RC TP2 PL54

Artur Luís Carlos Pina Luís Ferreira

March 2023

Índice

1 Primeira Parte - Resolução

1.1 Questão 1

"Prepare uma topologia CORE para verificar o comportamento do traceroute. Na topologia deve existir: um host (pc) cliente designado Lost, cujo router de acesso é RA1; o router RA1 está simultaneamente ligado a dois routers no core da rede RC1 e RC2; estes estão conectados a um router de acesso RA2, que por sua vez, se liga a um host (servidor) designado Found. Ajuste o nome dos equipamentos atribuídos por defeito para o enunciado. Apenas nas ligações (links) da rede de core, estabeleça um tempo de propagação de 15 ms. Após ativar a topologia, note que pode não existir conectividade IP imediata entre Lost e Found até que o anúncio de rotas entre routers estabilize."

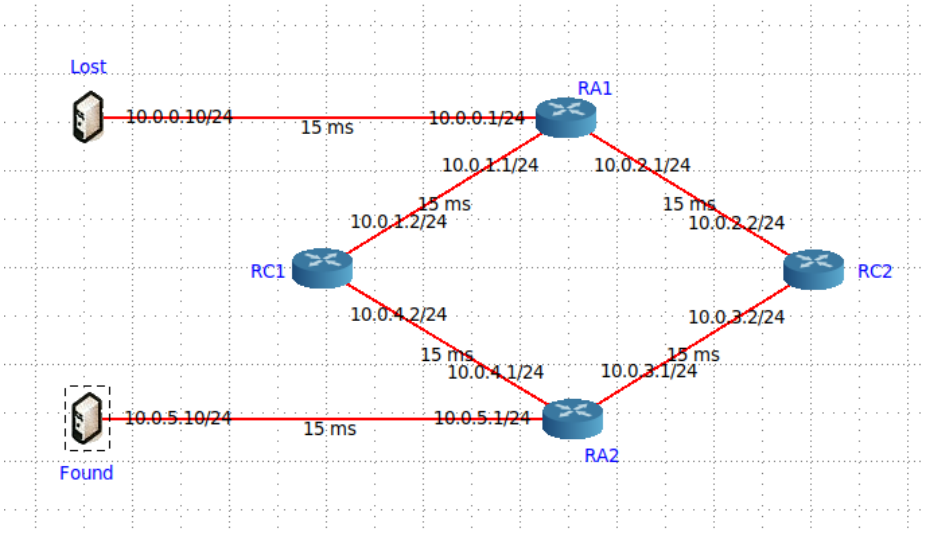


Figure 1: Modelo

1.1.1 Alínea A

"Ative o Wireshark no host Lost. Numa shell de Lost execute o comando traceroute -I para o endereço IP do Found. Registe e analise o tráfego ICMP enviado pelo sistema Lost e o tráfego ICMP recebido como resposta.

Explique os resultados obtidos tendo em conta o princípio de funcionamento do traceroute."

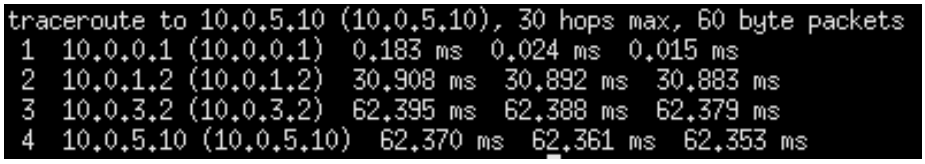


Figure 2: Resultado da execução do comando

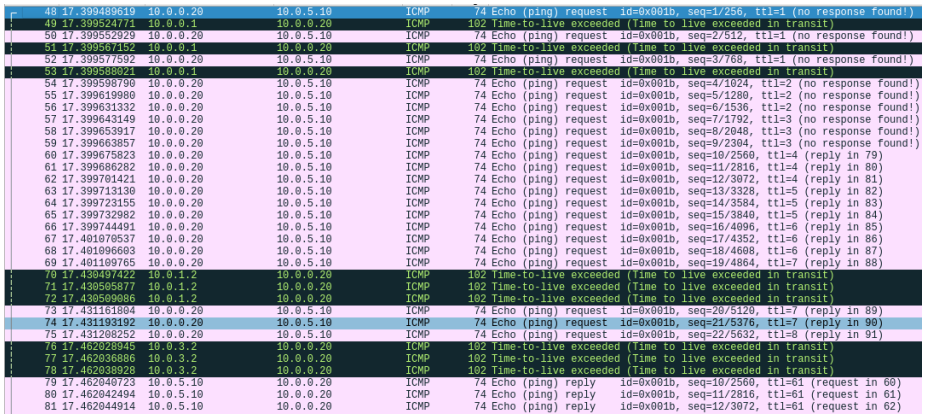


Figure 3:

- O traceroute é um comando utilizado para descobrir quantos dispositivos estão entre o destino e a origem do comando. Inicialmente, a origem envia um pacote com TTL (time to live) de 1. Este TTL é decrementado a cada vez que atinge um novo dispositivo, e quando chega a 0 esse dispositivo emite uma mensagem ICMP para a origem, que então volta a enviar um pacote com um TTL maior (se enviou previamente com TTL = 1, agora vai enviar com TTL = 2). Quando voltar a 0, o mesmo processo ocorre, o local do último salto envia uma mensagem para a origem e esta volta a enviar um pacote com TTL maior. Este processo ocorre até ter sido atingido o destino. Como podemos observar pela figura 3, vemos que as mensagens ICMP recebidas têm como objetivo avisar que os pacotes não conseguiram ser entregues(TTL chegou a 0).

1.1.2 Alínea B

"Qual deve ser o valor inicial mínimo do campo TTL para alcançar o servidor Found?"

- O valor inicial mínimo para alcançar o servidor é 4. Podemos observar na Figura 3 que os pacotes enviados com TTL = 1, TTL = 2 e TTL = 3 nunca chegam a devolver uma resposta, esta aparece apenas quando o TTL é igual ou superior a 4, concluindo assim que esse é o TTL mínimo para alcançar o servidor.

1.1.3 Alínea 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 pacotes de prova com a opção -q."

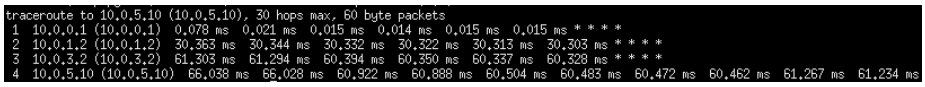


Figure 4: Tempo de ida e volta

- Como é possível observar na figura 4, foram enviados 10 pacotes, e na última linha podemos verificar o tempo entre o envio e a resposta do servidor. Assim sendo, basta fazer uma média dos 10 tempos medidos para obter o valor médio do tempo de ida-e-volta.

- *(66.038 + 66.028 + 60.922 + 60.888 + 60.504 + 60.483 + 60.472 + 60.462 + 61.267 + 61.234) / 10 =* ***61.8298 ms***

1.1.4 Alínea 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?"

- O valor médio de atraso não podia ser calculado dividindo o RTT por dois pois para isso estávamos a assumir que a distância percorrida era a mesma nos dois sentidos,o que não acontece. Um pacote pode percorrer um determinado caminho em direção ao destino e voltar à sua origem por um caminho completamente diferente.

1.2 Questão 2

"Pretende-se agora usar o traceroute na sua máquina nativa e gerar datagramas IP de diferentes tamanhos.

Procedimento a seguir:
Usando o wireshark capture o tráfego gerado pelo traceroute sem especificar o tamanho do pacote, i.e., quando é usado o tamanho do pacote de prova por defeito. Utilize como máquina destino o host marco.uminho.pt. Pare a captura. Com base no tráfego capturado, identifique os pedidos ICMP Echo Request e o conjunto de mensagens devolvidas como resposta.

Selecione a primeira mensagem ICMP capturada e centre a análise no nível protocolar IP e, em particular, do cabeçalho IP (expanda o tab correspondente na janela de detalhe do wireshark)."

1.2.1 Alínea A

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

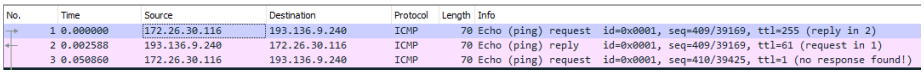


Figure 5: IP da interface ativa

- O endereço IP da interface ativa do computador é ***172.26.30.116***.
É possível retirar esta informação a partir da figura 5.

1.2.2 Alínea B

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

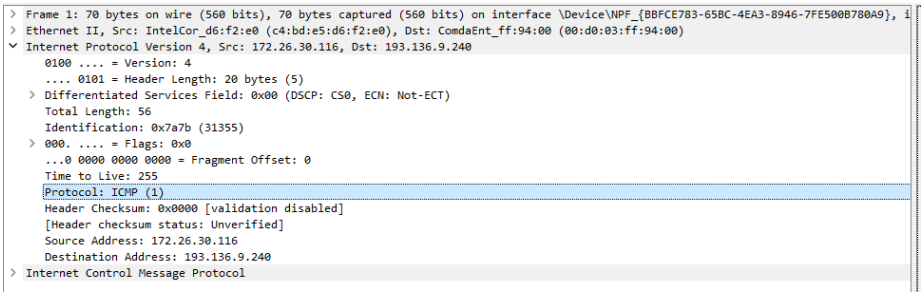


Figure 6: Campos de um Pacote - Protocol

- O campo protocol tem valor ***1***. Permite identificar o ***ICMP***.

1.2.3 Alínea C

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

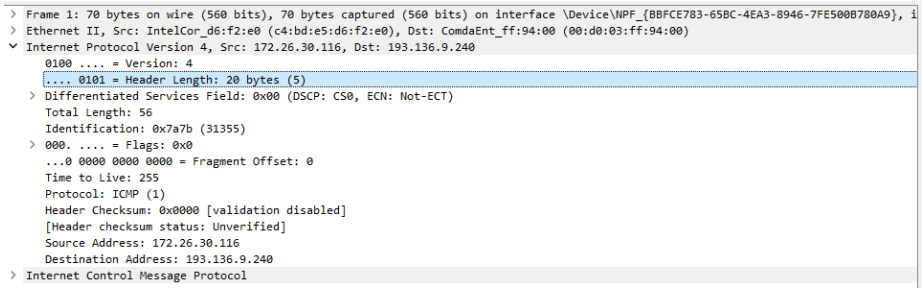


Figure 7: Campos de um Pacote - Header Length e Total Length

- O cabeçalho IPv4 contém ***20 bytes***. Para calcularmos o tamanho do payload necessitamos apenas de fazer a diferença entre o tamanho do pacote (Total Length) e tamanho do cabeçalho, ou seja, 56 - 20 = 36 bytes. Concluímos então o payload tem ***36 bytes***.

1.2.4 Alínea D

"O datagrama IP foi fragmentado? Justifique."

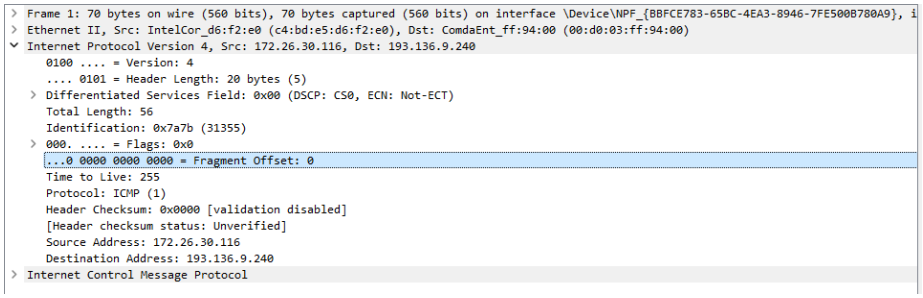


Figure 8: Campos de um Pacote - Fragment Offset

- Analisando o Fragment Offset, que tem valor 0, podemos concluir que o datagrama IP não foi fragmentado.

1.2.5 Alínea 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. "

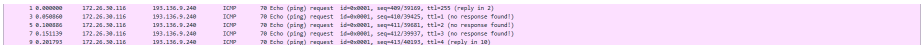


Figure 9: Pacotes ordenados

- Os campos do cabeçalho IP que variam de pacote para pacote são o do ***TTL*** e o de ***Identificação***.

Tal como podemos verificar nas seguintes imagens:

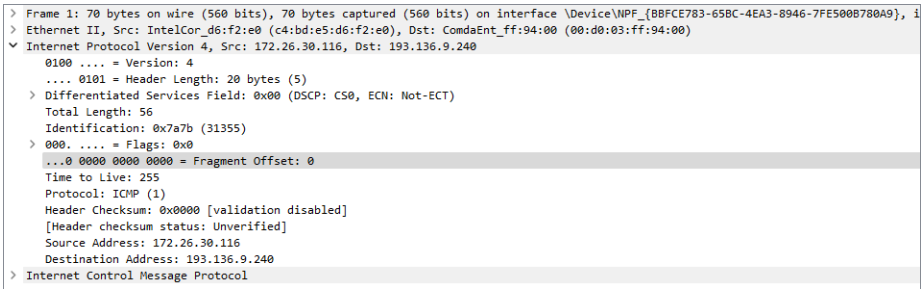


Figure 10: Pacote 1

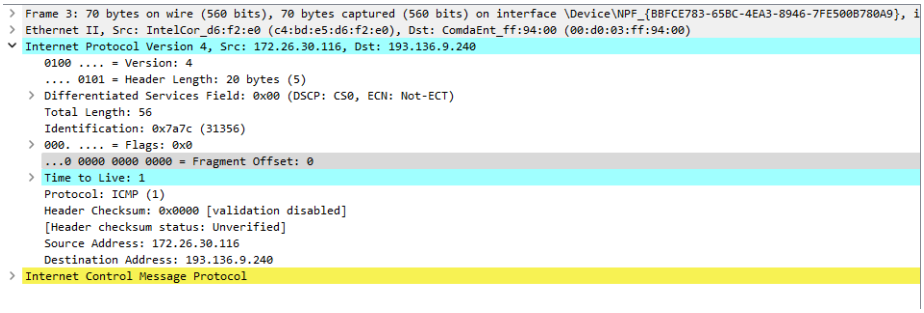


Figure 11: Pacote 2

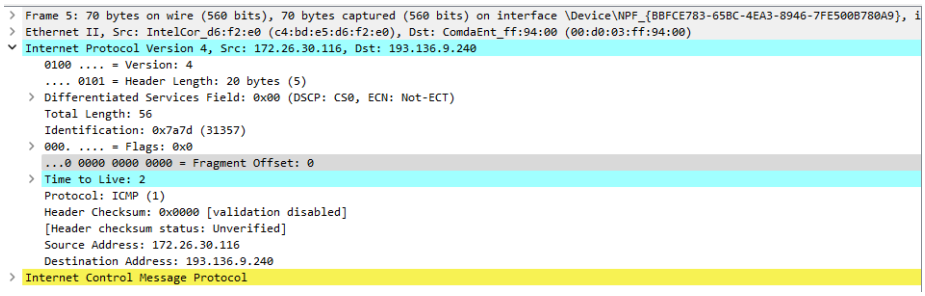


Figure 12: Pacote 3

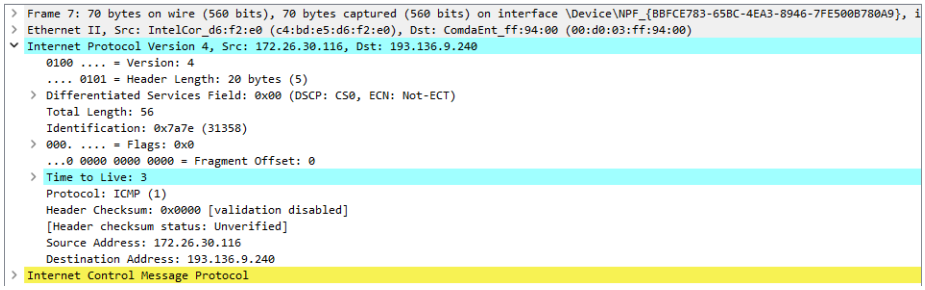


Figure 13: Pacote 4

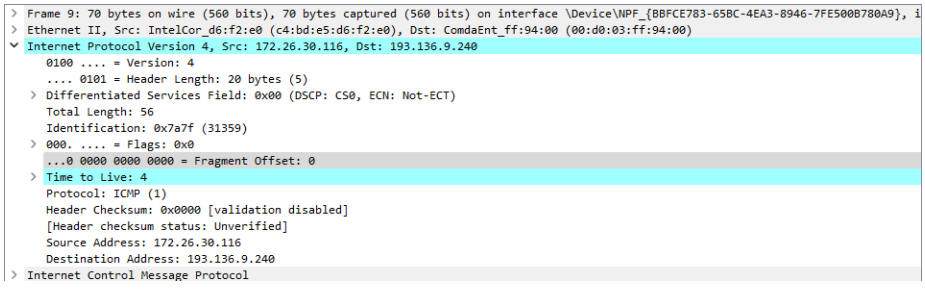


Figure 14: Pacote 5

1.2.6 Alínea F

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

- Analisando a forma como esses campos variam de pacote para pacote, podemos concluir que há um aumento no valor de 1.

Pode-se observar esse aumento progressivo de 1 no valor do campo Identification do pacote, como demonstrado pela variação dos valores de 0x7a7b a 0x7a7f.

No campo do TTL também há esse aumento, no entanto apenas nos últimos 4 pacotes, visto que o primeiro apresenta o valor de 255 (provavelmente o pingplotter envia um ping para saber se o destino está "vivo" e só depois inicia o traceroute).

1.2.7 Alínea G

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

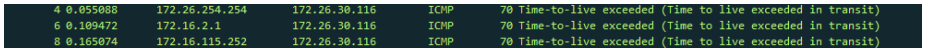


Figure 15:

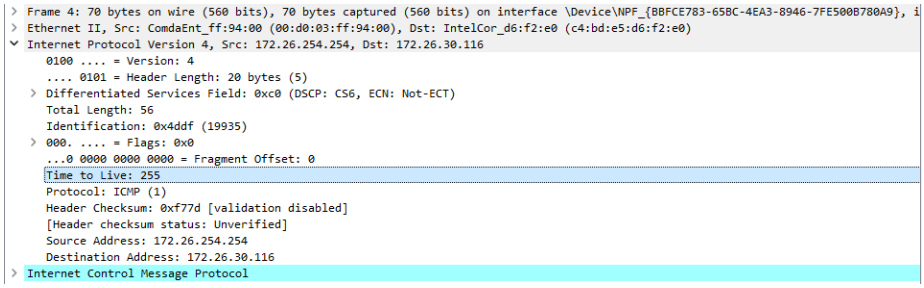


Figure 16:

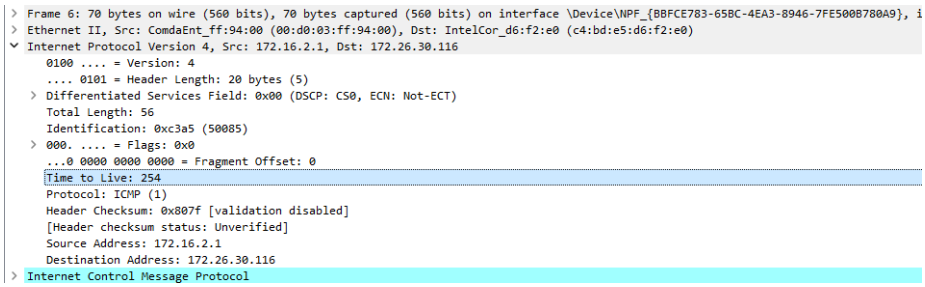


Figure 17:

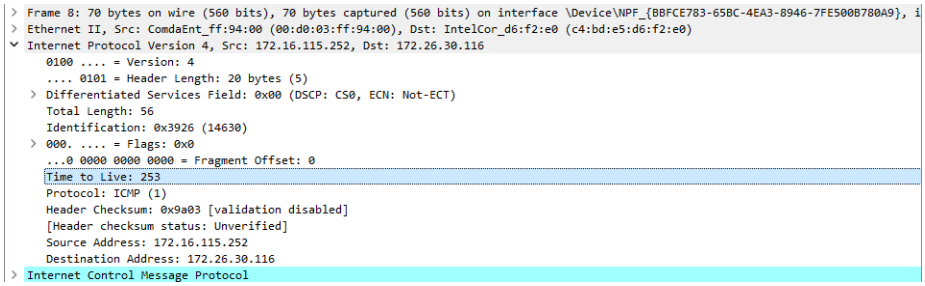


Figure 18:

"**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?"

- O TTL diminui ao longo do trajeto, devido à passagem da mensagem por diversos routers. Como as mensagens de erro são enviadas pelos routers mais distantes, a mensagem passa por mais routers intermédios, o que contribui para o decremento do TTL.

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

- Como dito anteriormente, as mensagens são enviadas de routers distantes, por isso o router arranca com um valor TTL relativamente alto para tentar garantir que o pacote chegue ao destino.

1.2.8 Alínea 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?"

- As vantagens e desvantagens de incluírmos as informações do cabeçalho ICMP no cabeçalho IPv4 seriam as seguintes:

VANTAGENS:
- reduzir o número de pacotes na rede o que poderia trazer benefícios substanciais em termos de eficiência de rede.

DESVANTAGENS:
- aumento do tamanho dos cabeçalhos, o que pode resultar num aumento da fragmentação o que leva à diminuição do desempenho da rede.

1.3 Questão 3

"Pretende-se agora analisar a fragmentação de pacotes IP. Usando o wireshark, capture e observe o tráfego gerado depois do tamanho de pacote ter sido definido para (3500 + 54=3554) bytes, em que 54 é o número do grupo de trabalho (PL54). De modo a poder visualizar os fragmentos, aceda a Edit -> Preferences -> Protocols e em IPv4 desative a opção "Reassemble fragmented IPv4 datagrams"."

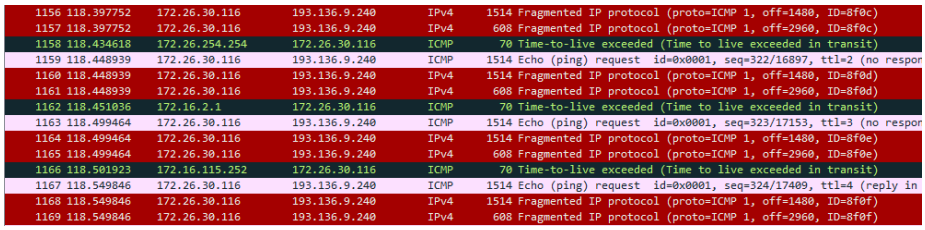


Figure 19: Pacotes ordenados

1.3.1 Alínea A

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

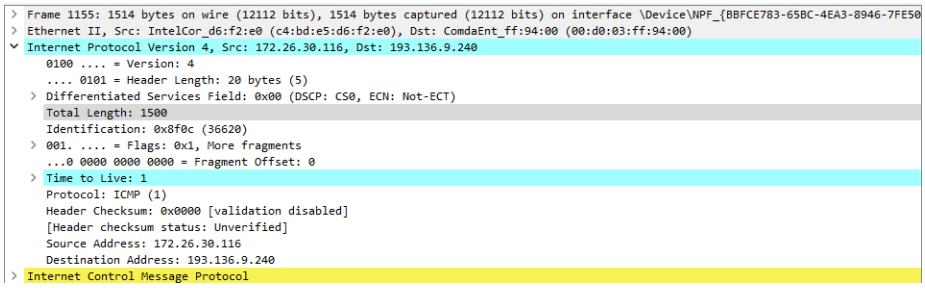


Figure 20: Fragmentação do pacote inicial

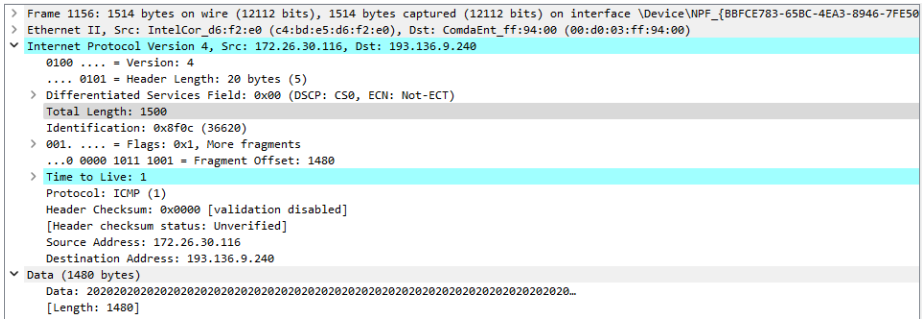


Figure 21: Fragmentação do pacote inicial

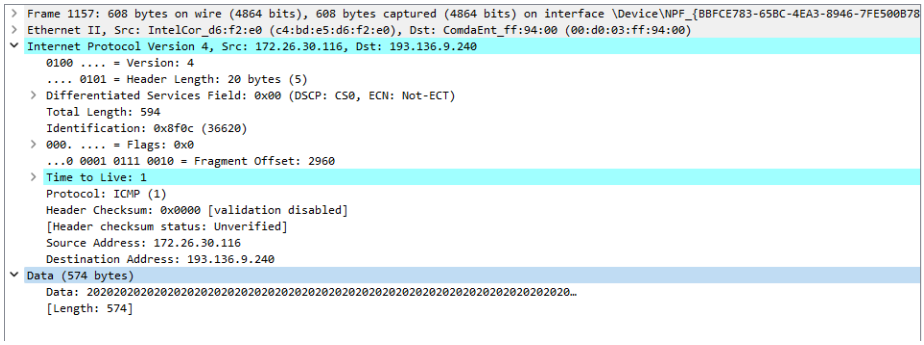


Figure 22: Fragmentação do pacote inicial

- Houve necessidade de fragmentar porque o pacote tem 3554bytes e o tamanho máximo de uma mensagem é de 1500 bytes.

1.3.2 Alínea 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?"

- Os campos de flags são utilizados para determinar se um pacote foi fragmentado ou não. Ao analisar os valores do offset de fragmento (0) e do bit "more fragments" (1, indicando a existência de mais fragmentos), podemos identificar o primeiro fragmento (figura 20). O tamanho deste datagrama IP é de 1500 bytes.

1.3.3 Alínea C

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

- Tal como foi referido anteriormente, os campos a analisar são o os valores do offset do fragmento e do more fragments, que devem ser diferente de 0 e 1, respetivamente, tal como é possível verificar na figura 21.

1.3.4 Alínea 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."

- Com base numa estimativa teórica, é esperado que o datagrama IP original seja fragmentado em três partes, sendo os dois primeiros fragmentos de 1500 bytes cada e o último fragmento de 554 bytes. No entanto, ao comparar esses valores estimados com os dados obtidos através do Wireshark, foi observado que o tamanho do último fragmento é 594 bytes, o que difere da estimativa teórica anteriormente feita.

1.3.5 Alínea E

"Como se deteta o último fragmento correspondente ao datagrama original? Estabeleça um filtro no Wireshark que permita listar o último fragmento do primeiro datagrama IP segmentado."

- O filtro usado é o ip.flags.mf == 0 && ip.frag_offset != 0. A 1ª parte (ip.flags.mf == 0) permite filtrar apenas os segmentos que não possuem mais fragmentos, enquanto que a 2ª parte filtra apenas os segmentos cujo offset é diferente de 0 (quando ocorreu fragmentação).

1.3.6 Alínea 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?"

- O datagrama é reconstruído no destino pois, caso fosse reconstruído noutro ponto, teria de ser desconstruído novamente para ser transportado até ao destino.

1.3.7 Alínea 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 são: fragment offset e More fragments. O fragment offset é inicialmente 0 e é incrementado a cada fragmento subsequente. O More Fragments é inicialmente 1 e permanece assim até ao último fragmento, onde o campo toma o valor de 0.

1.3.8 Alínea H

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

- O primeiro pacote é aquele que tem o header original, e por isso é um pacote ICMP. Os restantes possuem um header com informações sobre a fragmentação, logo não são enviados como pacotes ICMP.

1.3.9 Alínea 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?"

- O tamanho do datagrama é comparado com o tamanho máximo que um pacote pode ter para ser transmitido na rede. Neste caso é de 1500 bytes. Se este valor fosse diminuído, os datagramas poderiam ter de ser divididos num número maior de fragmentos. Caso o valor fosse maior, seriam necessários menos fragmentos para transmitir o pacote.

1.3.10 Alínea 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."

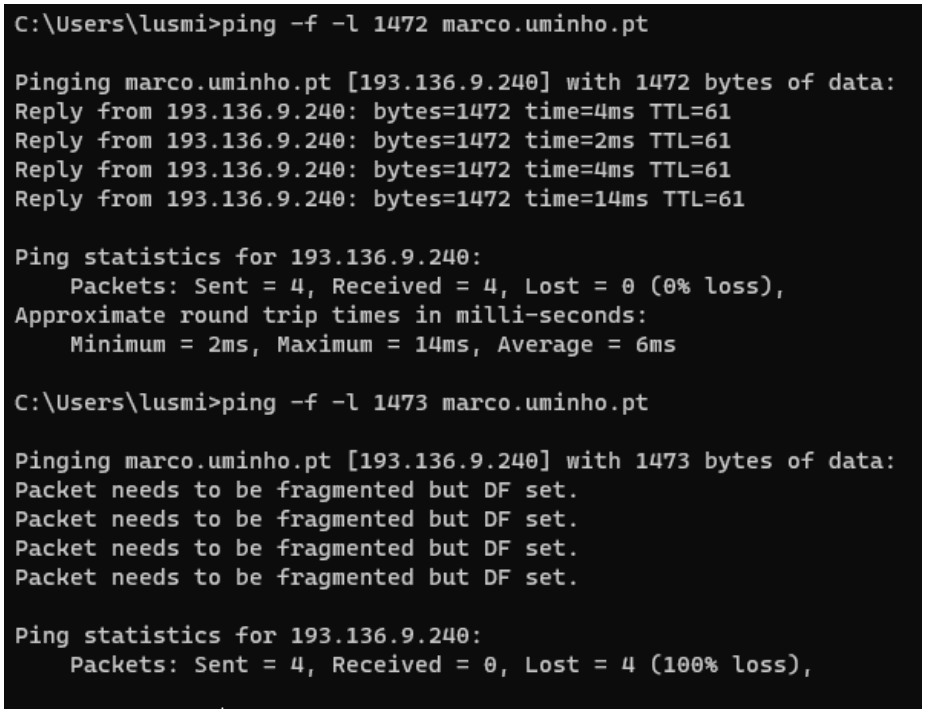


Figure 23:

- Como sabemos que o limite de tamanho que um pacote pode ter sem ser fragmentado é 1500 bytes, e sabemos que o cabeçalho ocupa 20 bytes, acreditamos que existe algum tipo de informação que ocupe 8 bytes, fazendo assim com que não seja possível enviar um pacote com 1473 bytes.

2 Segunda Parte - Resolução

"Considere a topologia da Figura 24, disponível no formato .imn via plataforma de e-learning em Conteúdo -> Material de Apoio PL."

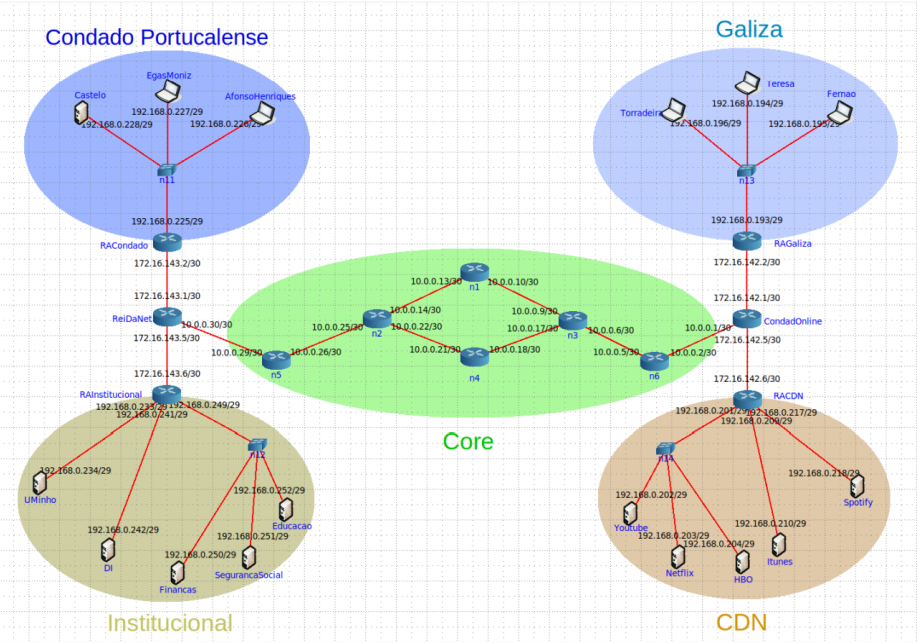


Figure 24: Topologia fornecida

"Ao longo do guião apenas irá fazer uso do endereçamento IPv4. Para facilitar a visualização, pode ocultar o endereçamento IPv6 em View -> Show -> IPv6 Addresses.

A topologia é constituída por quatro polos (Condado Portucalense, Galiza, Institucional e CDN (Content Delivery Network)).

Nos polos Condado e Galiza existe um router de acesso (que permite comunicação com o exterior) ligado a um comutador (switch), por modo a que todos os dispositivos partilhem a mesma rede local. Em cada um dos polos Institucional e CDN encontram-se três sub-redes distintas, criando-se uma segmentação dos dispositivos existentes.

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

2.1 Questão 1

"D.Afonso Henriques afirma ter problemas de comunicação com a sua mãe, D.Teresa. 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."

2.1.1 Alínea A

"Averigue, através do comando ping, que AfonsoHenriques tem efetivamente conectividade com o servidor Financas e com os servidores da CDN."

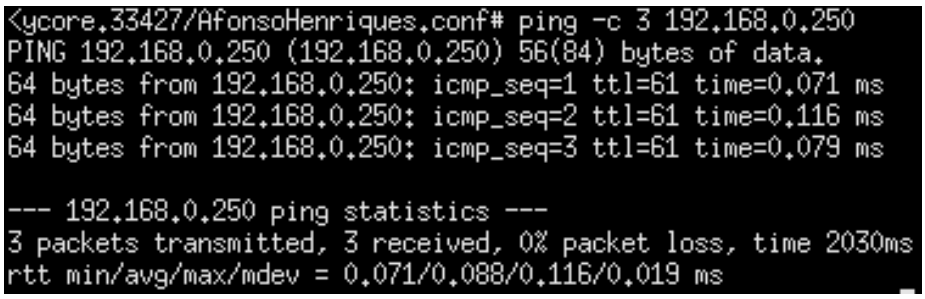


Figure 25: Servidor Financas

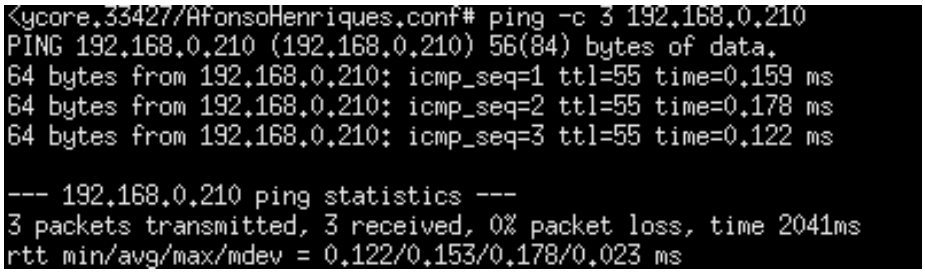


Figure 26: Servidores CDN

- Com base nas figuras 25 e 26, podemos concluir que AfonsoHenriques tem conectividade com o servidor Financas e com os servidores da CDN.

2.1.2 Alínea 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."

```
root@AfonsoHenriques:/tmp/pycore.33427/AfonsoHenriques.conf# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.0.225   0.0.0.0         UG        0 0          0 eth0
192.168.0.224   0.0.0.0         255.255.255.248 U         0 0          0 eth0
```

Figure 27: Tabela de Encaminhamento de AfonsoHenriques

```
root@Teresa:/tmp/pycore.33427/Teresa.conf# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.0.193   0.0.0.0         UG        0 0          0 eth0
192.168.0.192   0.0.0.0         255.255.255.248 U         0 0          0 eth0
```

Figure 28: Tabela de Encaminhamento de Teresa

- Ao analisar as Tabelas de Encaminhamento dos dispositivos AfonsoHenriques e Teresa utilizando o comando netstat -rn, observa-se o seguinte:

No dispositivo AfonsoHenriques:
O gateway sendo 0.0.0.0, indica que os pacotes têm como destino dispositivos dentro da mesma rede que AfonsoHenriques.
O destination sendo 0.0.0.0, indica que os pacotes são enviados para o RACondado para encaminhamento fora da rede.

No dispositivo Teresa:
O gateway sendo 0.0.0.0, indica que os pacotes têm como destino dispositivos dentro da mesma rede que Teresa.
O destination sendo 0.0.0.0, indica que os pacotes são enviados para o RAGaliza para encaminhamento fora da rede.

2.1.3 Alínea C

"Utilize o Wireshark para investigar 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.

Utilize o comando ip route add/del para adicionar as rotas necessárias ou remover rotas incorretas. Verifique a sintaxe completa do comando a usar com man ip-route ou man route. Poderá também utilizar o comando traceroute para se certificar do caminho nó a nó. Considere a alínea resolvida assim que houver tráfego a chegar ao ISP CondadOnline."

```
<ycore.46215/AfonsoHenriques.conf# traceroute -I 192.168.0.194
traceroute to 192.168.0.194 (192.168.0.194), 30 hops max, 60 byte packets
 1  192.168.0.225 (192.168.0.225)  0.054 ms  0.006 ms  0.004 ms
 2  172.16.143.1 (172.16.143.1)  0.025 ms  0.008 ms  0.007 ms
 3  10.0.0.29 (10.0.0.29)  0.016 ms !N  0.010 ms !N *
```

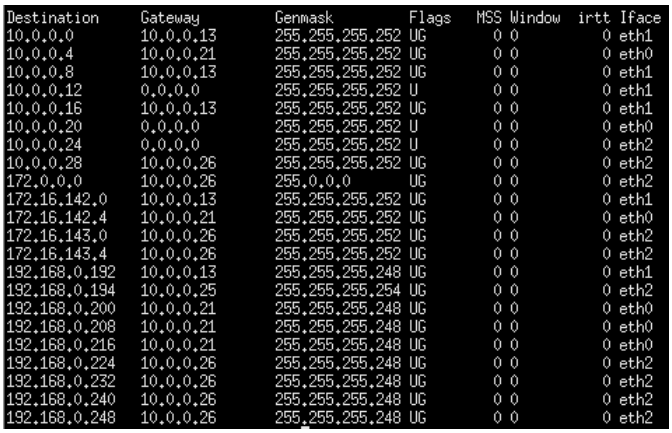
Figure 29: Traceroute AfonsoHenriques-Teresa Inicial

Ao analisar o traceroute para *Teresa* vemos que os pacotes chegam até 10.0.0.29 (n5) e não avançam mais. Assim, percebemos que não existia um reencaminhamento em n5 para permitir que os pacotes atravessem a rede em direção ao destino.

Através do comando *ip route add* adicionamos o endereço de n2 à tabela de encaminhamento de n5, permitindo assim a continuidade do tráfego dos pacotes.

```
<5/AfonsoHenriques.conf# traceroute -I 192.168.0.194
traceroute to 192.168.0.194 (192.168.0.194), 30 hops max, 60 byte packets
 1  192.168.0.225 (192.168.0.225)  0.027 ms  0.005 ms  0.005 ms
 2  172.16.143.1 (172.16.143.1)  0.014 ms  0.007 ms  0.007 ms
 3  10.0.0.29 (10.0.0.29)  0.017 ms  0.010 ms  0.010 ms
 4  10.0.0.25 (10.0.0.25)  0.040 ms  0.013 ms  0.012 ms
 5  10.0.0.25 (10.0.0.25)  3066.887 ms !H  3066.877 ms !H  3066.872 ms !H
```

Figure 30: Traceroute a passar pelo n5 e n2



Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.0.0	10.0.0.13	255.255.255.252	UG	0	0	0	eth1
10.0.0.4	10.0.0.21	255.255.255.252	UG	0	0	0	eth0
10.0.0.8	10.0.0.13	255.255.255.252	UG	0	0	0	eth1
10.0.0.12	0.0.0.0	255.255.255.252	U	0	0	0	eth1
10.0.0.16	10.0.0.13	255.255.255.252	UG	0	0	0	eth1
10.0.0.20	0.0.0.0	255.255.255.252	U	0	0	0	eth0
10.0.0.24	0.0.0.0	255.255.255.252	U	0	0	0	eth2
10.0.0.28	10.0.0.26	255.255.255.252	UG	0	0	0	eth2
172.0.0.0	10.0.0.26	255.0.0.0	UG	0	0	0	eth2
172.16.142.0	10.0.0.13	255.255.255.252	UG	0	0	0	eth1
172.16.142.4	10.0.0.21	255.255.255.252	UG	0	0	0	eth0
172.16.143.0	10.0.0.26	255.255.255.252	UG	0	0	0	eth2
172.16.143.4	10.0.0.26	255.255.255.252	UG	0	0	0	eth2
192.168.0.192	10.0.0.13	255.255.255.248	UG	0	0	0	eth1
192.168.0.194	10.0.0.25	255.255.255.254	UG	0	0	0	eth2
192.168.0.200	10.0.0.21	255.255.255.248	UG	0	0	0	eth0
192.168.0.208	10.0.0.21	255.255.255.248	UG	0	0	0	eth0
192.168.0.216	10.0.0.21	255.255.255.248	UG	0	0	0	eth0
192.168.0.224	10.0.0.26	255.255.255.248	UG	0	0	0	eth2
192.168.0.232	10.0.0.26	255.255.255.248	UG	0	0	0	eth2
192.168.0.240	10.0.0.26	255.255.255.248	UG	0	0	0	eth2
192.168.0.248	10.0.0.26	255.255.255.248	UG	0	0	0	eth2

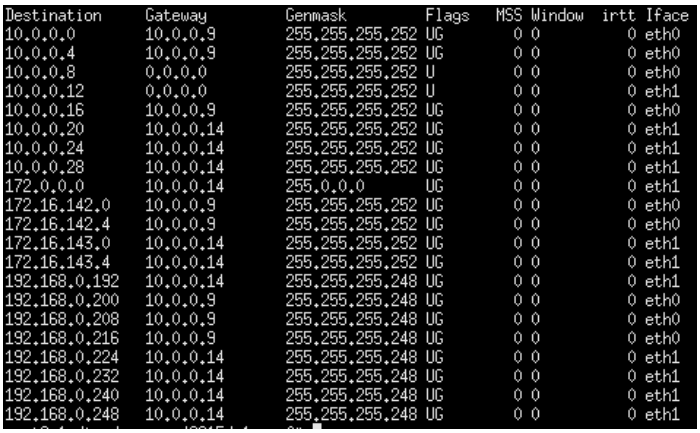
Figure 31: Tabela de Encaminhamento de n2

Como podemos observar na tabela de Encaminhamento, quando o endereço de Destino é *192.168.0.194* os pacotes são encaminhados para *10.0.0.25* que se observarmos a imagem da topologia, é o endereço do próprio n2. Para resolver este conflito utilizamos o comando *ip route del* para remover esta entrada, e de seguida o *ip route add* para que o tráfego fosse enviado para o endereço de n1.

```
traceroute to 192.168.0.194 (192.168.0.194), 30 hops max, 60 byte packets
 1  192.168.0.225 (192.168.0.225)  0.027 ms  0.006 ms  0.005 ms
 2  172.16.143.1 (172.16.143.1)  0.015 ms  0.008 ms  0.008 ms
 3  10.0.0.29 (10.0.0.29)  0.015 ms  0.009 ms  0.010 ms
 4  10.0.0.25 (10.0.0.25)  0.018 ms  0.013 ms  0.012 ms
 5  10.0.0.13 (10.0.0.13)  0.045 ms  0.016 ms  0.015 ms
 6  10.0.0.25 (10.0.0.25)  0.014 ms  0.022 ms  0.015 ms
 7  10.0.0.13 (10.0.0.13)  0.017 ms  0.017 ms  0.016 ms
```

Figure 32: Traceroute a passar pelo n1

Como podemos observar aqui o tráfego volta a passar por n2 depois de n1, o que gera um loop e não um caminho eficiente, pelo que removemos a entrada com destino *192.168.0.192* da tabela de Encaminhamento seguinte, e adicionando em seguida uma entrada com o mesmo destino mas com Gateway para n3.



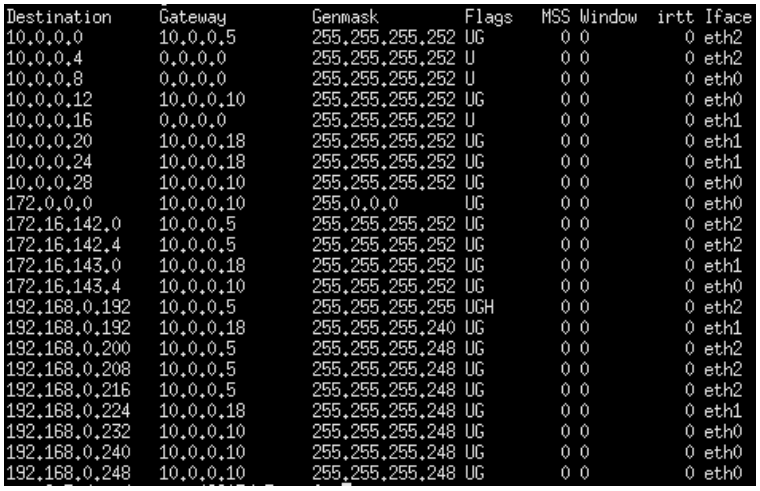
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.0.0	10.0.0.9	255.255.255.252	UG	0	0	0	eth0
10.0.0.4	10.0.0.9	255.255.255.252	UG	0	0	0	eth0
10.0.0.8	0.0.0.0	255.255.255.252	U	0	0	0	eth0
10.0.0.12	0.0.0.0	255.255.255.252	U	0	0	0	eth1
10.0.0.16	10.0.0.9	255.255.255.252	UG	0	0	0	eth0
10.0.0.20	10.0.0.14	255.255.255.252	UG	0	0	0	eth1
10.0.0.24	10.0.0.14	255.255.255.252	UG	0	0	0	eth1
10.0.0.28	10.0.0.14	255.255.255.252	UG	0	0	0	eth1
172.0.0.0	10.0.0.14	255.0.0.0	UG	0	0	0	eth1
172.16.142.0	10.0.0.9	255.255.255.252	UG	0	0	0	eth0
172.16.142.4	10.0.0.9	255.255.255.252	UG	0	0	0	eth0
172.16.143.0	10.0.0.14	255.255.255.252	UG	0	0	0	eth1
172.16.143.4	10.0.0.14	255.255.255.252	UG	0	0	0	eth1
192.168.0.192	10.0.0.14	255.255.255.248	UG	0	0	0	eth1
192.168.0.200	10.0.0.9	255.255.255.248	UG	0	0	0	eth0
192.168.0.208	10.0.0.9	255.255.255.248	UG	0	0	0	eth0
192.168.0.216	10.0.0.9	255.255.255.248	UG	0	0	0	eth0
192.168.0.224	10.0.0.14	255.255.255.248	UG	0	0	0	eth1
192.168.0.232	10.0.0.14	255.255.255.248	UG	0	0	0	eth1
192.168.0.240	10.0.0.14	255.255.255.248	UG	0	0	0	eth1
192.168.0.248	10.0.0.14	255.255.255.248	UG	0	0	0	eth1

Figure 33: Tabela de Encaminhamento de n1

```
traceroute to 192.168.0.194 (192.168.0.194), 30 hops max, 60 byte packets
 1  192.168.0.225 (192.168.0.225)  0.026 ms  0.005 ms  0.005 ms
 2  172.16.143.1 (172.16.143.1)  0.014 ms  0.008 ms  0.007 ms
 3  10.0.0.29 (10.0.0.29)  0.016 ms  0.010 ms  0.009 ms
 4  10.0.0.25 (10.0.0.25)  0.018 ms  0.012 ms  0.012 ms
 5  10.0.0.13 (10.0.0.13)  0.022 ms  0.016 ms  0.015 ms
 6  10.0.0.17 (10.0.0.17)  0.030 ms !N  0.028 ms !N *
```

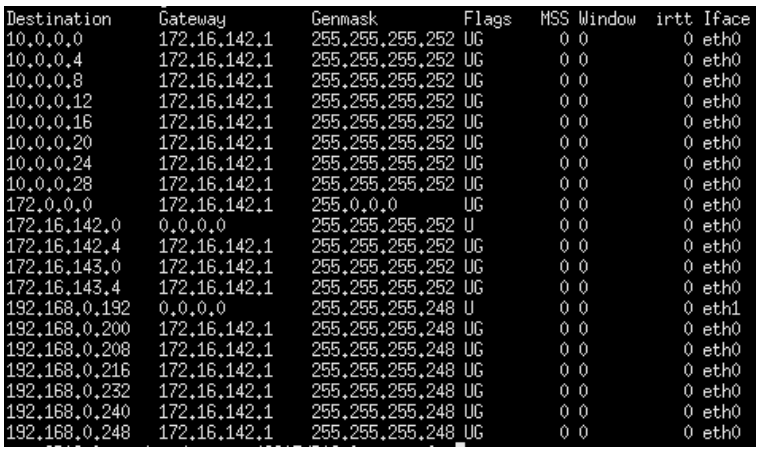
Figure 34: Traceroute até n3

Mais uma vez, podemos observar pelo Traceroute que os pacotes são enviados para n3, porém ao observar a sua Tabela de Encaminhamento percebemos que existe uma entrada para *192.168.0.192/28* que envia o tráfego para *10.0.0.18* (n4), o que possibilitaria a criação de um loop, pelo que o removemos com o comando *ip route del*.



Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.0.0	10.0.0.5	255.255.255.252	UG	0	0	0	eth2
10.0.0.4	0.0.0.0	255.255.255.252	U	0	0	0	eth2
10.0.0.8	0.0.0.0	255.255.255.252	U	0	0	0	eth0
10.0.0.12	10.0.0.10	255.255.255.252	UG	0	0	0	eth0
10.0.0.16	0.0.0.0	255.255.255.252	U	0	0	0	eth1
10.0.0.20	10.0.0.18	255.255.255.252	UG	0	0	0	eth1
10.0.0.24	10.0.0.18	255.255.255.252	UG	0	0	0	eth1
10.0.0.28	10.0.0.10	255.255.255.252	UG	0	0	0	eth0
172.0.0.0	10.0.0.10	255.0.0.0	UG	0	0	0	eth0
172.16.142.0	10.0.0.5	255.255.255.252	UG	0	0	0	eth2
172.16.142.4	10.0.0.5	255.255.255.252	UG	0	0	0	eth2
172.16.143.0	10.0.0.18	255.255.255.252	UG	0	0	0	eth1
172.16.143.4	10.0.0.10	255.255.255.252	UG	0	0	0	eth0
192.168.0.192	10.0.0.5	255.255.255.255	UGH	0	0	0	eth2
192.168.0.192	10.0.0.18	255.255.255.240	UG	0	0	0	eth1
192.168.0.200	10.0.0.5	255.255.255.248	UG	0	0	0	eth2
192.168.0.208	10.0.0.5	255.255.255.248	UG	0	0	0	eth2
192.168.0.216	10.0.0.5	255.255.255.248	UG	0	0	0	eth2
192.168.0.224	10.0.0.18	255.255.255.248	UG	0	0	0	eth1
192.168.0.232	10.0.0.10	255.255.255.248	UG	0	0	0	eth0
192.168.0.240	10.0.0.10	255.255.255.248	UG	0	0	0	eth0
192.168.0.248	10.0.0.10	255.255.255.248	UG	0	0	0	eth0

Figure 35: Tabela de Encaminhamento de n3



Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.0.0	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
10.0.0.4	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
10.0.0.8	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
10.0.0.12	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
10.0.0.16	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
10.0.0.20	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
10.0.0.24	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
10.0.0.28	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
172.0.0.0	172.16.142.1	255.0.0.0	UG	0	0	0	eth0
172.16.142.0	0.0.0.0	255.255.255.252	U	0	0	0	eth0
172.16.142.4	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
172.16.143.0	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
172.16.143.4	172.16.142.1	255.255.255.252	UG	0	0	0	eth0
192.168.0.192	0.0.0.0	255.255.255.248	U	0	0	0	eth1
192.168.0.200	172.16.142.1	255.255.255.248	UG	0	0	0	eth0
192.168.0.208	172.16.142.1	255.255.255.248	UG	0	0	0	eth0
192.168.0.216	172.16.142.1	255.255.255.248	UG	0	0	0	eth0
192.168.0.232	172.16.142.1	255.255.255.248	UG	0	0	0	eth0
192.168.0.240	172.16.142.1	255.255.255.248	UG	0	0	0	eth0
192.168.0.248	172.16.142.1	255.255.255.248	UG	0	0	0	eth0

Figure 36: Tabela de Encaminhamento RAGaliza

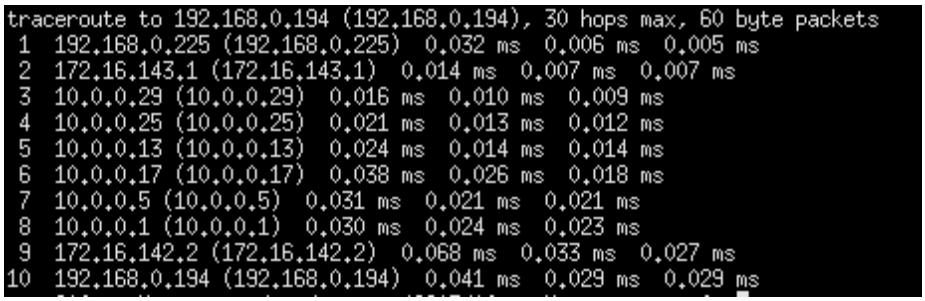


Figure 37: Traceroute Completo

Depois de estabelecer as rotas entre todos os nós é possível verificar que o traceroute permite chegar a *Teresa* a partir de *AfonsoHenriques*.

2.1.4 Alínea 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. "

"**i.** 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."

```
root@AfonsoHenriques:/tmp/pycore.46215/AfonsoHenriques.conf# ping 192.168.0.194
PING 192.168.0.194 (192.168.0.194) 56(84) bytes of data.
64 bytes from 192.168.0.194: icmp_seq=1 ttl=55 time=0.129 ms
64 bytes from 192.168.0.194: icmp_seq=2 ttl=55 time=0.220 ms
64 bytes from 192.168.0.194: icmp_seq=3 ttl=55 time=0.213 ms
64 bytes from 192.168.0.194: icmp_seq=4 ttl=55 time=0.306 ms
64 bytes from 192.168.0.194: icmp_seq=5 ttl=55 time=0.141 ms
64 bytes from 192.168.0.194: icmp_seq=6 ttl=55 time=0.498 ms
64 bytes from 192.168.0.194: icmp_seq=7 ttl=55 time=0.089 ms
64 bytes from 192.168.0.194: icmp_seq=8 ttl=55 time=0.292 ms
64 bytes from 192.168.0.194: icmp_seq=9 ttl=55 time=0.204 ms
64 bytes from 192.168.0.194: icmp_seq=10 ttl=55 time=0.215 ms
64 bytes from 192.168.0.194: icmp_seq=11 ttl=55 time=0.206 ms
64 bytes from 192.168.0.194: icmp_seq=12 ttl=55 time=0.210 ms
64 bytes from 192.168.0.194: icmp_seq=13 ttl=55 time=0.197 ms
```

Figure 38:

- Como obtemos um reply do ping entao os dispositivos estao conectados.

"**ii.** 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?"

```
traceroute to 192.168.0.226 (192.168.0.226), 30 hops max, 60 byte packets
 1  192.168.0.193 (192.168.0.193)  0.029 ms  0.006 ms  0.005 ms
 2  172.16.142.1 (172.16.142.1)  0.016 ms  0.007 ms  0.007 ms
 3  10.0.0.2 (10.0.0.2)  0.018 ms  0.052 ms  0.015 ms
 4  10.0.0.6 (10.0.0.6)  0.020 ms  0.012 ms  0.012 ms
 5  10.0.0.18 (10.0.0.18)  0.023 ms  0.016 ms  0.016 ms
 6  10.0.0.14 (10.0.0.14)  0.027 ms  0.036 ms  0.020 ms
 7  10.0.0.26 (10.0.0.26)  0.029 ms  0.022 ms  0.022 ms
 8  10.0.0.30 (10.0.0.30)  0.029 ms  0.025 ms  0.024 ms
 9  172.16.143.2 (172.16.143.2)  0.033 ms  0.028 ms  0.027 ms
10  192.168.0.226 (192.168.0.226)  0.035 ms  0.030 ms  0.029 ms
```

Figure 39: Traceroute Teresa-AfonsoHenriques

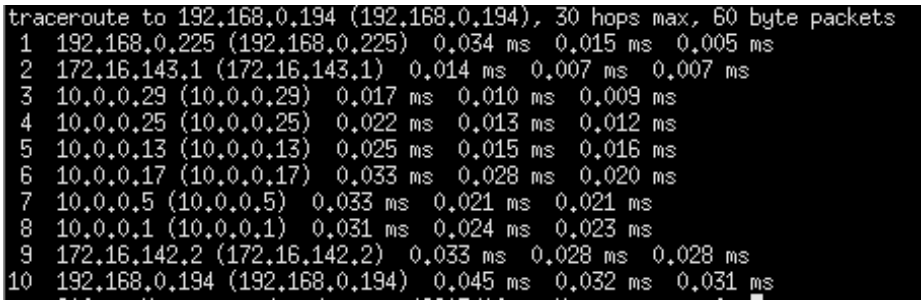


Figure 40: Traceroute AfonsoHenriques-Teresa

-

2.1.5 Alínea E

"Estando restabelecida a conectividade entre os dois hosts, obtenha a tabela de encaminhamento de n3 e foque-se na seguinte entrada:

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."

-

2.1.6 Alínea F

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

-

2.1.7 Alínea G

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

-

2.2 Questão 2

"Tendo feito as pazes com a mãe, D. Afonso Henriques vê-se com algum tempo livre e decide fazer remodelações no condado:"

2.2.1 Alínea A

"Não estando satisfeito com a decoração do Castelo, opta por eliminar a sua rota default.

Adicione as rotas necessárias para que o Castelo continue a ter acesso a cada um dos três polos. Mostre que a conectividade é restabelecida, assim como a tabela de encaminhamento resultante. Explicite ainda a utilidade de uma rota default."

```
root@Castelo:/tmp/pycore.46215/Castelo.conf# ip route del default
root@Castelo:/tmp/pycore.46215/Castelo.conf# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.224   0.0.0.0         255.255.255.248 U         0 0          0 eth0
```

Figure 41: Tabela de Encaminhamento após eliminar a rota default

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.192   192.168.0.225   255.255.255.248 UG        0 0          0 eth0
192.168.0.200   192.168.0.225   255.255.255.248 UG        0 0          0 eth0
192.168.0.208   192.168.0.225   255.255.255.248 UG        0 0          0 eth0
192.168.0.216   192.168.0.225   255.255.255.248 UG        0 0          0 eth0
192.168.0.224   0.0.0.0         255.255.255.248 U         0 0          0 eth0
192.168.0.232   192.168.0.225   255.255.255.248 UG        0 0          0 eth0
192.168.0.240   192.168.0.225   255.255.255.248 UG        0 0          0 eth0
192.168.0.248   192.168.0.225   255.255.255.248 UG        0 0          0 eth0
```

Figure 42: Tabela de Encaminhamento Final

-

2.2.2 Alínea B

"Por modo a garantir uma posição estrategicamente mais vantajosa e ter casa de férias para relaxar entre batalhas, ordena também a construção de um segundo Castelo, em Braga. Não tendo qualquer queixa do serviço prestado, recorre novamente aos serviços do ISP ReiDaNet para ter acesso à rede no segundo Castelo. O ISP atribuiu-lhe o endereço de rede IP 172.16.XX.128/26 em que XX corresponde ao seu número de grupo (PLXX). Defina um esquema de endereçamento que permita o estabelecimento de pelo menos 3 redes e que garanta que cada uma destas possa ter 10 ou mais hosts. Assuma que todos os endereços de sub-redes são utilizáveis."

-

2.2.3 Alínea C

"Ligue um novo host 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 diferentes polos.

Existe algum host com o qual não seja possível comunicar? Porquê?"

-

2.3 Questão 3

"Ao planear um novo ataque, D. Afonso Henriques constata que o seu exército não só perde bastante tempo a decidir que direção tomar a cada salto como, por vezes, inclusivamente se perde."

2.3.1 Alínea 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."

-

2.3.2 Alínea B

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

-

2.3.3 Alínea C

"Comente os aspetos positivos e negativos do uso do Supernetting."

-