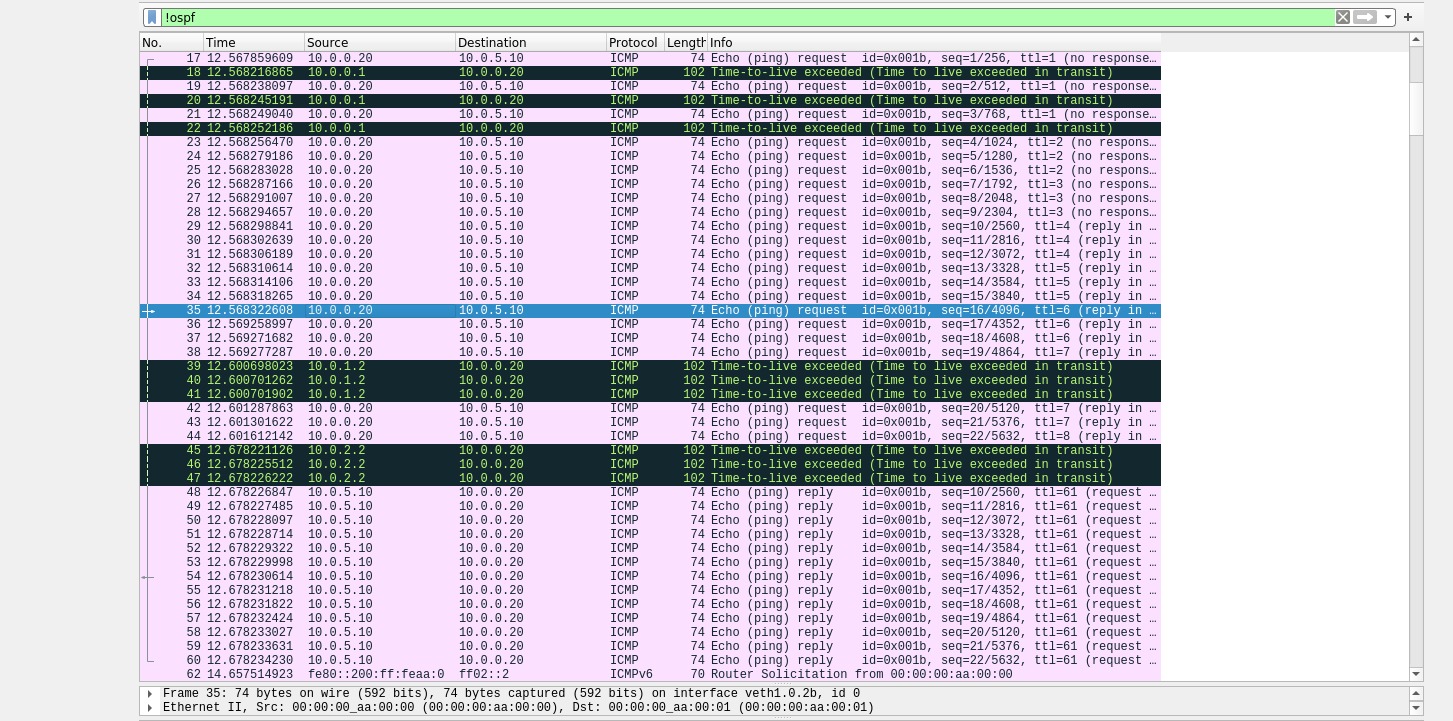
1.

1. **Active 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**

R: Analisando os resultados obtidos depois de inserir o código “traceroute -I “com o respetivo IP do servidor designado por Found, observamos que dentro do grupo que o trajeto optado durante o percurso foi diferente bem como os respetivos tempos.

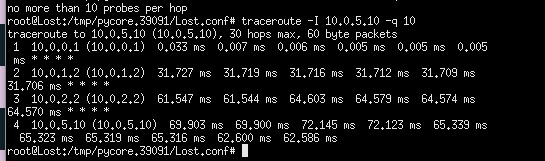
Verificando o IP do host, Found, e os dos routers concluímos que foram feitos os 4 saltos e foi possível chegar ao destino final

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

R:O valor mínimo de TTL para alcançar o servidor “Found” terá de ser 4. Através da ferramenta Wireshark, conseguimos observar que apenas obtemos resposta ao nosso “ping” quando o TTL é maior ou igual a 4. De facto, ao analisar a rede, facilmente concluímos que os caminhos mais curtos são de 4 saltos, sendo estes os caminhos: Lost->RA1->RC1->RA2->Found e Lost->RA1->RC2->RA2->Found.

1. **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.**

R:Após realizar o comando “traceroute -I 10.0.5.10 -q 10“, chegamos aos seguintes valores:

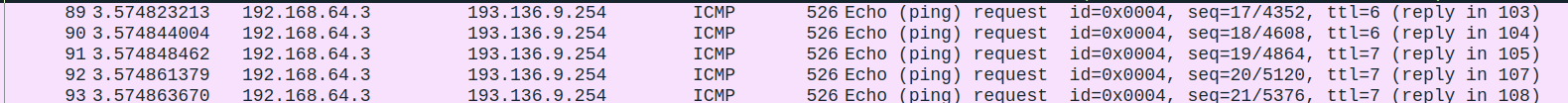


Estes valores correspondem a 10 sondas enviadas que nos permitem concluir que o RTT médio é de 67.0554 ms. De forma a justificar o RTT obtido, considerando que o tamanho dos pacotes (L) é igual a 74 bytes, e que a taxa de bits (R) é de 100 Mb/s, conseguimos concluir que o tempo de transmissão é equivalente a 5.92 \*10^-6 ms. Para além disso, com base nos dados da questão, sabemos que o tempo de propagação irá ser equivalente ao delay (15 ms) multiplicado pelos dois routers por onde o pacote passa, chegando a 30 ms de tempo de propagação. Uma vez que o valor estimado é equivalente a 67.0554 ms e que não há processamento de pacote (tempo de processamento igual a 0), aplicando a equação do atraso da comunicação de pacotes, podemos concluir que o tempo de fila de espera é igual 37.05539 ms.

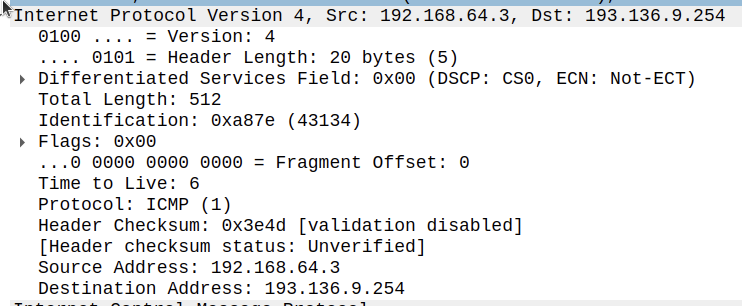
1. **O valor médio do atraso num sentido (One-Way Delay) poderia ser calculado com precisão dividindo o RTT por dois? O que torna difícil o cálculo desta métrica numa rede real?**

R: O One-Way Delay não é medido com precisão dividindo o RTT por dois, visto que o RTT inclui o tempo que a resposta demora a ser processada e transmitida, o que por sua vez, mesmo sendo apenas metade, não faz parte do atraso num só sentido. No caso de uma rede real, ainda é mais difícil de determinar, pois existem mais variáveis que podem tornar mais complicada a medição. Alguns destes obstáculos são: O tamanho dos pacotes, que pode ser variado, o delay entre routers que pode não ser ambíguo e também a possível falta de conhecimento do tempo de “queueing”,”processamento” e de “transmissão”.

**2- a) Qual é o endereço IP da interface ativa do seu computador?**

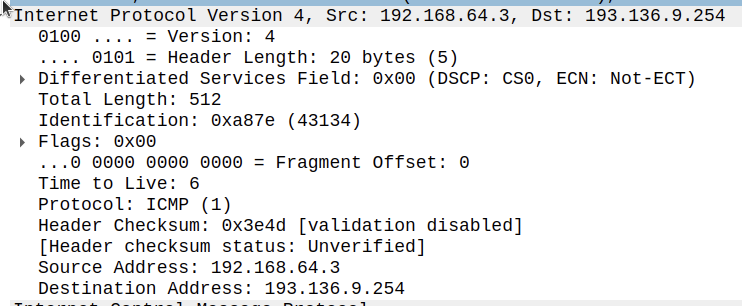
****

R: O endereço IP da interface ativa da nossa máquina é 192.168.64.3

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

R: O valor do campo protocolo é ICMP (1). Este tem como propósito identificar o protocolo utilizado em um pacote de dados ip.

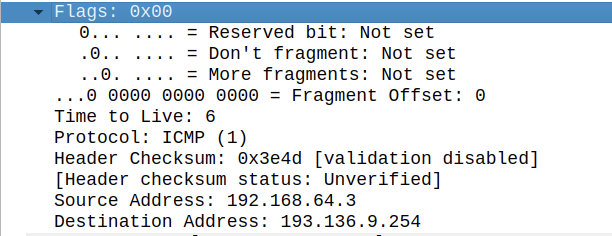
**c)** **Quantos bytes tem o cabeçalho IPv4? Quantos bytes tem o campo de dados (payload) do datagrama? Como se calcula o tamanho do payload?**

****



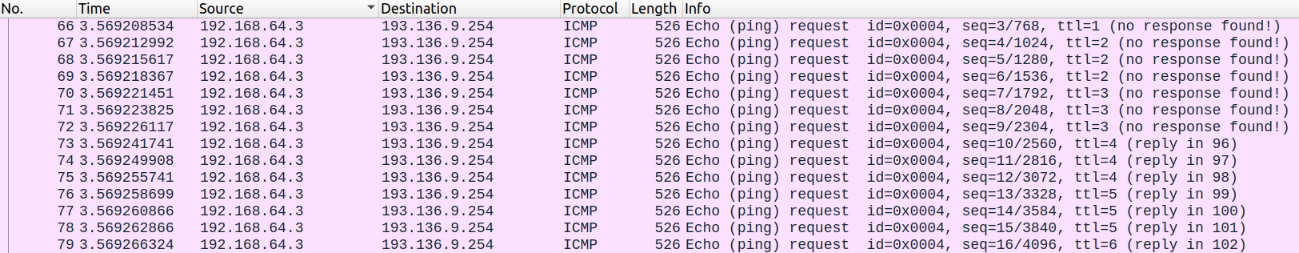
R:O cabeçalho possui 20 bytes (rodeado na imagem a vermelho). Para calcular a dimensão em bytes do campo de dados “payload”, precisamos de fazer a diferença entre a dimensão total do pacote (rodeado a azul), com o cabeçalho. Esta equação resulta no valor 492 bytes de “payload”.

1. **O datagrama IP foi fragmentado? Justifique.**

****

R: Como podemos ver pela imagem supramencionada, os valores das flags e do “Offset” apresentam um valor nulo o que comprova que o datagrama IP não foi fragmentado.

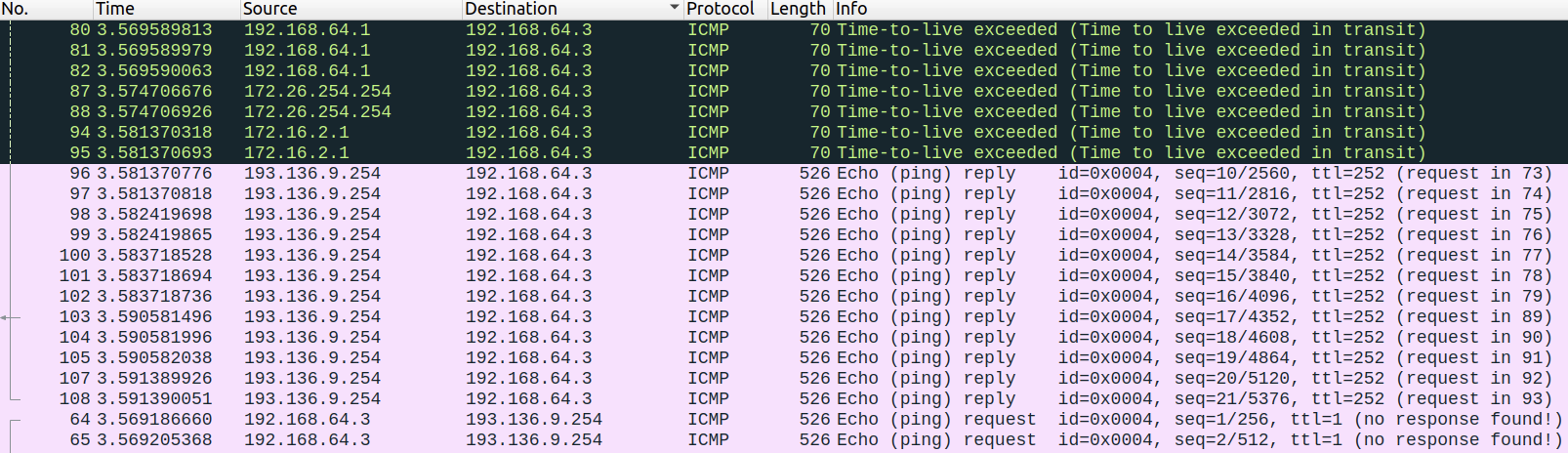
1. **Ordene os pacotes capturados de acordo com o endereço IP fonte e analise a sequência de tráfego ICMP gerado a partir do endereço IP atribuído à interface da sua máquina. Para a sequência de mensagens ICMP enviadas pelo seu computador, indique que campos do cabeçalho IP variam de pacote para pacote.**

****

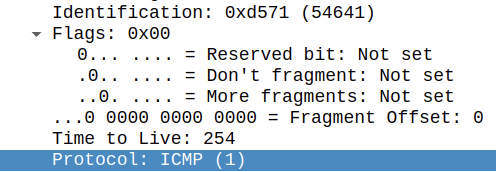
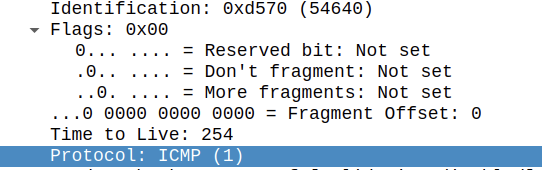
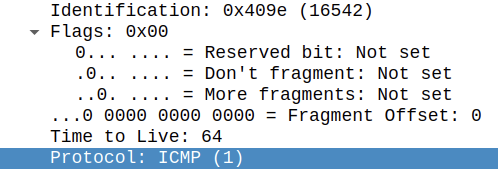
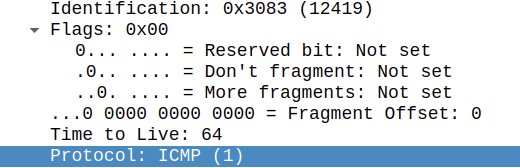
Analisando a imagem em cima é possível identificar que os únicos campos que variam ao longo dos pacotes é o “Time” ,o “Length” e o “info”. Desta forma, podemos concluir que a parte que altera no cabeçalho são os bits que fornecem informação relativa ao tamanho do pacote e sobre o TTL.

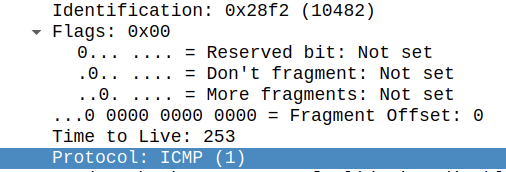
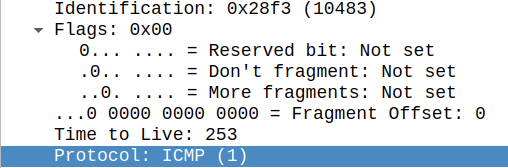
1. **Observa algum padrão nos valores do campo de Identificação do datagrama IP e TTL?**

R: Utilizando os dados da imagem na alínea anterior vemos que o valor do campo de identificação do datagrama IP é incrementado uma unidade a cada pacote tal como o TTL.

1. **Ordene o tráfego capturado por endereço destino e encontre a série de respostas ICMP TTL Exceeded enviadas ao seu computador.**
2. ** 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?**

****

****

****

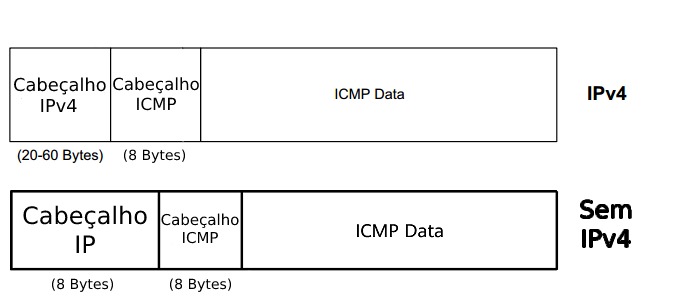
Nota: *Para cada linha foi realizado um print onde é apenas alterado o valor da identificação*

R: Pelas imagens anteriores podemos comprovar que o valor do campo TTL(Time to Live) permanece sempre constante, com valor igual a 1, o que significa que o mesmo pode apenas alcançar o próximo dispositivo de rede e não pode ser encaminhado para outros dispositivos

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

**As mensagens ICMP TTL Exceeded**

R: Para as mensagens de resposta “ICMP TTL Exceeded” são enviadas na origem com um valor TTL significativamente alto de forma a assegurar que estas mensagens não sejam descartadas antes de chegarem ao destino, o que impossibilitava à origem de saber se o pacote alcançou o destino final.

1. **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?**

*Estrutura ICMP com e sem IPv4*

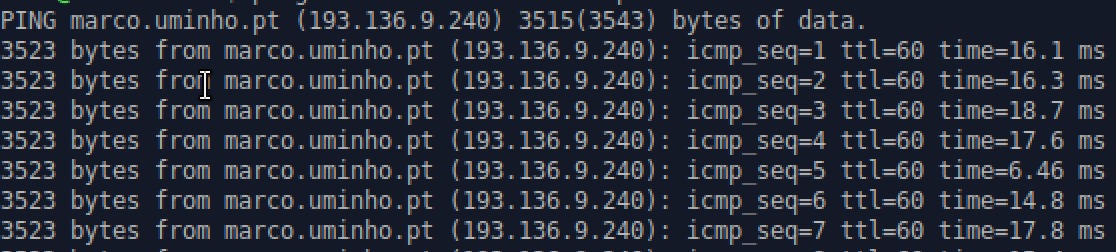
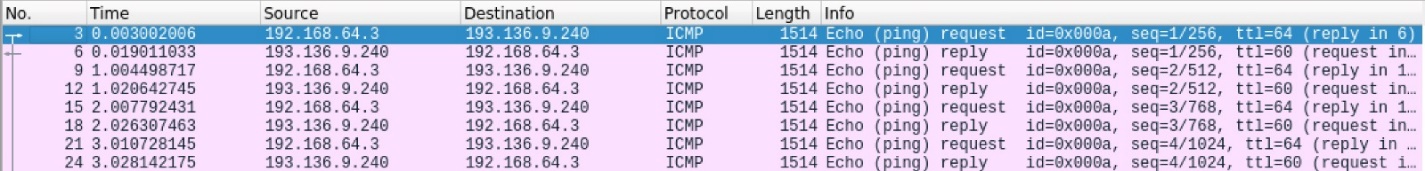
R:O ICMP e o IPv4 são ambos protocolos utilizados na rede. O ICMP é utilizado para fornecer um *feedback* sobre a comunicação de rede, mais concretamente, para comunicar mensagens de erro e diagnóstico. Em comparação com os outros protocolos IPv4, o ICMP possui um cabeçalho fixo de 8 bytes e, de forma diferente, os outros cabeçalhos possuem um cabeçalho de 20 ou mais bytes.

A integração do ICMP ao cabeçalho IPv4 é vantajosa, na medida em que o ICMP é objetivado para ser transportado dentro do cabeçalho IP, em conjunto com os dados do pacote IP. Tal, fornece um mecanismo de envio de mensagens de controlo de erro de rede entre dispositivos como é o caso dos roteadores e “hosts”. Para além disso, permite também que a rede forneça uma camada de controle e gerenciamento que auxilia os pacotes garantindo que os mesmos são entregues corretamente e de forma eficiente.

No entanto, existem também desvantagens em colocar o ICMP no cabeçalho IPv4. Estes inconvenientes correspondem ao aumento do tamanho dos pacotes e do tráfego de rede, à possibilidade de ataques de negação de serviço e problemas de segurança.

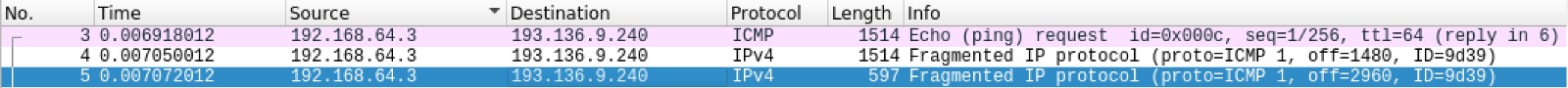
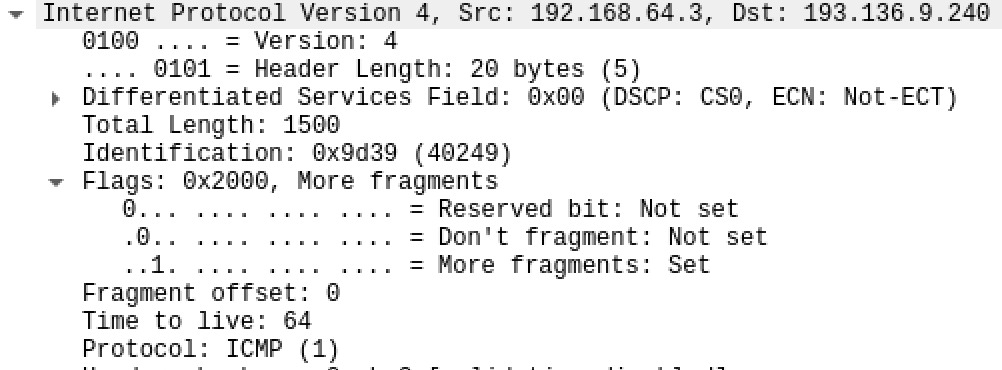
De forma geral, as mensagens ficariam mais longas, o que tornaria necessário uma maior fragmentação dos pacotes, em contrapartida, haveria um maior controlo e velocidade a nível da entrega de pacotes.

3-

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

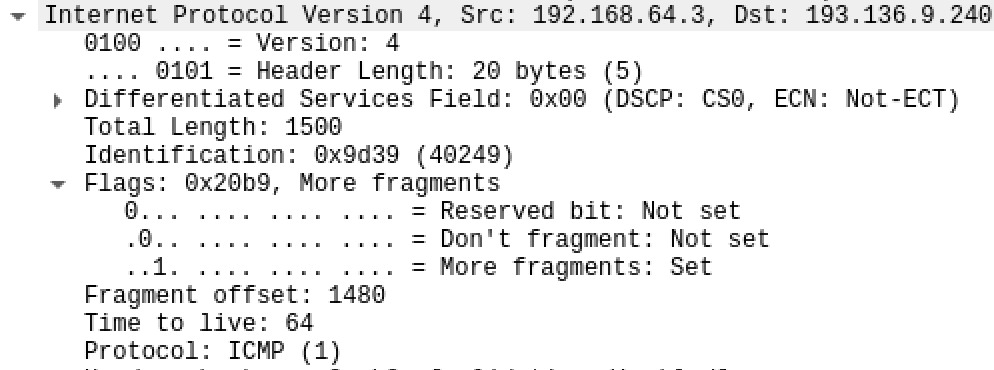
*Primeira mensagem no Wireshark*

R: Após localizar a primeira mensagem ICMP, uma vez que a mensagem inicial possuía 3515 bytes de dados, é necessário que haja fragmentação, pois o tamanho de cada mensagem individual não pode exceder os 1500 bytes incluindo o cabeçalho.

1. **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?**

*Primeiro fragmento do datagrama ip*

R: No cabeçalho do primeiro fragmento, a existência da flag com valor um correspondente ao valor “More fragments” indicia a existência de pelo menos mais um fragmento daquele pacote. No cabeçalho como o “Offset” equivale a 0, sabemos que se trata do primeiro fragmento. O tamanho do pacote é igual a 1500 bytes que corresponde ao tamanho máximo que pode ser transmitido (com apenas 1480 bytes de dados).

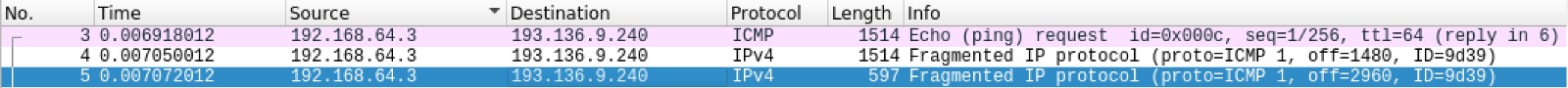
1. **Imprima o segundo fragmento do datagrama IP original. Que informação do cabeçalho IP indica que não se trata do 1º fragmento? Existem mais fragmentos? O que nos permite afirmar isso?**

*Segundo fragmento do datagrama ip*

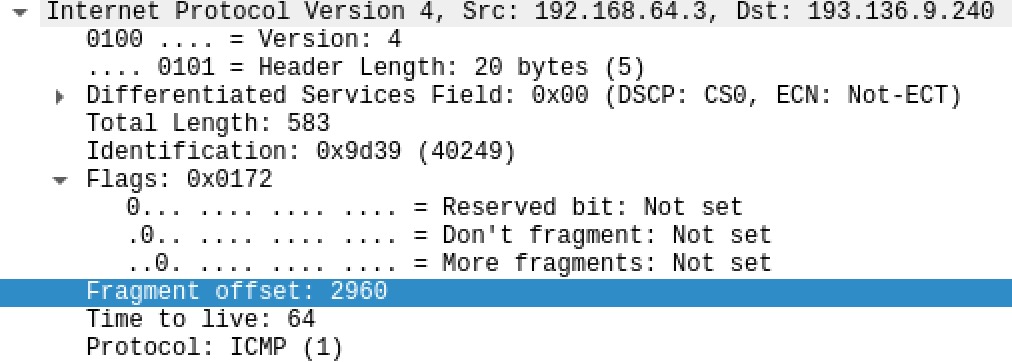
R: Uma vez que o “Offset” é diferente de 0, sabemos que houve fragmentação. Como a flag “More fragments” é igual a 1, sabemos que vai haver pelo menos mais uma fragmentação.

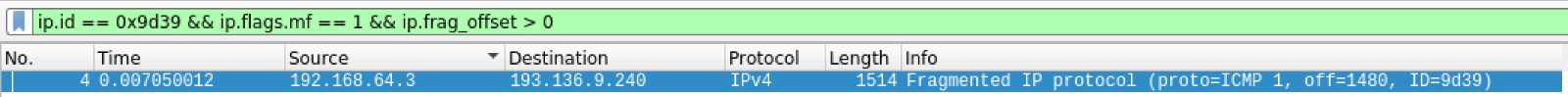
1. **Estime teoricamente o número de fragmentos gerados a partir do datagrama IP original e o número de bytes transportados no último fragmento desse datagrama. Compare os dois valores estimados com os obtidos através do wireshark.**

R:

**** Uma vez que o número de fragmentos tem de ser obrigatoriamente inteiro, o N é igual a 3.

Na seguinte imagem, é possível observar os 3 fragmentos teóricos no programa Wireshark.

1. **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.**



R: Quando o “Offset” é maior do que zero (o que indicia fragmentação passada), e quando a flag “More fragments” é também 0 (o que indica que não vai ocorrer mais fragmentação), sabemos que estamos perante o último fragmento.

1. **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?**

R: f. A reconstrução do datagrama IP original é feita no equipamento recetor (Found). Apesar disto, o equipamento recetor não é o único lugar aonde a reconstrução pode acontecer, se todos os fragmentos pertencentes a um datagrama forem recebidos por um dispositivo intermediário ele próprio pode reconstruir o datagrama, só necessita de ter acesso a todos os fragmentos.

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

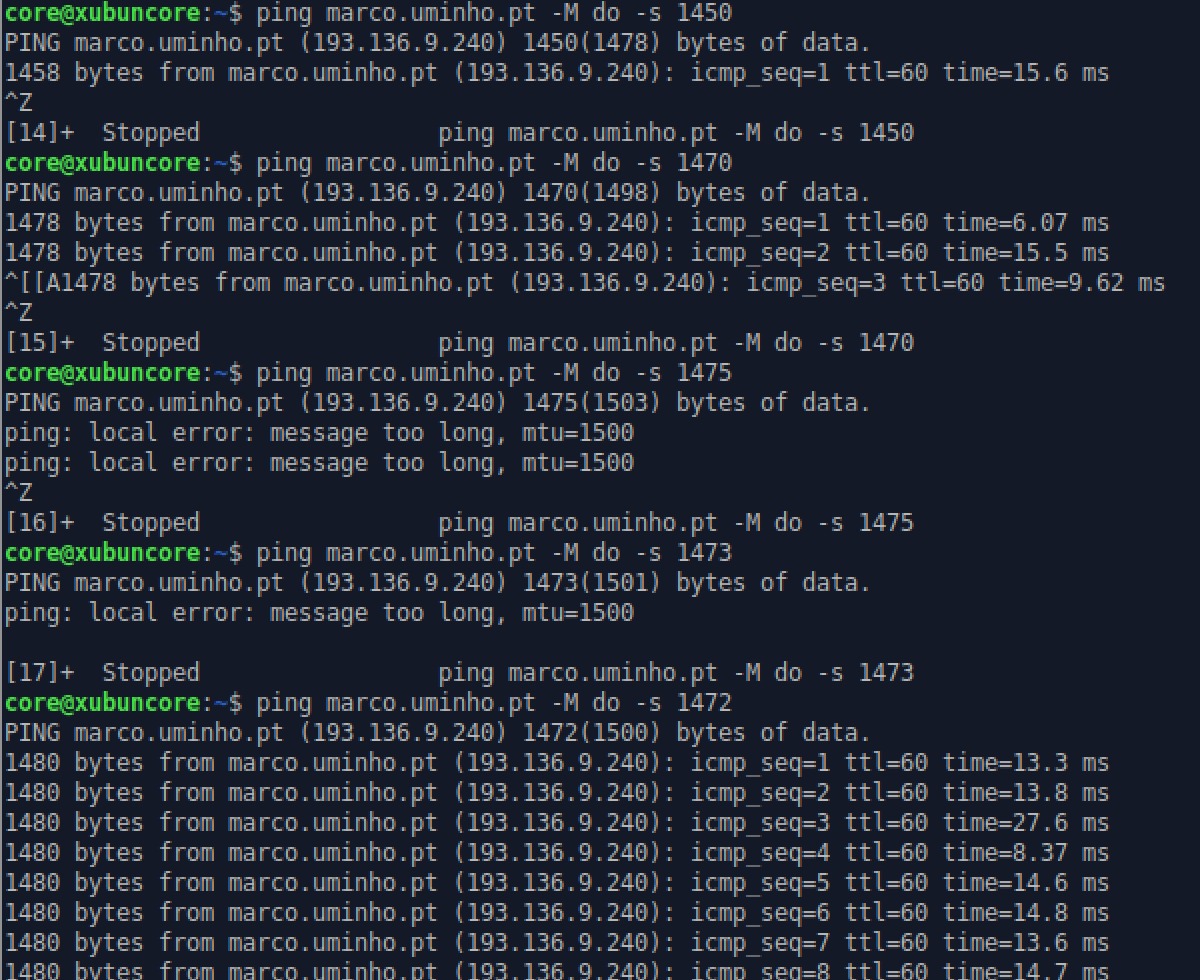
R: Os campos do cabeçalho IP que vão variando entre os fragmentos é o das Flags “Offset” e “More Fragments”. O valor da Flag “Offset” organiza os fragmentos por ordem, já o valor da Flag “More Fragments” apenas indica se existem mais fragmentos. É a partir dos valores da Flag “Offset” que é possível reconstruir o datagrama original.

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

R: O motivo pelo qual apenas o primeiro fragmento de cada pacote é identificado como sendo um pacote ICMP tem a ver com o facto de que este é o único com informações suficientes para identificar o protocolo que está sendo usado para encapsular os dados, incluindo se é um pacote ICMP ou não

1. **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?**

R: Para que seja possível saber se há fragmentação ou não, o valor do tamanho do datagrama é comparado ao tamanho máximo de pacote que pode ser transmitido. Subtraindo ao conjunto de dados o resultado da subtração do tamanho do máximo a transmitir menos o tamanho do cabeçalho, repetindo as vezes necessárias até que o conjunto de dados seja inferior ao valor a subtrair.

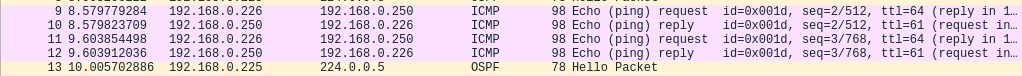
1. **Sabendo que no comando ping a opção -f (Windows), -M do (Linux) ou –D (Mac) ativa a flag “Don’t Fragment” (DF) no cabeçalho do IPv4, usando ping SIZE marco.uminho.pt, (opção pkt\_size = –l (Windows) ou –s (Linux, Mac), determine o valor máximo de SIZE sem que ocorra fragmentação do pacote? Justifique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

R: O valor máximo de dados que podem ser enviados num só um pacote é ditado pela “MTU” (Maximum transmission unit). Desta forma, quando pensamos nos dados que queremos enviar de uma vez, temos que ter em consideração que o limite de 1500 bytes não pode ser ultrapasso pela junção do cabeçalho mais os dados. Na imagem em cima, conseguimos observar que, por tentativa e erro, o valor máximo de dados que pode ser enviado é de 1472.

2ºParte

**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.**

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



R: Através desta figura, podemos observar que um pacote com origem no ip

“192.168.0.226” (AfonsoHenriques) e destino em “192.168.0.250”(Financas) chega ao destino e recebe uma resposta com a origem e destino invertidos.

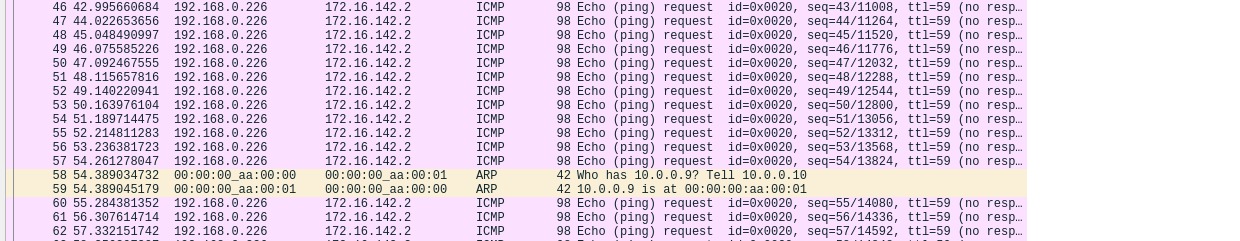
**b) Recorrendo ao comando netstat -rn, analise as tabelas de encaminhamento dos dispositivos AfonsoHenriques e Teresa. Existe algum problema com as suas entradas? Identifique e descreva a utilidade de cada uma das entradas destes dois hosts**

R: Observando as tabelas de encaminhamento, sendo a primeira do dispositivo AfosnoHenriques e a segunda do dispositivo Teresa, encontramos duas situações bastante semelhantes.

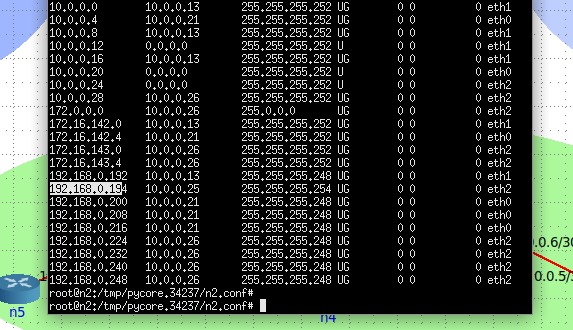
No primeiro caso, o endereço de destino corresponde ao “0.0.0.0”, possui um endereço de “Gateway” de “192.168.0.255”, uma máscara “0.0.0.0” e por fim a “Flag” igual a “UG”. Desta forma, podemos concluir que a seguinte rota é a rota “Default”.A outra rota da primeira tabela, corresponde a uma rota com o endereço de destino corresponde ao “192.168.0.224”, possui um endereço de “Gateway” de “0.0.0.0”, uma máscara “255.255.255.248” e por fim a “Flag” igual a “U”.

No segundo caso, o endereço de destino corresponde ao “0.0.0.0”, possui um endereço de “Gateway” de “192.168.0.193”, uma máscara “0.0.0.0” e por fim a “Flag” igual a “UG”. Desta forma, podemos concluir que a seguinte rota é a rota “Default”. A outra rota da primeira tabela, corresponde a uma rota com o endereço de destino corresponde ao “192.168.0.192”, possui um endereço de “Gateway” de “0.0.0.0”, uma máscara “255.255.255.248” e por fim a “Flag” igual a “U”.

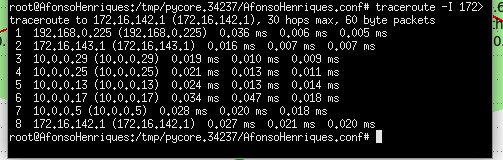
**c)** **Utilize o Wireshark para investigar o comportamento dos routers do core da rede (n1 a n6) quando tenta estabelecer comunicação entre os hosts AfonsoHenriques e Teresa. Indique que dispositivo(s) não permite(m) o encaminhamento correto dos pacotes. Seguidamente, avalie e explique a(s) causa(s) 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.**

R: Após realizar um “ping” com origem no host AfonsoHenriques e destino na Teresa, averiguamos que não alacançamos o nosso destino. Desta forma, através do Wireshark visualizamos que de facto há algum impedimento entre a comunicação dos hosts.

Após vários, descobrimos que nos routers pertencentes ao core, como por exemplo o “n2” existe um problema com a rota que têm como destino o host Teresa.

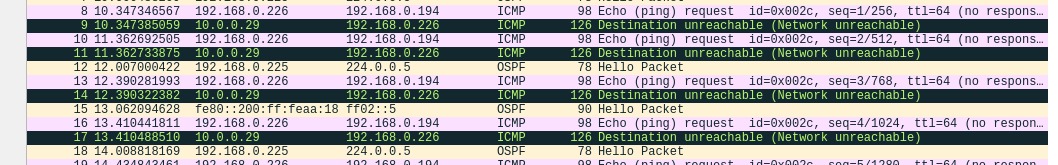
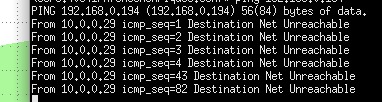


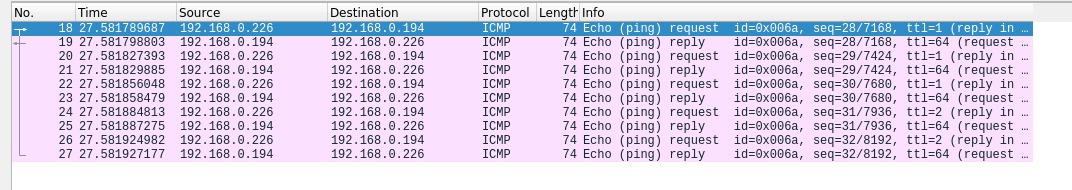
Assim, fomos individualmente incluir o caminho em cada nó com problema de forma a que fosse capaz de alcançar o ISP CondadOnline como se verifica na seguinte figura.

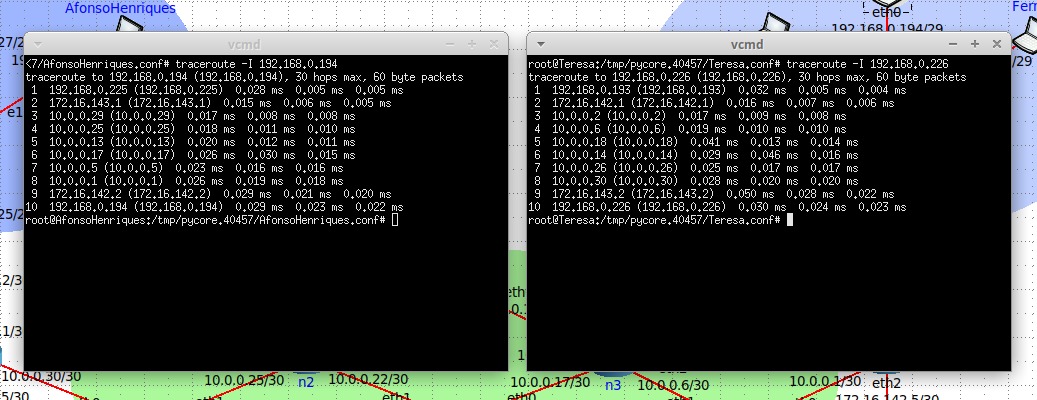


**d) Uma vez que o core da rede esteja a encaminhar corretamente os pacotes enviados por AfonsoHenriques, confira com o Wireshark se estes são recebidos por Teresa.**

1. **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.**

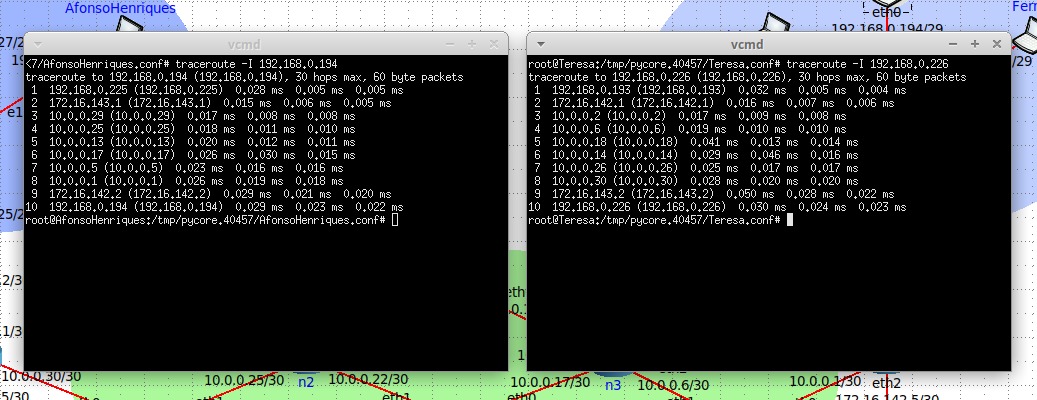
R: Após tentar novamente realizar um “ping” com de AfonsoHenriques com destino em Teresa, observamos que o mesmo não chegava o destino.

Este fenómeno deve-se ao facto de não existirem rotas capazes de direcionar um pacote desde o AfonsoHenriques até à Teresa. De modo a conseguir uma conexão, fomos individualmente a cada nó verificar se de facto haveria problemas com as rotas dos pacotes. Reparamos em nós como o n2 e o n1, não haviam rotas que realizariam a conexão á rede de endereço “192.168.0.192” ou as rotas existentes causavam um loop dentro do core. De modo a corrigir as rotas, fomos a cada um dos nós com rotas defeituosas e eliminamos ou adicionamos as rotas corretas. O resultado obtido foi o seguinte:

Através do “ping” (imagem 1) e do “traceroute” (imagem 2) concluímos que a ligação entre mãe e filho foi efetuada com sucesso.

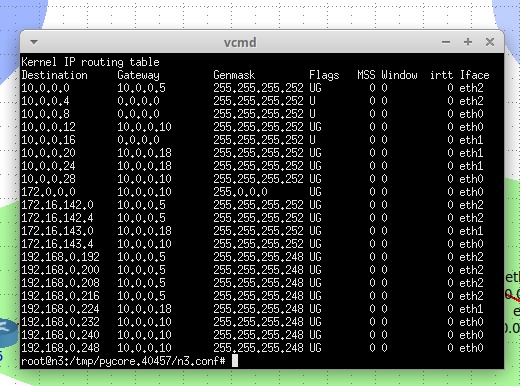
**ii) As rotas dos pacotes ICMP echo reply são as mesmas, mas em sentido inverso, que as rotas dos pacotes ICMP echo request enviados entre AfonsoHenriques e Teresa? (Sugestão: analise as rotas nos dois sentidos com o traceroute). Mostre graficamente a rota seguida nos dois sentidos por esses pacotes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

R: A seguinte imagem corresponde a dois “traceroutes” realizados de forma a perceber as rotas dos pacotes “icmp”:

Com base nos dados desta imagem, podemos ver que a nivél da network core à uma escolha de caminhos diferentes. Nos pacotes de AfonsoHenriques a Teresa, o caminho a nível de core desloca-se internamente pelos routers “n5->n2->n1->n3->n6”, enquanto que de Teresa a AfonsoHenriques, o caminho não é o inverso mas sim: “n6->n3->n4->n2->n5”.Este fenómeno deve-se às rotas definidas internamente nos routers do core que permitem a existência de diferentes caminhos com exatamente o mesmo numero de saltos que passam por routers diferentes.

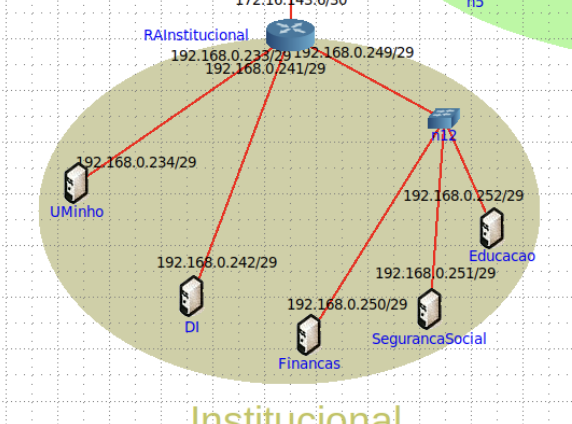
**e)Existe uma correspondência (match) nesta entrada para pacotes enviados para o polo Galiza? E para CDN? Caso seja essa a entrada utilizada para o encaminhamento, permitirá o funcionamento esperado do dispositivo? Ofereça uma explicação pela qual essa entrada é ou não utilizada.**

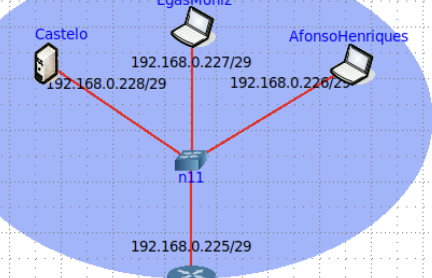
**R:**  Após realizar o comando “netstat -rn” para o router n3, obetemos a seguinte tabela:

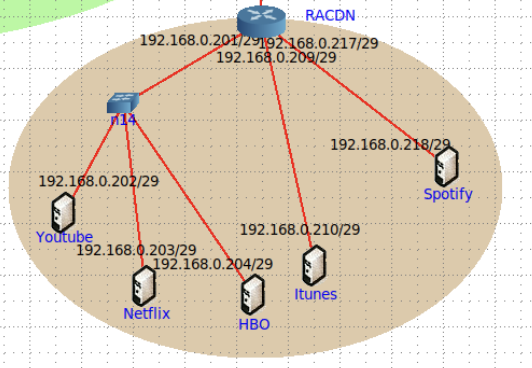
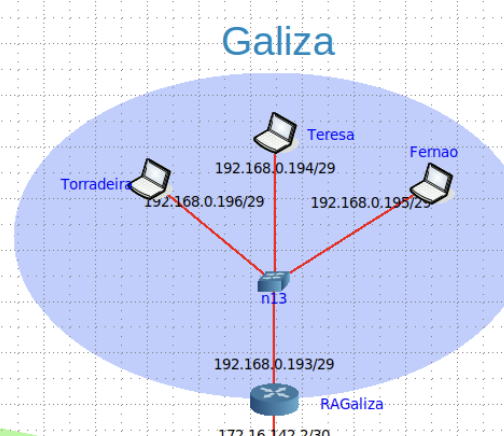


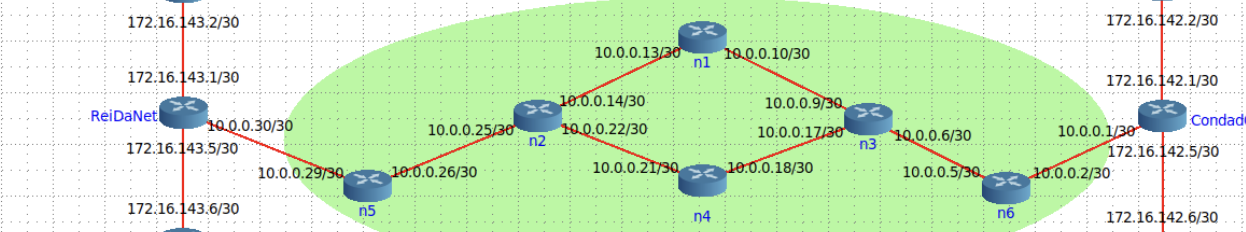
Tendo em conta a entrada da tabela fornecida, não há nenhum “match” com as entradas que nós obtemos. Relativamente ao encaminhamento de pacotes para o polo “Galiza” e “CDN”, uma vez que não existe nenhum router com o endereço “20.0.0.18”, o tráfego proveniente do core com destino na rede Galiza seria perdido, enquanto o tráfego com destino ao polo “CDN” poderia ou não continuar dependendo se existe uma rota não defeituosa definida. Desta forma, caso apenas houvesse a entrada fornecida a encaminhar tráfego para a Galiza este seria perdido, mas pode ou não continuar a haver tráfego para o polo “CDN” caso exista uma rota bem definida.

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

****R: Observando os endereços dos quatro polos, podemos ver que estes começam todos com octetos que indiciam endereços privados. Os endereços dos polos têm 192.168 em todos os 2 primeiros octetos de cada endereço como se pode ver pelas seguintes imagens:

****

****

****Relativamente à rede core, surgem agora dois octetos diferentes aos utilizados nos diferentes polos. Contudo, estes endereços são na mesma endereços que pertencem na mesma ao conjunto dos endereços privados.

Na imagem, observamos que os endereços são pertencentes ao intervalo 172.16.0.0 até 172.31.255.255 (fora do core) ou ao intervalo 10.0.0.0 até 10.255.255.255 (dentro do core).

Deste modo, concluímos que todos os endereços utilizados no esquema são privados, inclusive endereços que tipicamente são públicos como os endereços do ISP “ReiDaNet”.

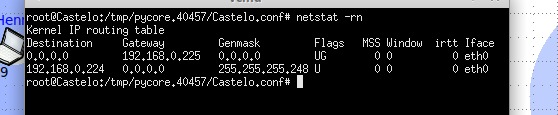
**g) Os switches localizados em cada um dos polos têm um endereço IP atribuído? Porquê?**

R: Apesar de switches poderem receber IP's, os deste modelo não possuem nenhum endereço. O objetivo dos switches é gerenciar e encaminhar a entrada de pacotes de dados numa “Network”.Normalmente, em grandes networks, os switches podem receber um IP o que lhe permite serem gerenciáveis remotamente. No entanto, como as networks dos exercícios, são relativamente pouco complexas, não há necessidade de haver um gerenciamento remoto dos switches.

**2-**

1. **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.**

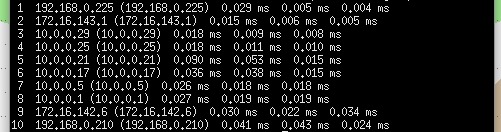
R: Antes das remodelações, o castelo possuía uma tabela de e endereçamento com as seguintes entradas:



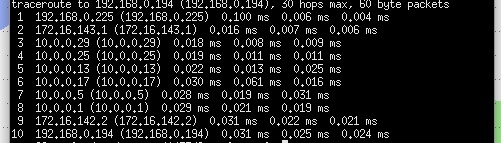
Na seguinte tabela existem apenas duas rotas, sendo a “default”, que aparece sombreada a cor branca. Além disso, constatamos que atualmente o castelo é capaz de chegar aos vários hosts dos diferentes polos, como se pode ver nas seguintes imagens:



*Traceroute com destino a um “host” do polo institucional*



*Traceroute com destino a um “host” do polo Cdn*

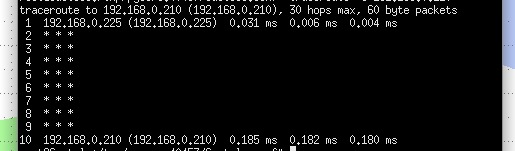
**

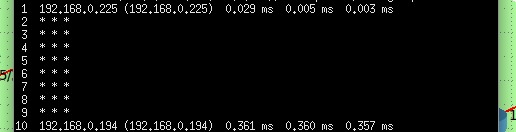
*Traceroute com destino a um “host” do polo Galiza*

Após realizar a limpeza, é necessária estabelecer novamente as rotas de forma a que haja conexão a todos os outros polos, o que resultou na seguinte tabela de encaminhamento:



E os respetivos “traceroutes” anteriores:





Com isto, concluímos que as ligações estão feitas baseado nos resultados do “traceroute”. Contudo, a falta de uma rota “default” tem como problema um pequeno aumento na latência, e há uma pequena perda de pacotes que culmina em por exemplo nos traceroutes falta de informação respetivamente ao percurso dos pacotes.

**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.**