Universidade do Minho

Mestrado Integrado em Engenharia Informática

TP2: Protocolo IP

Redes de Computadores

Grupo 1 – PL4

Ana Pereira A81712

Ana Ribeiro A82474

Jéssica Lemos A82061

1 Questões e Respostas

1.1 Parte I - Datagramas IP e Fragmentação

Questão 1

Prepare uma topologia CORE para verificar o comportamento do traceroute. Ligue um host (pc) h1 a um router r2; o router r2 a um router r3, que por sua vez, se liga a um host (servidor) s4. (Note que pode não existir conectividade IP imediata entre h1 e s4 até que o routing estabilize). Ajuste o nome dos equipamentos atribuídos por defeito para a topologia do enunciado.

Implementamos a seguinte topologia core:

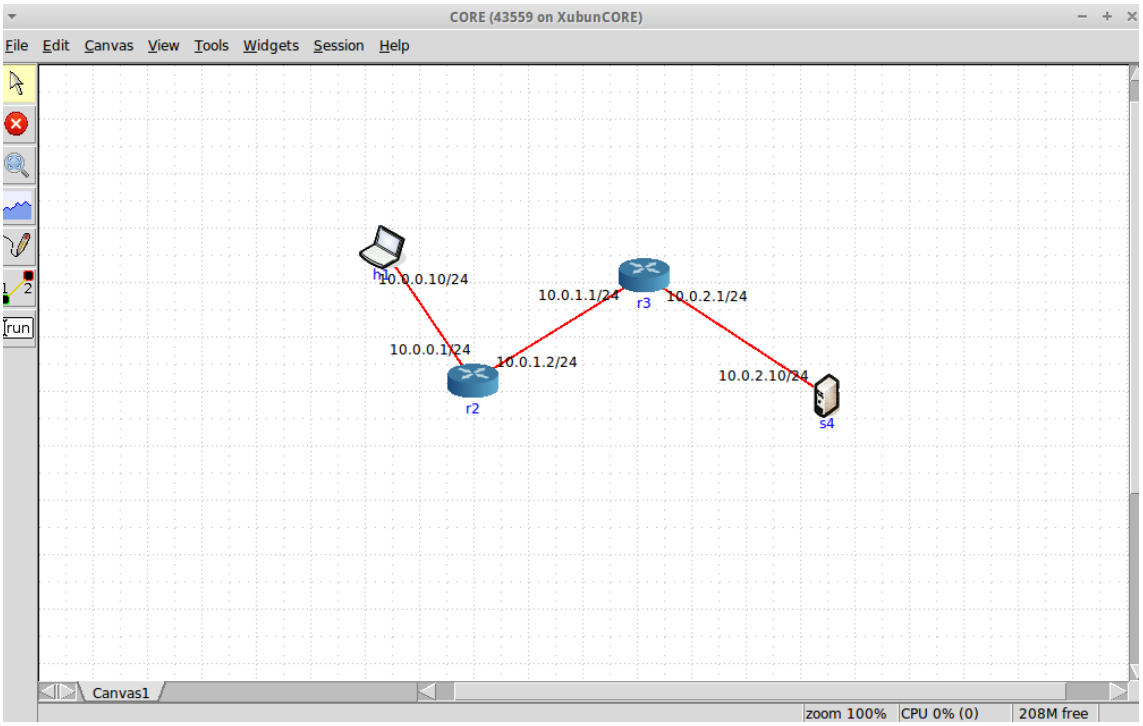


Figura 1 - Topologia CORE

a. Active o wireshark ou o tcpdump no pc h1. Numa shell de h1, execute o comando traceroute -I para o endereço IP do host s4.

Ativamos o wireshark no pc h1, executando o comando traceroute -I para o endereço IP do host s4 (10.0.2.10):

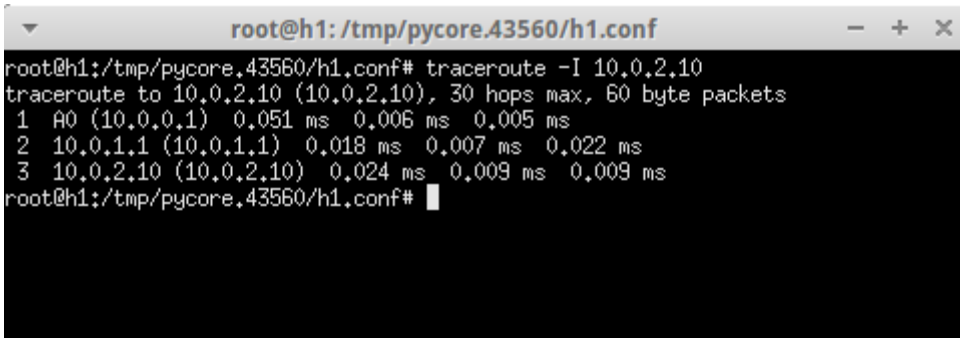
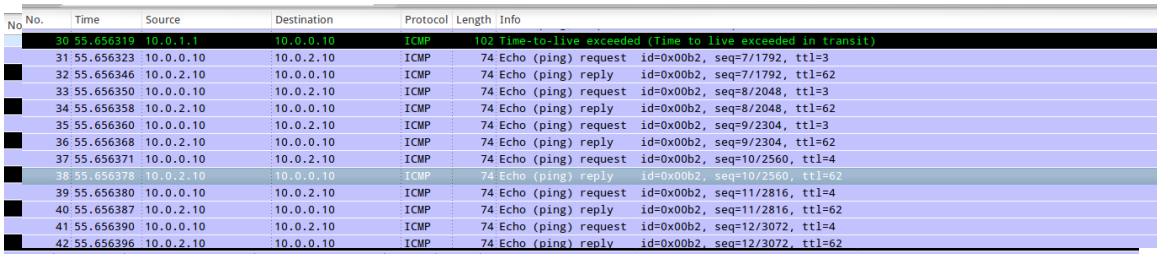


Figura 2 - Comando traceroute -I para o endereço IP do host s4

b. Registe e analise o tráfego ICMP enviado por h1 e o tráfego ICMP recebido como resposta. Comente os resultados face ao comportamento esperado.



No.	Time	Source	Destination	Protocol	Length	Info
30	55.656319	10.0.1.1	10.0.0.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
31	55.656323	10.0.0.10	10.0.2.10	ICMP	74	Echo (ping) request id=0x00b2, seq=7/1792, ttl=3
32	55.656346	10.0.2.10	10.0.0.10	ICMP	74	Echo (ping) reply id=0x00b2, seq=7/1792, ttl=62
33	55.656350	10.0.0.10	10.0.2.10	ICMP	74	Echo (ping) request id=0x00b2, seq=8/2048, ttl=3
34	55.656358	10.0.2.10	10.0.0.10	ICMP	74	Echo (ping) reply id=0x00b2, seq=8/2048, ttl=62
35	55.656360	10.0.0.10	10.0.2.10	ICMP	74	Echo (ping) request id=0x00b2, seq=9/2304, ttl=3
36	55.656368	10.0.2.10	10.0.0.10	ICMP	74	Echo (ping) reply id=0x00b2, seq=9/2304, ttl=62
37	55.656371	10.0.0.10	10.0.2.10	ICMP	74	Echo (ping) request id=0x00b2, seq=10/2560, ttl=4
38	55.656378	10.0.2.10	10.0.0.10	ICMP	74	Echo (ping) reply id=0x00b2, seq=10/2560, ttl=62
39	55.656380	10.0.0.10	10.0.2.10	ICMP	74	Echo (ping) request id=0x00b2, seq=11/2816, ttl=4
40	55.656387	10.0.2.10	10.0.0.10	ICMP	74	Echo (ping) reply id=0x00b2, seq=11/2816, ttl=62
41	55.656390	10.0.0.10	10.0.2.10	ICMP	74	Echo (ping) request id=0x00b2, seq=12/3072, ttl=4
42	55.656396	10.0.2.10	10.0.0.10	ICMP	74	Echo (ping) reply id=0x00b2, seq=12/3072, ttl=62

Figura 3 - Tráfego ICMP enviado e recebido por h1

Esperávamos que enquanto o TTL de cada pacote fosse inferior a 3 o pacote não chegasse ao s4. Quando o TTL atinge o valor 0 o router descarta o datagrama e devolve uma mensagem de controlo ICMP (Internet Control Message Protocol) ao host de origem, indicando que o TTL foi excedido. Cada vez que passa no router é decrementado o TTL de cada datagrama. Assim, e atendendo ao facto que neste percurso existem dois routers seria necessário um TTL mínimo de 3.

Inicialmente foram lançados 3 pacotes com TTL=1 que deveriam chegar ao servidor s4, contudo não passaram do router r2 sendo emitida uma mensagem de erro. De seguida, foram enviados mais 3 pacotes, mas com o TTL=2 que também não conseguiram alcançar s4, falhando no router r3. Foi-se repetindo o processo incrementando o valor do TTL e como é possível constatar o pacote atinge o destino. Deste modo, verificamos que é recebida uma mensagem de erro ("Time-to-live exceeded") sempre que o TTL é inferior a 3, tal como previámos.

c. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o destino s4? Verifique na prática que a sua resposta está correta.

O valor inicial mínimo do campo TTL para alcançar o destino s4 deverá ser 3, como se pode verificar na Figura 3, em que os pacotes com TTL inferior a 3 recebem uma mensagem de erro.

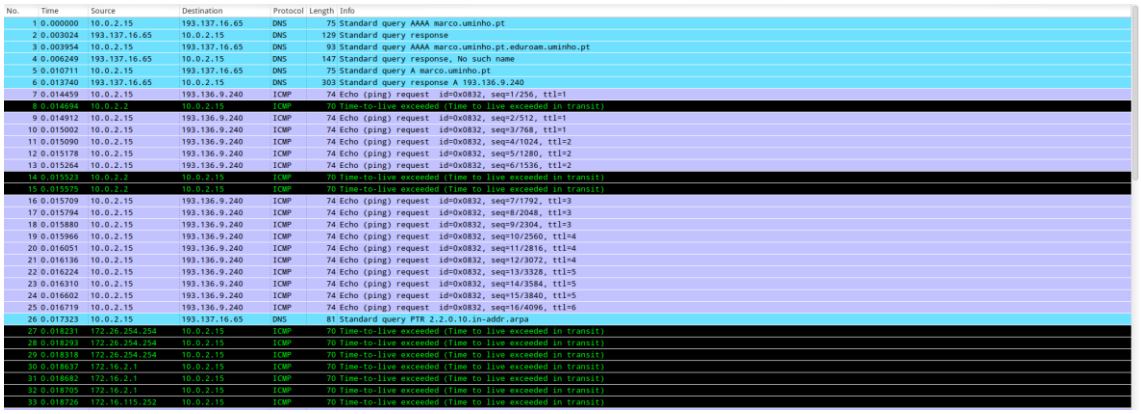
d. Qual o valor médio do tempo de ida-e-volta (Round-Trip Time) obtido?

Tendo em conta a Figura 2,

RTT ≈ ((0.051 + 0.06 + 0.005) /3 + (0.018 + 0.007 + 0.022) /3 + (0.024 + 0.009 + 0.009) /3) x 2 ≈ 0.137

Questão 2

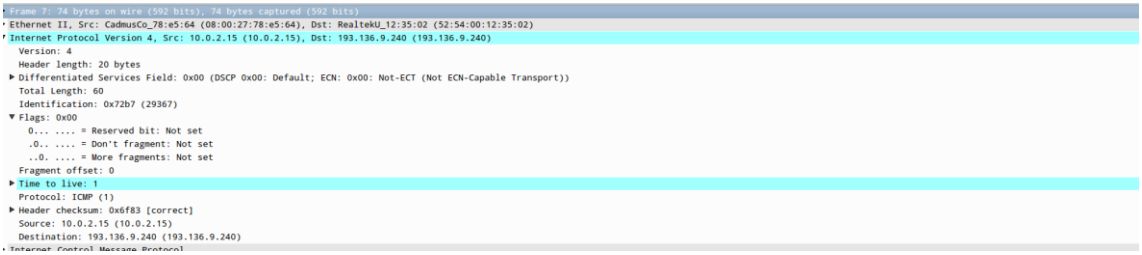
Começamos por fazer *traceroute -I marco.uminho.pt* obtendo a seguinte tráfego.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	193.137.16.65	DNS	75	Standard query AAAA marco.uminho.pt
2	0.003024	193.137.16.65	10.0.2.15	DNS	129	Standard query response
3	0.003954	10.0.2.15	193.137.16.65	DNS	93	Standard query AAAA marco.uminho.pt.eduroam.uminho.pt
4	0.006249	193.137.16.65	10.0.2.15	DNS	147	Standard query response, No such name
5	0.010711	10.0.2.15	193.137.16.65	DNS	75	Standard query A marco.uminho.pt
6	0.013740	193.137.16.65	10.0.2.15	DNS	303	Standard query response A 193.136.9.240
7	0.014459	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=1/256, ttl=1
8	0.014694	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
9	0.014912	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=2/512, ttl=1
10	0.015002	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=3/768, ttl=1
11	0.015090	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=4/1024, ttl=2
12	0.015178	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=5/1280, ttl=2
13	0.015264	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=6/1536, ttl=2
14	0.015523	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
15	0.015575	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
16	0.015709	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=7/1792, ttl=3
17	0.015794	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=8/2048, ttl=3
18	0.015880	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=9/2304, ttl=3
19	0.015966	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=10/2560, ttl=4
20	0.016051	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=11/2816, ttl=4
21	0.016136	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=12/3072, ttl=4
22	0.016224	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=13/3328, ttl=5
23	0.016310	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=14/3584, ttl=5
24	0.016602	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=15/3840, ttl=5
25	0.016719	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=16/4096, ttl=6
26	0.017323	10.0.2.15	193.137.16.65	DNS	81	Standard query PTR 2.2.0.10.in-addr.arpa
27	0.018231	172.26.254.254	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
28	0.018293	172.26.254.254	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
29	0.018318	172.26.254.254	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
30	0.018627	172.16.2.1	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
31	0.018682	172.16.2.1	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
32	0.018705	172.16.2.1	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
33	0.018726	172.16.115.252	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Figura 4 - Tráfego de pacotes

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



```
Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: CadmusCo_78:e5:64 (08:00:27:78:e5:64), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 193.136.9.240 (193.136.9.240)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 60
  Identification: 0x72b7 (29367)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x6f83 [correct]
  Source: 10.0.2.15 (10.0.2.15)
  Destination: 193.136.9.240 (193.136.9.240)
Internet Control Message Protocol
```

Figura 5 - Primeiro datagrama

O endereço IP da interface ativa do computador é 10.0.2.15 indicado pelo campo *Source*.

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

O valor do campo protocolo é 1 que identifica o protocolo ICMP.

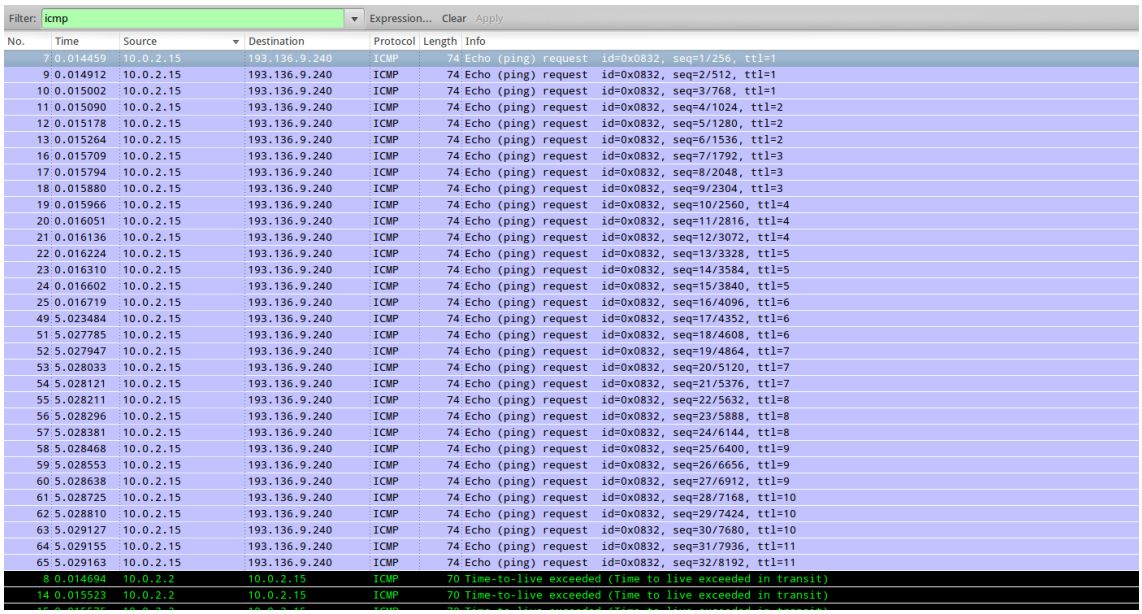
c. Quantos bytes tem o cabeçalho IP(v4)? Quantos bytes tem o campo de dados (payload) do datagrama? Como se calcula o tamanho do payload?

O cabeçalho IP tem 20 bytes, verificado no campo *Header length* na Figura 5. O campo de dados (payload) terá como tamanho a diferença entre o número total de bytes e o tamanho do cabeçalho do datagrama, ou seja, será 60-20=40 bytes.

d. O datagrama IP foi fragmentado? Justifique

Podemos observar no Figura 5 que no campo *Flags* o *Fragment offset* tem valor 0. Assim, se existirem mais fragmentos, este será o primeiro. Na flag *More fragments* podemos verificar se existem mais fragmentos para além do atual, se o valor for 1 existem, se for 0 então não existem. Como estamos no primeiro fragmento e não existem mais (o valor de *More fragments* é 0) podemos concluir que este é o datagrama original.

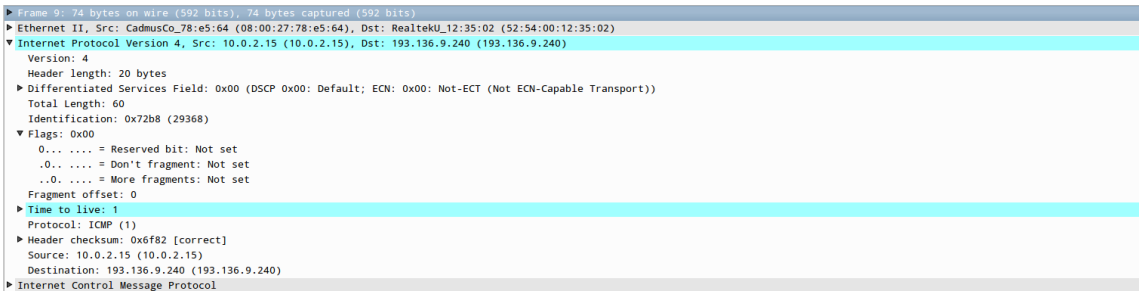
e. Ordene os pacotes capturados de acordo com o endereço IP fonte (e.g., selecionando o cabeçalho da coluna Source), e analise a sequência de tráfego ICMP gerado a partir do endereço IP atribuído à interface da sua máquina. Para a sequência de mensagens ICMP enviadas pelo seu computador, indique que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



Filter: icmp — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
7	0.014459	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=1/256, ttl=1
9	0.014912	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=2/512, ttl=1
10	0.015002	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=3/768, ttl=1
11	0.015090	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=4/1024, ttl=2
12	0.015178	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=5/1280, ttl=2
13	0.015264	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=6/1536, ttl=2
16	0.015709	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=7/1792, ttl=3
17	0.015794	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=8/2048, ttl=3
18	0.015880	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=9/2304, ttl=3
19	0.015966	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=10/2560, ttl=4
20	0.016051	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=11/2816, ttl=4
21	0.016136	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=12/3072, ttl=4
22	0.016224	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=13/3328, ttl=5
23	0.016310	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=14/3584, ttl=5
24	0.016602	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=15/3840, ttl=5
25	0.016719	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=16/4096, ttl=6
49	5.023484	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=17/4352, ttl=6
51	5.027785	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=18/4608, ttl=6
52	5.027947	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=19/4864, ttl=7
53	5.028033	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=20/5120, ttl=7
54	5.028121	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=21/5376, ttl=7
55	5.028211	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=22/5632, ttl=8
56	5.028296	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=23/5888, ttl=8
57	5.028381	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=24/6144, ttl=8
58	5.028468	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=25/6400, ttl=9
59	5.028553	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=26/6656, ttl=9
60	5.028638	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=27/6912, ttl=9
61	5.028725	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=28/7168, ttl=10
62	5.028810	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=29/7424, ttl=10
63	5.029127	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=30/7680, ttl=10
64	5.029155	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=31/7936, ttl=11
65	5.029163	10.0.2.15	193.136.9.240	ICMP	74	Echo (ping) request id=0x0832, seq=32/8192, ttl=11
8	0.014694	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	0.015523	10.0.2.2	10.0.2.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Figura 6 - Pacotes capturados de acordo com o endereço IP fonte



```
▶ Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: CadmusCo_78:e5:64 (08:00:27:78:e5:64), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▼ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 193.136.9.240 (193.136.9.240)
    Version: 4
    Header length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x72b8 (29368)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
  ▶ Time to live: 1
    Protocol: ICMP (1)
  ▶ Header checksum: 0x6f82 [correct]
    Source: 10.0.2.15 (10.0.2.15)
    Destination: 193.136.9.240 (193.136.9.240)
▶ Internet Control Message Protocol
```

Figura 7 - Segundo datagrama

Como podemos verificar os campos do cabeçalho IP que variam de pacote em pacote são o TTL e o identificador do pacote como podemos ver nas Figuras 5 e 7 no campo *Identification*.

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

Podemos de verificar que tanto os valores do TTL como o identificador do pacote incrementam em 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?

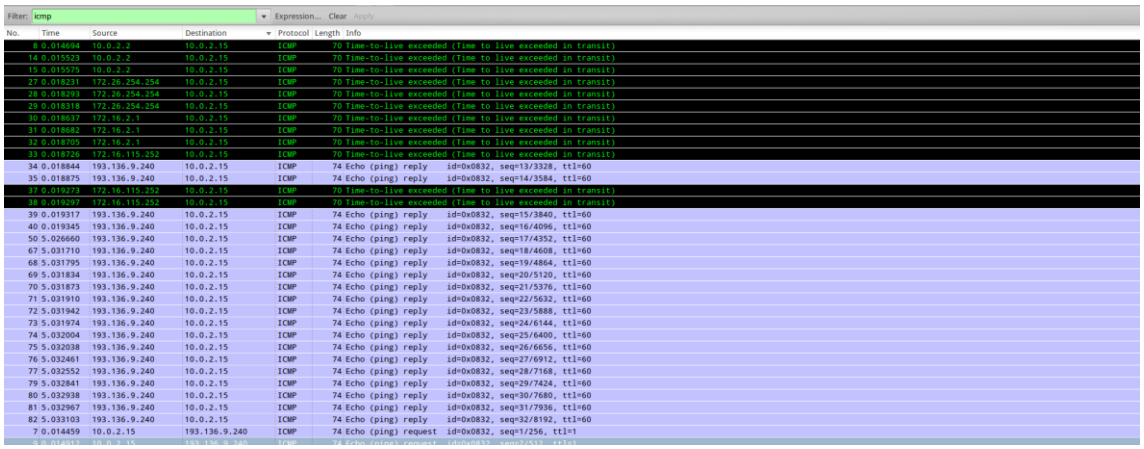


Figura 8 - Pacotes capturados de acordo com o endereço IP destino

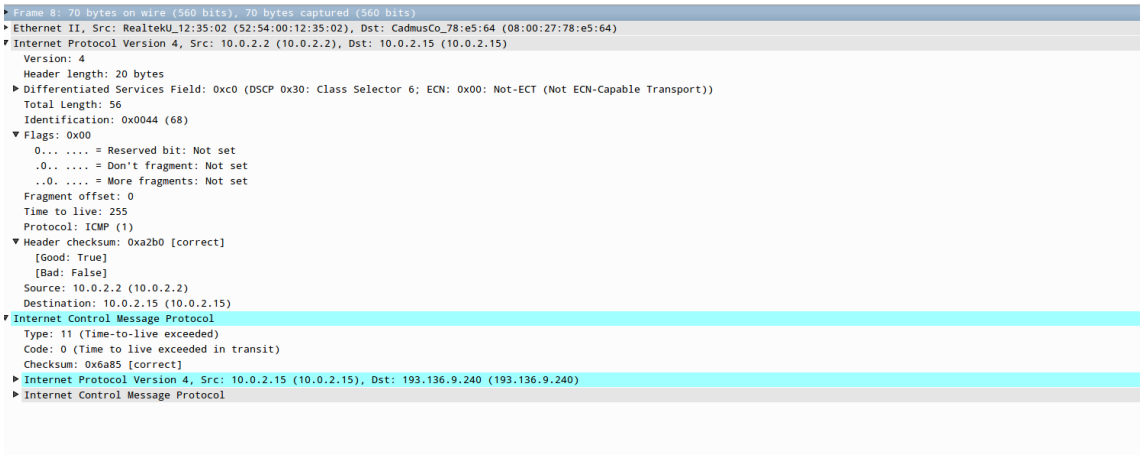


Figura 9 - Primeiro datagrama da captura anterior

O valor do campo TTL da primeira mensagem de erro ICMP (“Time-to-live exceeded”) é 255. Este valor não permanece constante para todas as mensagens de resposta ICMP, dado que é sempre decrementada uma unidade uma vez que as mensagens de erro para chegarem ao *host* necessitam de passar pelos routers.

Questão 3

Pretende-se agora analisar a fragmentação de pacotes IP. Reponha a ordem do tráfego capturado usando a coluna do tempo de captura. Observe o tráfego depois do tamanho de pacote ter sido definido para 35XX bytes.

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

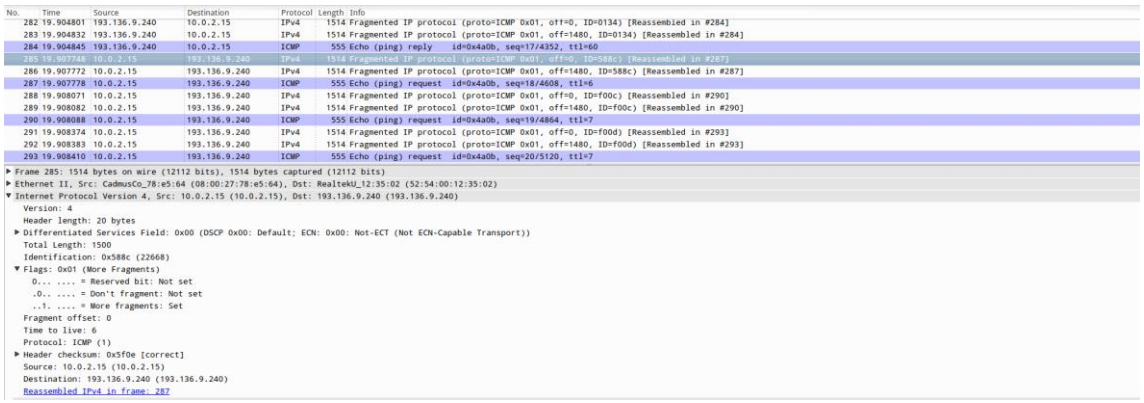


Figura 10 - Tráfego de pacotes com tamanho 3501 bytes com informação sobre o primeiro fragmento do datagrama

O tamanho máximo do pacote permitido é 1500 bytes como verificado no campo *Total Length.* Dado que o tamanho do pacote é 3501 bytes, o tamanho do pacote é demasiado grande para circular na rede pelo que houve a necessidade de fragmentar o pacote.

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?

Na Figura 10 apresenta-se o primeiro fragmento do datagrama em que podemos verificar que a flag *More fragments* tem valor 1, pelo que existem mais fragmentos. O valor do *Fragment offset* é 0 pelo que ficamos a saber que se trata do primeiro fragmento, uma vez que esta flag nos indica a que parte do pacote corresponde este fragmento. O indicador *Total Length* infere o tamanho total do fragmento, que tem como valor 1500. O tamanho do datagrama IP é de 1480 bytes, uma vez que é retirado os 20 bytes do *Header*.

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?

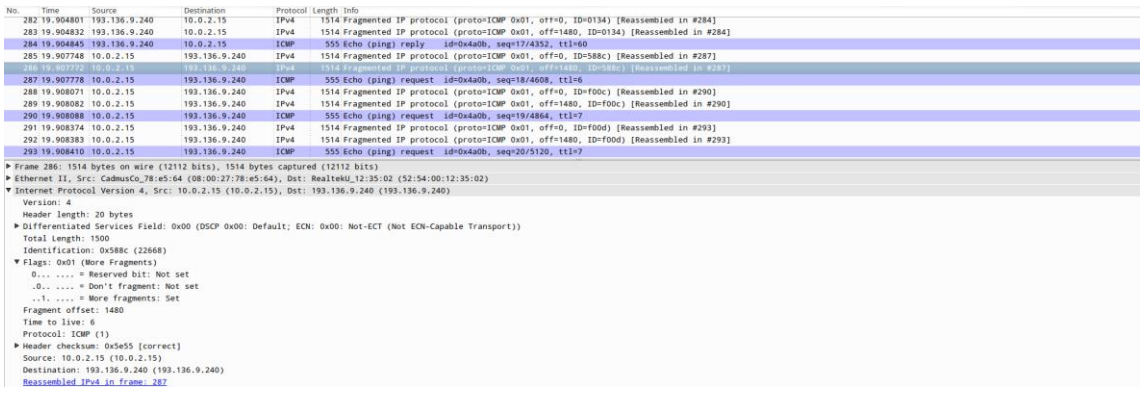


Figura 11 - Tráfego de pacotes com tamanho 3501 bytes com informação sobre o segundo fragmento do datagrama

Como podemos verificar na imagem acima, o indicador *Fragment offset* é 1480, começando assim onde o anterior acaba, ou seja, este é o segundo fragmento. Dado que o valor de *More Fragments* é 1, concluímos que existem mais fragmentos.

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

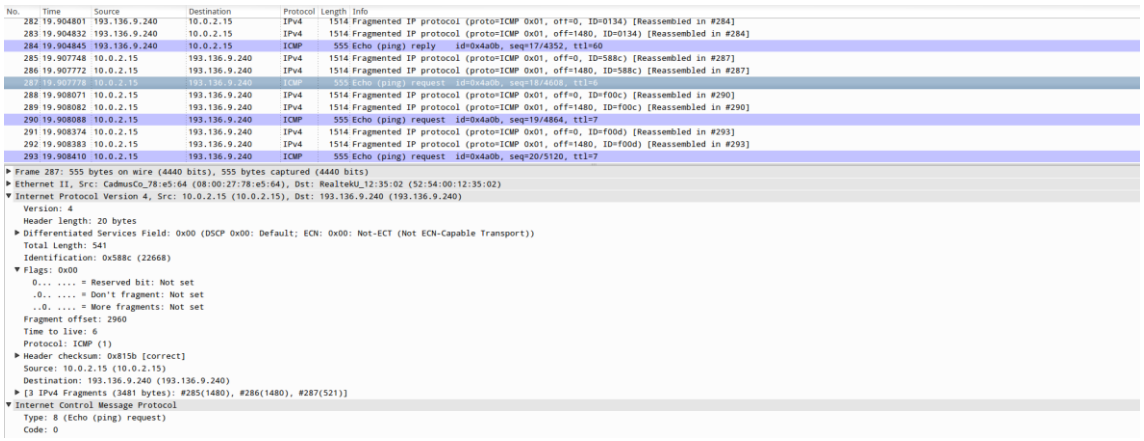


Figura 12 - Tráfego de pacotes com tamanho 3501 bytes com informação sobre o último fragmento do datagrama

Foram criados 3 fragmentos a partir do datagrama original, sendo que todos estes têm a mesma identificação (Ox588c) permitindo assim perceber que pertencem todos ao mesmo datagrama inicial. Como podemos verificar pela Figura 10 o *Fragment offset* é 2960 (1480+1480), a soma do tamanho dos dois primeiros fragmentos. Também constatamos que se trata do último fragmento uma vez que o valor da flag *More Fragments* é 0.

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.

Os campos que diferem nos cabeçalhos IP dos diferentes fragmentos são as flags *Fragment offset*, que permite identificar a posição do fragmento no datagrama original, e More Fragments, que indica se há mais fragmentos do datagrama original. Assim, é possível reconstituir o pacote original agrupando os fragmentos por ordem crescente do *Fragment offset*.

1.2 Parte II - Endereçamento e Encaminhamento IP

Questão 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 definida e o endereçamento usado.

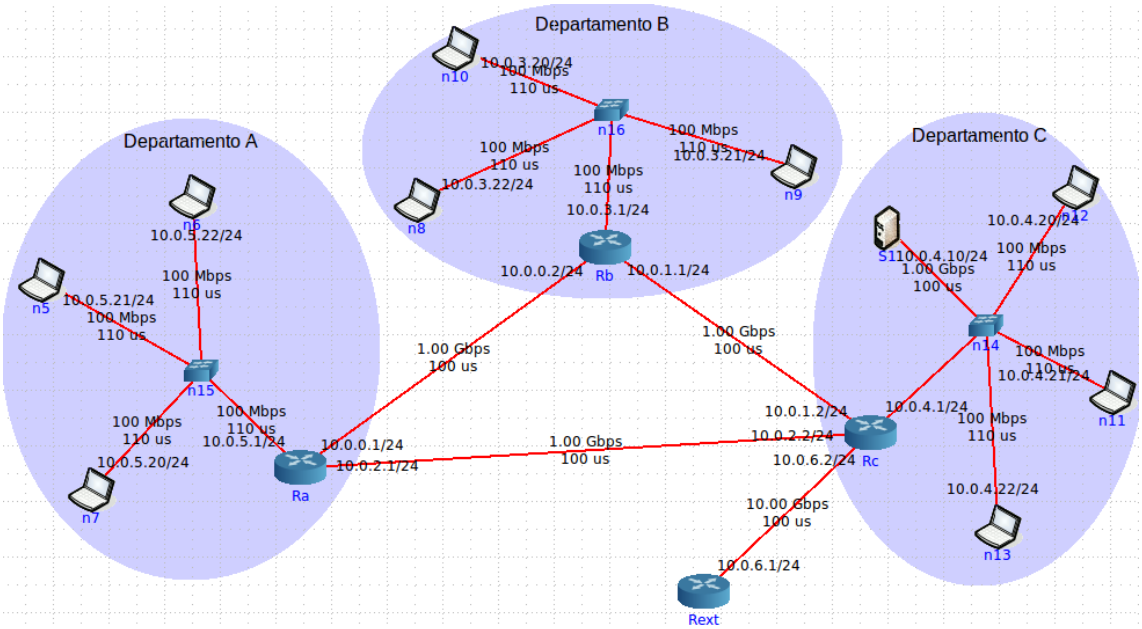


Figura 13 - Topologia da organização MIEI-RC

Na Figura 13, é possível observar os endereços IP de cada equipamento. Também podemos verificar que a máscara de rede é 255.255.255.0, dado que na notação CIDR o número de bits é 24 (/24).

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

Uma vez que os endereços privados então nas gamas:

- 192.168.0.0 – 192.168.255.255 / 16
- 172.16.0.0 – 172.31.255.255 / 12
- 10.0.0.0 – 10.255.255.255 / 8

E como todos os endereços IP da rede pertencem ao terceiro intervalo, podemos concluir que se tratam de endereços privados.

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

Os switches intervêm na camada de ligação 2, pelo que são transparentes à camada de ligação 3 onde se encontram os endereços IP, assim não será necessário atribuir-lhes um endereço. Este encaminha os pacotes, tendo em conta apenas os endereços MAC do equipamento.

d. Usando o comando ping certifique-se que existe conectividade IP entre os laptops dos vários departamentos e o servidor do departamento C (basta certificar-se da conectividade de um laptop por departamento).

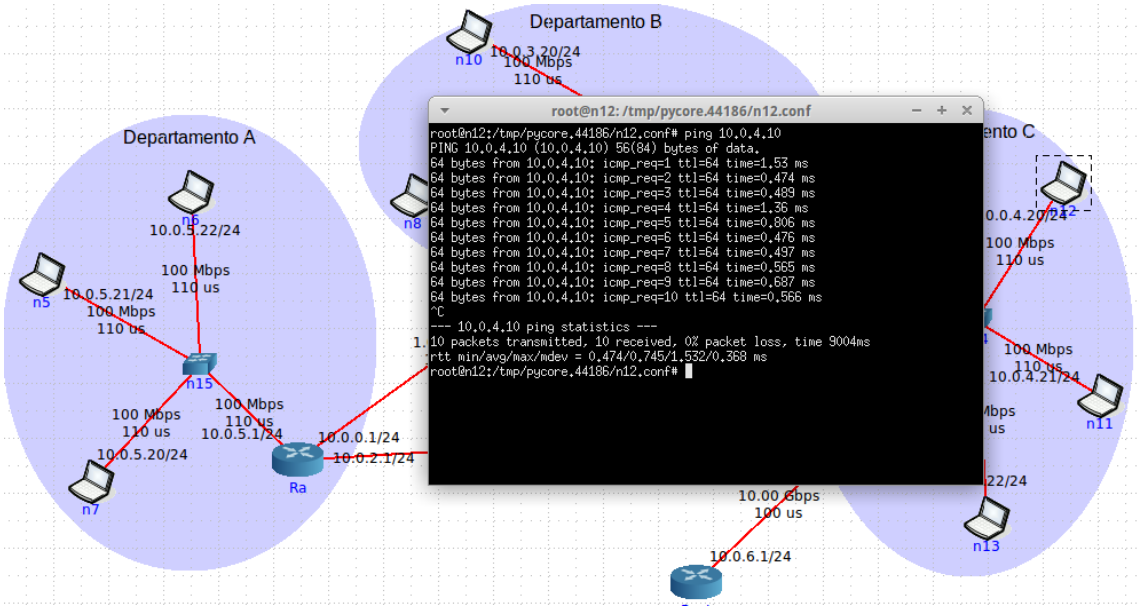


Figura 14 - Conectividade entre laptop do departamento C e o servidor

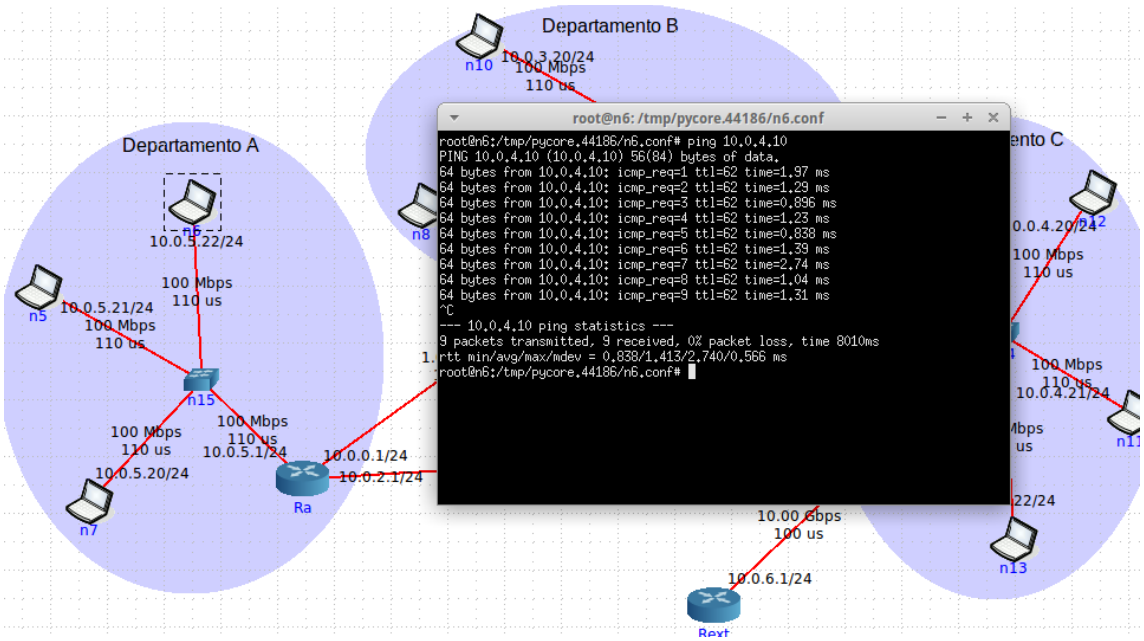


Figura 15 - Conectividade entre laptop do departamento A e o servidor

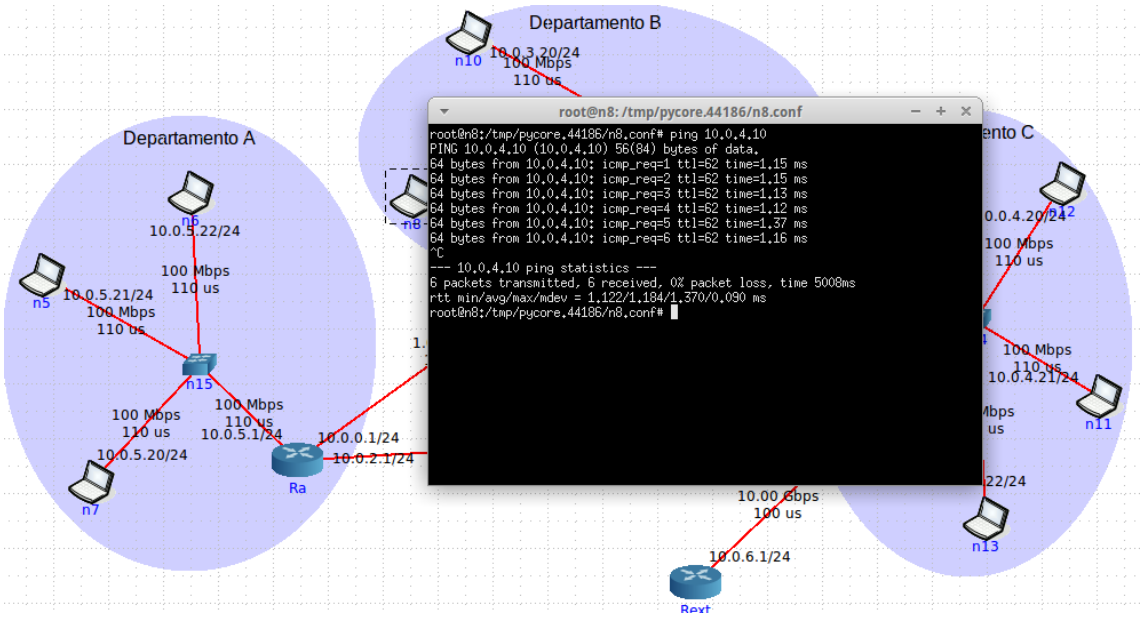


Figura 16 - Conectividade entre laptop do departamento B e o servidor

Para verificar se existia conectividade, utilizamos o comando ping que envia pacotes para o servidor. Quando este o recebe envia uma mensagem de volta, que contém por exemplo o número do pacote e o tempo de ida e volta. Caso tal não se verifique, envia uma mensagem de erro. Como podemos observar nas figuras apresentadas anteriormente todos os pacotes foram entregues, podendo assim concluir que existe conectividade entre cada um dos laptops de cada departamento e o servidor S1.

e. Verifique se existe conectividade IP do router de acesso Rext para o servidor S1.

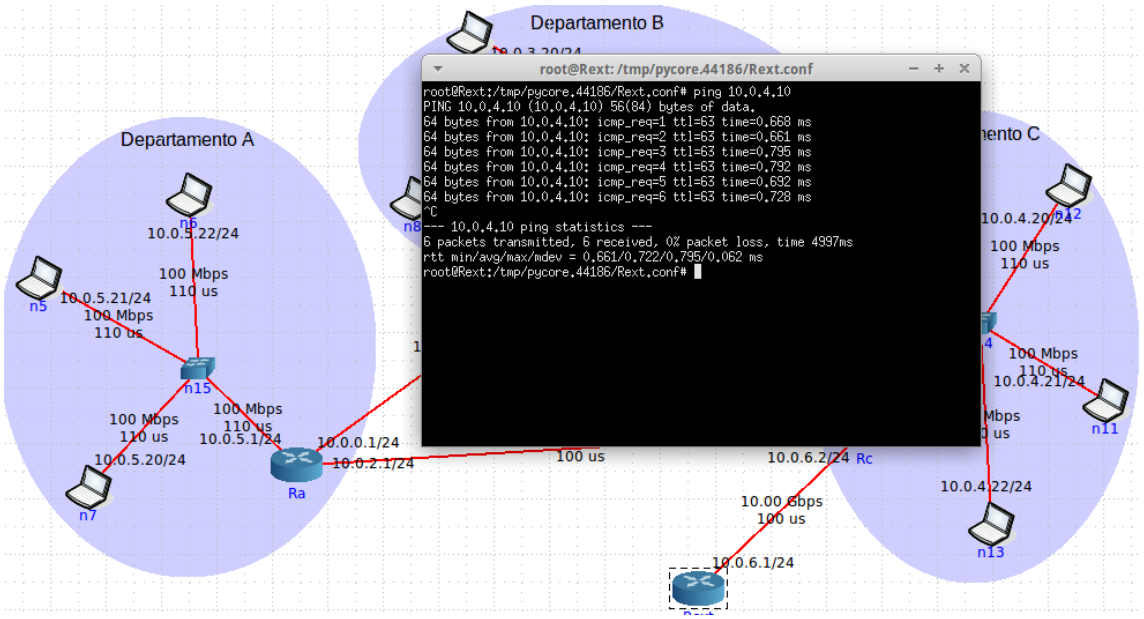


Figura 17 - Conectividade entre o router de acesso Rext e o servidor S1

Seguindo o raciocínio utilizado na alínea anterior, verificamos que existe conectividade do router Rext para o servidor S1.

Questão 2

Para o router e um laptop do departamento A:

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).

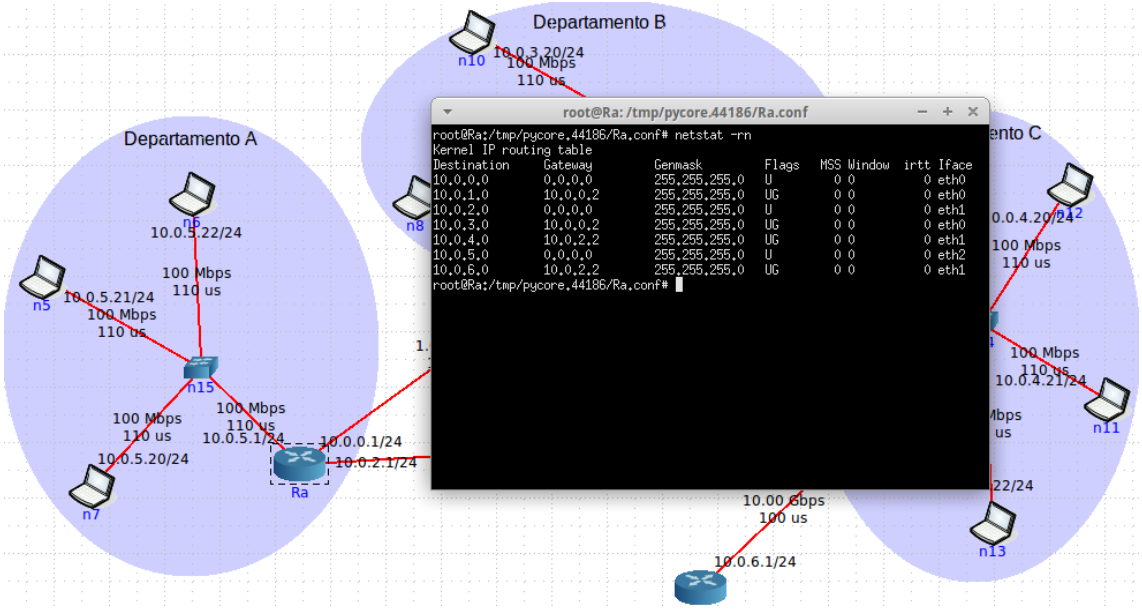


Figura 18 - Tabela de encaminhamento de Ra

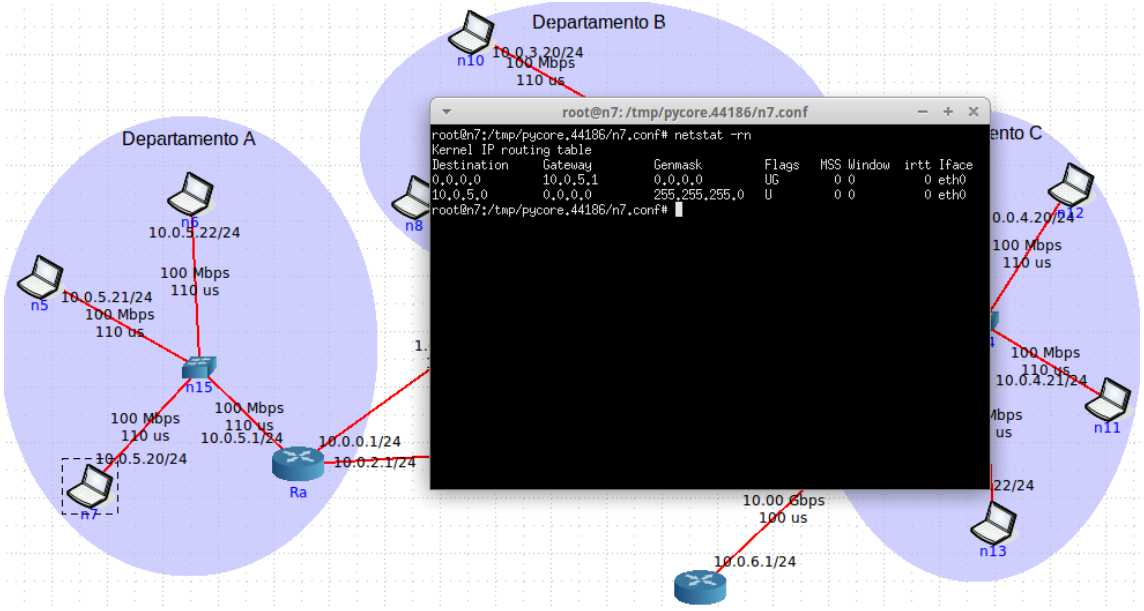


Figura 19 - Tabela de encaminhamento de n7

Nas tabelas de encaminhamento podemos retirar informação relativa à rota que o pacote irá fazer. A coluna *Destination* é nos indicada a sub-rede destino, enquanto a *Gateway* dá-nos a informação do equipamento pelo qual o pacote irá passar. Por último, a coluna *Genmask* indica o tipo da máscara utilizada.

No caso do laptop (n7) existem duas hipóteses. A primeira em que independentemente do endereço de destino o pacote irá para o router Ra e a segunda em que indica que se o pacote destino tiver o endereço da sub-rede do Departamento A pode optar por um destino.

No caso do router (Ra), quando o Gateway tem valor 0.0.0.0 então o pacote pode seguir qualquer caminho. Os pacotes que tenham como destino um equipamento da sub-rede 10.0.1.0 e 10.0.3.0 terão de passar pelo router Rb (10.0.0.2). Quanto aos pacotes com destino nas sub-redes 10.0.4.0 e 10.0.6.0 passarão pelo Rc (10.0.2.2).

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

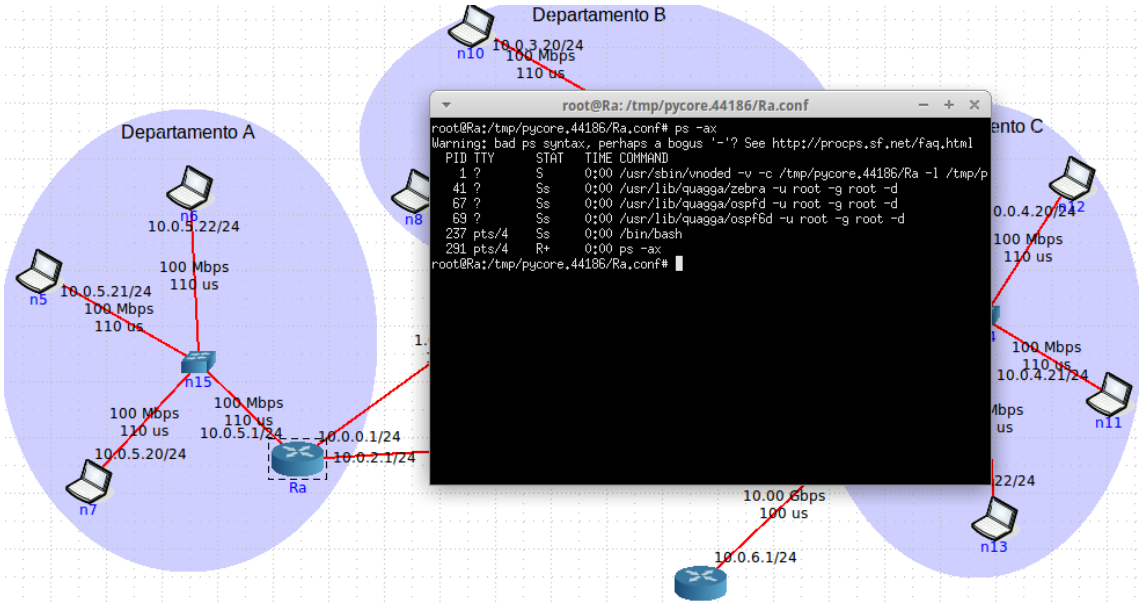


Figura 20 - Processos a correr no router Ra

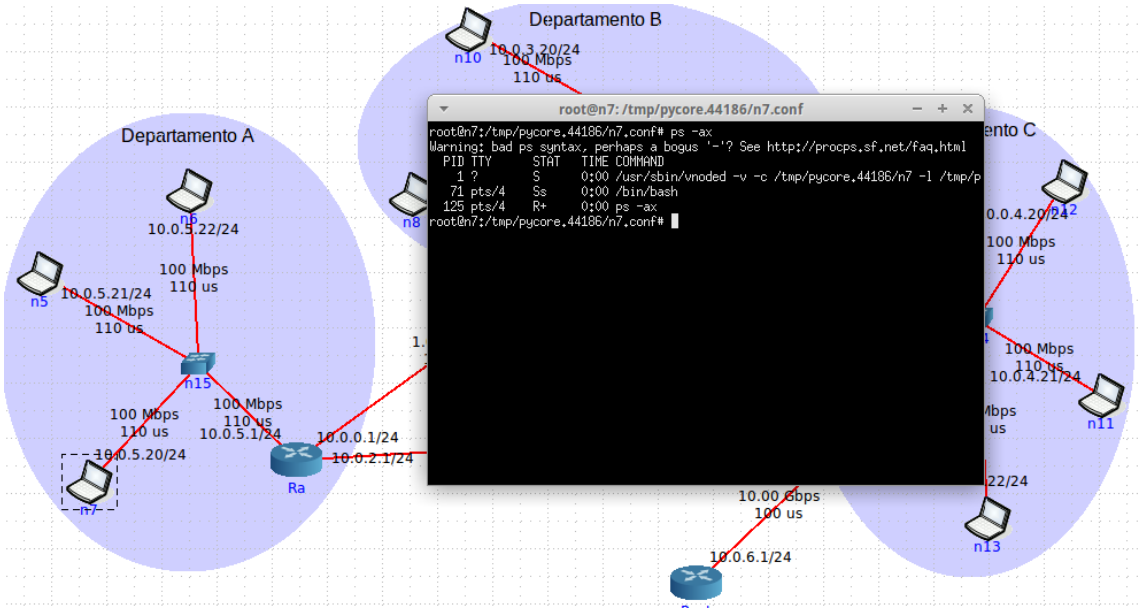


Figura 21 - Processos a correr no laptop n7

Como podemos verificar na Figura 20, o encaminhamento no router Ra é dinâmico dado que na coluna COMMAND verificamos que é utilizado o protocolo ospfd. Este tipo de encaminhamento permite que o pacote siga diferentes caminhos quando não é possível seguir o esperado. No entanto, constatamos na Figura 21 que o encaminhamento é estático dado que neste não é usado nenhum protocolo.

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 C. Use o comando route delete para o efeito. Que implicações tem esta medida para os utilizadores da empresa que acedem ao servidor. Justifique.

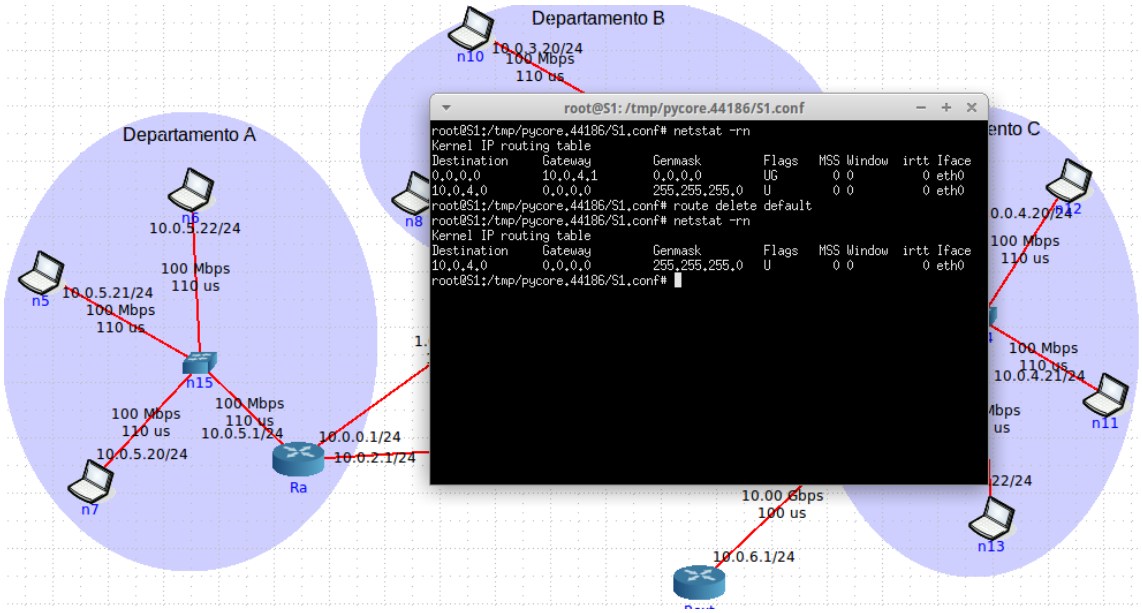


Figura 22 - Tabela de encaminhamento do S1 antes e depois de ser removida a rota default

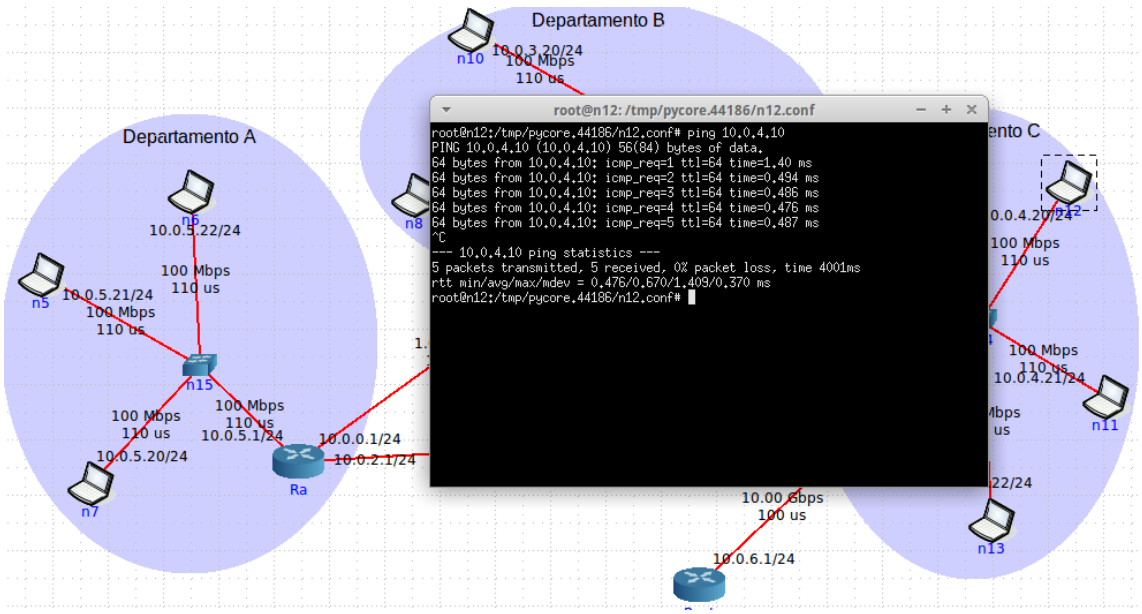


Figura 23 - Conectividade entre laptop do departamento C e o servidor S1

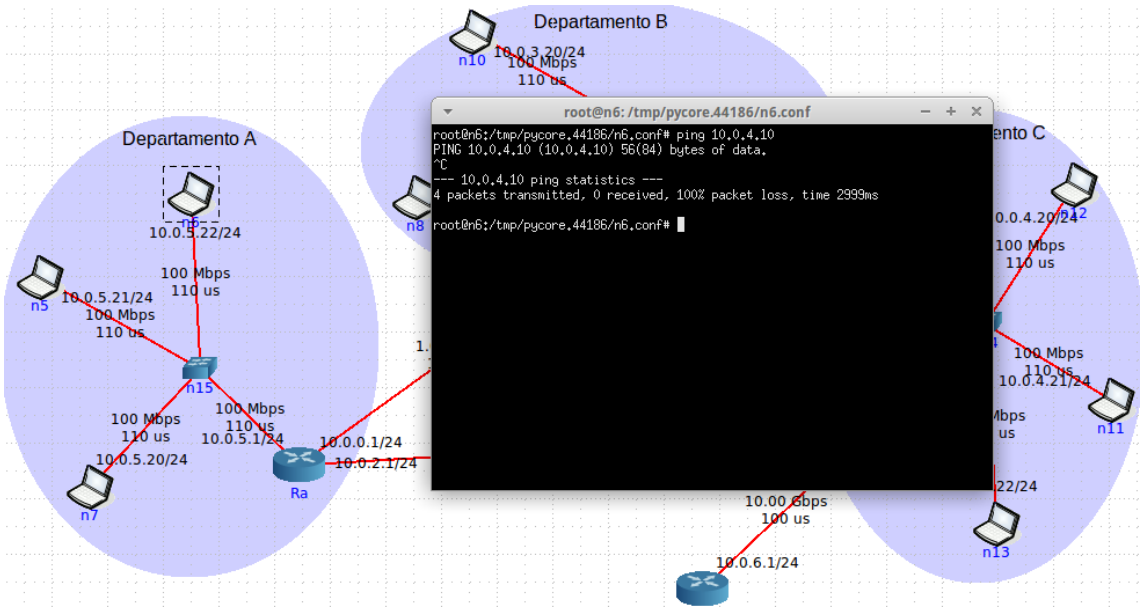


Figura 24 - Conectividade entre laptop do departamento A e o servidor S1

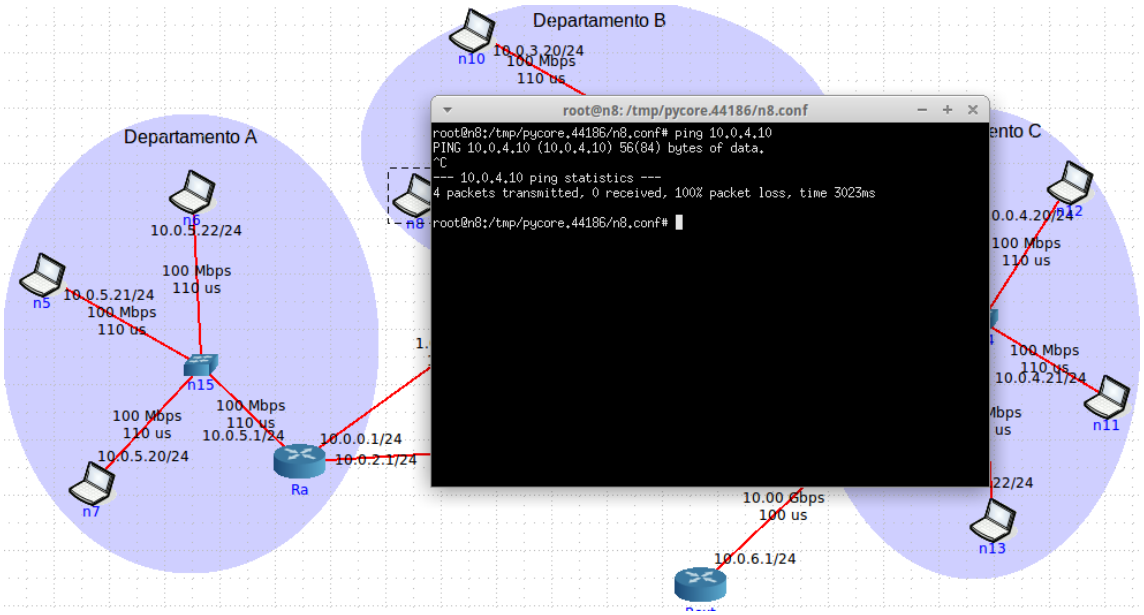


Figura 25 - Conectividade entre laptop do departamento B e o servidor S1

Como podemos constatar nas Figuras 23, 24 e 25 ao testarmos a conectividade entre os diferentes laptops e o servidor S1 verificamos que apenas os laptops do departamento onde se encontra o servidor têm conectividade com este. Quanto aos restantes laptops dos outros departamentos o mesmo não se verifica, uma vez que são enviados 4 pacotes e nenhum é recebido, ou seja, não se obtém nenhuma resposta. Tal deve-se ao facto de eliminarmos a rota por defeito do servidor.

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

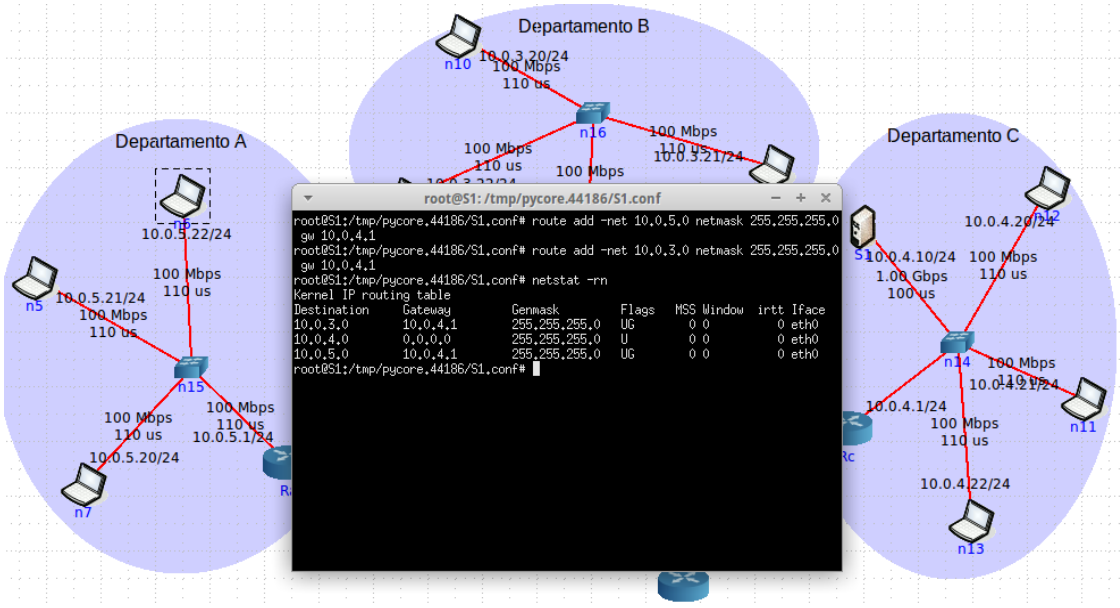


Figura 26 - Adição das rotas estáticas para restaurar a conectividade

O primeiro comando permite indicar que os pacotes que tenham como destino a sub-rede 10.0.5.0 com máscara /24 tem de entrar no gateway 10.0.4.1. Repetimos o mesmo processo para os pacotes que tenham o destino 10.0.3.0.

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.

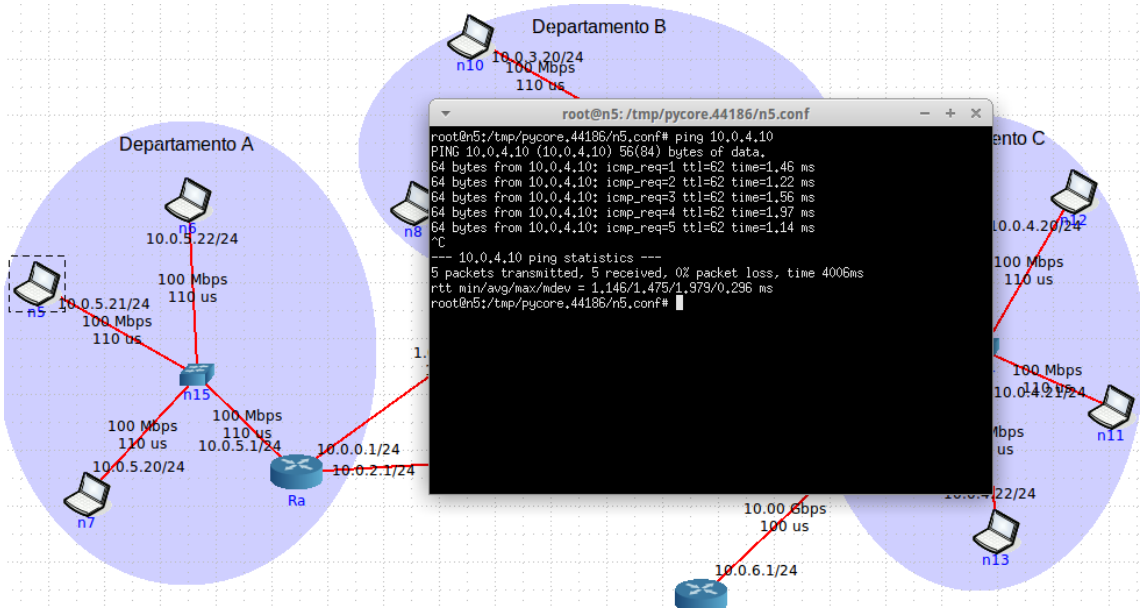


Figura 27 - Verificação da conectividade entre o Departamento A e S1

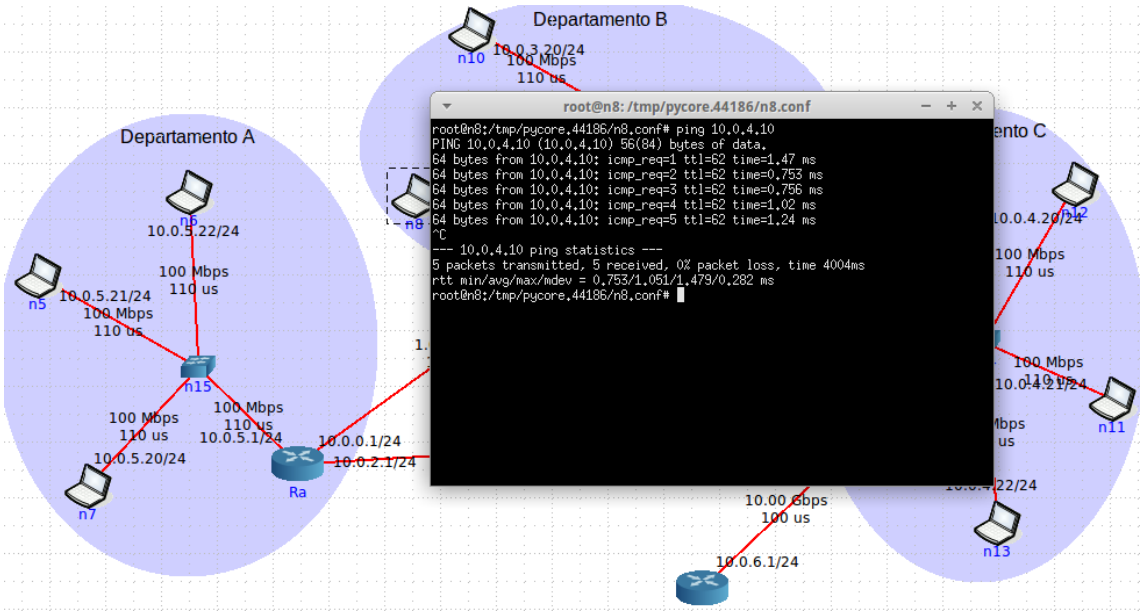


Figura 28 - Verificação da conectividade entre o Departamento B e S1

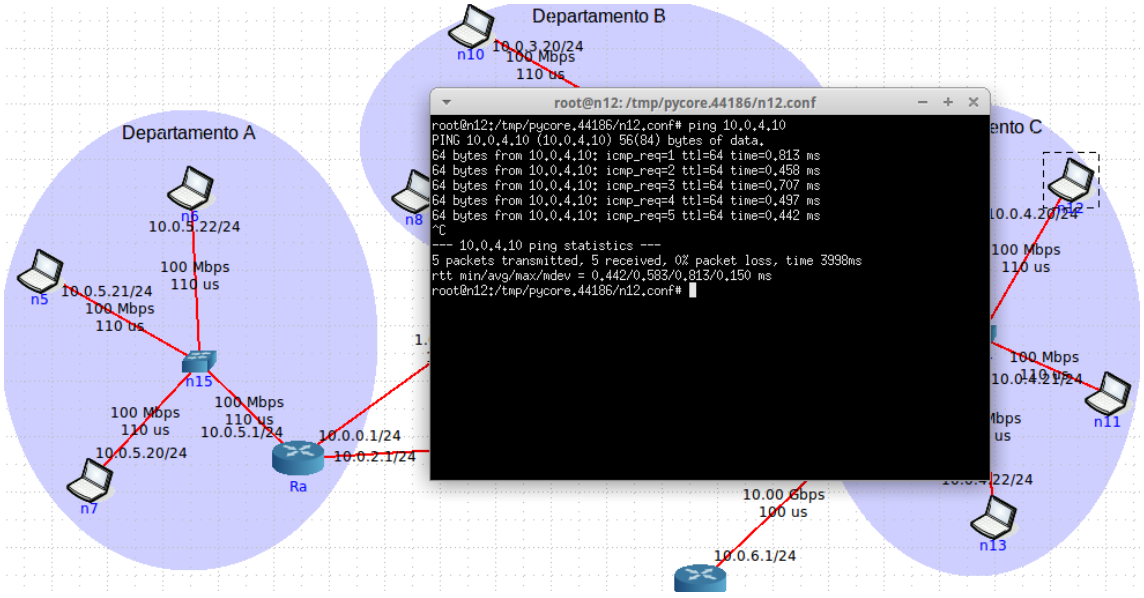


Figura 29 - Verificação da conectividade entre o Departamento C e S1

Como podemos verificar nas Figuras 27, 28 e 29 através do comando *ping*, bem como na Figura 26 através da tabela de encaminhamento, existe conectividade entre os laptops de cada departamento com o servidor S1.

Questão 3

1. Considere que dispõe apenas do endereço de rede IP 172.XX.48.0/20, em que XX é o decimal correspondendo ao seu número de grupo (PLXX). 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.

Para o endereço IP 172.41.48.0/20 sobram-nos 12 bits para gerir as sub-redes. Tendo *n* bits reservados para subnetting teremos *2^n - 2* sub-redes. Para suportar a topologia atual

apenas seriam necessários 2 bits, mas para evitar ter de modificar a configuração da rede na sua totalidade quando sejam adicionados novos departamentos decidimos não utilizar este número. Como com 3 bits não seria possível expandir todos os departamentos sem alterar a configuração da rede, optamos por utilizar 4 bits, sobrando 8 bits para o host. Assim, possuímos 14 sub-redes para atribuir aos 3 departamentos. Desta forma, optamos por:

- *Departamento A:* sub-rede 172.41.50.0/24
- *Departamento B:* sub-rede 172.41.52.0/24
- *Departamento C:* sub-rede 172.41.56.0/24

Desta forma, ficam por usar as sub-redes 172.41.49.0/24, 172.41.51.0/24, 172.41.53.0/24, 172.41.54.0/24, 172.41.55.0/24, 172.41.57.0/24, 172.41.58.0/24, 172.41.59.0/24, 172.41.60.0/24, 172.41.61.0/24, 172.41.62.0/24. Assim em caso de expansão, será possível agregar os endereços de cada departamento com:

- *Departamento A:* 172.41.51.0/24;
- *Departamento B:* 172.41.53.0/24, 172.41.54.0/24, 172.41.55.0/24;
- *Departamento C:* 172.41.57.0/24, 172.41.58.0/24, 172.41.59.0/24;

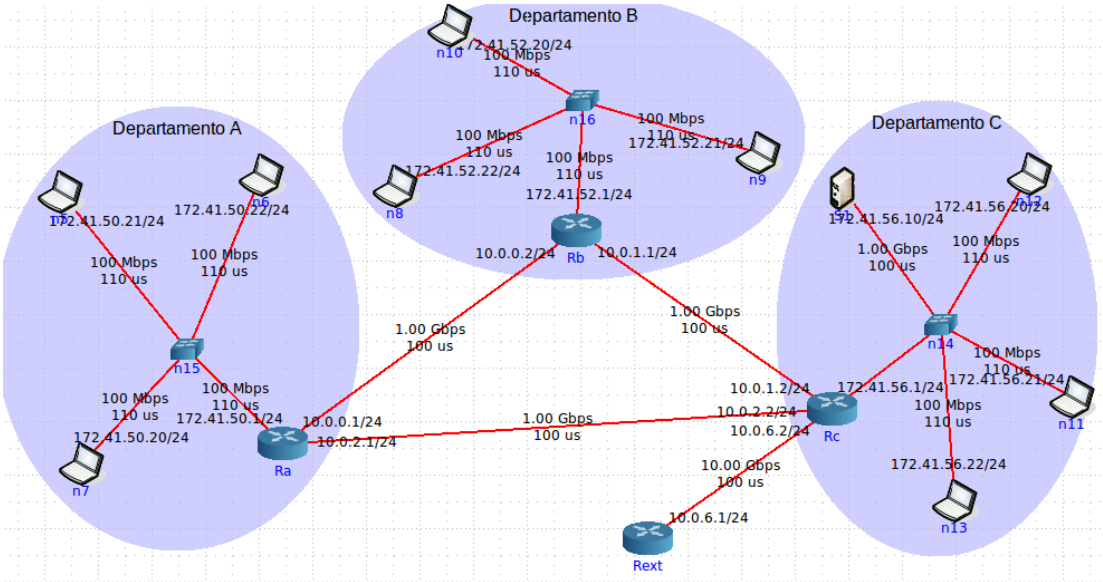


Figura 30 - Topologia do novo endereçamento

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

A máscara de rede usada foi /24, na notação CIDR, o que corresponde a 255.255.255.0. Sendo com uma máscara /24 temos 8 bits disponíveis para hosts, logo a quantidade de hosts IP que podemos interligar em cada departamento é 2^8 - 2, ou seja, 254 hosts.

3. Garanta e verifique que conectividade IP entre as várias redes locais da organização MIEI-RC é mantida. Explique como procedeu.

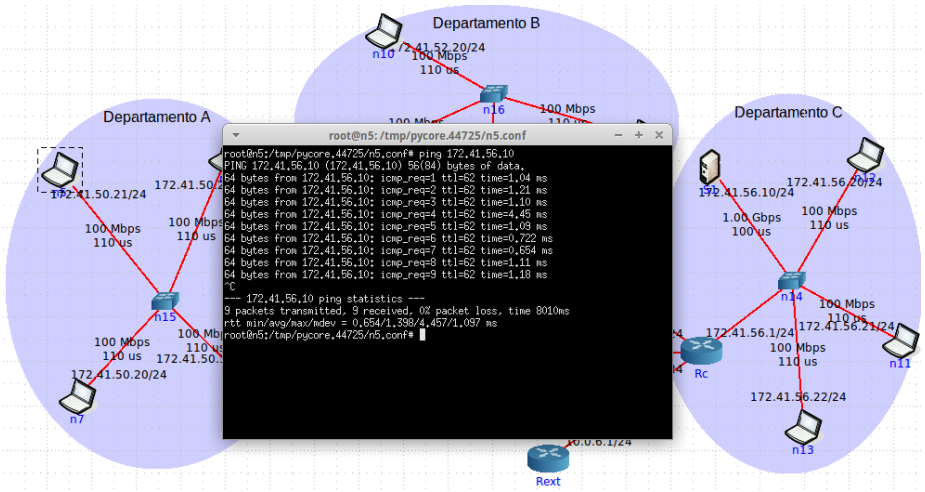


Figura 31 - Conectividade entre laptop do Departamento A e S1

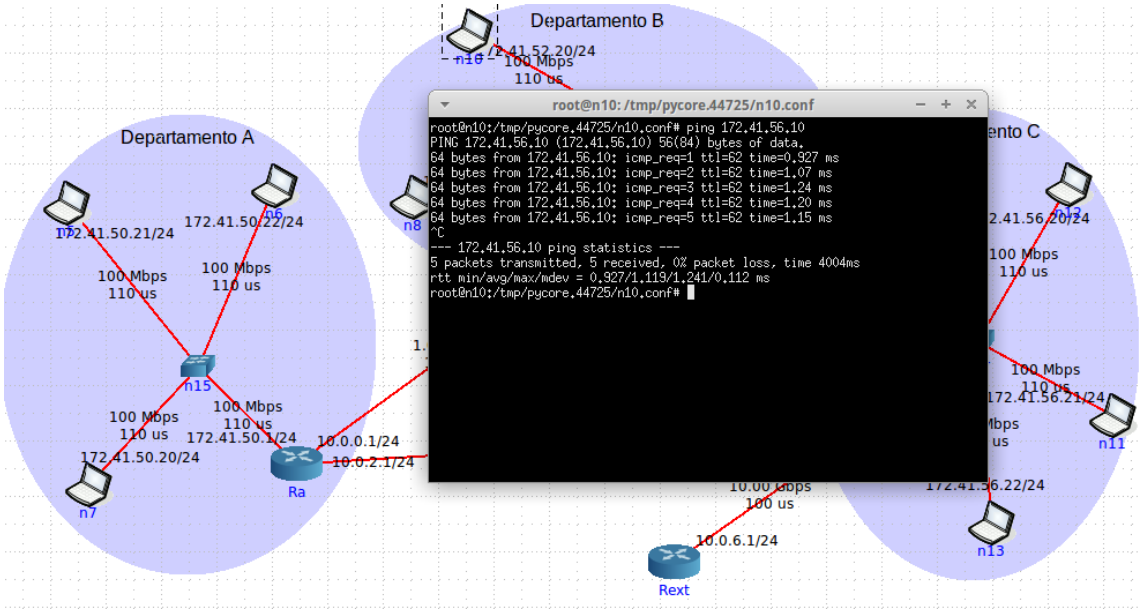


Figura 32 - Conectividade entre laptop do Departamento B e S1

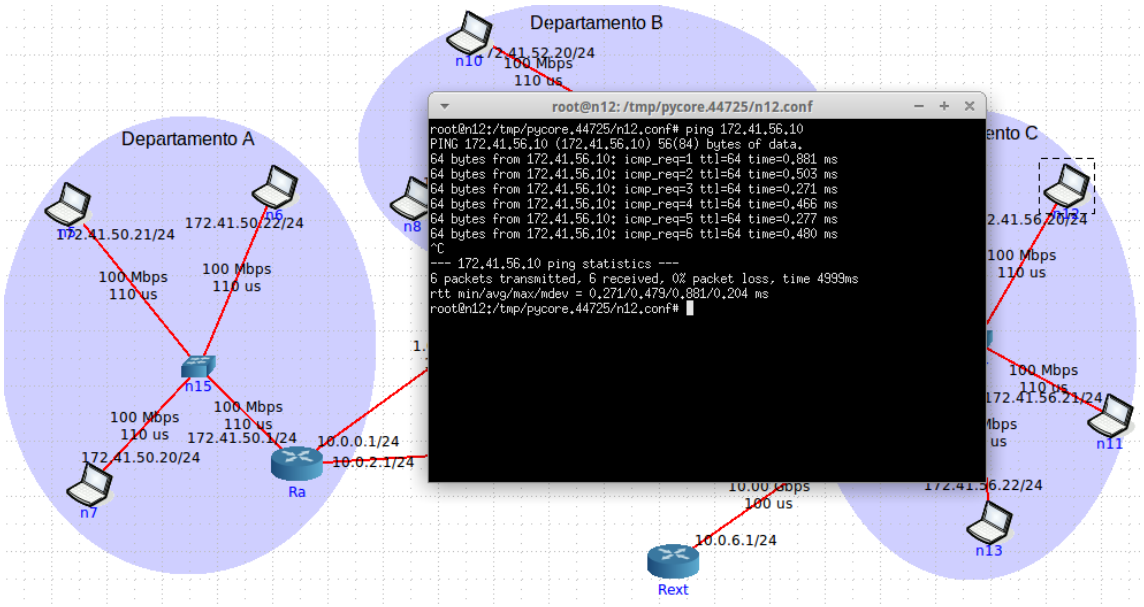


Figura 33 - Conectividade entre laptop do Departamento C e S1

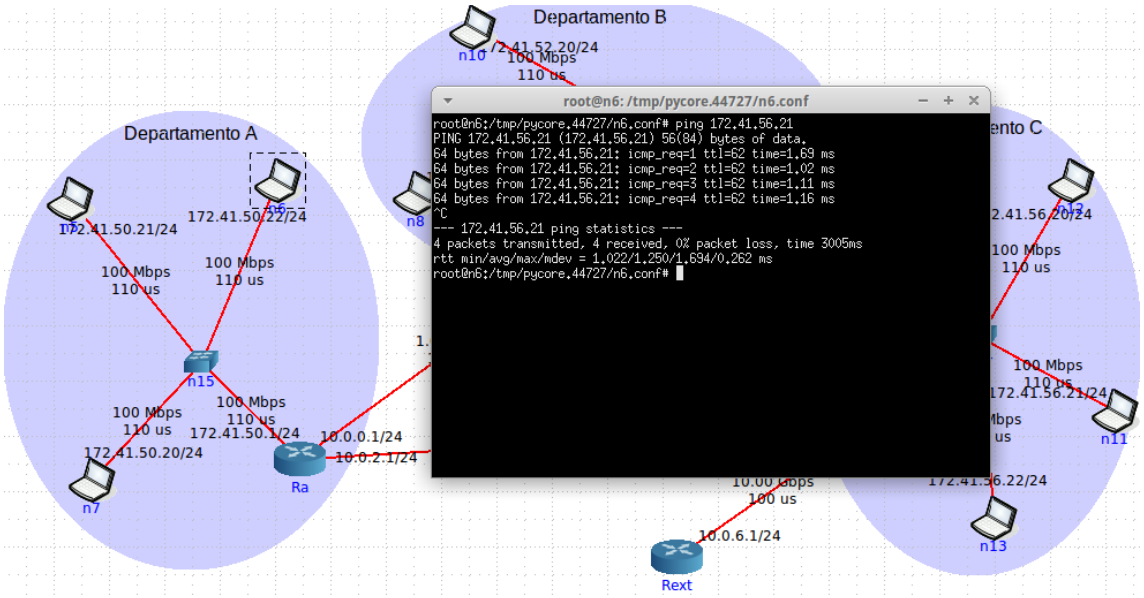


Figura 34 - Conectividade entre os laptops do Departamento A e C

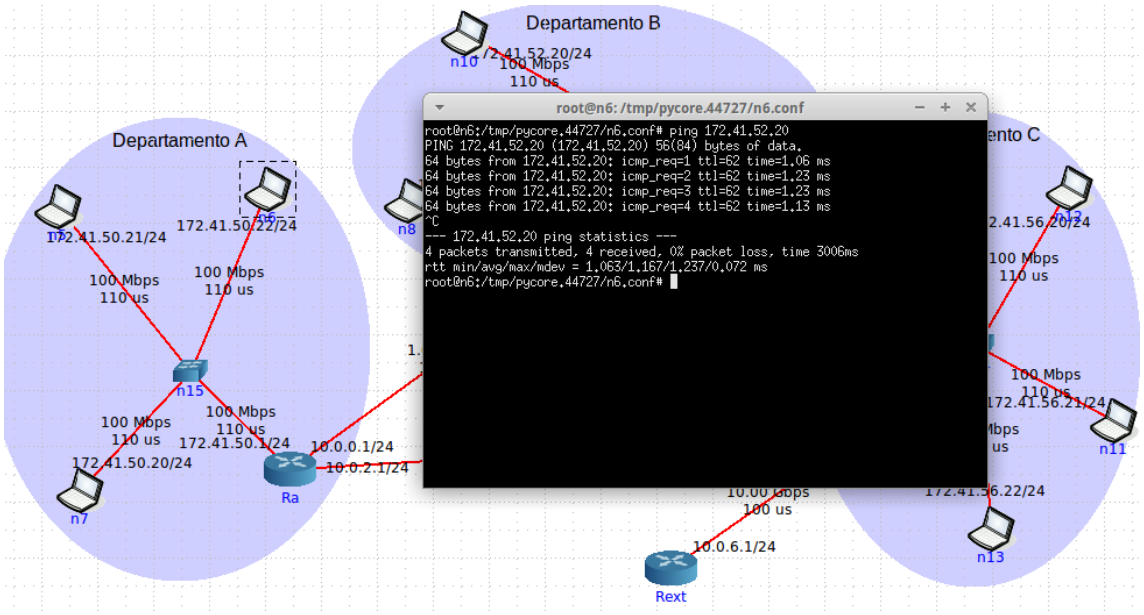


Figura 35 - Conectividade entre os laptops do Departamento A e B

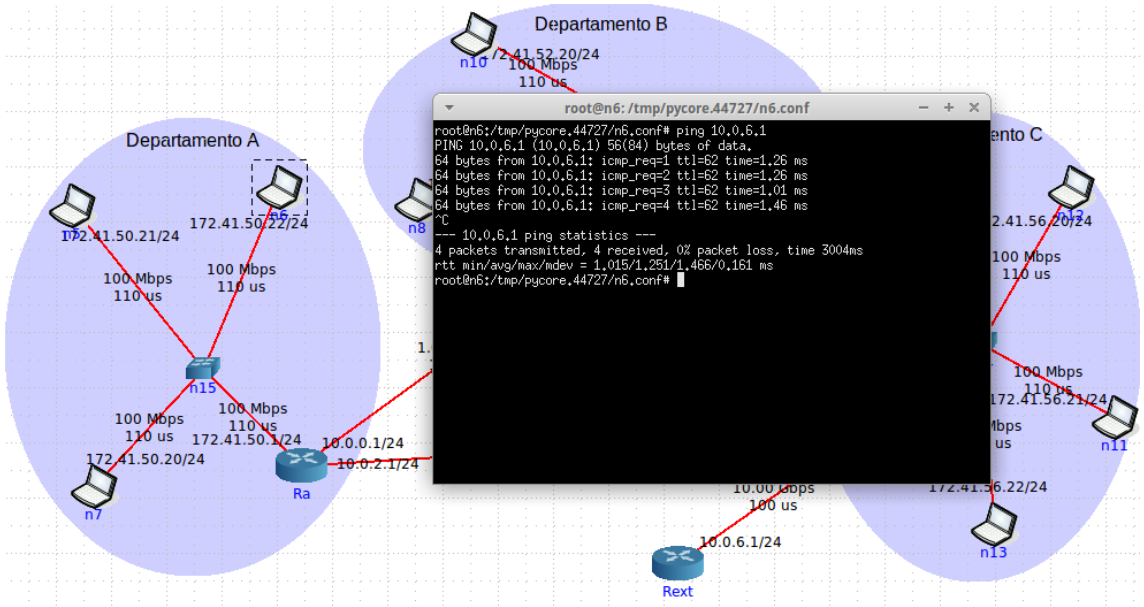


Figura 36 - Conectividade entre os laptops do Departamento A e o router exterior

Como podemos verificar pela Figuras 31, 32, 33, 34, 35 e 36 através do comando *ping*, verificamos que existe conectividade IP entre as várias redes locais.

2 Conclusões

A realização deste trabalho permitiu-nos aprender a utilizar ferramentas de simulação de redes, nomeadamente o CORE, e de captura de tráfego, o WIRESHARK. Na primeira fase, vimos como analisar o tráfego de rede, de modo a verificar os pacotes enviados e se estes chegam ao destino. Observamos também as várias características do datagrama, como por exemplo o número de bytes do cabeçalho IP, do campo de dados e verificar se este foi fragmentado e a que fragmento corresponde. Na segunda parte, observamos tabelas de encaminhamento unicast, nas quais é possível verificar as diferentes rotas e o tipo de encaminhamento. Constatamos também, o impacto de remover a rota por defeito de uma tabela. Para contornar este problema, adicionamos as rotas necessárias para repor a conectividade. Para definir o novo esquema de endereçamento, aplicamos os conceitos adquiridos na teórica sobre sub-redes.

As nossas maiores dificuldades, numa fase inicial foram a utilização do WIRESHARK e a interpretação do enunciado em algumas questões, o que contribui para uma má gestão do tempo para a realização do trabalho. Na segunda parte, consideramos que o mais complicado foi decidir o número de sub-redes para suportar a topologia, tendo em conta uma possível expansão de departamentos. Contudo, acreditamos que os objetivos propostos foram alcançados.