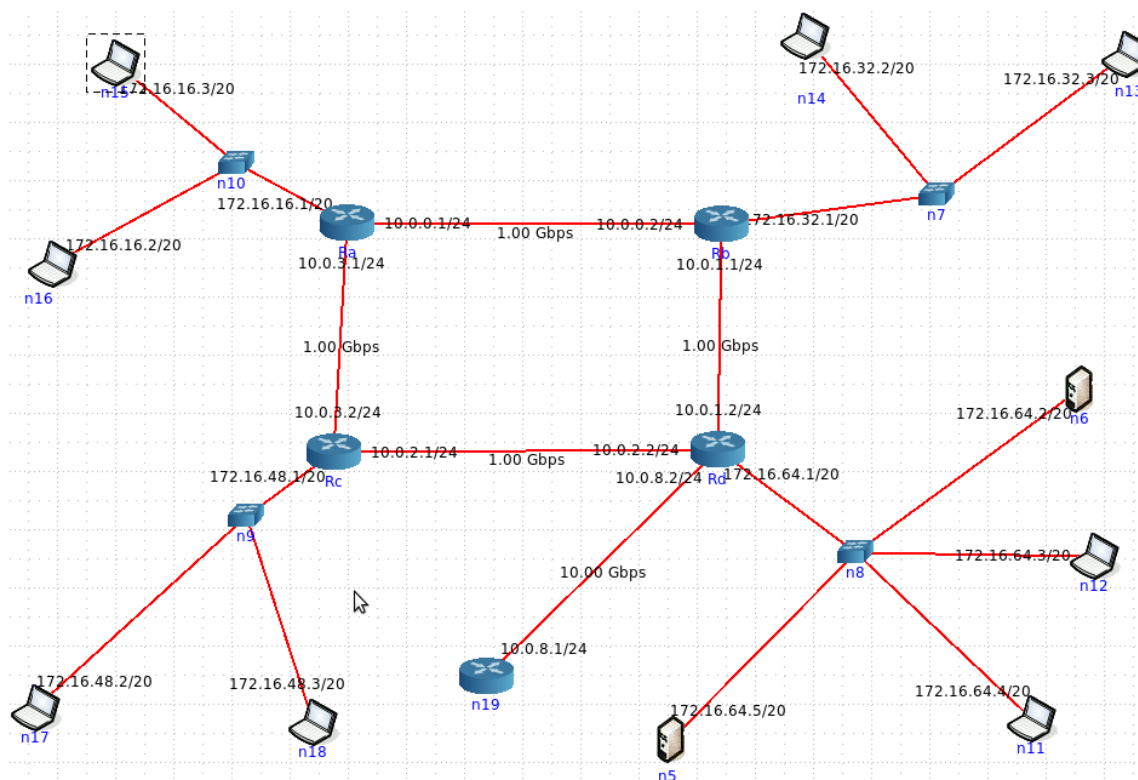
- 10.0.5.20 ping statistics ---
packets transmitted, 7 received, 0% packet loss, time 5999ms
t min/avg/max/mdev = 0.263/0.306/0.346/0.029 ms
ot@n5:/tmp/pycore.54266/n5.conf#

```

3) Assuma que o endereçamento entre os routers se mantém inalterado, contudo, o endereçamento em cada departamento deve ser redefinido.

1) Considere que dispõe apenas do endereço de rede IP 172.16.0.0/16, defina um novo esquema de endereçamento para as redes dos departamentos (mantendo a rede de acesso e core inalteradas) e atribua endereços às interfaces dos vários sistemas envolvidos. Deve justificar as opções usadas.

R:



Na nossa topologia temos 4 sub-redes e 10 interfaces. Como tal pretendemos definir um esquema de endereçamento de modo a que seja possível um futuro avanço na mesma para um aumento do numero de hosts e de sub-redes a endereçar.

Sabendo que temos um único endereço de rede IP: 172.16.0.0/16 verifica-se que apenas dispomos de 16 bits para o nosso novo esquema de endereçamento pois $32-16 = 16$ bits.

Decidimos dividir a nossa topologia em 14 sub-redes (2^4-2) e 4096 ($2^{12}-2$) hosts tendo em conta as necessidades futuras de estender a rede.(sub-traímos -2 aos hosts e sub-redes devido aos endereços reservados)

NetMask:

255.255.240.0 11111111.11111111.11110000.00000000 /20 16 Class C's

Sub-rede A:

N15-172.16.16.3/20

N16-172.16.16.2/20

Ra-172.16.16.1/20

Sub-rede B:

N14-172.16.32.2/20

N13-172.16.32.3/20

Rb-172.16.32.1/20

Sub-rede C:

N17-172.16.48.2/20

N18-172.16.48.3/20

Rc-172.16.48.1/20

Sub-rede D:

N5-172.16.64.5/20

N11-172.16.64.4/20

N12-172.16.64.3/20

N6-172.16.64.2/20

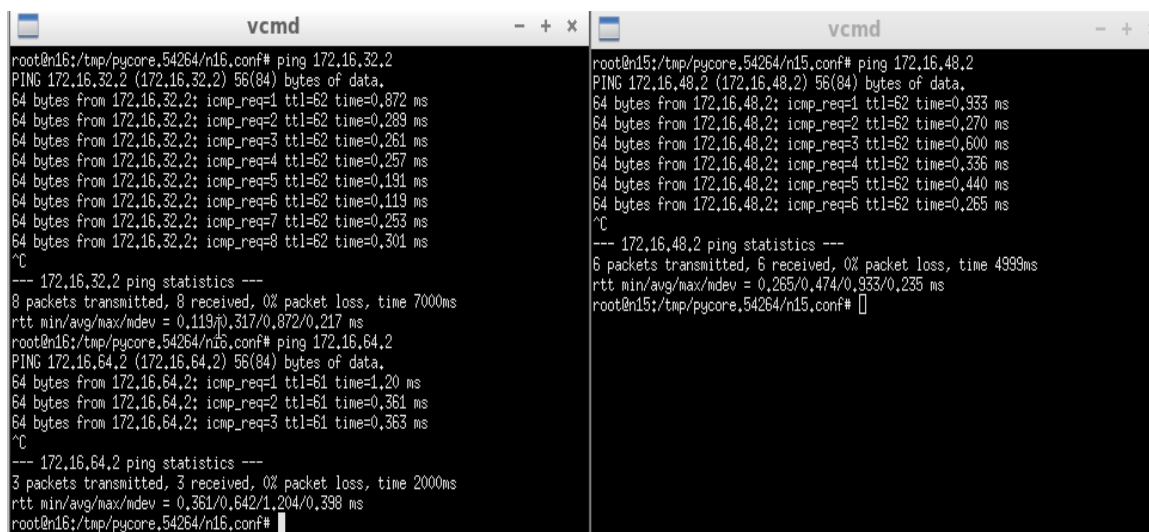
Rd-172.16.64.1/20

- 2) Qual a máscara de rede que usou (em formato decimal)?
Quantos hosts IP pode interligar em cada departamento?
Justifique

R: 255.255.240.0₁₀. Existem 16 bits para identificar a rede, sendo 4 destes usados para especificar a sub-rede. Por isso, e como para criar a máscara de rede é necessário colocar todos os bits identificadores da rede a 1, o número obtido em decimal foi 255.255.240.0₁₀. Os 12 bits restantes são para os *hosts* -> $2^{12} = 4096$. Há dois endereços reservados, logo há $4096 - 2 = 4094$ endereços possíveis para *hosts*. Assim, é possível interligar 4094 *hosts* em cada departamento, assumindo que apenas vamos ligar *hosts*.

- 3) Garanta que conectividade IP entre as várias redes locais da empresa MIEInet é mantida.

R: Como se pode ver na figura abaixo, há conetividade entre todas as redes locais da empresa.



The image shows two terminal windows side-by-side, both titled 'vcmd'. The left window shows a ping test from root@n16 to 172.16.32.2, which is successful with 8 packets received and 0% loss. It then shows a ping test from root@n16 to 172.16.64.2, which is also successful with 3 packets received and 0% loss. The right window shows a ping test from root@n15 to 172.16.48.2, which is successful with 6 packets received and 0% loss. It then shows a ping test from root@n15 to 172.16.64.2, which is also successful with 3 packets received and 0% loss. The output of the ping tests is as follows:

```
root@n16:/tmp/pycore.54264/n16.conf# ping 172.16.32.2
PING 172.16.32.2 (172.16.32.2) 56(84) bytes of data.
64 bytes from 172.16.32.2: icmp_req=1 ttl=62 time=0.872 ms
64 bytes from 172.16.32.2: icmp_req=2 ttl=62 time=0.289 ms
64 bytes from 172.16.32.2: icmp_req=3 ttl=62 time=0.261 ms
64 bytes from 172.16.32.2: icmp_req=4 ttl=62 time=0.257 ms
64 bytes from 172.16.32.2: icmp_req=5 ttl=62 time=0.191 ms
64 bytes from 172.16.32.2: icmp_req=6 ttl=62 time=0.119 ms
64 bytes from 172.16.32.2: icmp_req=7 ttl=62 time=0.253 ms
64 bytes from 172.16.32.2: icmp_req=8 ttl=62 time=0.301 ms
^C
--- 172.16.32.2 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7000ms
rtt min/avg/max/mdev = 0.119/0.317/0.872/0.217 ms
root@n16:/tmp/pycore.54264/n16.conf# ping 172.16.64.2
PING 172.16.64.2 (172.16.64.2) 56(84) bytes of data.
64 bytes from 172.16.64.2: icmp_req=1 ttl=61 time=1.20 ms
64 bytes from 172.16.64.2: icmp_req=2 ttl=61 time=0.361 ms
64 bytes from 172.16.64.2: icmp_req=3 ttl=61 time=0.363 ms
^C
--- 172.16.64.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.361/0.642/1.204/0.398 ms
root@n16:/tmp/pycore.54264/n16.conf#

root@n15:/tmp/pycore.54264/n15.conf# ping 172.16.48.2
PING 172.16.48.2 (172.16.48.2) 56(84) bytes of data.
64 bytes from 172.16.48.2: icmp_req=1 ttl=62 time=0.933 ms
64 bytes from 172.16.48.2: icmp_req=2 ttl=62 time=0.270 ms
64 bytes from 172.16.48.2: icmp_req=3 ttl=62 time=0.600 ms
64 bytes from 172.16.48.2: icmp_req=4 ttl=62 time=0.336 ms
64 bytes from 172.16.48.2: icmp_req=5 ttl=62 time=0.440 ms
64 bytes from 172.16.48.2: icmp_req=6 ttl=62 time=0.265 ms
^C
--- 172.16.48.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.265/0.474/0.933/0.235 ms
root@n15:/tmp/pycore.54264/n15.conf#
```