



Universidade do Minho
Licenciatura em Engenharia Informática

Unidade Curricular de Redes de Computadores

Ano Lectivo de 2023/2024

Trabalho prático 2

Grupo 53

David Figueiredo (a104360)

Diogo Ferreira (a104266)

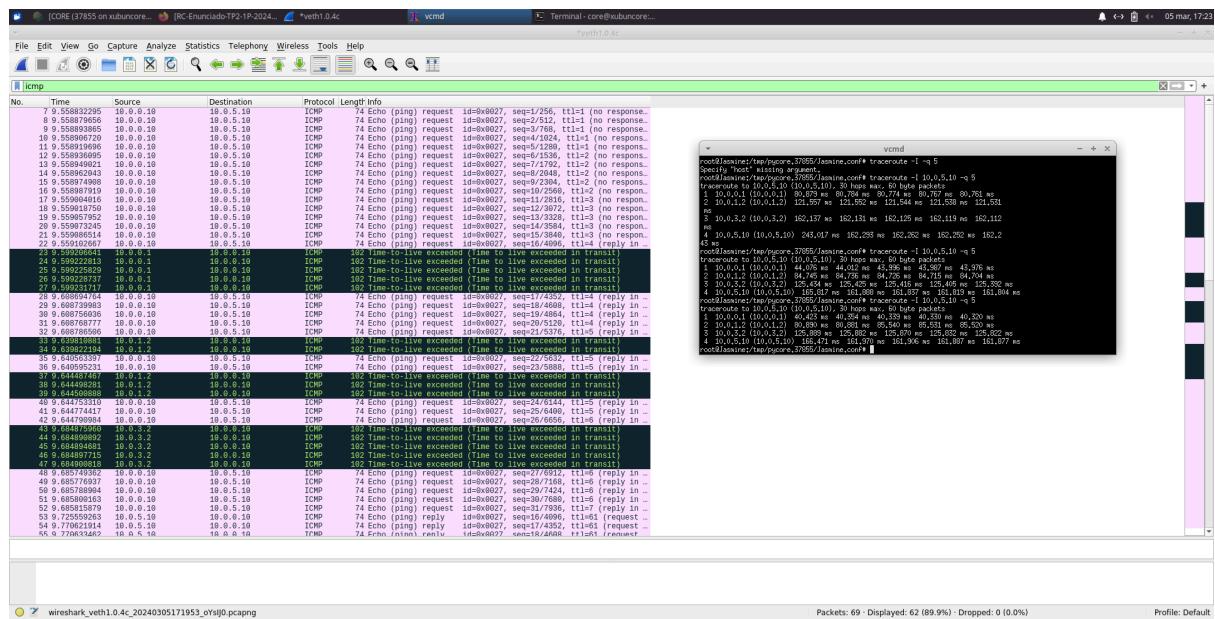
Manuel Fernandes (a93213)

RC

Parte 1

Questão 1

- A. Active o wireshark no host Jasmine. Numa *shell* de Jasmine execute o comando traceroute -l para o endereço IP do Aladdin. Registe e analise o tráfego ICMP enviado pelo sistema Jasmine e o tráfego ICMP recebido como resposta. Explique os resultados obtidos tendo em conta o princípio de funcionamento do traceroute.



O traceroute é uma ferramenta de diagnóstico de rede que é usada para rastrear a rota que os pacotes de dados fazem de um computador para outro na Internet. Ele funciona enviando pacotes de dados ICMP com incrementos crescentes no valor do TTL (Time to Live) no cabeçalho IP. O TTL é um campo no cabeçalho IP que especifica quantos saltos um pacote pode fazer antes de ser descartado e cada router ao longo do caminho decrementa o valor do TTL por 1. Se o TTL atinge 0, o router descarta o pacote e envia de volta uma mensagem de erro ICMP "Time Exceeded".

O traceroute explora esse comportamento para determinar a rota que os pacotes de dados estão a seguir. Ele envia pacotes ICMP com um TTL inicial de 1 e, em seguida, aumenta gradualmente o valor do TTL em cada iteração subsequente. Isso faz com que os pacotes sigam a rota até ao seu destino, mas com TTL crescentes, de modo a fazer com que cada

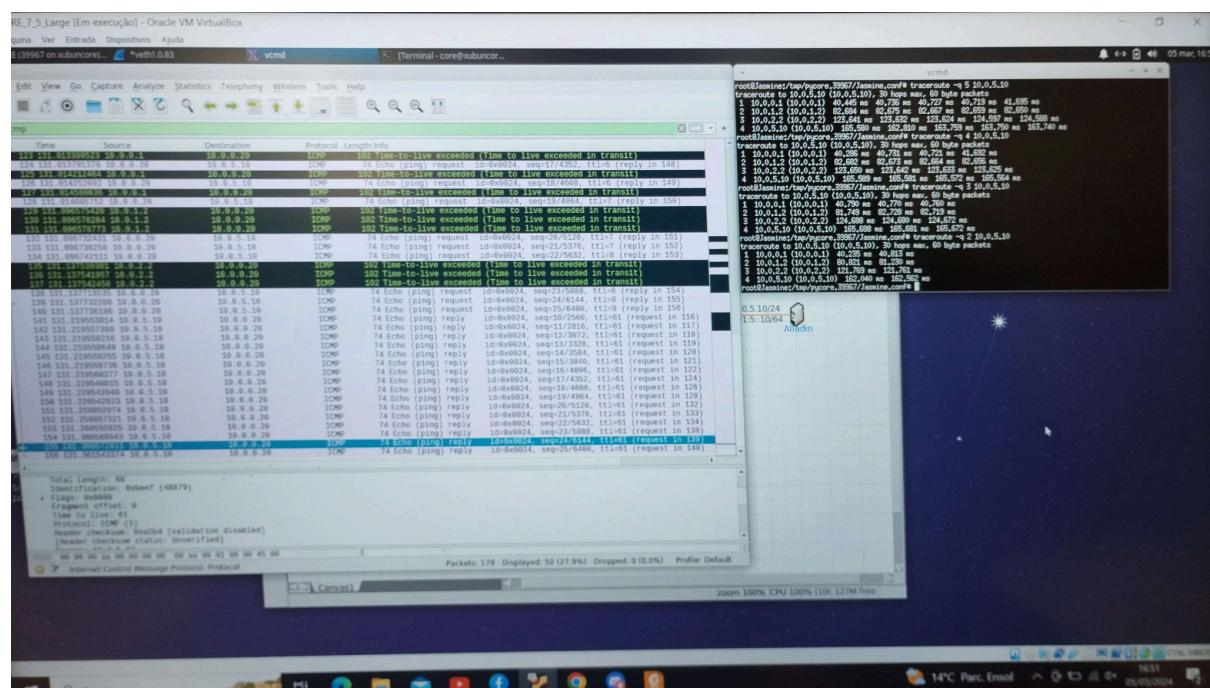
router ao longo do caminho seja obrigado a responder com um "Time Exceeded" quando o TTL do pacote chega a 0.

Ao receber essas mensagens de erro ICMP "Time Exceeded", o traceroute pode identificar o endereço IP de cada router ao longo do caminho. Ao fazer isso repetidamente com TTL crescentes, ele pode construir uma lista de todos os routers intermediários que os pacotes de dados encontram até ao seu destino final. Na imagem podemos ver que os pacotes No. 7, 8, 9, 10, 11 que apresentavam um TTL de 1 passaram por um router que decrementou o TTL para 0, devolvendo uma mensagem de erro "Time Exceeded", como se pode ver nos No. 23, 24, 25, 26, 27.

B. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o servidor Aladdin? Verifique na prática que a sua resposta está correta.

O valor mínimo do TTL para que os pacotes alcancem o servidor Aladdin é 4. Tal como se pode ver na figura da alínea anterior, apenas os primeiros 15 pacotes enviados é que resultaram numa resposta com a mensagem de erro “Time Exceeded”, os pacotes seguintes, que eram os pacotes com TTL de 5, já resultaram numa resposta do servidor Aladdin, como se pode ver pelo pacote No. 53, que foi a primeira resposta enviada pelo servidor Aladdin.

C. Calcule o valor médio do tempo de ida-e-volta (RTT - Round-Trip Time) obtido no acesso ao servidor. Por modo a obter uma média mais confiável, poderá alterar o número de pacotes de prova com a opção -q.



Podemos tirar da imagem que o valor médio é de cerca de 165ms.

D. O valor médio do atraso num sentido (One-Way Delay) poderia ser calculado com precisão dividindo o RTT por dois? O que torna difícil o cálculo desta métrica numa rede real?

Dividir o round-trip delay (atraso de ida e volta) por 2 para estimar o one-way delay não é uma prática comum e pode não ser preciso, pois assume uma simetria perfeita na rede, o que raramente é o caso na prática. Na verdade, calcular o one-way delay em uma rede real pode ser desafiador devido a vários fatores, incluindo:

Assimetria de rota: Os pacotes podem seguir rotas diferentes de ida e volta, devido a roteamento dinâmico, congestionamento de rede ou falhas de roteamento.

Variação na latência: A latência em uma rede pode variar ao longo do tempo devido a congestionamentos temporários, mudanças na carga da rede, qualidade da conexão, entre outros fatores.

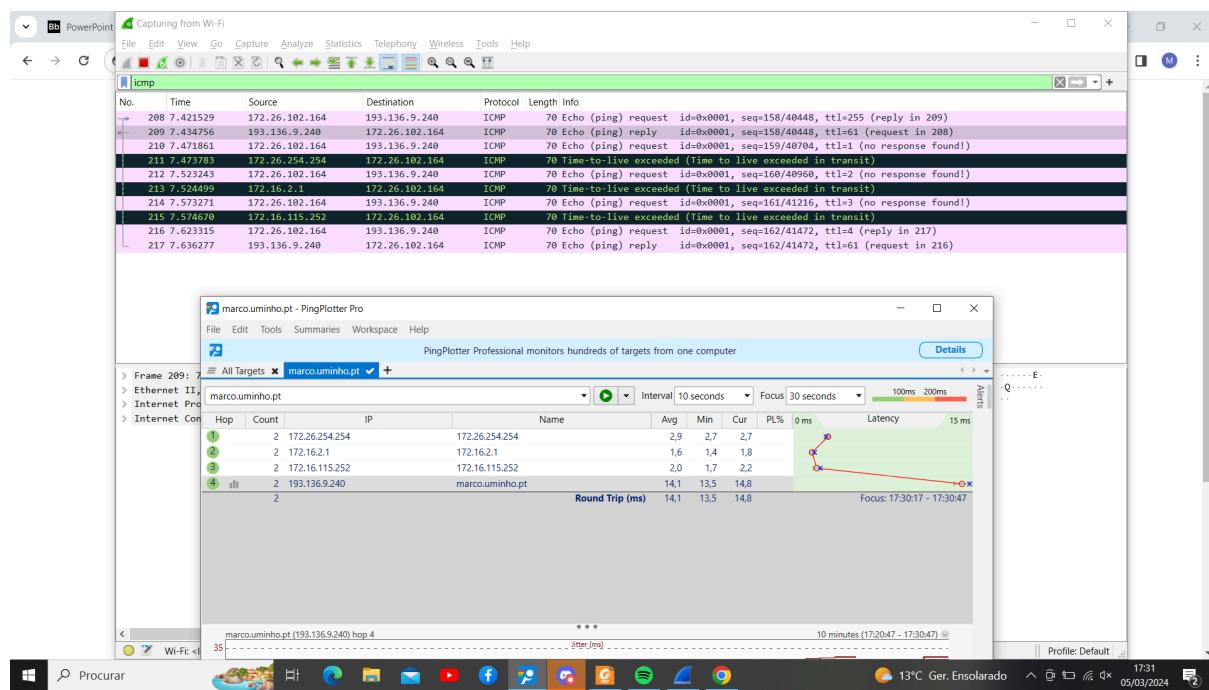
Processamento em dispositivos de rede: Dispositivos de rede, como roteadores e switches, introduzem atrasos no processamento de pacotes, que podem variar dependendo da carga de trabalho e do hardware específico.

Métodos de medição: A medição precisa do one-way delay pode exigir o uso de ferramentas especializadas de monitoramento de rede e a coordenação entre pontos de medição em diferentes locais.

Portanto, enquanto é possível estimar o one-way delay dividindo o round-trip delay por 2 em alguns cenários simplificados, é importante reconhecer que essa abordagem pode não refletir com precisão o desempenho real da rede em situações mais complexas. Em redes reais, é preferível usar métodos de medição mais sofisticados e precisos para avaliar o one-way delay.

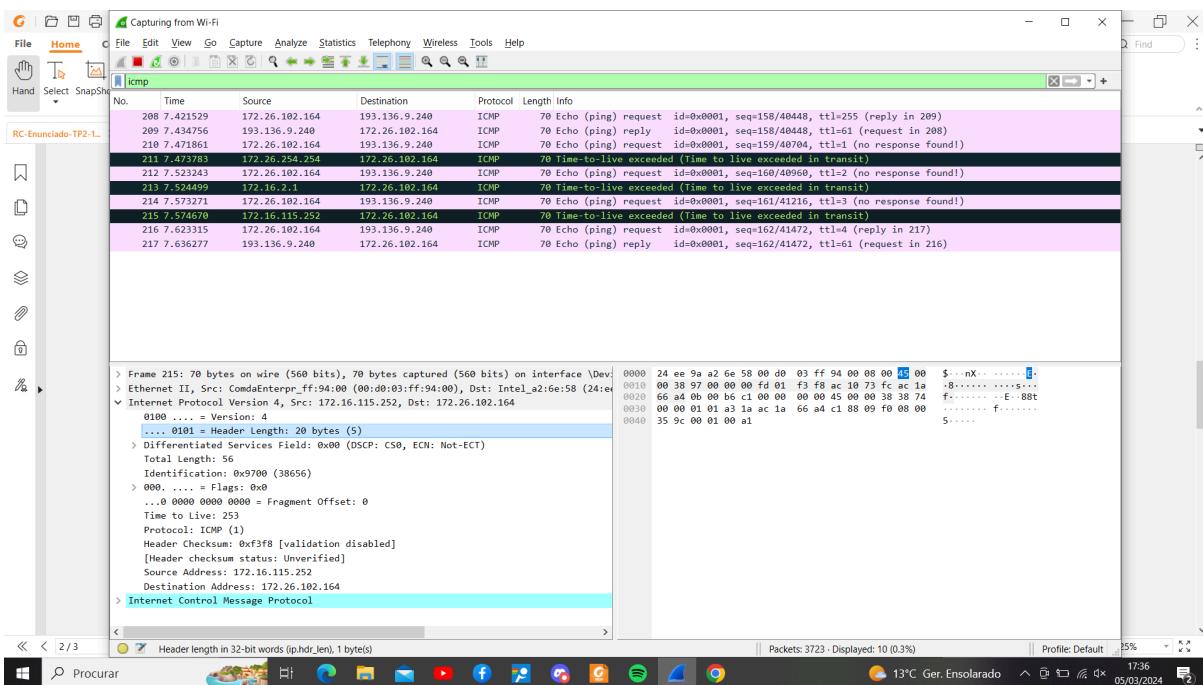
Questão 2

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



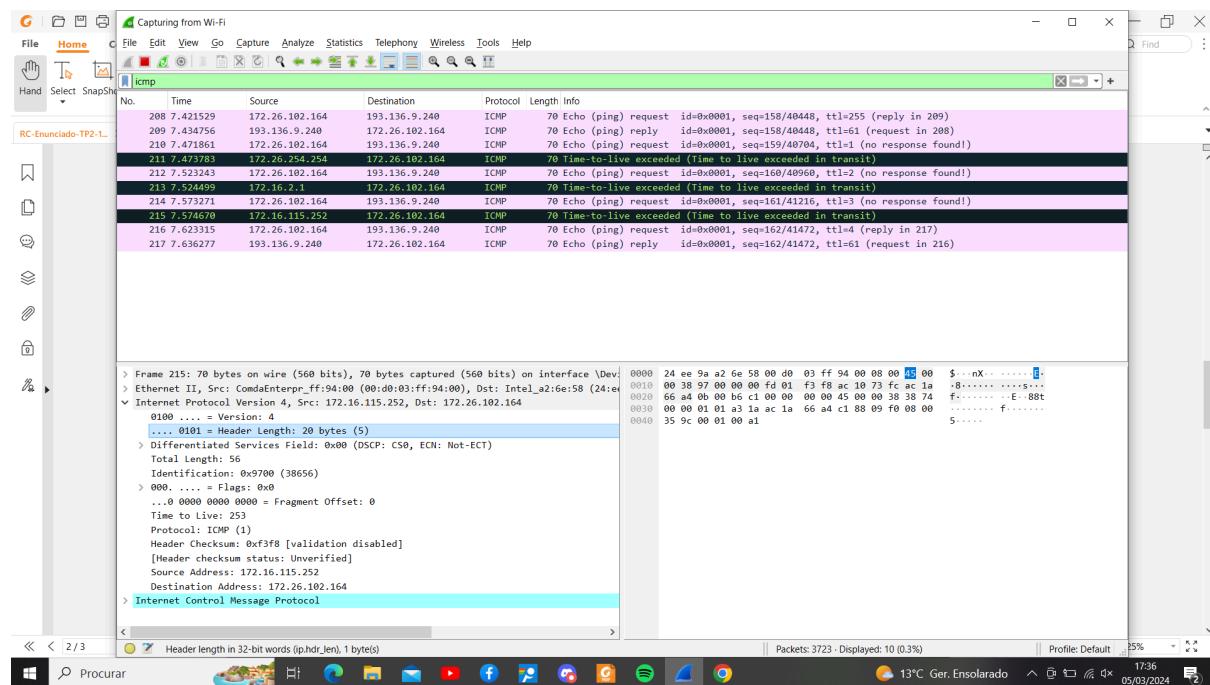
172.26.102.164

B. Qual é o valor do campo protocol? O que permite identificar?



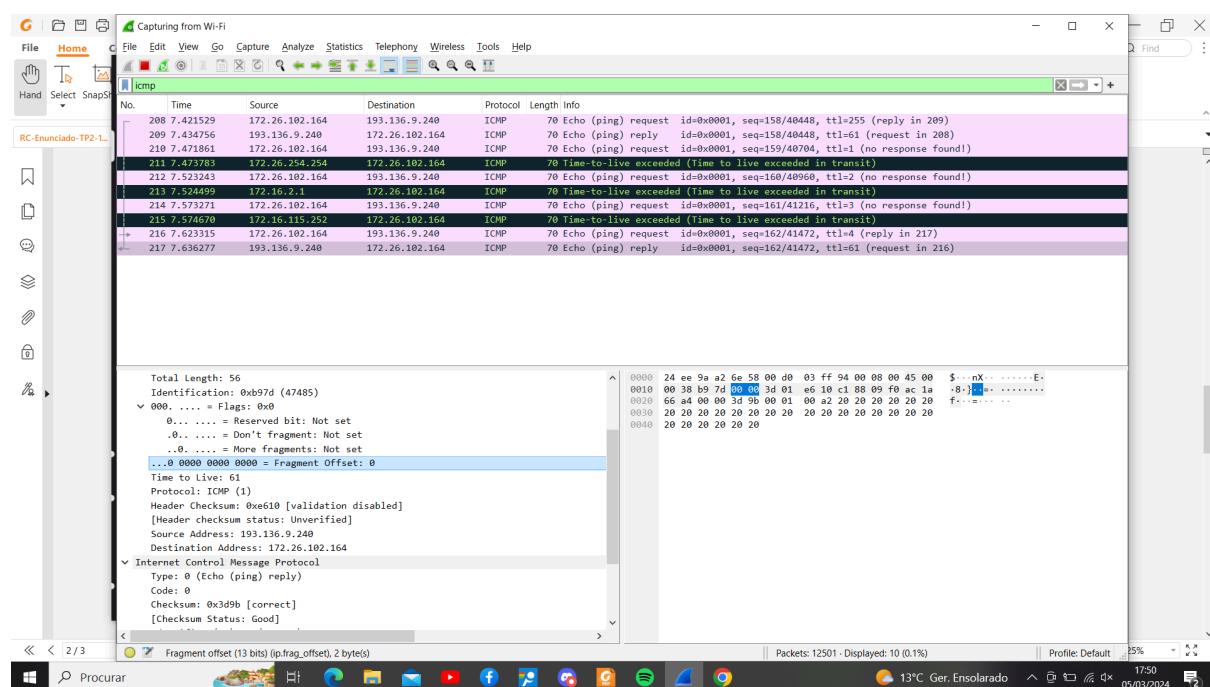
O valor do campo protocol é 1, o que permite ao receptor saber que o pacote ip contém um pacote icmp.

C. Quantos bytes tem o cabeçalho IPv4? Quantos bytes tem o campo de dados (payload) do datagrama? Como se calcula o tamanho do payload?



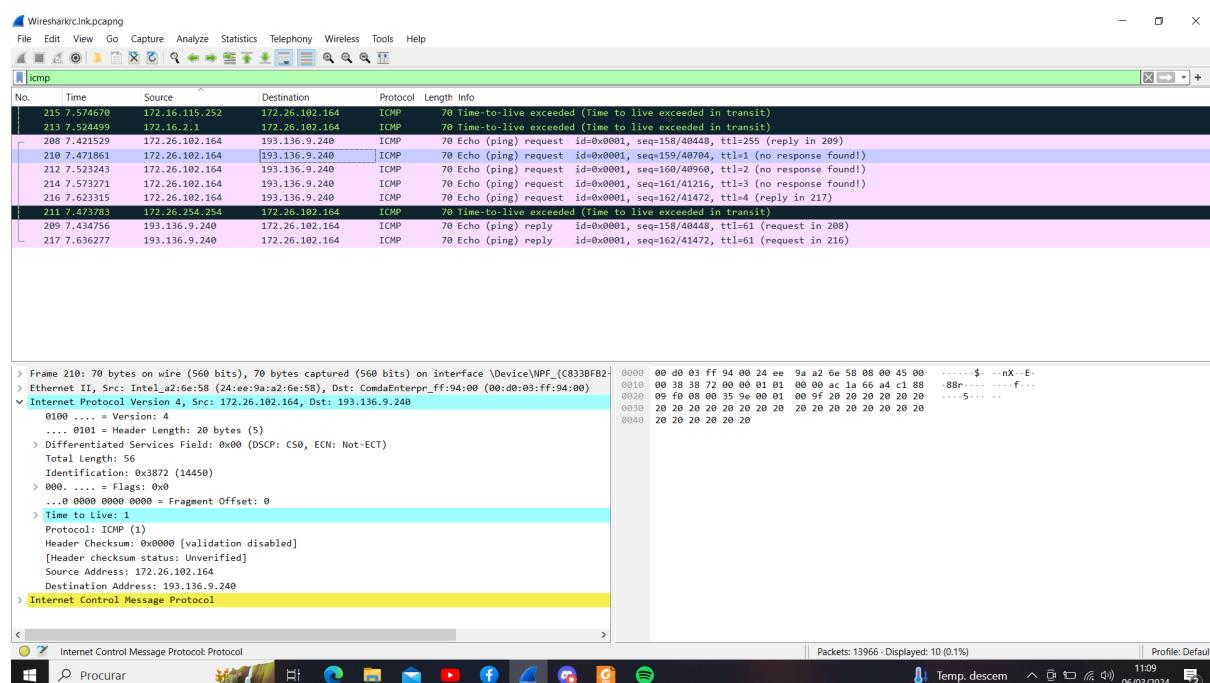
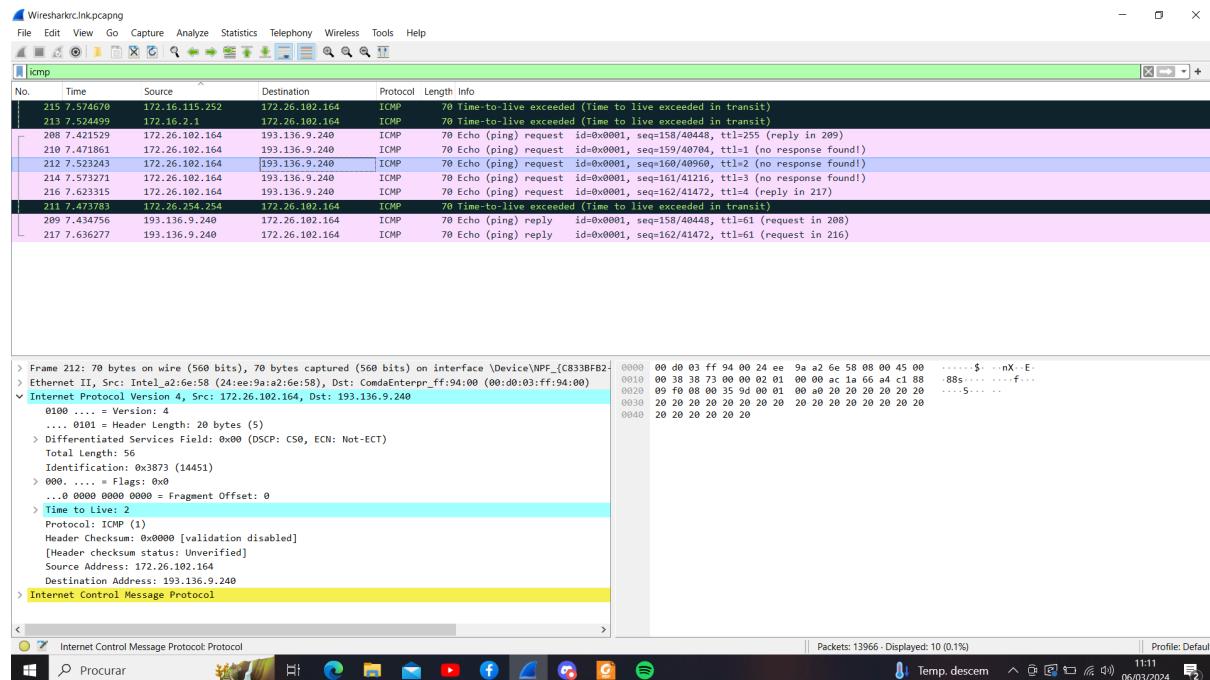
O cabeçalho IPv4 tem 20 bytes e o payload pode ser calculado subtraindo o tamanho total do datagrama IP pelo tamanho do cabeçalho IPv4, sendo assim o seu valor é 36.

D. O datagrama IP foi fragmentado? Justifique.



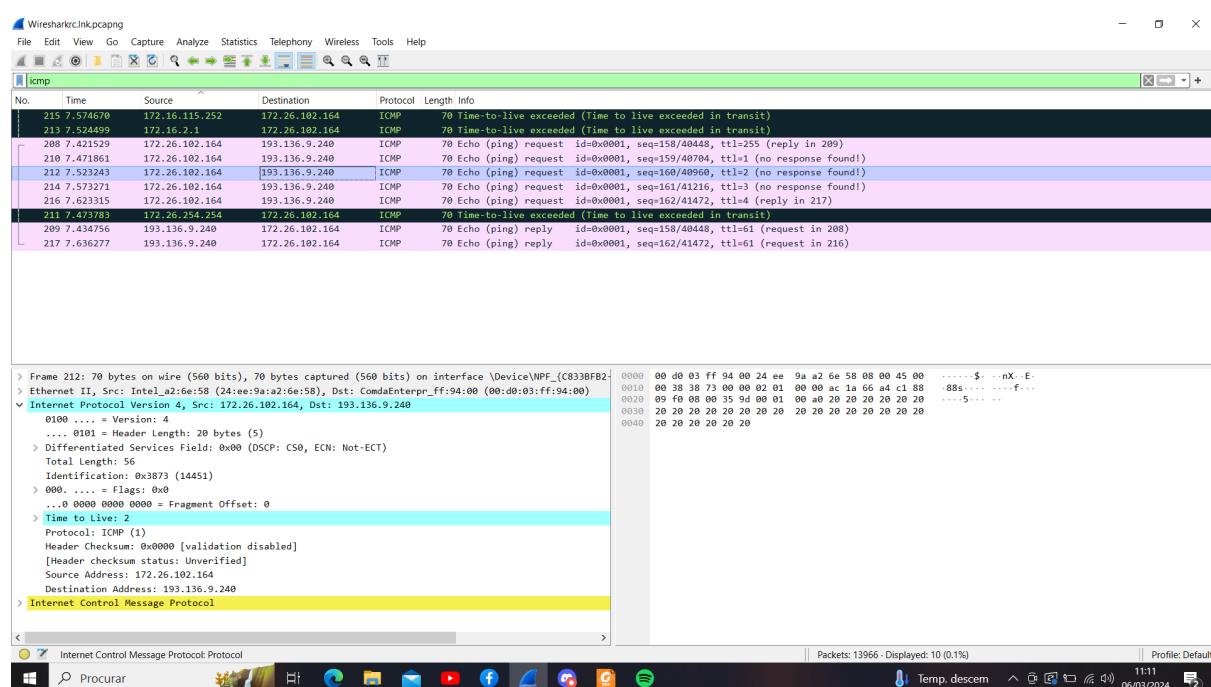
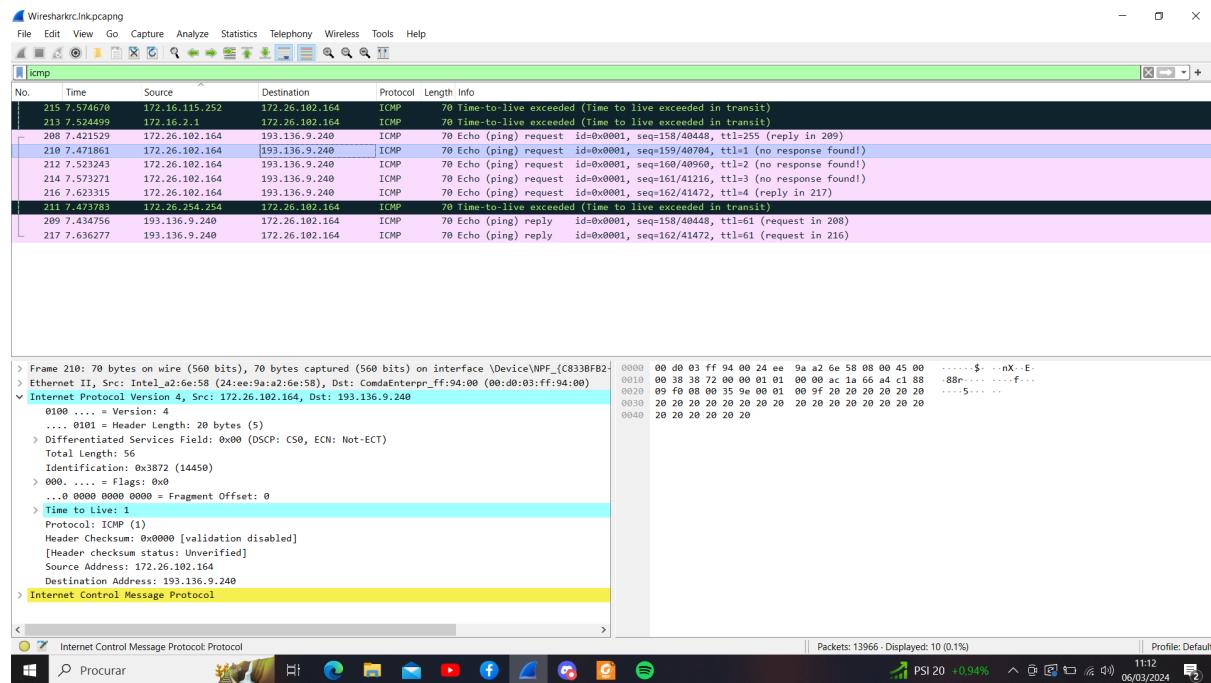
O datagrama não foi fragmentado uma vez que o fragment offset está a 0 e a flag more fragments também se encontra a 0.

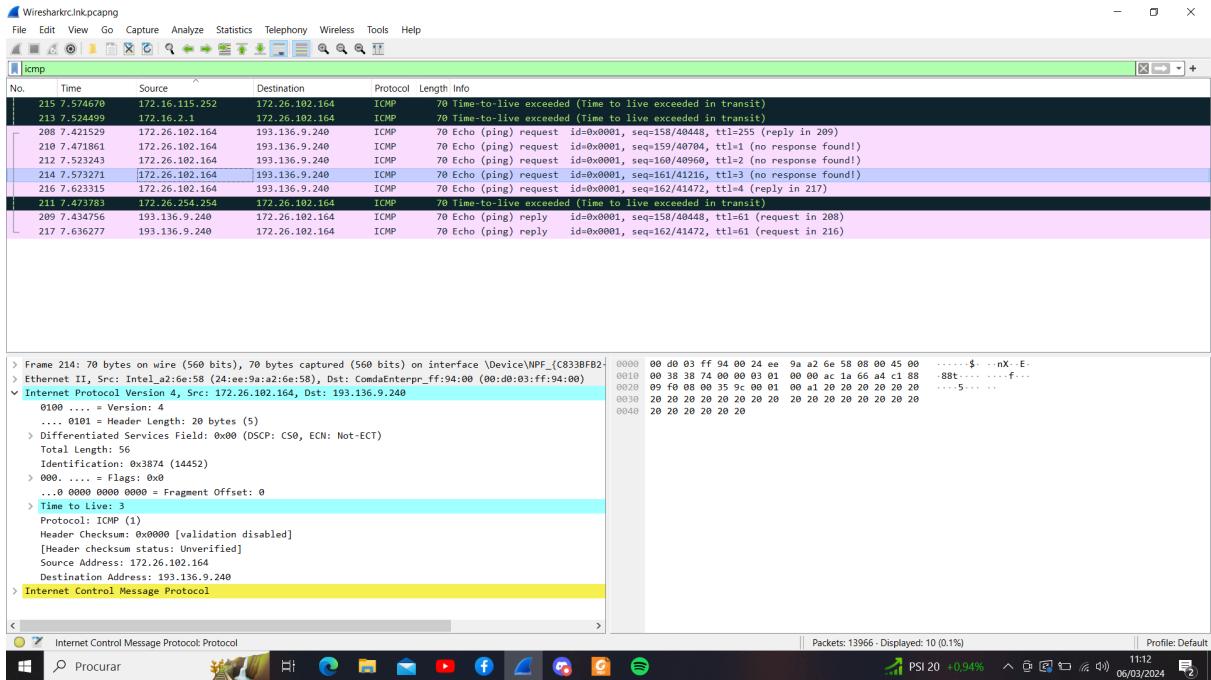
E. Ordene os pacotes capturados de acordo com o endereço IP fonte (e.g., selecionando o cabeçalho da coluna Source), e analise a sequência de tráfego ICMP gerado a partir do endereço IP atribuído à interface da sua máquina. Para a sequência de mensagens ICMP enviadas pelo seu computador, indique que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



Pelas imagens podemos perceber que os campos que se alteram são os de identificação do datagrama ip e o do time to live.

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

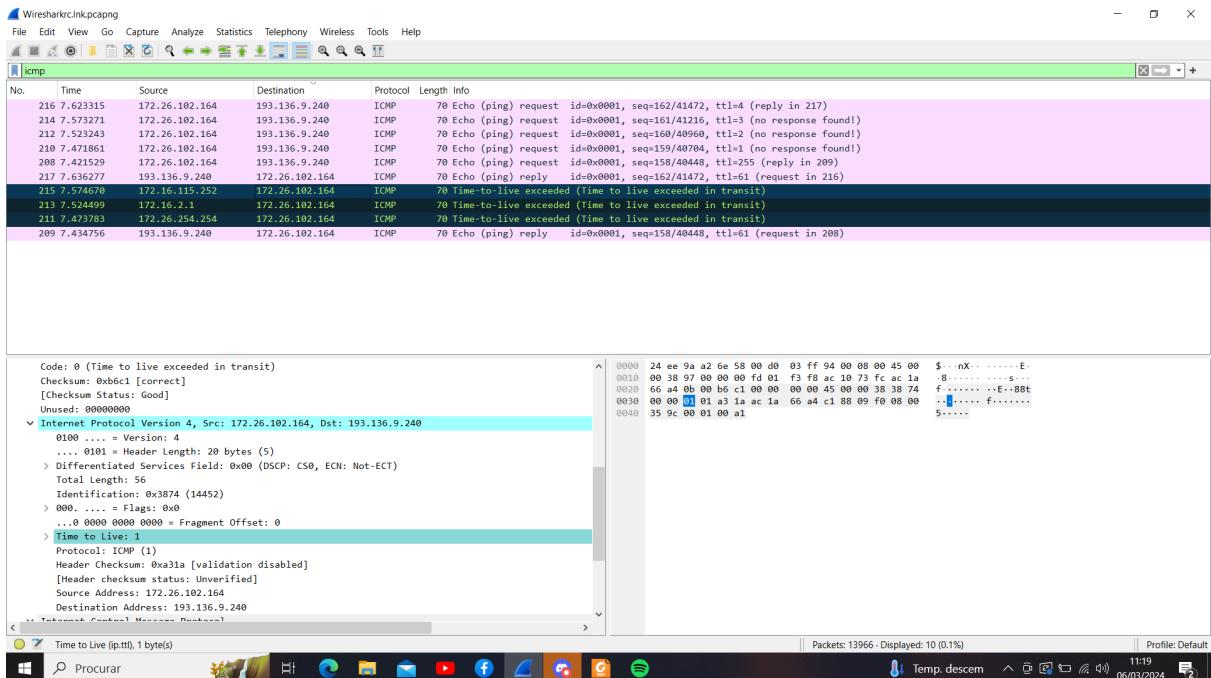


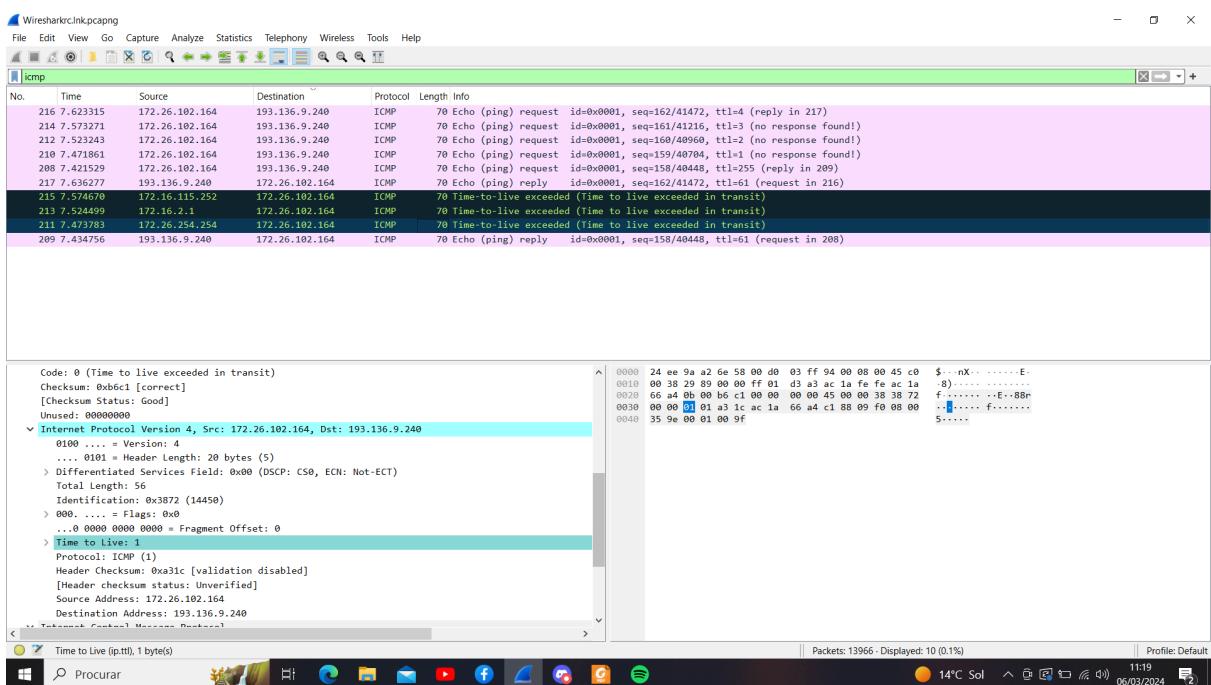
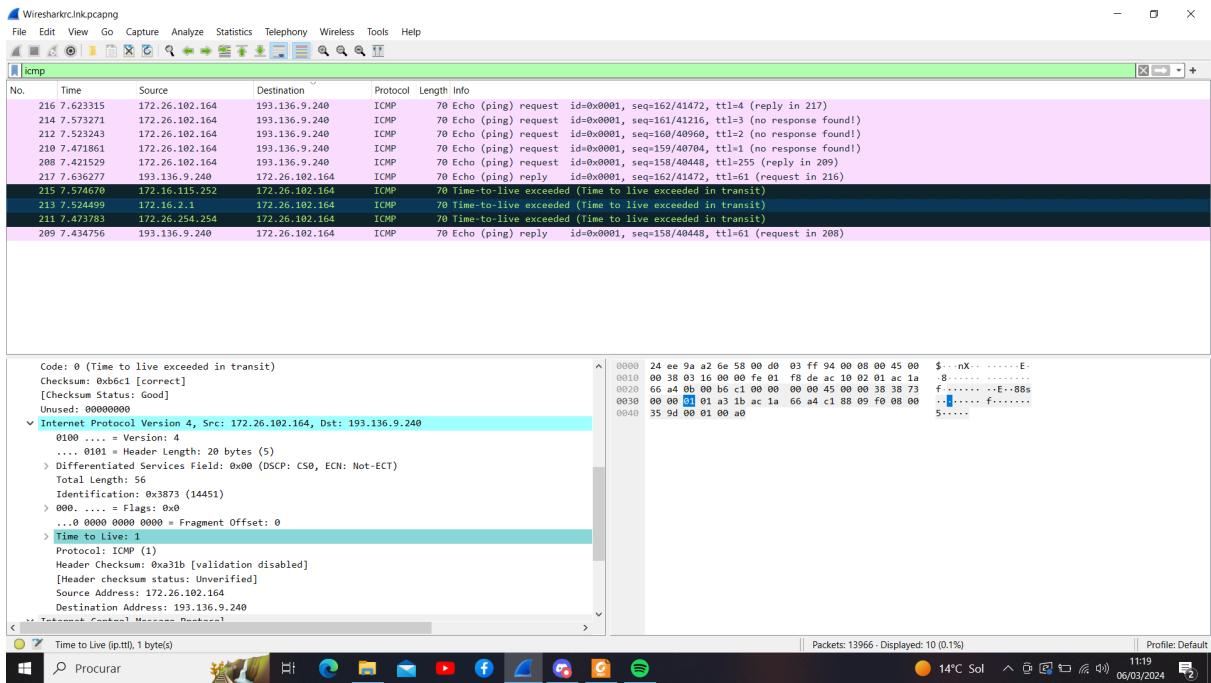


Podemos reparar que tanto o campo de identificação do datagrama ip como o ttl são incrementados por 1 de pacote para pacote.

G. Ordene o tráfego capturado por endereço destino e encontre a série de respostas ICMP TTL Exceeded enviadas ao seu computador.

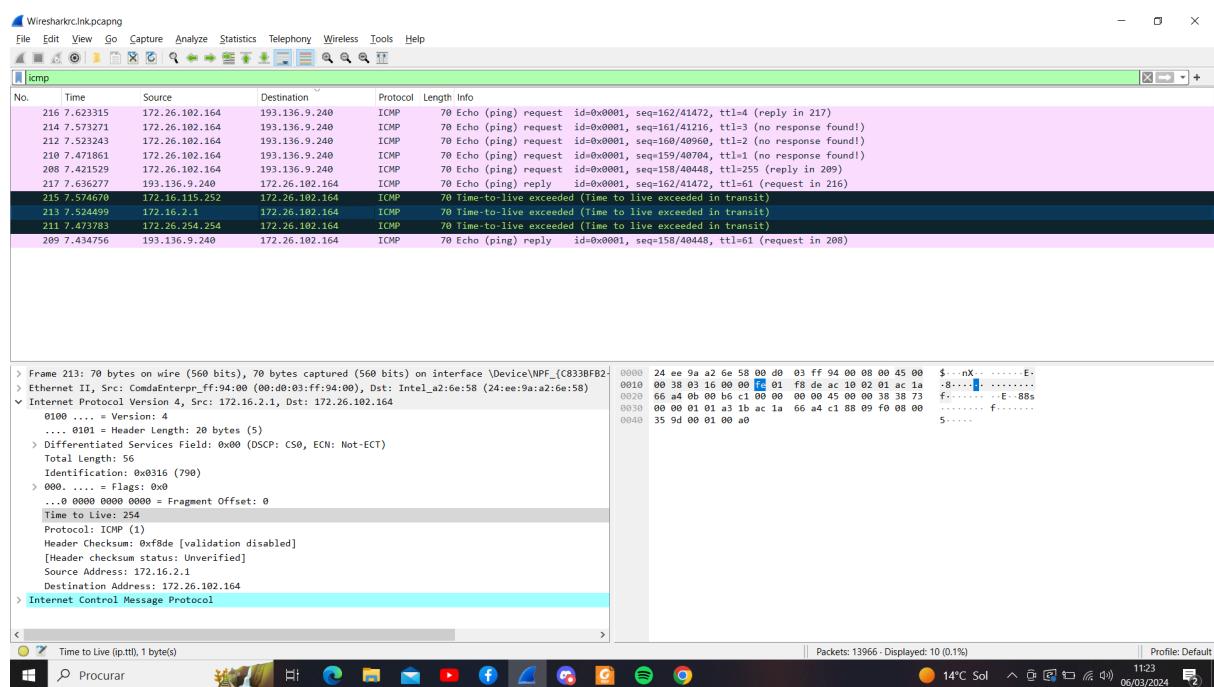
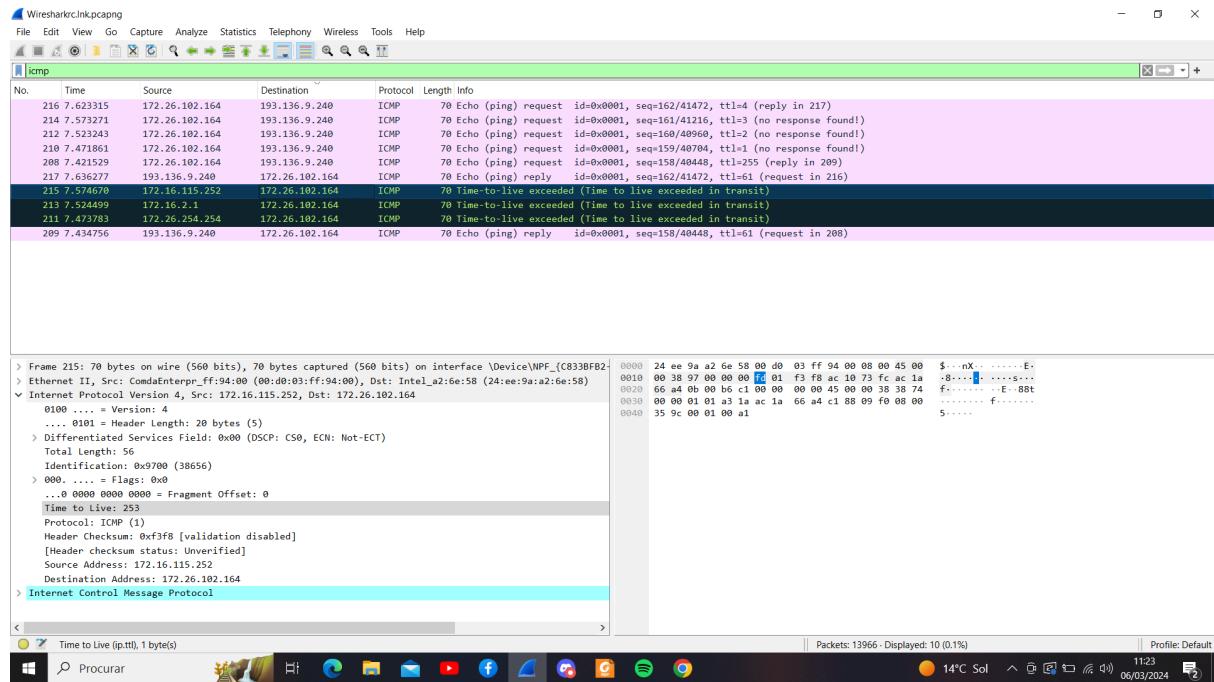
i. Qual é o valor do campo TTL recebido no seu computador? Esse valor permanece constante para todas as mensagens de resposta ICMP TTL Exceeded recebidas no seu computador? Porquê?

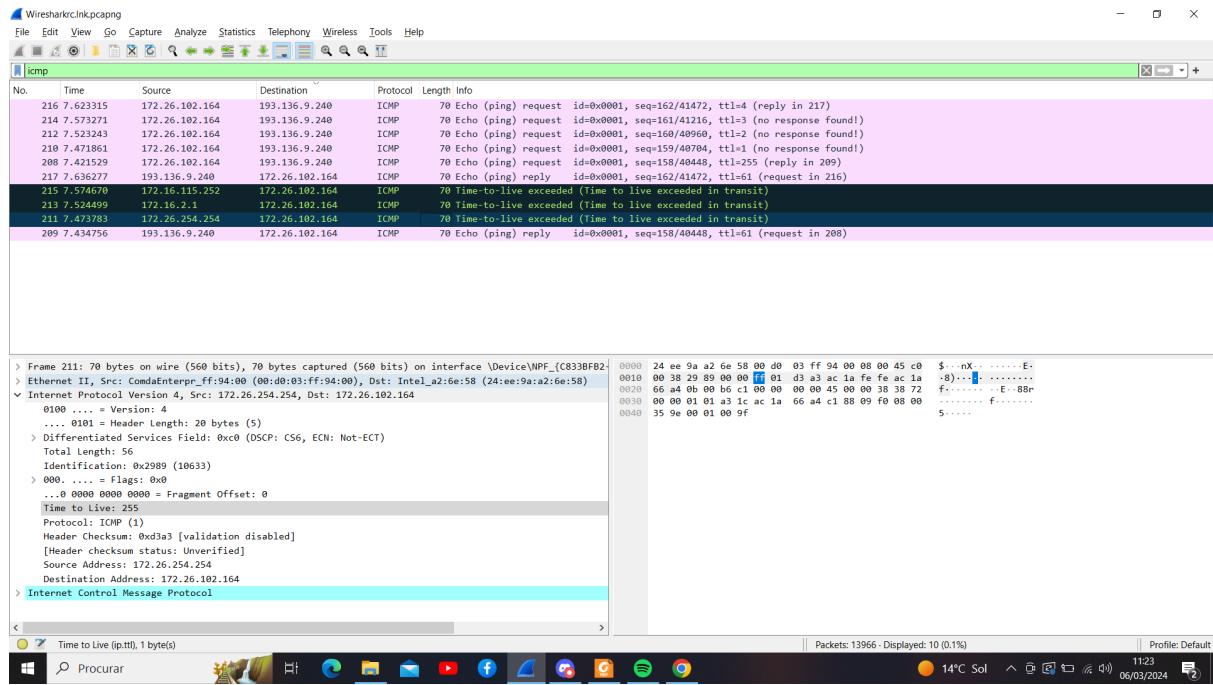




Podemos reparar que o valor do time to live recebido é sempre 1, recebendo mensagens de resposta ICMP TTL Exceeded constantemente com um valor de TTL de 1, isso sugere que os pacotes estão a ser descartados imediatamente após o primeiro salto.

ii. Porque razão as mensagens de resposta ICMP TTL Exceeded são sempre enviadas na origem com um valor TTL relativamente alto?





As mensagens de resposta ICMP TTL Exceeded são enviadas de volta à origem com um valor TTL relativamente alto para garantir que o pacote que excedeu o limite de tempo ainda tenha a chance de chegar ao destino original. Se a mensagem ICMP TTL Exceeded fosse enviada de volta com um TTL baixo, poderia ser descartada por roteadores no caminho de volta para a origem antes de alcançar o destino. Portanto, um valor TTL alto é usado para permitir que a mensagem de erro percorra a maior parte do caminho de volta para o remetente, fornecendo informações úteis sobre onde o pacote excedeu o limite de tempo. Isso ajuda na depuração e na identificação de problemas de rede.

H. Sabendo que o ICMP é um protocolo pertencente ao nível de rede, discuta se a informação contida no cabeçalho ICMP poderia ser incluída no cabeçalho IPv4? Quais seriam as vantagens/desvantagens resultantes dessa hipotética inclusão?

Incorporar as informações do cabeçalho ICMP diretamente no cabeçalho IPv4 apresenta tanto vantagens quanto desvantagens.

Uma vantagem seria a redução do overhead na rede. Atualmente, as mensagens ICMP são enviadas em pacotes IP separados, o que aumenta a carga na rede. Ao incluir essas informações diretamente no cabeçalho IPv4, poderíamos diminuir essa sobrecarga, especialmente em redes com tráfego ICMP considerável.

Outra vantagem seria uma potencial melhoria na eficiência. Ao consolidar as informações no cabeçalho IPv4, o processamento nos roteadores poderia ser simplificado, o que poderia resultar em tempos de resposta mais rápidos e um tráfego de rede mais fluido.

Por outro lado, há desvantagens a serem consideradas. A complexidade do protocolo IPv4 poderia aumentar com a inclusão das informações do ICMP, o que poderia dificultar sua implementação e interoperabilidade entre diferentes dispositivos de rede.

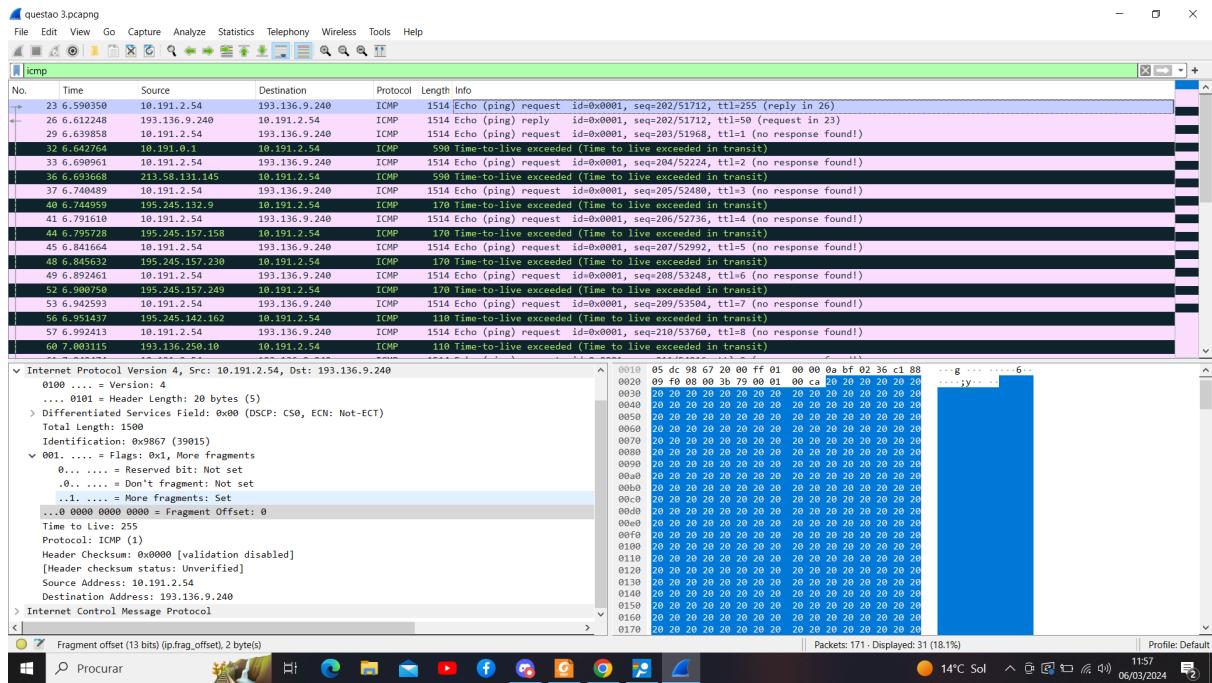
Além disso, a flexibilidade do protocolo IPv4 poderia ser comprometida, já que seria necessário expandir o cabeçalho para acomodar as informações do ICMP. Isso poderia limitar a capacidade de introduzir futuras alterações ou adições de funcionalidades ao protocolo.

Por fim, modificar o formato do cabeçalho IPv4 poderia gerar desafios de compatibilidade com dispositivos de rede existentes que não suportam a nova estrutura. Isso poderia resultar em problemas de comunicação e interoperabilidade entre diferentes dispositivos de rede.

Em resumo, enquanto a integração das informações do ICMP no cabeçalho IPv4 poderia trazer benefícios de eficiência e redução de overhead, isso também acrescentaria desafios significativos em termos de complexidade do protocolo e compatibilidade com dispositivos existentes.

Questão 3

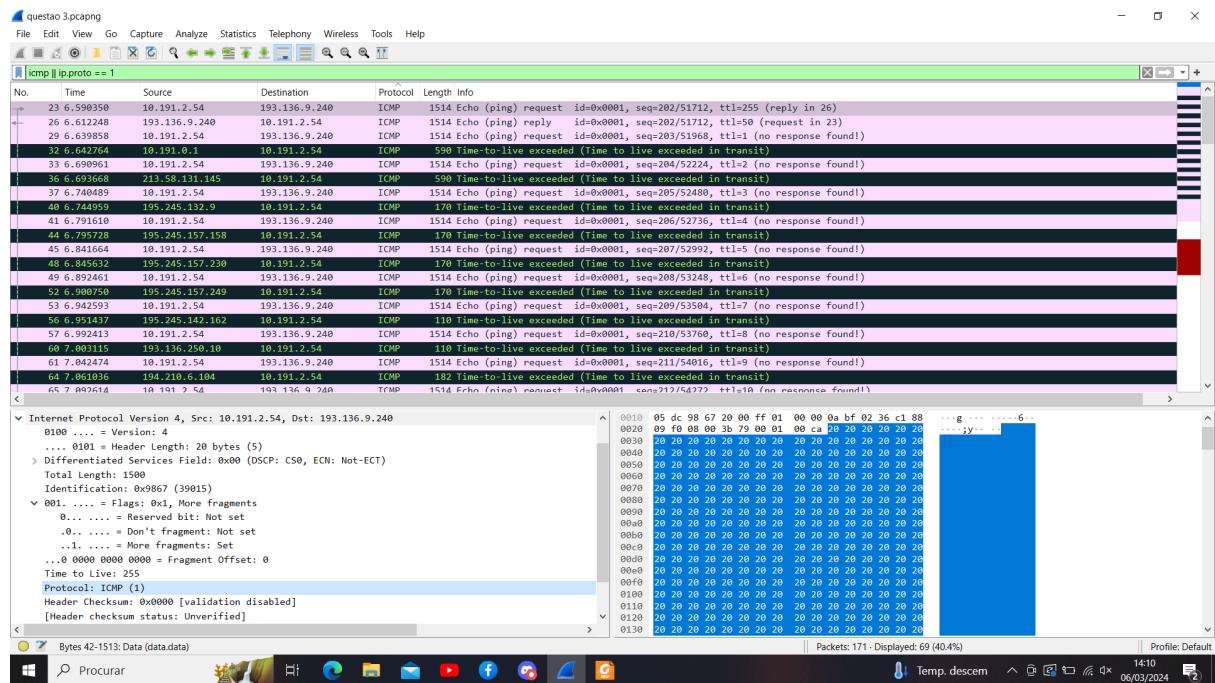
- A. Localize a primeira mensagem ICMP. Porque é que houve necessidade de fragmentar o pacote inicial?



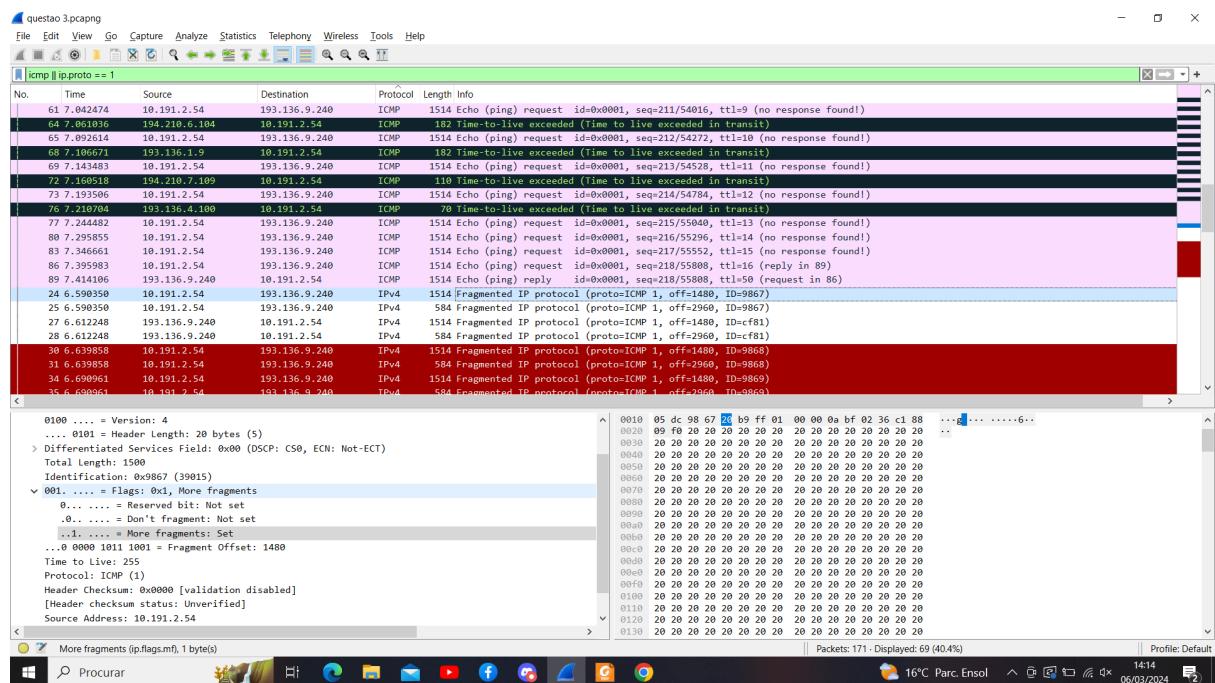
A fragmentação de pacotes é necessária quando um pacote é maior do que o MTU da interface de rede pela qual ele está sendo transmitido. O MTU é o tamanho máximo de um pacote que pode ser transmitido pela interface de rede sem precisar ser dividido em partes menores. Quando um pacote excede o MTU, ele precisa ser fragmentado em pedaços menores para que possa ser transmitido com sucesso através da rede.

- B. Imprima o primeiro fragmento do datagrama IP original. 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?

Podemos perceber que o datagrama foi fragmentado uma vez que a flag de More fragments está como set, além disso, é possível perceber que é o primeiro fragmento uma vez que o Fragment Offset é 0.

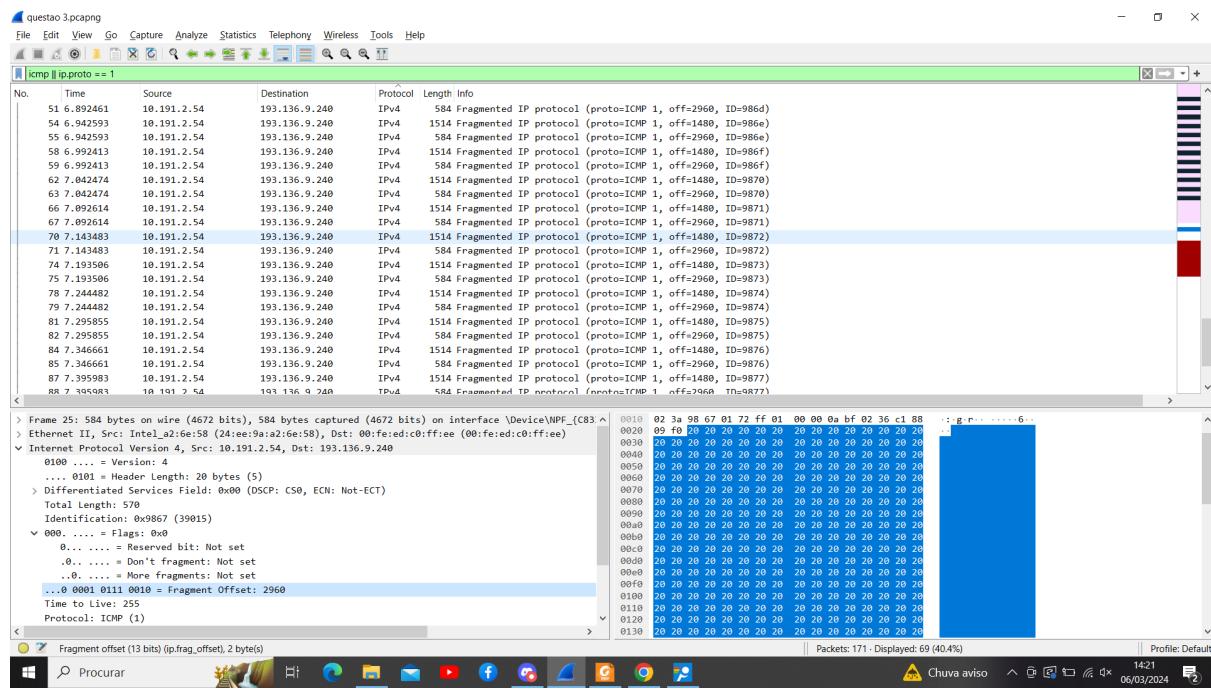


C. Imprima o segundo fragmento do datagrama IP original. Que informação do cabeçalho IP indica que não se trata do primeiro fragmento? Existem mais fragmentos? O que nos permite afirmar isso?



Podemos perceber que se trata do segundo fragmento do datagrama ip original uma vez que tem a mesma identificação que o fragmento da alínea anterior e o seu offset é 1480, também temos a informação de que existem mais fragmentos uma vez que a flag More fragments se encontra como "Set".

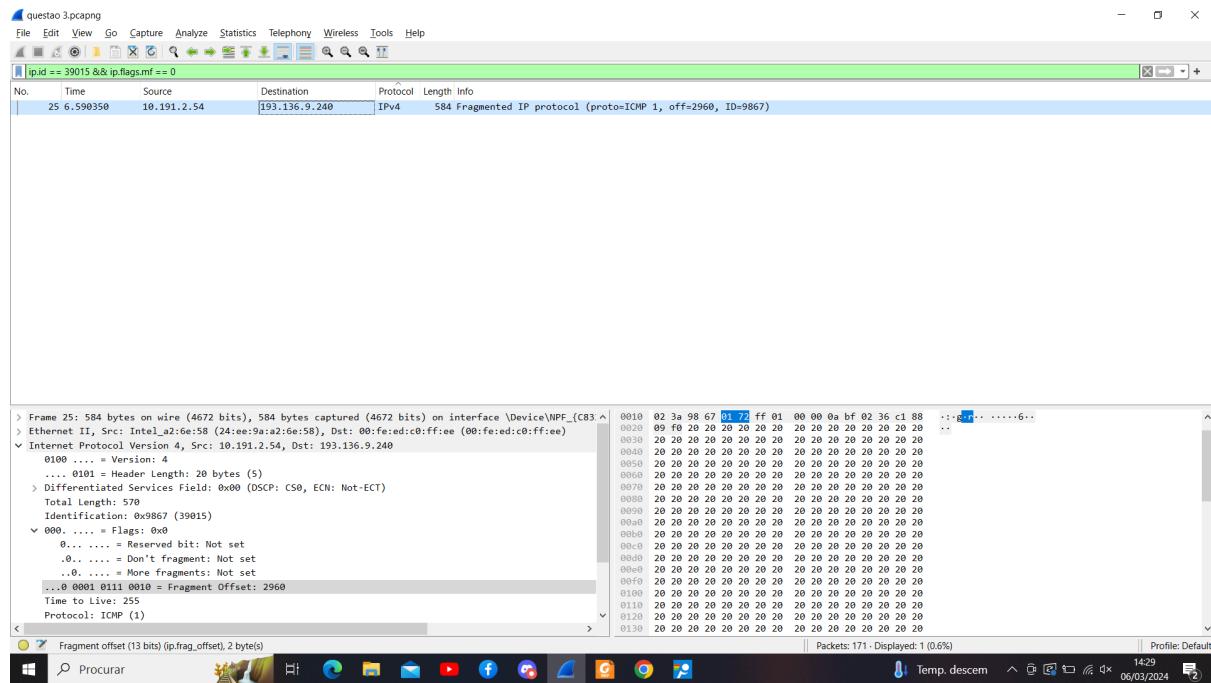
D. Estime teoricamente o número de fragmentos gerados a partir do datagrama IP original e o número de bytes transportados no último fragmento desse datagrama. Compare os dois valores estimados com os obtidos através do wireshark.



Tendo em conta que neste caso o MTU é de 1500 bytes, seria esperado a existência de 3 fragmentos. Como é possível ver na imagem a flag More fragments encontra-se a "Not set" o que nos indica que este se trata do último fragmento. Lembrando que o pacote enviado tinha um tamanho de 3530 bytes seria de esperar que no final, somando o valor do Fragment Offset do último fragmento com o seu tamanho, se obtivesse os 3530 bytes que neste caso é o que se confirma, uma vez que, $2960+570=3530$.

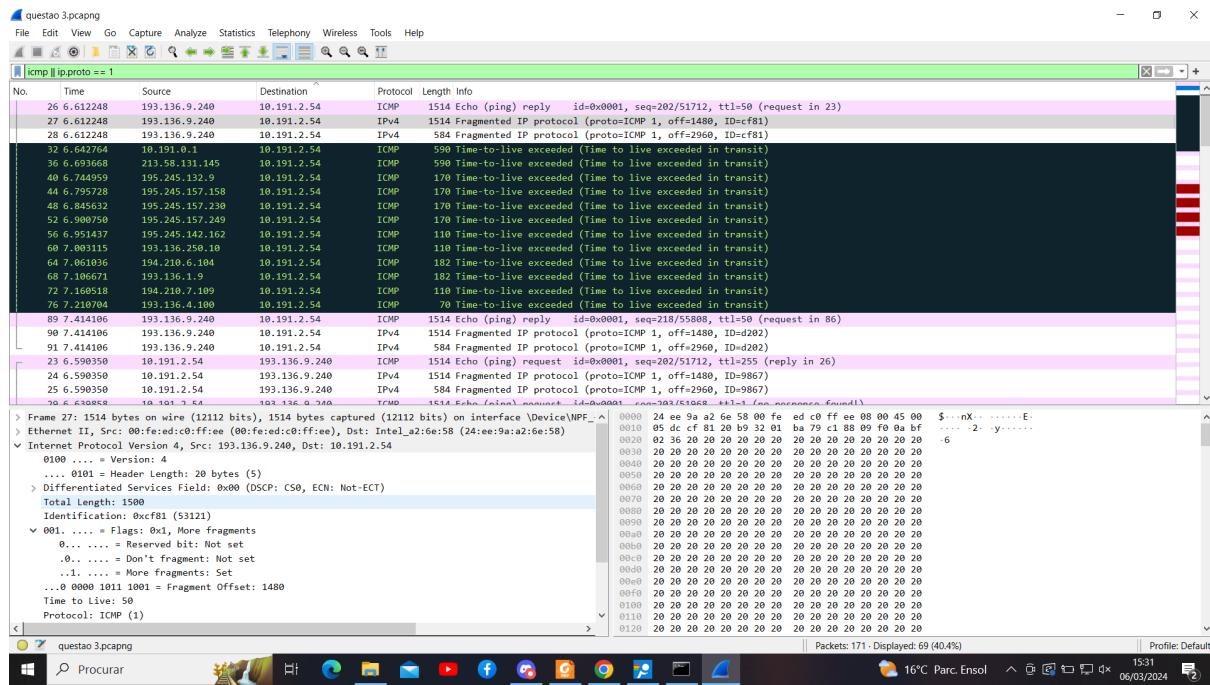
E. Como se detecta o último fragmento correspondente ao datagrama original?

Estabeleça um filtro no wireshark que permita listar o último fragmento do primeiro datagrama IP segmentado.



Como demonstrado na imagem, para detectar o último fragmento correspondente ao datagrama original utilizamos o filtro ip.id == 39015 uma vez que o datagrama original tinha como identificação 39015, acrescentando o filtro ip.flags.mf == 0 para que apenas apareça o fragmento cuja flag More fragments se encontra a “Not set” que é o último fragmento.

F. Identifique o equipamento onde o datagrama IP original é reconstruído a partir dos fragmentos. A reconstrução poderia ter ocorrido noutro equipamento diferente do identificado? Porquê?



Neste caso o equipamento onde o datagrama IP original é reconstruído é no nosso computador uma vez que a reconstrução geralmente é feita no destino final da comunicação. Teoricamente a reconstrução poderia ocorrer em qualquer equipamento que tenha acesso a todos os fragmentos, mas na prática, é mais comum ocorrer no destino final.

G. 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 mudam nos diferentes fragmentos são principalmente o "Fragment Offset" e o bit "More Fragments". O "Fragment Offset" indica a posição do fragmento no datagrama original, enquanto o bit "More Fragments" indica se ainda existem mais fragmentos a seguir. Essas informações permitem reconstruir o datagrama original uma vez que fornecem a sequência correta dos fragmentos e a posição de cada fragmento dentro do datagrama original. Quando os fragmentos são recebidos, o dispositivo de destino reagrupa-os de acordo com os seus offsets e o bit "More Fragments", reconstruindo assim o datagrama IP original. O dispositivo de destino sabe que todos os fragmentos foram recebidos quando encontra um fragmento com o bit "More Fragments" definido como 0.

H. Por que razão apenas o primeiro fragmento de cada pacote é identificado como sendo um pacote ICMP?

Apenas o primeiro fragmento é identificado como um pacote ICMP porque é o único que contém o cabeçalho IP completo, incluindo as informações necessárias para identificar o tipo de pacote. Os fragmentos subsequentes contêm apenas parte dos dados originais e não incluem o cabeçalho ICMP.

I. Com que valor é o tamanho do datagrama comparado a fim de se determinar se este deve ser fragmentado? Quais seriam os efeitos na rede ao aumentar/diminuir este valor?

```
| en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
```

O tamanho do datagrama é comparado com o MTU (Maximum Transmission Unit) que no caso é 1500 bytes. No nosso caso o pacote original tinha tamanho 3530, excedendo assim o MTU, tornando necessária a sua fragmentação.

Ao aumentar o MTU:

A eficiência de transmissão pode aumentar, pois menos fragmentação é necessária, resultando em menos pacotes transmitidos para enviar o mesmo volume de dados. O overhead de fragmentação é reduzido, já que menos fragmentação significa menos sobrecarga de cabeçalhos IP adicionais. Pode haver uma redução potencial na latência devido a menos tempo de espera para a transmissão e recebimento de pacotes.

Ao diminuir o MTU:

A fragmentação ocorre com mais frequência, resultando em mais sobrecarga de fragmentação na rede e nos dispositivos intermediários. O overhead de fragmentação aumenta devido a mais fragmentação, o que pode afetar o desempenho da rede. Pode haver um aumento potencial na latência e na perda de pacotes devido à fragmentação adicional, especialmente em redes congestionadas ou com baixa confiabilidade. Portanto, ajustar o valor do MTU deve ser feito com cautela para equilibrar eficiência de transmissão, overhead de fragmentação e potencial para latência e perda de pacotes.

- J. Sabendo que no comando ping a opção -f (Windows), -M do (Linux) ou -D (Mac) ativa a flag “Don’t Fragment” (DF) no cabeçalho do IPv4, usando ping <opção DF> <opção pkt_size> SIZE marco.uminho.pt, (opção pkt_size = -l (Windows) ou -s (Linux, Mac), determine o valor máximo de SIZE sem que ocorra fragmentação do pacote? Justifique o valor obtido.

```
[diogoferreira@MacBook-Pro-de-Diogo ~ % ping -D -s 1473 marco.uminho.pt
PING marco.uminho.pt (193.136.9.240): 1473 data bytes
ping: sendto: Message too long
ping: sendto: Message too long
Request timeout for icmp_seq 0
^C
--- marco.uminho.pt ping statistics ---
2 packets transmitted, 0 packets received, 100.0% packet loss
[diogoferreira@MacBook-Pro-de-Diogo ~ % ping -D -s 1472 marco.uminho.pt
PING marco.uminho.pt (193.136.9.240): 1472 data bytes
1480 bytes from 193.136.9.240: icmp_seq=0 ttl=61 time=201.408 ms
1480 bytes from 193.136.9.240: icmp_seq=1 ttl=61 time=247.713 ms
1480 bytes from 193.136.9.240: icmp_seq=2 ttl=61 time=297.584 ms
1480 bytes from 193.136.9.240: icmp_seq=3 ttl=61 time=5.194 ms
^C
```

Apesar do MTU ser 1500 bytes, o valor máximo de SIZE sem que ocorra fragmentação do pacote foi 1472 uma vez que são necessários 8 bytes para o cabeçalho ICMP e 20 bytes para o cabeçalho IPV4, fazendo com que não seja possível colocar um SIZE superior a 1472, mesmo tendo um MTU de 1500 bytes.

Parte 2

Os polos Condado Portucalense e Institucional estão ligados ao router do ISP ReiDaNet, enquanto Galiza e CDN estão ligados ao ISP CondadoOnline. Interligando os dois ISPs existe um ISP de trânsito cuja rede Core é constituída pelos dispositivos n1 a n6.

Questão 1

Com os avanços da Inteligência Artificial, D. Afonso Henriques termina todas as suas tarefas mais cedo e vê-se com algum tempo livre. Decide então fazer remodelações no reino:

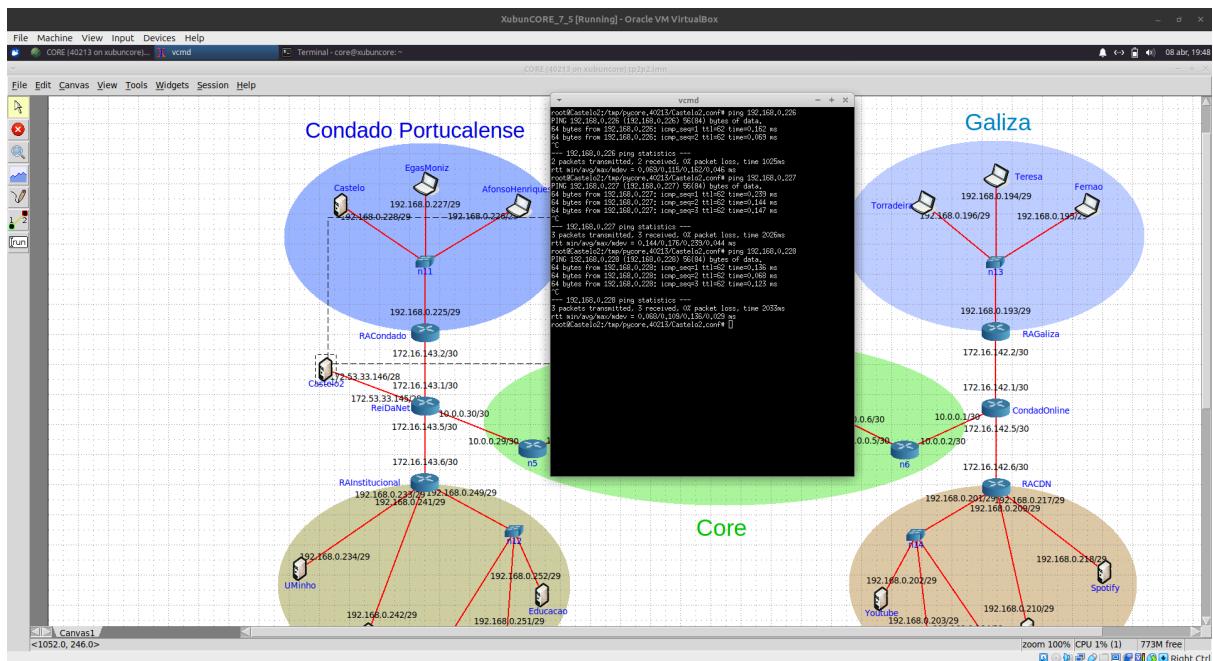
A) De modo a garantir uma posição estrategicamente mais vantajosa e ter casa de férias para relaxar entre batalhas, ordena a construção de um segundo Castelo, em Braga. Não tendo qualquer queixa do serviço prestado, recorre aos serviços do ISP ReiDaNet, que já utiliza no condado, para ter acesso à rede no segundo Castelo. O ISP atribuiu-lhe o endereço de rede IP 172.53.33.128/26. Defina um esquema de endereçamento que permita o estabelecimento de pelo menos 3 redes e que garanta que cada uma destas possa ter 12 ou mais hosts. Assuma que todos os endereços de sub-redes são utilizáveis.

R.: Para definir um esquema de sub-redes, teremos de considerar o binário da rede com a máscara que nos é proposta. Sabemos que a rede possui 26 bits de dígitos fixos para identificar a rede. Ou seja, se 3 números de 8 bits cada equivale a 24 bits, 26 ocupam os primeiros 2 bits do último número (128). Se $128 = 10000000$ e, se considerarmos que necessitamos de criar 3 redes ou mais, o indicado seria utilizar uma máscara de $26 + 2 = 28$ bits. Assim ficaremos com as redes $172.53.33.144/28$ (10010000), $172.53.33.160/28$ (10100000) e $172.53.33.176/28$ ($10110001 - 10111110$). De notar que os endereços reservam 1 endereço para a rede, onde os bits da porção dos hosts ficam a 0, e outro para broadcast, onde a porção dos hosts ficam todos a 1. Esta é a razão por os endereços de unicast variarem apenas entre 172.53.33.145 até 172.53.33.158, por exemplo.

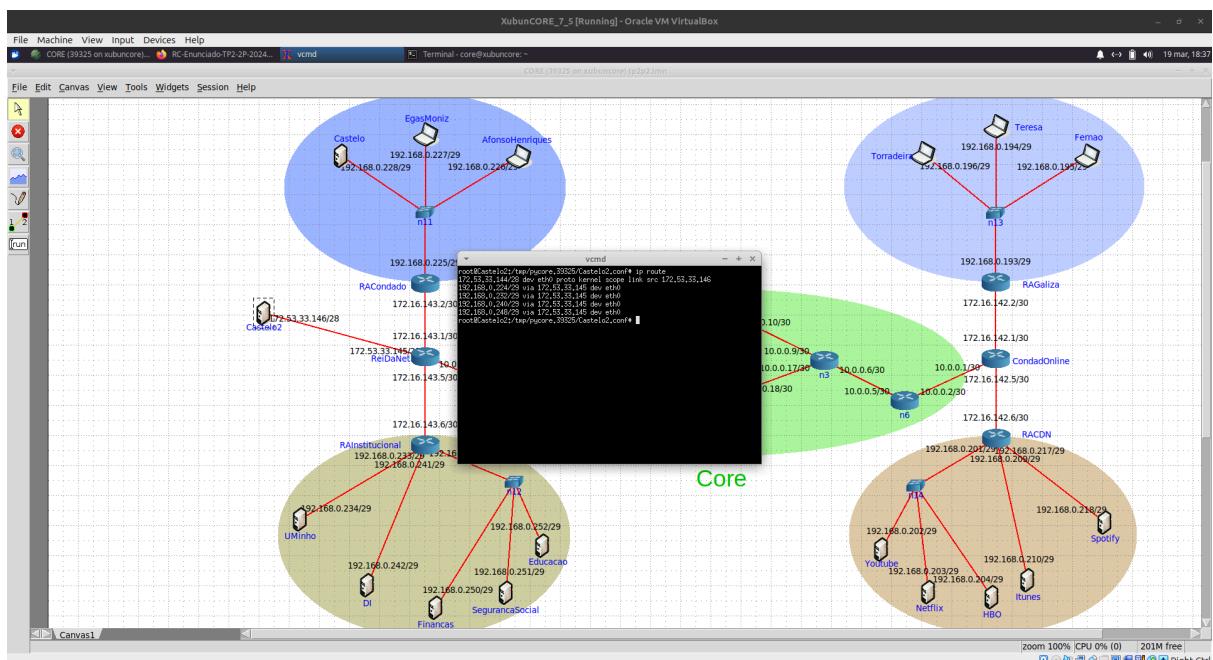
Relativamente a hosts, é possível possuir até 13 hosts por rede, onde ficam um total de 4 bits para a porção dos hosts, onde existe um máximo de 15 hosts. No entanto, é necessário retirar o endereço identificativo da rede, com a porção dos hosts a zero, e o endereço para broadcast, com a porção dos hosts a 1. Daí advém os 13 endereços disponíveis.

B) Ligue um novo host Castelo2 diretamente ao router ReiDaNet. Associe-lhe um endereço, à sua escolha, pertencente a uma sub-rede disponível das criadas na alínea anterior (garanta que a interface do router ReiDaNet utiliza o primeiro endereço da sub-rede escolhida). Verifique que tem conectividade com os dispositivos do Condado Portucalense.

R.
..



C) Não estando satisfeito com a decoração deste novo Castelo, opta por eliminar a sua rota default. Adicione as rotas necessárias para que o Castelo2 continue a ter acesso ao Condado Portucalense e à rede Institucional. Mostre que a conectividade é restabelecida, assim como a tabela de encaminhamento resultante. Explicite ainda a utilidade de uma rota default.

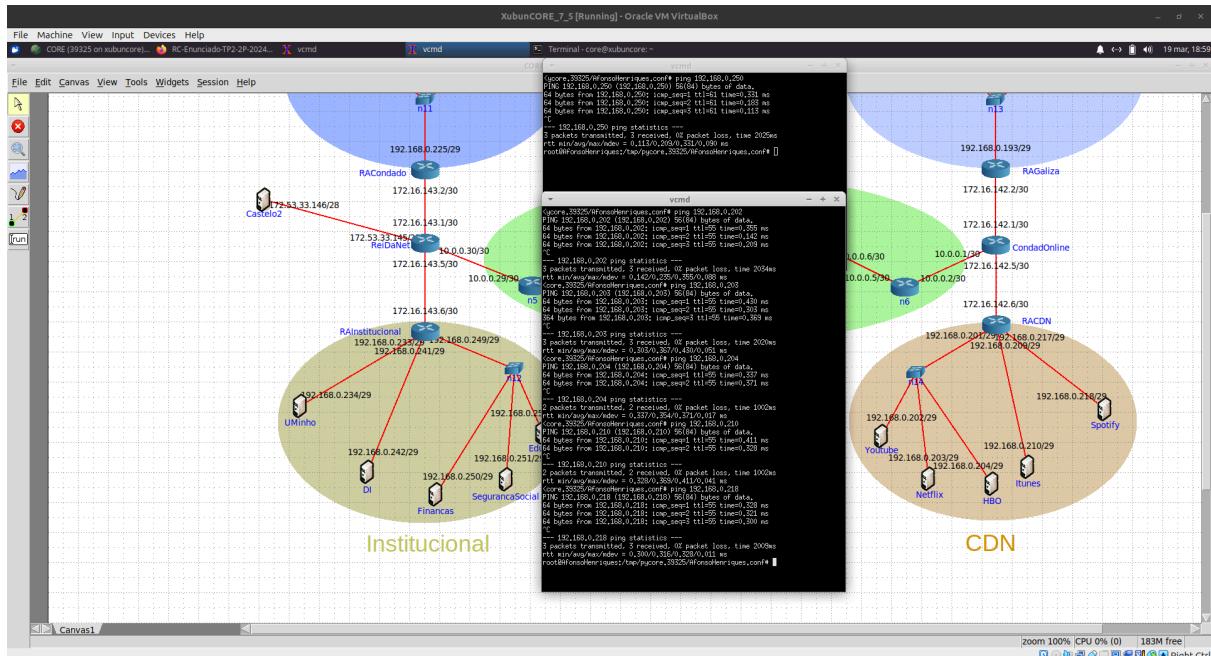


R.: Neste caso, a rota default permite que não seja necessário tantas entradas na routing table, permitindo que o tráfego seja encaminhado para o router através da rota default, caso não exista nenhuma entrada para o destino do pacote. Isto leva a um routing mais eficiente.

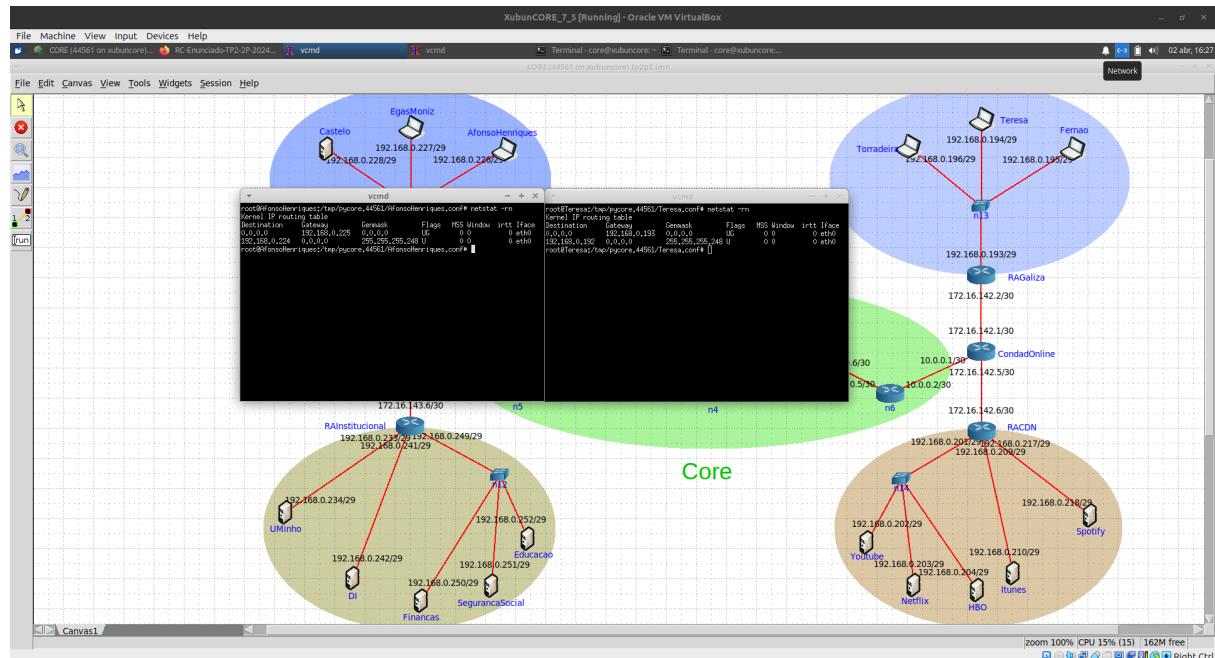
Questão 2

D.Afonso Henriques quer enviar fotos do novo Castelo à sua mãe, D.Teresa, mas está a ter alguns problemas de comunicação. Este alega que o problema deverá estar no dispositivo de D.Teresa, uma vez que no dia anterior conseguiu enviar a sua declaração do IRS para o portal das finanças, e não tem qualquer problema em ver as suas séries favoritas, disponíveis na rede de conteúdos.

A) Confirme, através do comando ping, que AfonsoHenriques tem efetivamente conectividade com o servidor Financas e com os servidores da CDN

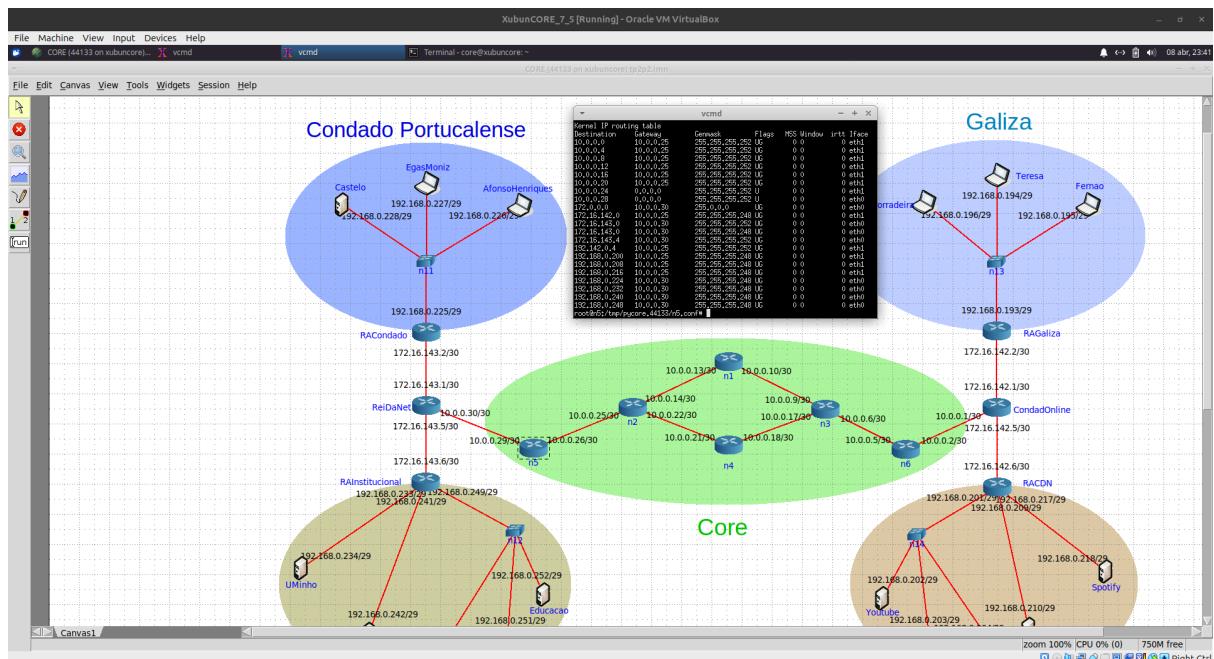


- B) Recorrendo ao comando netstat -rn, analise as tabelas de encaminhamento dos dispositivos AfonsoHenriques e Teresa. Existe algum problema com as suas entradas? Identifique e descreva a utilidade de cada uma das entradas destes dois hosts

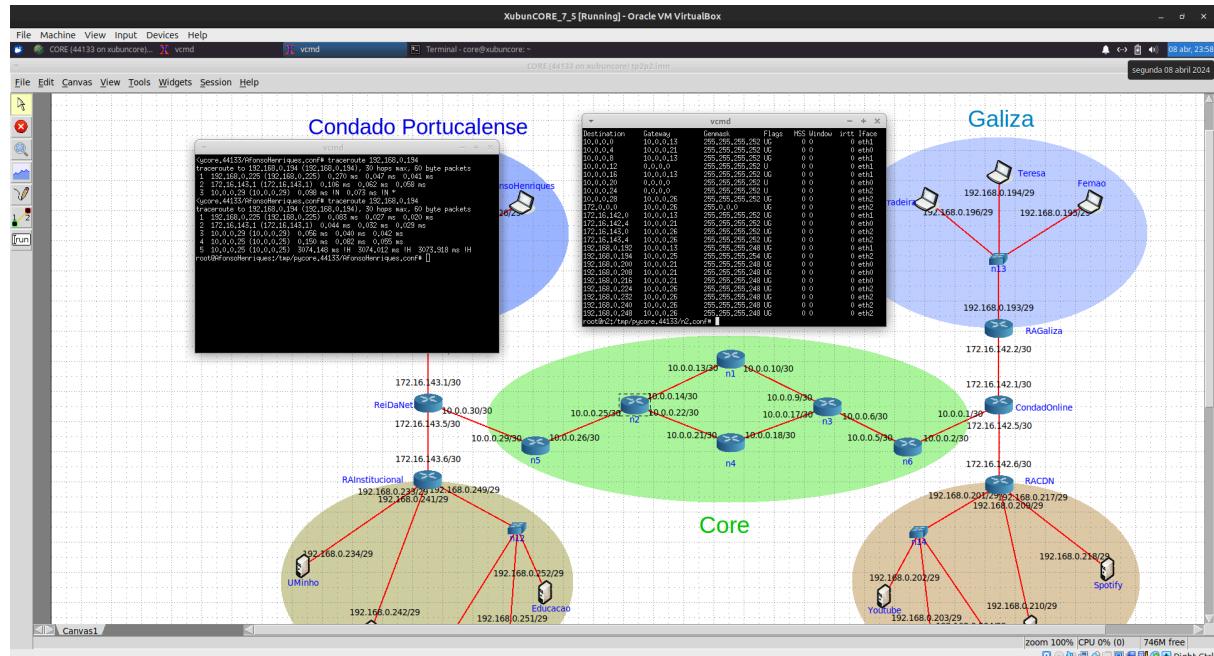


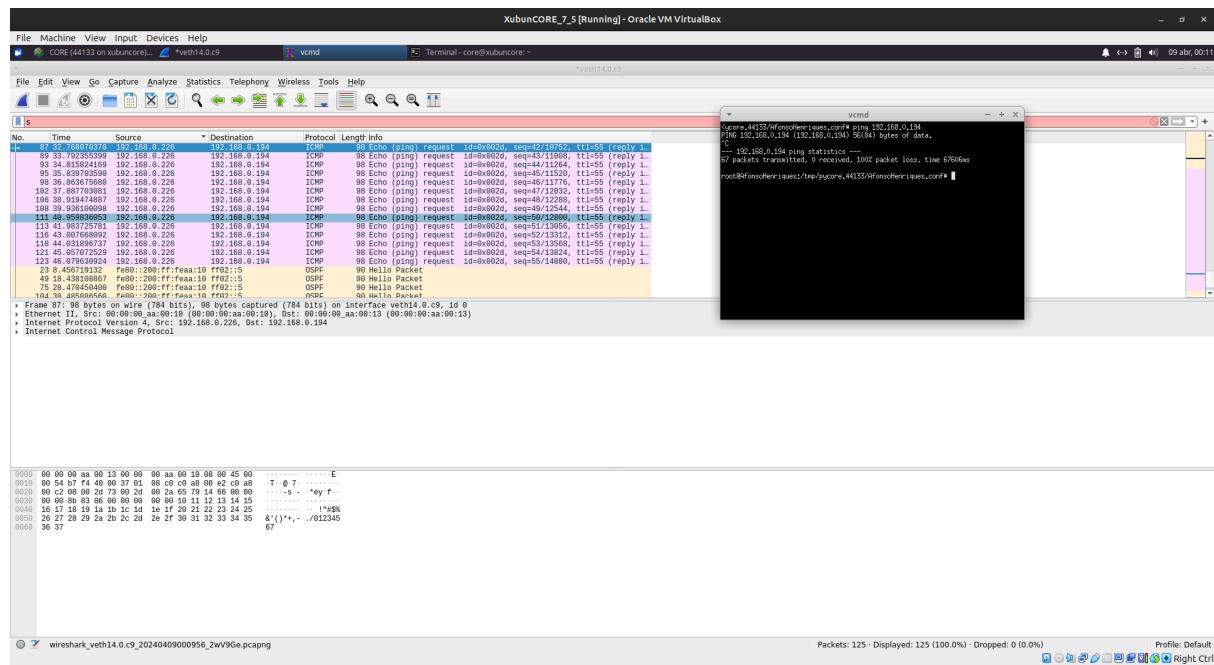
Com estas tabelas, percebemos que o problema não está nos hosts de cada rede, pois estes possuem ambos uma route default para o respetivo router da sua rede, representado na primeira entrada das duas tabelas. As segundas entradas das tabelas representam a route para receber os pacotes que estiverem na rede, pois a função de diferenciar o destino específico fica ao encargo do router/switch. Isto faz com que a entrada da tabela dos hosts traduz a premissa de que todos os pacotes que seja para sua rede, que seja dirigidos para si.

- C) Analise o comportamento dos routers do core da rede (n1 a n6) quando tenta estabelecer comunicação entre os hosts AfonsoHenriques e Teresa. Indique que dispositivo(s) não permite(m) o encaminhamento correto dos pacotes. Seguidamente, avalie e explique a(s) causa(s) do funcionamento incorreto do dispositivo.



É possível perceber que o router n5, sendo ele o primeiro do caminho pela região core, não possui a entrada para a rede desejada (192.168.0.192/29). Isto leva a que se perca o pacote logo aqui.



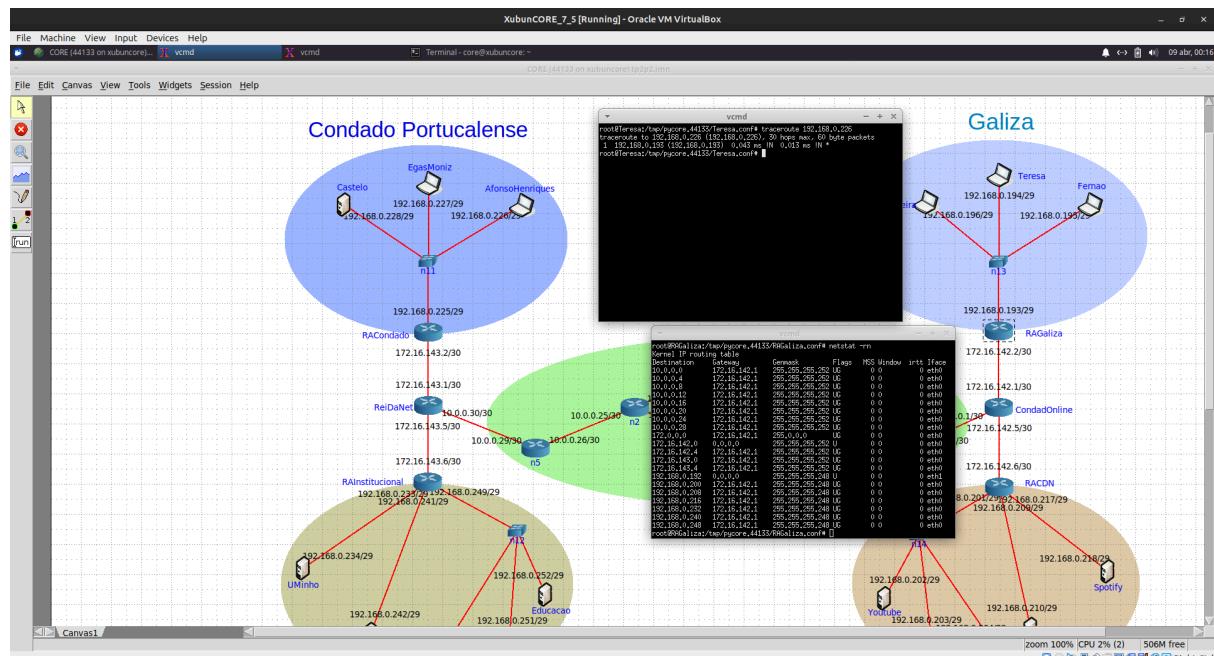


Através do Wireshark, sabemos então que, com as alterações às tabelas, chega tráfego do AfonsoHenriques até à Teresa, apesar de não existir conectividade ainda.

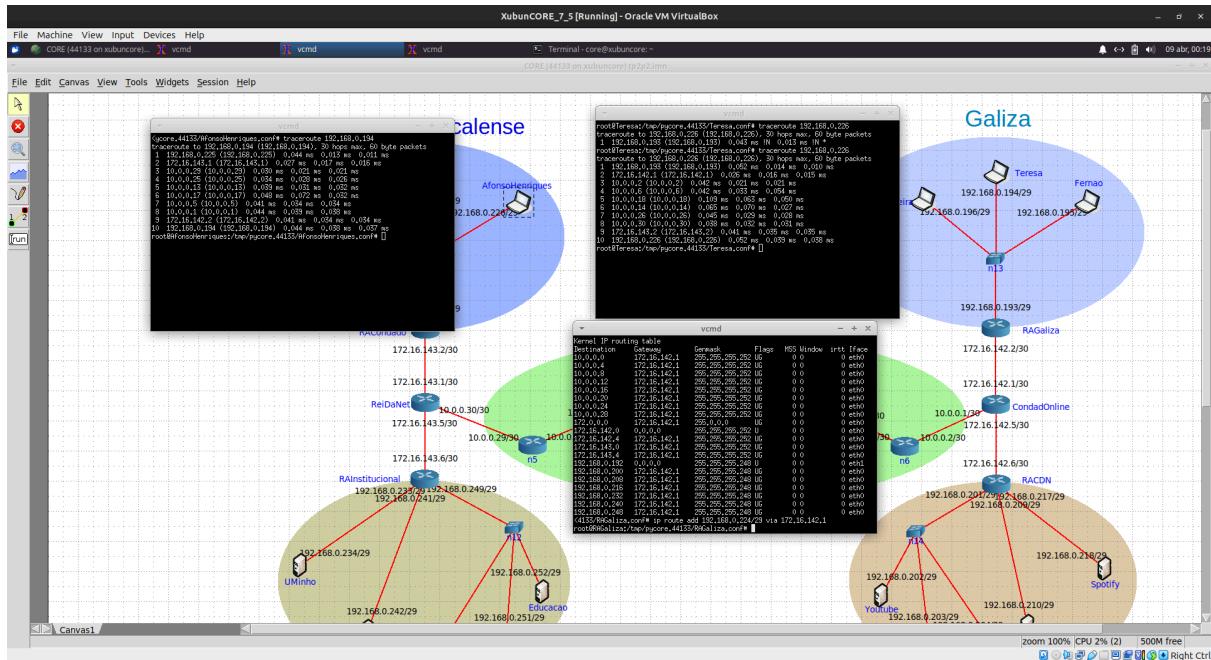
D) Uma vez que o core da rede esteja a encaminhar corretamente os pacotes enviados por AfonsoHenriques, confira com o Wireshark se estes são recebidos por Teresa.

- a) Em caso afirmativo, porque é que continua a não existir conectividade entre D.Teresa e D.Afonso Henriques? Efetue as alterações necessárias para garantir que a conectividade é restabelecida e o confronto entre os dois é evitado.

R.: Não existe conectividade devido ao facto de haver o mesmo problema que foi resolvido no envio de informação mas na receção da resposta. Isto é as tabelas de encaminhamento não estão correctamente definidas.



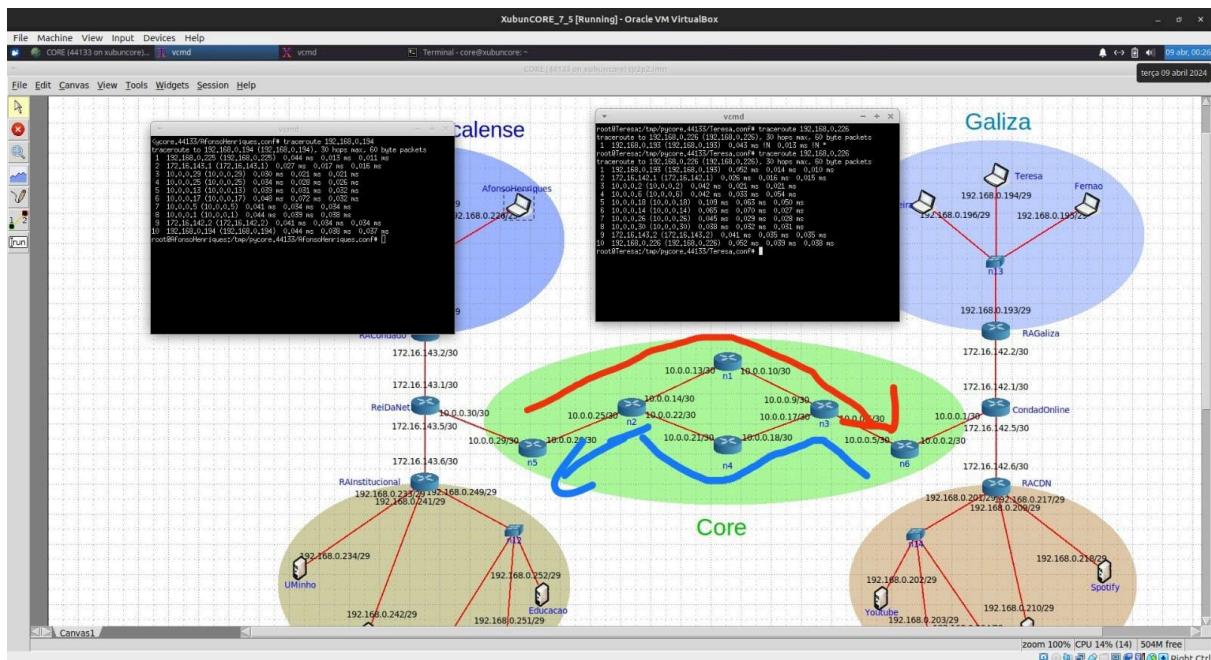
Executando um traceroute a partir da Teresa, é possível constatar que o router da rede não possui uma entrada para a rede do AfonsoHenriques, levando a que se percam os pacotes. É necessário, portanto, introduzir a entrada na tabela.



Corrigindo esse detalhe, é possível ver que a conexão ficou estabelecida.

- b) As rotas dos pacotes ICMP echo reply são as mesmas, mas em sentido inverso, que as rotas dos pacotes ICMP echo request enviados entre AfonsoHenriques e Teresa? (Sugestão: analise as rotas nos dois sentidos com o traceroute). Mostre graficamente a rota seguida nos dois sentidos por esses pacotes ICMP

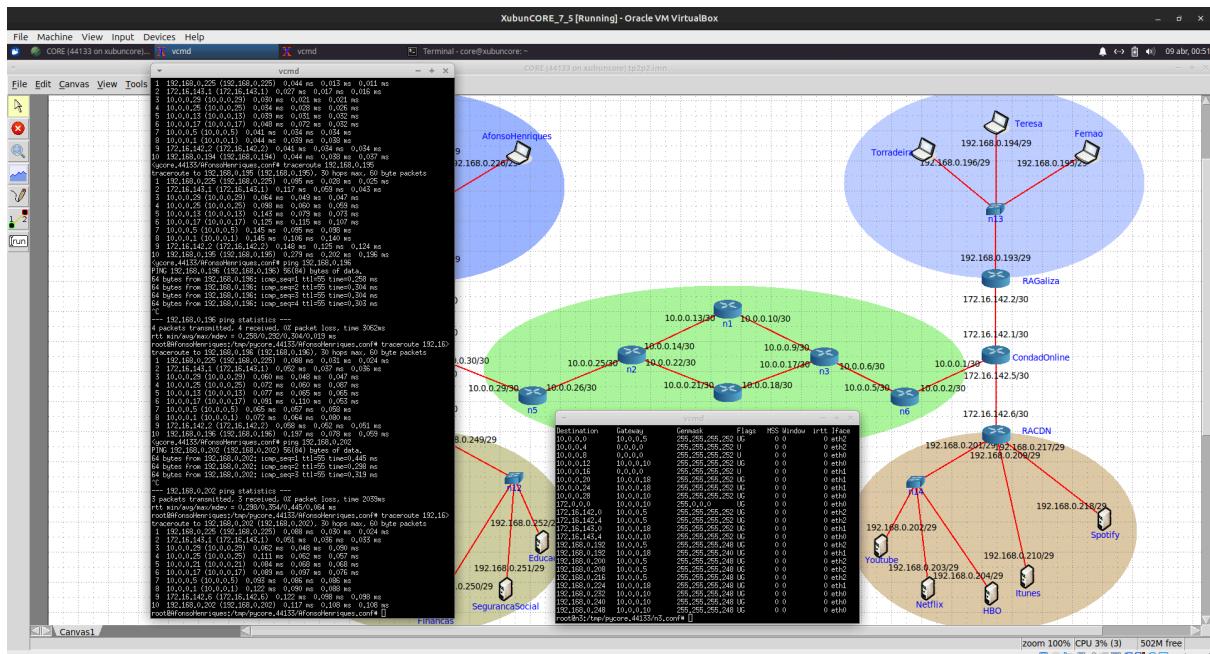
R.: As rotas tomadas pelos pacotes ICMP echo reply são diferentes dos ICMP echo request. Isto porque é possível averiguar que o ICMP echo request faz o caminho do n2 para o n1 enquanto que o ICMP echo reply faz os saltos do n3 para o n4, e para o n2.



- E) Estando restabelecida a conectividade entre os dois hosts, obtenha a tabela de encaminhamento de n3 e foque-se na seguinte entrada: 192.168.0.192 | 10.0.0.18

Existe uma correspondência (match) nesta entrada para pacotes enviados para o polo Galiza? E para CDN? Caso seja essa a entrada utilizada para o encaminhamento, permitirá o funcionamento esperado do dispositivo?
Ofereça uma explicação pela qual essa entrada é ou não utilizada.

R.: A entrada não possui nenhum match para pacotes enviados para a Galiza. Para a CDN, já existem matches para essa entrada.



Não, se esta entrada for utilizada para encaminhamento, o dispositivo não terá um funcionamento adequado, porque entrariam num ciclo e perder-se-iam os pacotes. Com isso, esta entrada não é utilizada por existir uma entrada para outro gateway com mais prioridade do que essa entrada. Essa prioridade é devida ao facto de que a máscara da entrada da entrada utilizada permite lidar com menos endereços (mais restritivos).

F) Os endereços utilizados pelos quatro polos são endereços públicos ou privados? E os utilizados no core da rede/ISPs? Justifique convenientemente.

R.: Os endereços utilizados pelos polos são privados (192.168.0.0/16 - Classe C, gama utilizada em redes domésticas e corporativas). Os endereços utilizados na rede core também são privados, apesar de uma gama diferente que é frequentemente utilizada por redes corporativas (10.0.0.0/8 - Classe A). Os outros endereços utilizados para os routers também são privados, assumindo a gama de classe B (172.16.0.0/12), utilizados em redes corporativas e de médio porte.

Esta utilização de endereços advém do facto de que estes endereços, apesar de diferentes gamas/classes, pertencem aos endereços reservados como privados. A topologia dos ISP's recorrem a este método para evitar o uso de endereços públicos, porque os caminhos são do conhecimento e domínio deles. Devido a esse domínio, os endereços não necessitam de ser endereços públicos.

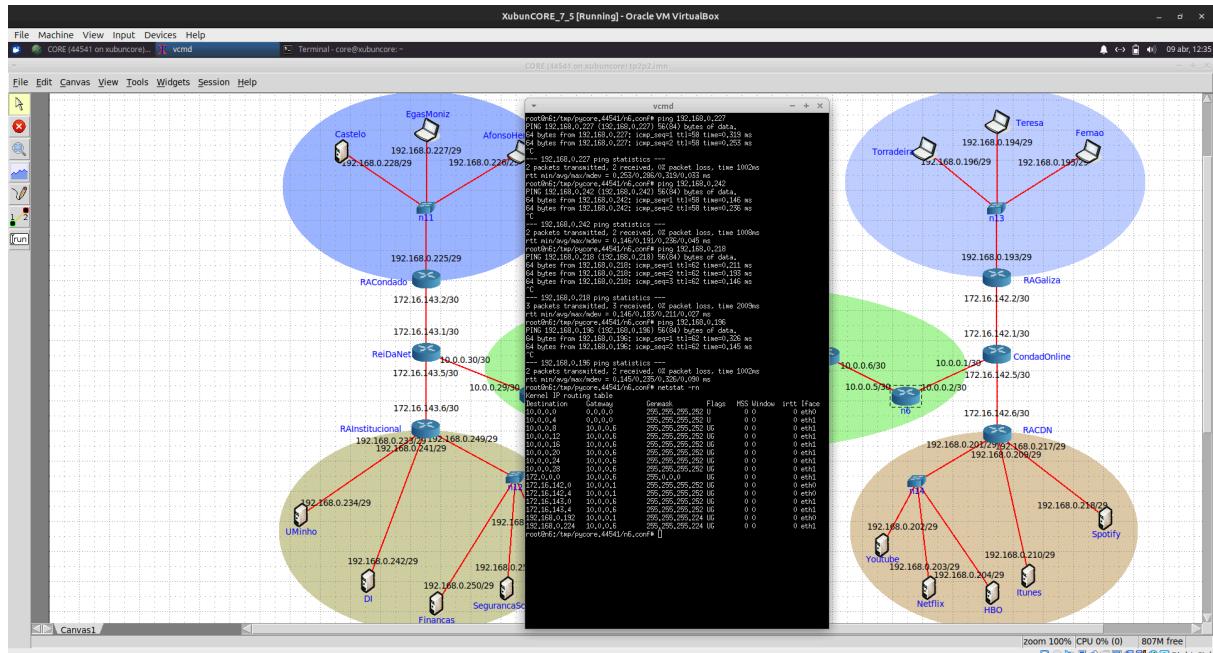
G) Os switches localizados em cada um dos polos têm um endereço IP atribuído? Porquê?

R.: Os switches localizados em cada um dos polos não possuem um endereço IP atribuído. Isto acontece porque o switch não precisa de ter um endereço IP. A sua função será apenas distribuir os pacotes para o respetivo destino, o que leva a que haja uma necessidade de se criarem sub-redes, podendo existir mais hosts dentro da sub-rede em questão.

Questão 3

Ao ver as fotos no CondadoGram, D. Teresa não ficou convencida com as novas alterações e ordena que Afonso Henriques vá arrumar o castelo. Inconformado, este decide planear um novo ataque, mas constata que o seu exército não só perde bastante tempo a decidir que direção tomar a cada salto como, por vezes, inclusivamente se perde.

- a) De modo a facilitar a travessia, elimine as rotas referentes a Galiza e CDN no dispositivo n6 e defina um esquema de sumarização de rotas (*Supernetting*) que permita o uso de apenas uma rota para ambos os polos. Confirme que a conectividade é mantida.



- b) Repita o processo descrito na alínea anterior para CondadoPortucalense e Institucional, também no dispositivo n6.

- c) Comente os aspectos positivos e negativos do uso do *Supernetting*.

R.: Como vantagens do uso do Supernetting, há uma redução drástica da tabela de entrada, reduzindo sobrecarga na memória e processamento, melhorando a eficiência. Também pode levar a um tráfego na rede menor, porque com menos entradas na tabela, há menos informações para propagar através dos protocolos de routing, o que pode levar a uma redução no tráfego e melhoria no desempenho da rede. Ao invés de configurar e gerenciar várias rotas para cada sub-rede individualmente, o supernetting simplifica o processo, exigindo menos configuração e manutenção, que resulta em uma administração mais fácil e menos propensa a erros.

No entanto, também apresenta desvantagens: há uma perda de controlo fino do tráfego porque, ao combinar várias sub-redes em uma única rota, pode-se perder a granularidade necessária para o controle fino do tráfego. Também passa a haver um maior risco de erros de configuração, uma vez que se as sub-redes não forem agrupadas corretamente ou se a máscara de sub-rede não for aplicada adequadamente, pode resultar em problemas de conectividade e dificuldades de resolução de problemas. Em redes muito grandes ou complexas, o supernetting pode atingir limitações de escalabilidade. À medida que o número de sub-redes aumenta, pode se tornar mais difícil ou impraticável combinar todas em uma única rota supernet. Reconfigurar uma rede supernetizada pode ser mais complexo do que reconfigurar redes divididas em sub-redes menores.