TP2

Protocolo IPv4 (802.11)

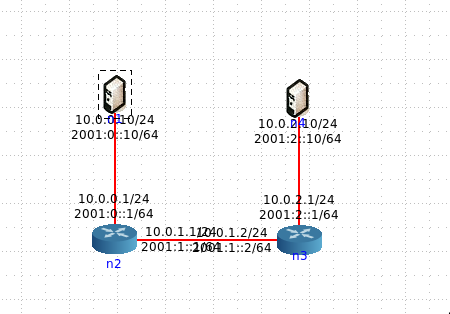
Daniel Vieira A73974

José Cunha A74702

João Palmeira A73864

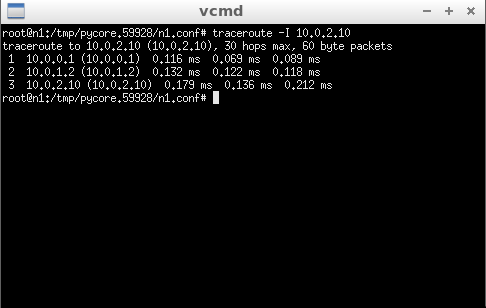
PARTE 1





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

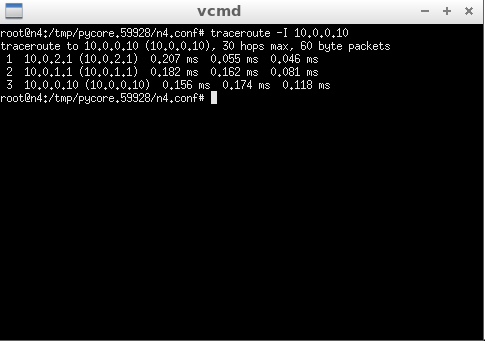
**R:**



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

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

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



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

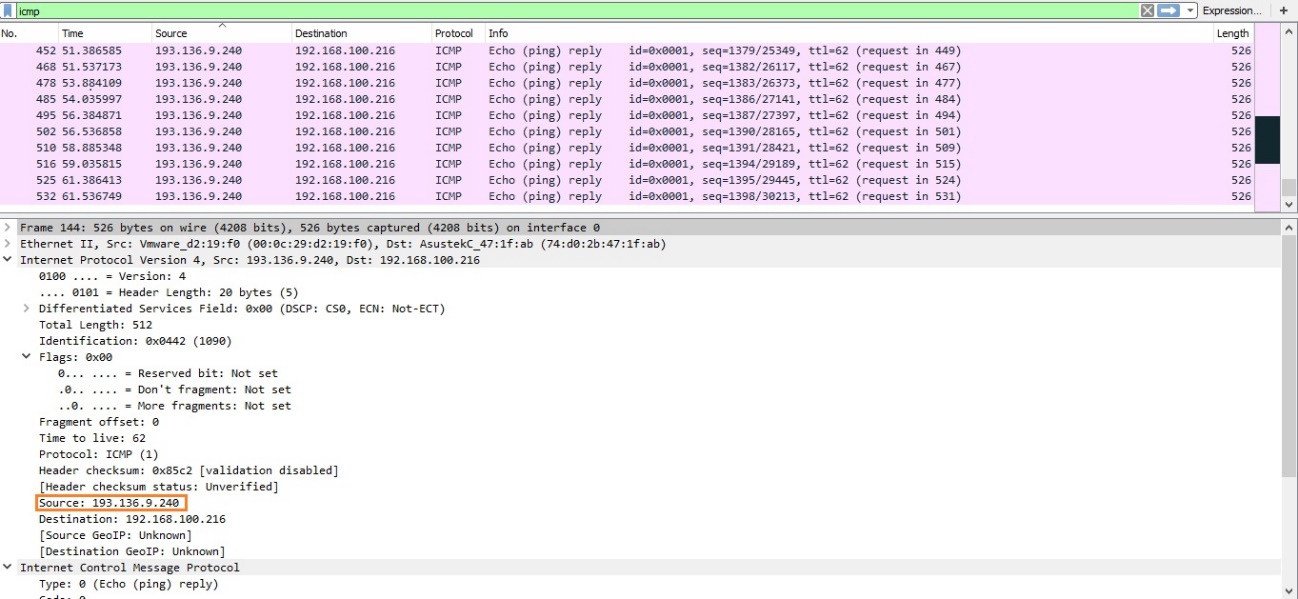
* 1. Qual o valor médio do tempo de ida-e-volta (Round-Trip Time) obtido?

**R:** 1: (0.207 + 0.055 + 0.046) / 3 = 0.102(6) ms

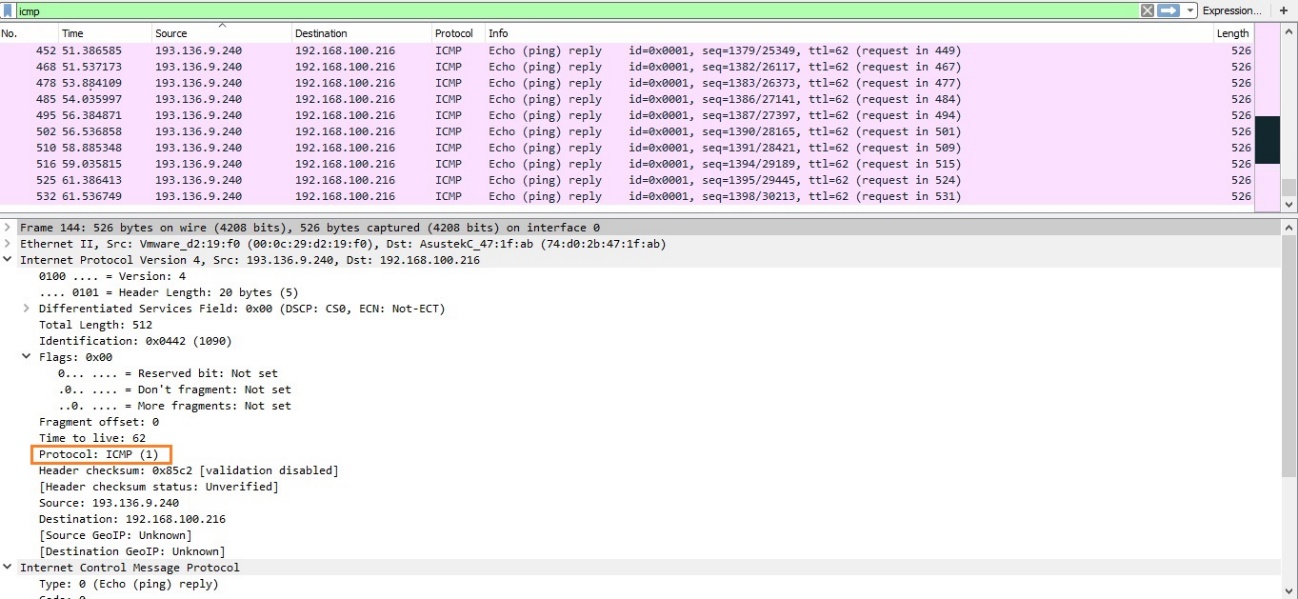
2: (0.182 + 0.162 + 0.081) / 3 = 0.141(6) ms

3: (0.156 + 0.174 + 0.118) / 3 = 0.149(3) ms

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

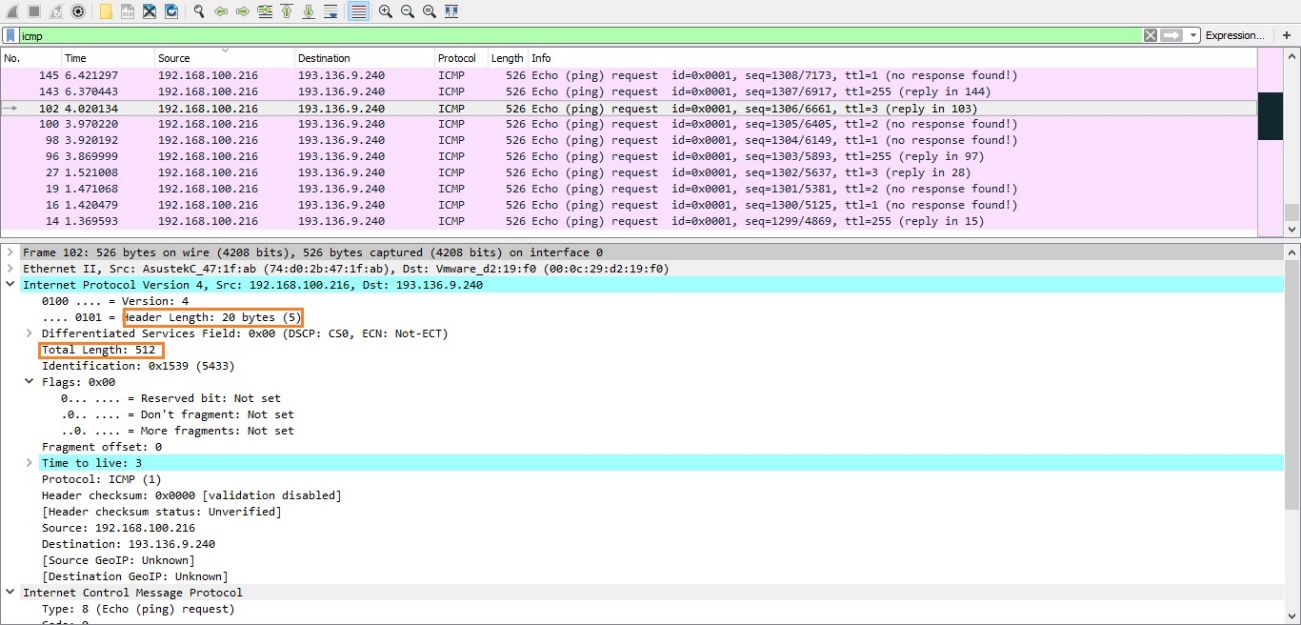


**R:** O endereço IP da interface ativa do computador é o endereço “Source”, que tem o valor 193.136.9.248

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

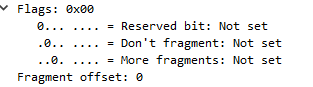
**R:** O valor do campo protocolo é 1. Este campo identifica o tipo de protocolo e neste caso trata-se de ICMP.

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



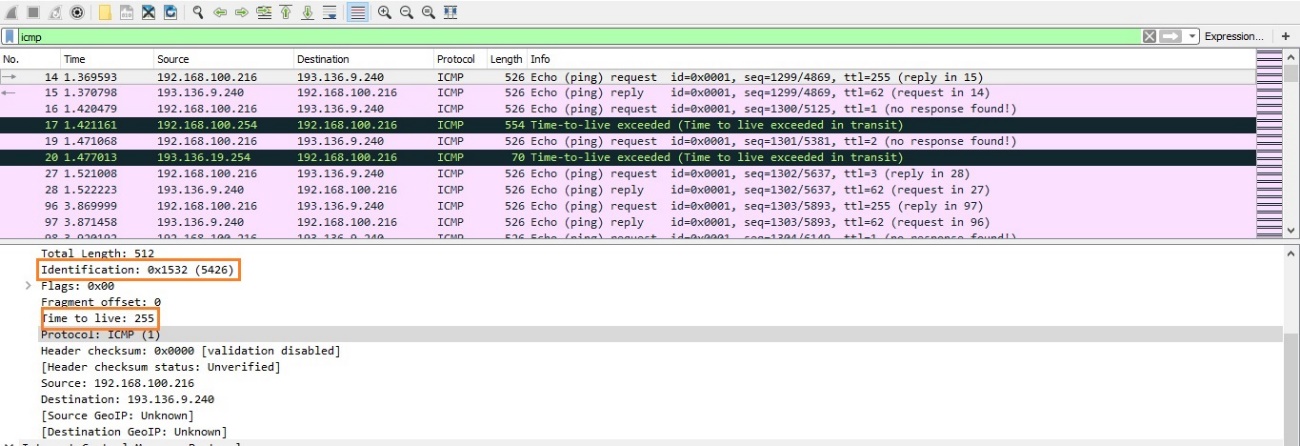
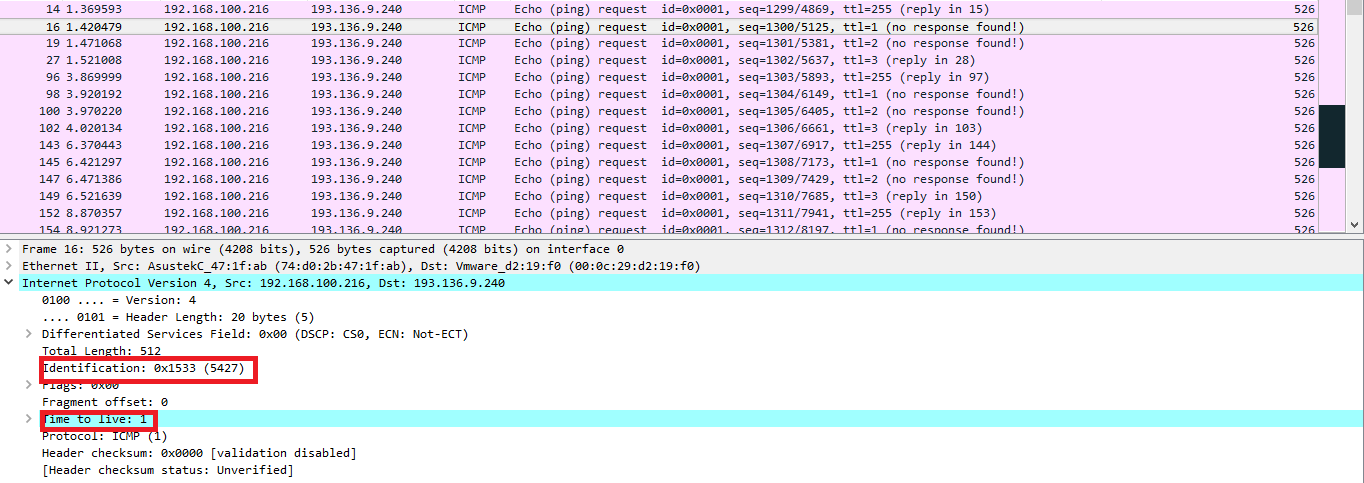
**R:** O cabeçalho IP(v4) tem 20 *bytes*. O tamanho do campo de dados é 512 e o número de *bytes* deste é 512-20=492 *bytes*.

* 1. O datagrama IP foi fragmentado?Justifique.



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

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

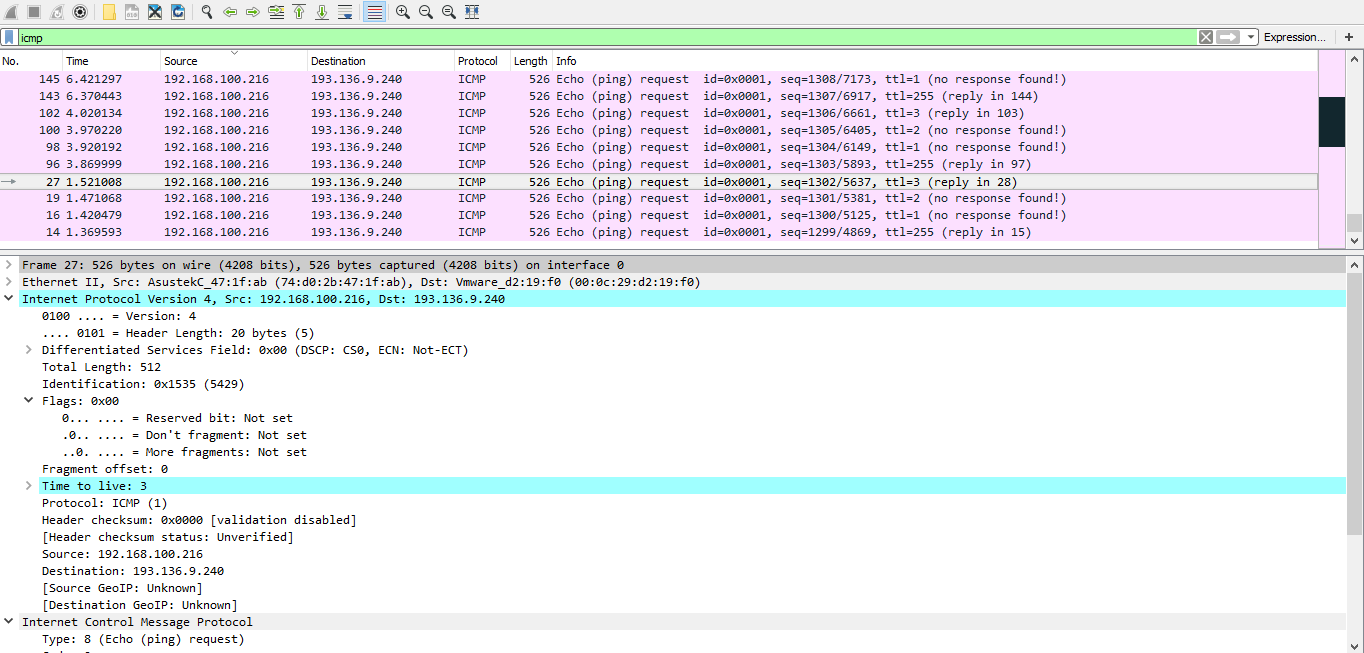


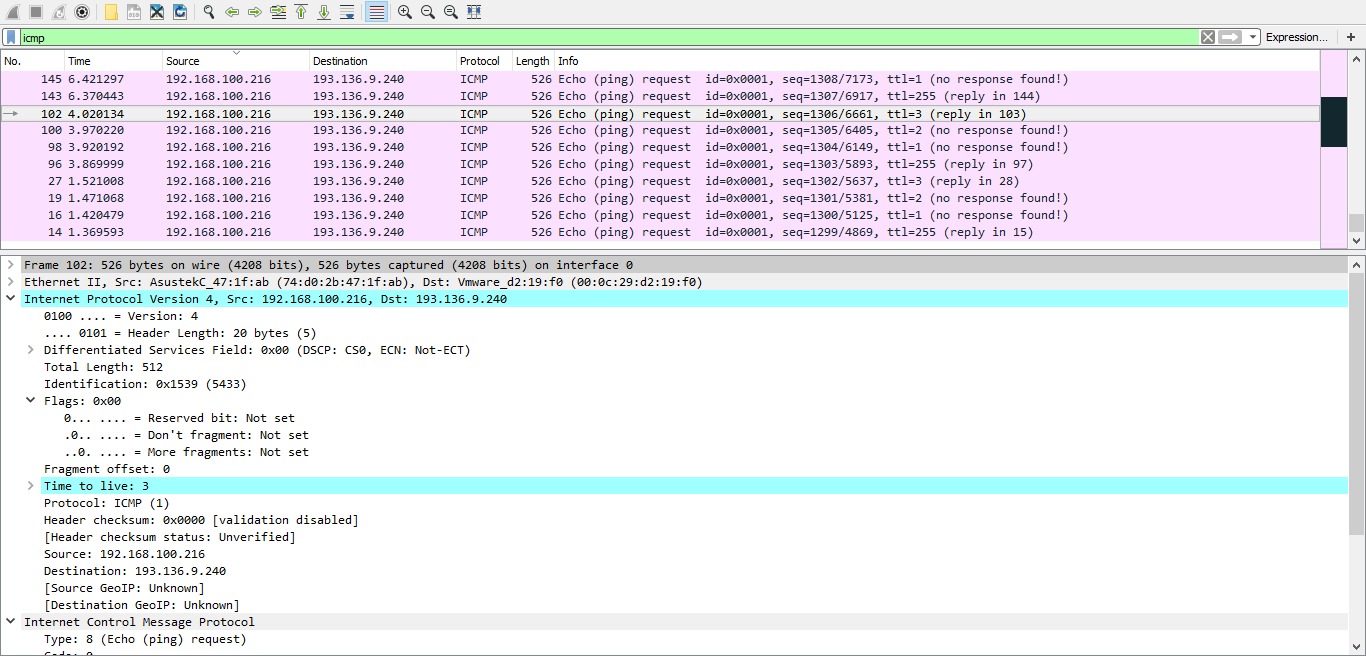
**R:** Os campos do cabeçalho IP que variam de pacote para pacote são o “Time to live” e o “Identification”.

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

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

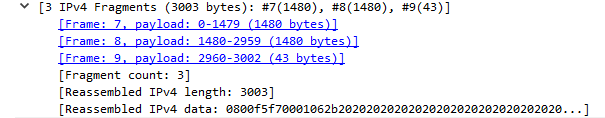
* 1. Ordene o tráfego capturado por endereço destino e encontre a série de respostas ICMP TTL *exceeded* enviadas ao seu computador. Qual é o valor do campo TTL? Esse valor permanece constate para todas as mensagens de resposta ICMP TTL *exceeded* enviados ao seu *host*? Porquê?



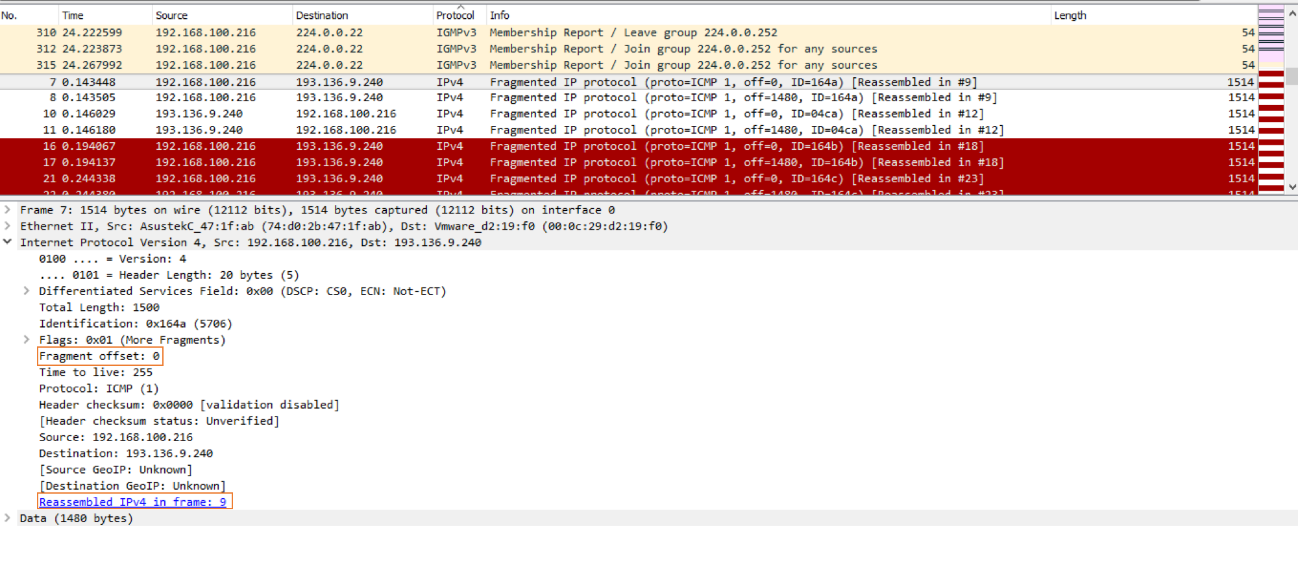


**R:** O valor do campo TTL é 3. Permanece constante para todas as mensagens de resposta enviadas, pois trata-se de um *reply*. Este valor de tempo de vida serve para garantir que o *reply* chega ao destino independentemente dos saltos que possa vir a dar.

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

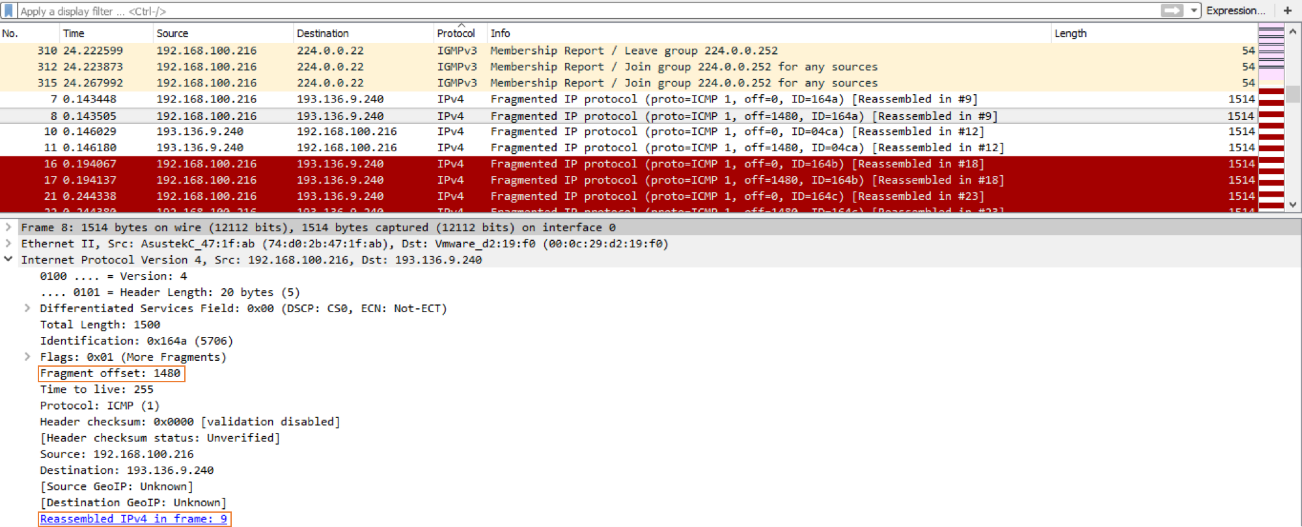


**R:** Houve necessidade de fragmentar o pacote inicial, pois este era demasiado grande, tendo de se dividir, neste caso, em 3 fragmentos.

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

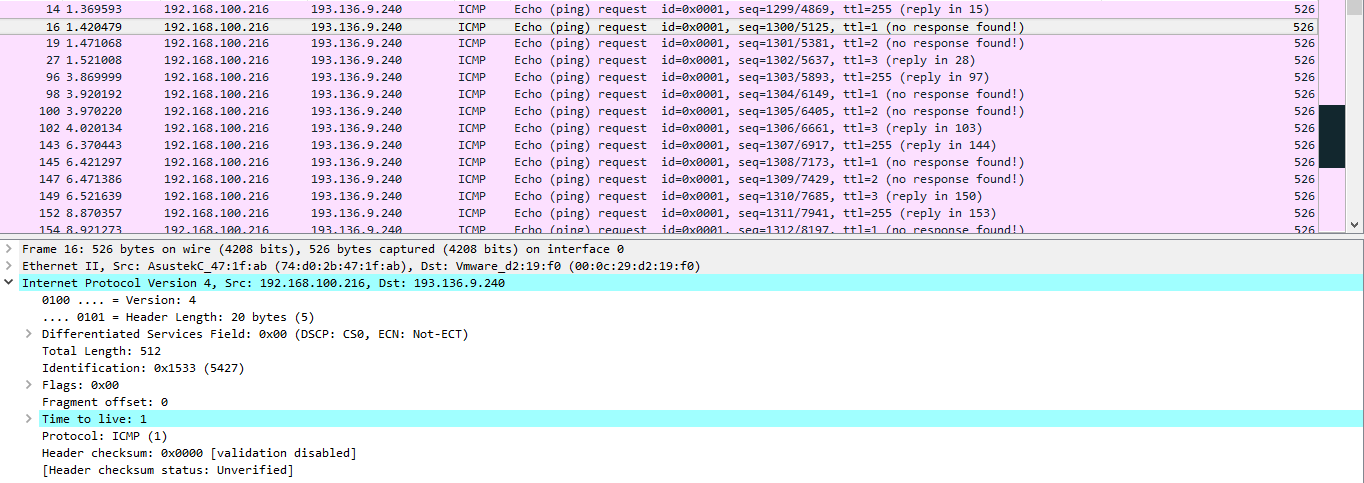
**R:** “Reassembled IPv4 in frame: 9” indica-nos que é um fragmento que vai ser reconstruído na trama 9. “More Fragments: Set” (toma valor 1) indica que existem mais fragmentos para além deste. Trata-se do primeiro fragmento pois o offset é igual a 0. O segundo fragmento vai ter o offset igual a 1480.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

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



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

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



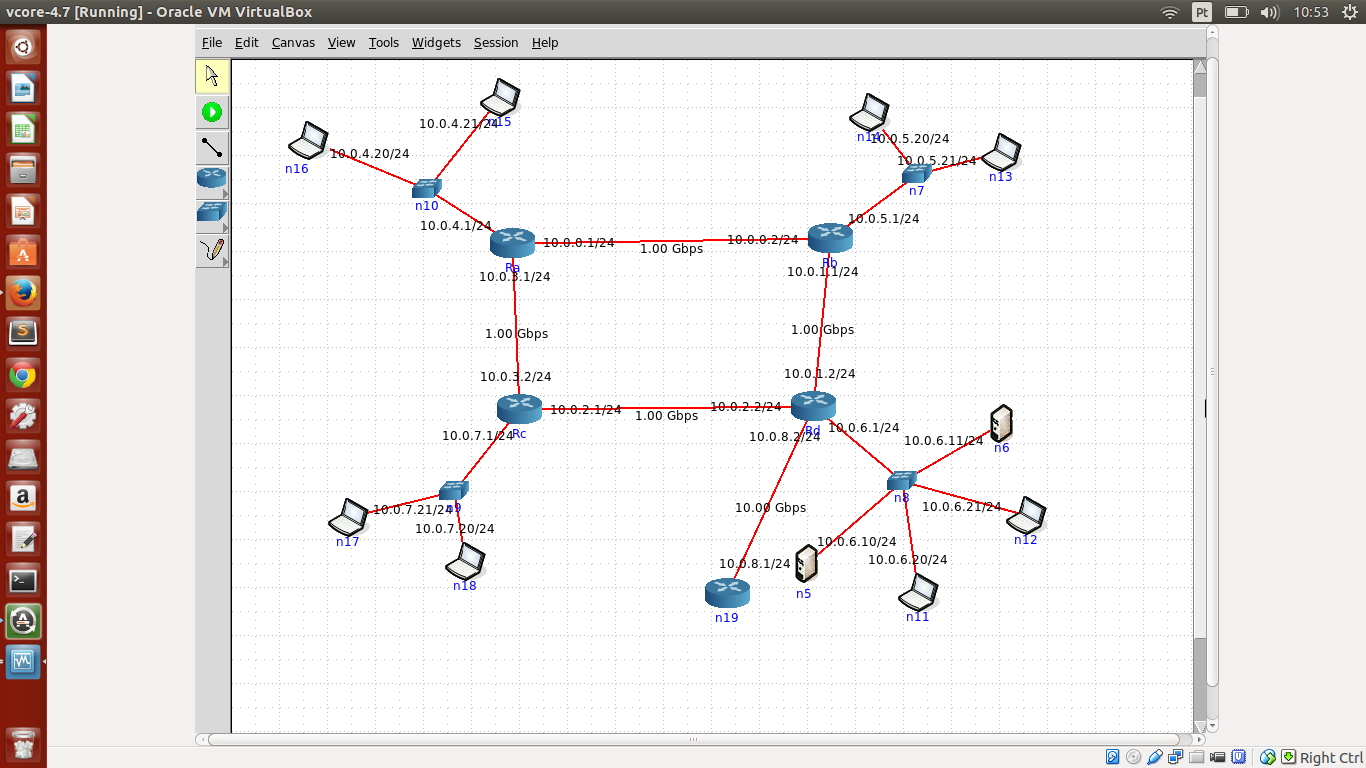
**R:** Foram criados 3 fragmentos a partir do datagrama original. Como estes 3 fragmentos vão ser reconstruídos na trama 9, a trama 9 corresponderá ao último fragmento do datagrama original. Através da flag “More Fragments: Not Set” (toma valor 0) sabemos que não há mais fragmentos, e através do offset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

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

PARTE 2

1. Atenda aos endereços IP atribuídos automaticamente pelo CORE aos diversos equipamentos da topologia.
2. Indique que endereços IP e máscaras de rede foram atribuídos pelo CORE a cada equipamento. Para simplificar, pode incluir uma imagem que ilustre de forma clara a topologia e o endereçamento.



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

Ra to Rb: ip=10.0.0.1 Mascara de rede= 255.255.255.0

Ra to Rc: ip=10.0.3.1 Mascara de rede= 255.255.255.0

Rc to Rd: ip=10.0.2.1 Mascara de rede= 255.255.255.0

Rc to Ra: ip= 10.0.3.2 Mascara de rede= 255.255.255.0

Rd to Rc: ip=10.0.2.2 Mascara de rede= 255.255.255.0

Rd to Rb: ip=10.0.1.2 Mascara de rede= 255.255.255.0

Rb to Ra: ip=10.0.0.2 Mascara de rede= 255.255.255.0

Rb to Rd: ip=10.0.1.1 Mascara de rede= 255.255.255.0

Rd to n19: ip=10.0.8.2 Mascara de rede= 255.255.255.0

N5: ip=10.0.6.10 Mascara de rede= 255.255.255.0

N6: ip= 10.0.6.11 Mascara de rede= 255.255.255.0

N11: ip=10.0.6.20 Mascara de rede= 255.255.255.0

N12: ip = 10.0.6.21 Mascara de rede= 255.255.255.0

N13: ip=10.0.5.21 Mascara de rede= 255.255.255.0

N14: ip=10.0.5.20 Mascara de rede= 255.255.255.0

N15: ip=10.0.4.21 Mascara de rede= 255.255.255.0

N16: ip=10.0.4.20 Mascara de rede= 255.255.255.0

N17: ip=10.0.7.21 Mascara de rede= 255.255.255.0

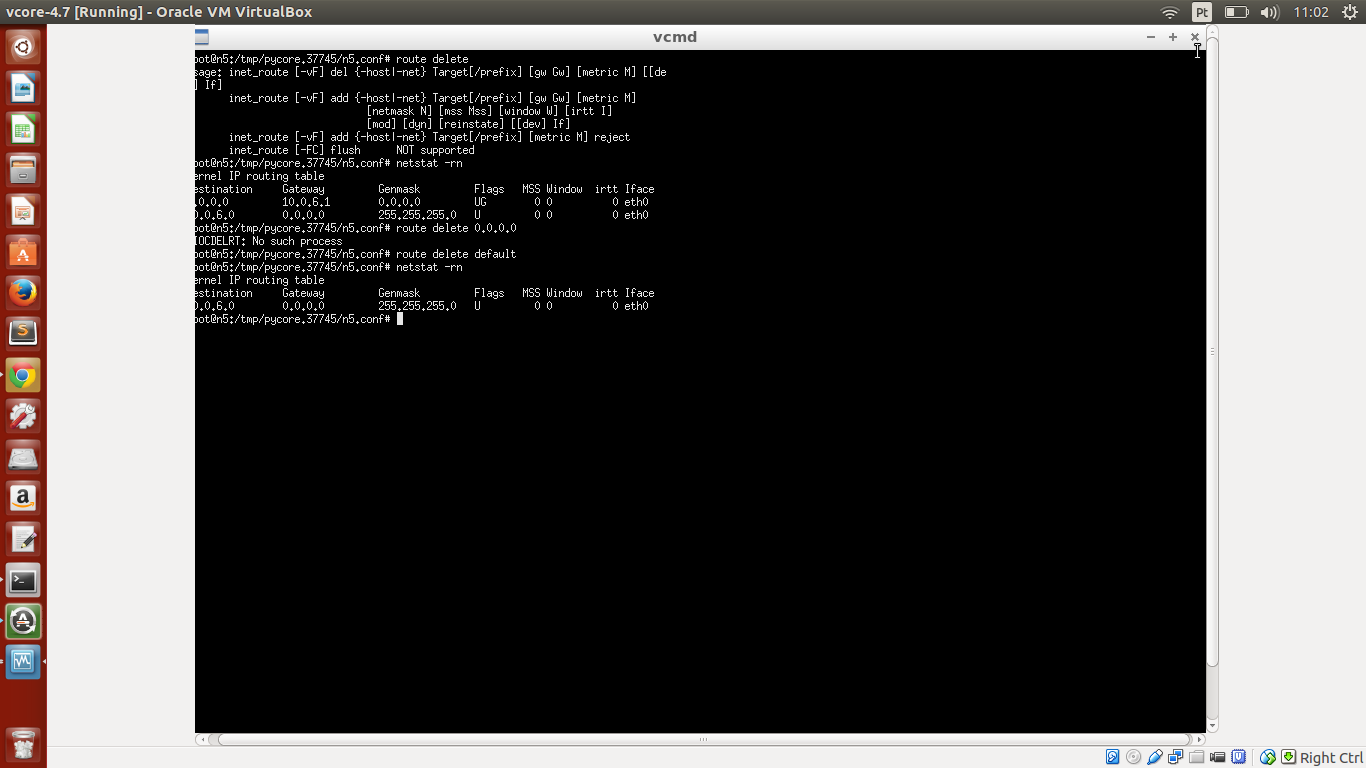
N18: ip=10.0.7.20 Mascara de rede= 255.255.255.0

N19 to Rd: ip=10.0.8.1 Mascara de rede= 255.255.255.0

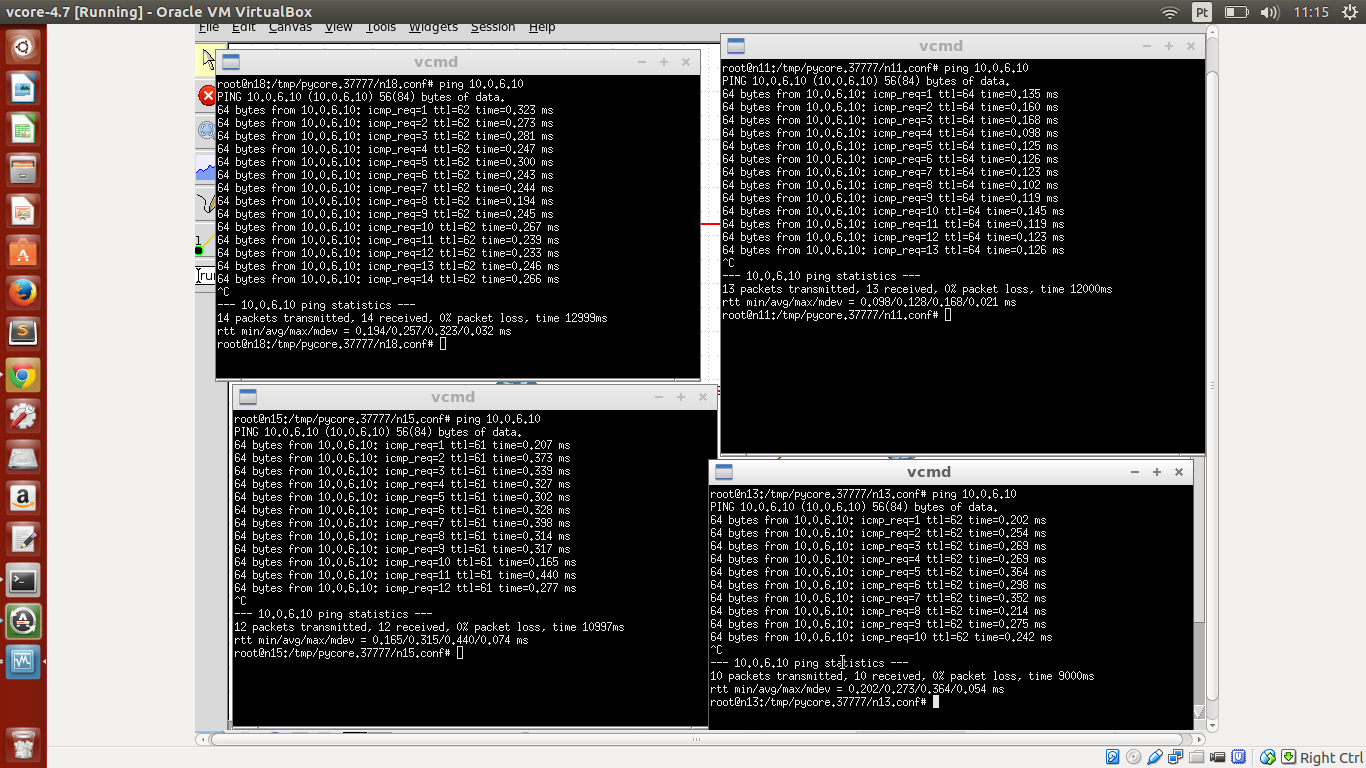
1. Tratam-se de endereços públicos ou privados? Porquê?

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

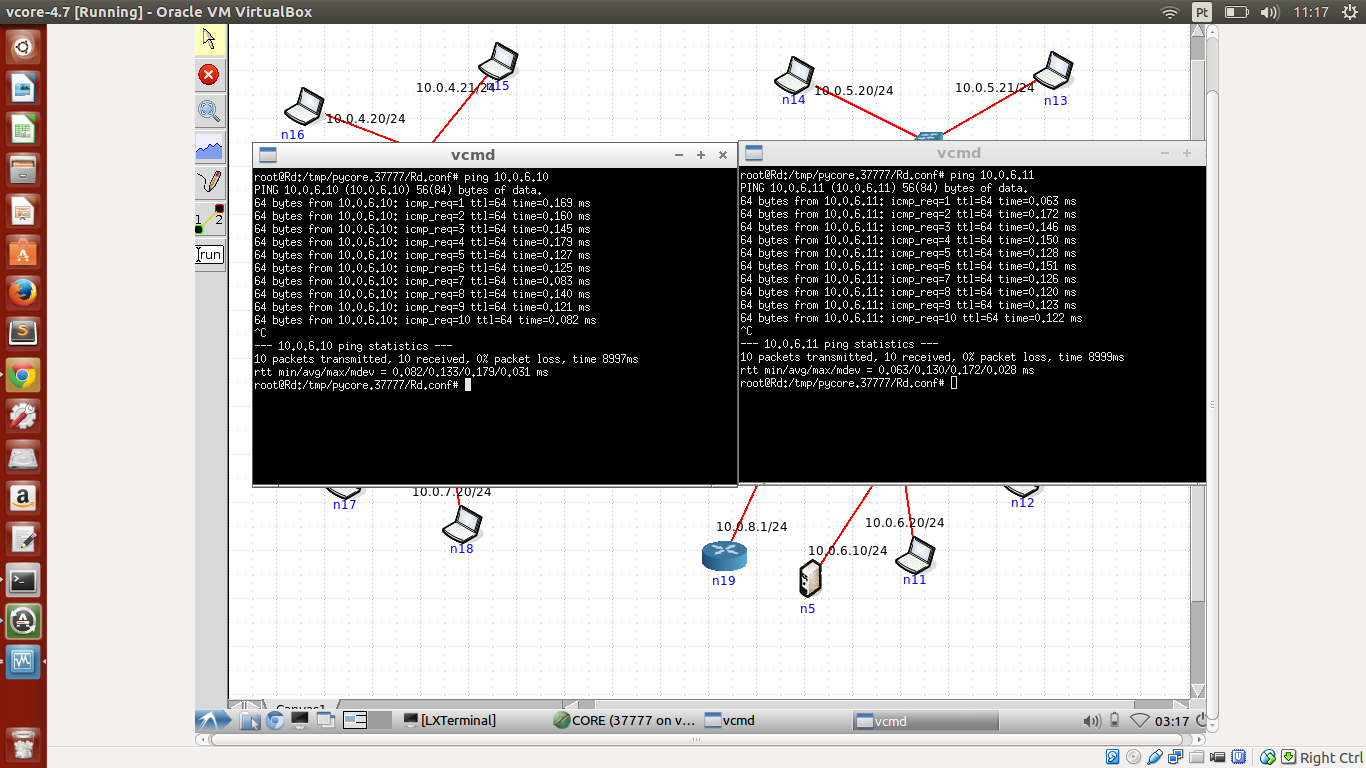
1. Porque razão não é atribuído um endereço IP aos *switches*?



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

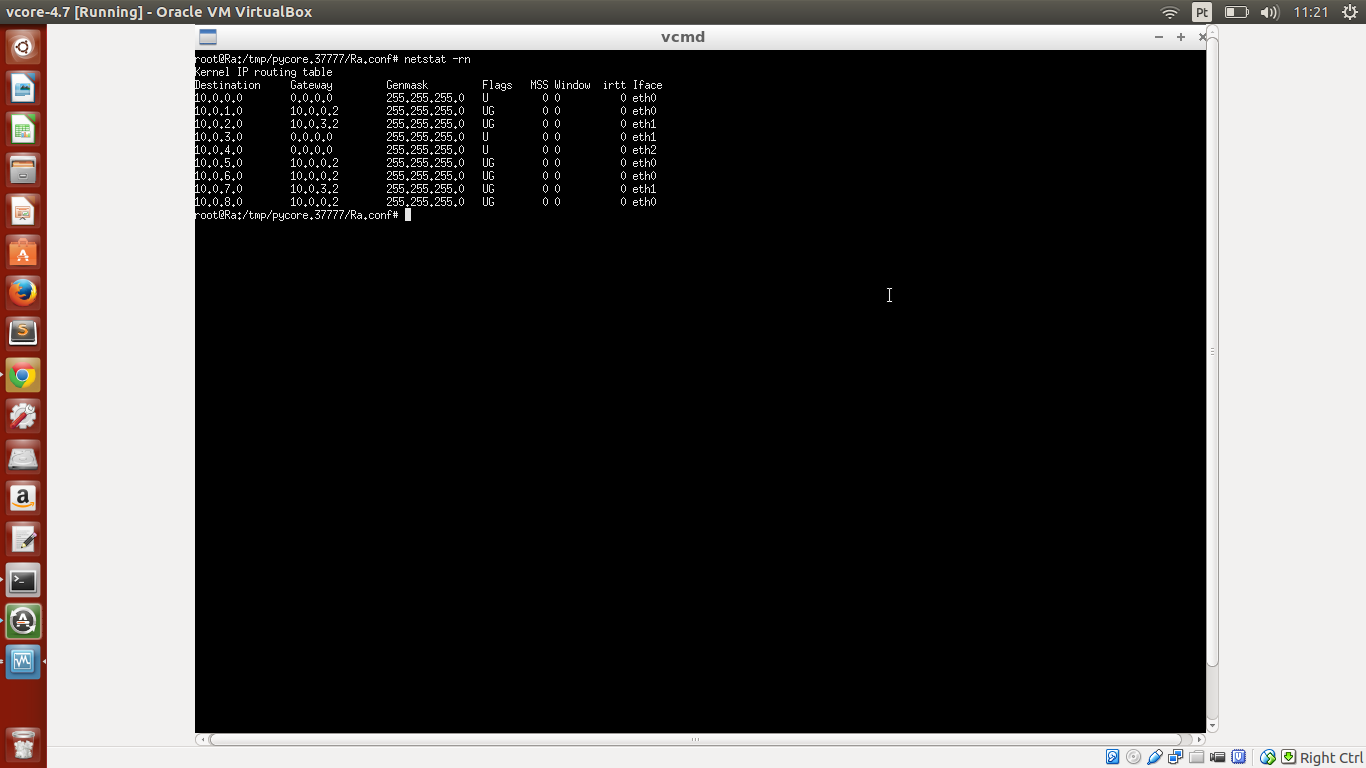
1. Usando o comando *ping* certifique-se que existe conectividade IP entre os laptops dos utilizadores e o servidor do departamento D (basta certificar a conectividade de um laptop por departamento).

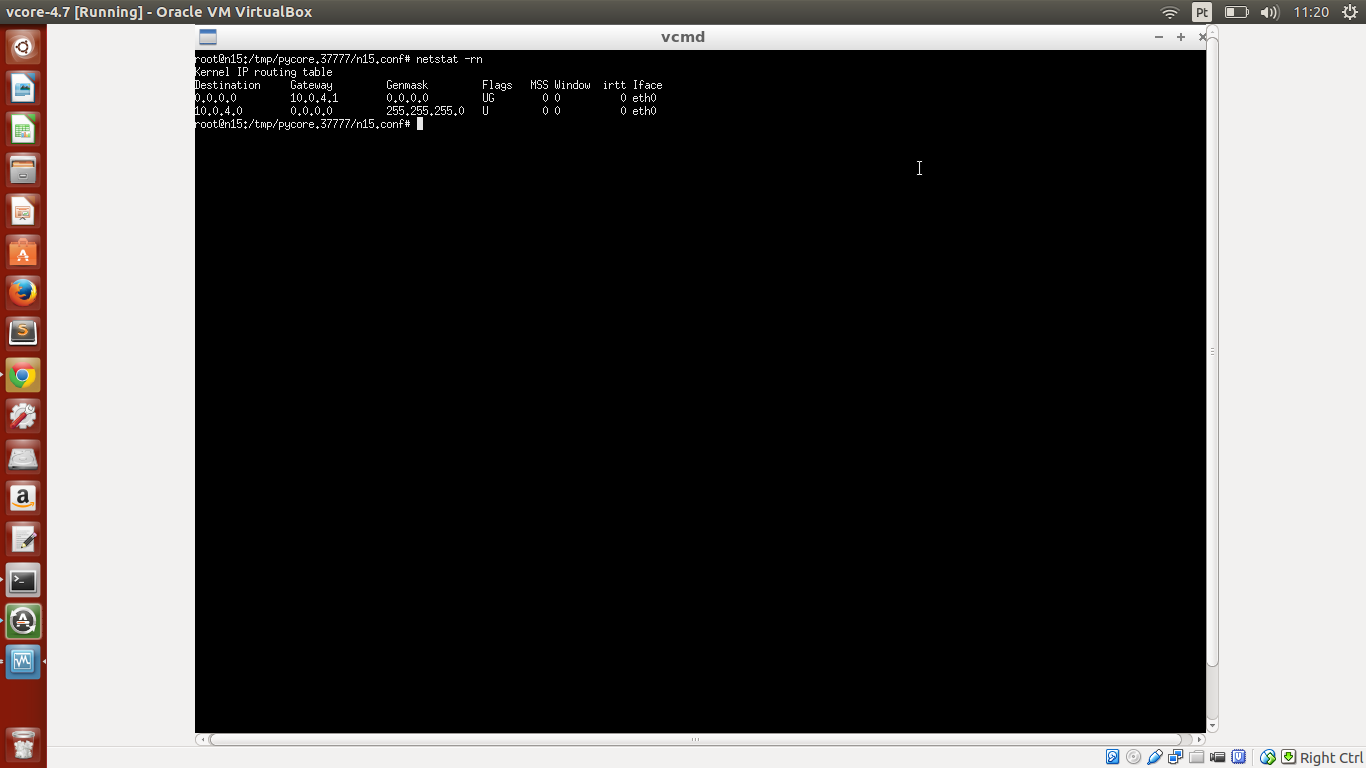
**R:** Como se pode ver pela figura acima, existe conetividade entre um laptop de cada departamento e o servidor do departamento D, sendo n18 do departamento C, n15 do departamento A, n11 do departamento D, e n13 do departamento B e 10.0.6.10 o endereço IP do servidor do departamento D.

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

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

1. Para o router e um laptop do departamento B:
2. Execute o comando netstat –rn por forma a poder consultar a tabela de encaminhamento unicast (Ipv4). Inclua no seu relatório as tabelas de encaminhamento obtidas; interprete as várias entradas de cada tabela. Se necessário, consulte o manual respetivo (man netstat).

*Router:*

 *Laptop:*

**R:** Relativamente ao router Ra:

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

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

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

Para a quarta entrada, o destino é a rede dos routers entre Rd e Rc (10.0.3.2) e o próximo salto vai corresponder ao router Rd (10.0.1.2) visto ser o caminho mais próximo de chegarmos a essa rede através do router Rc.

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

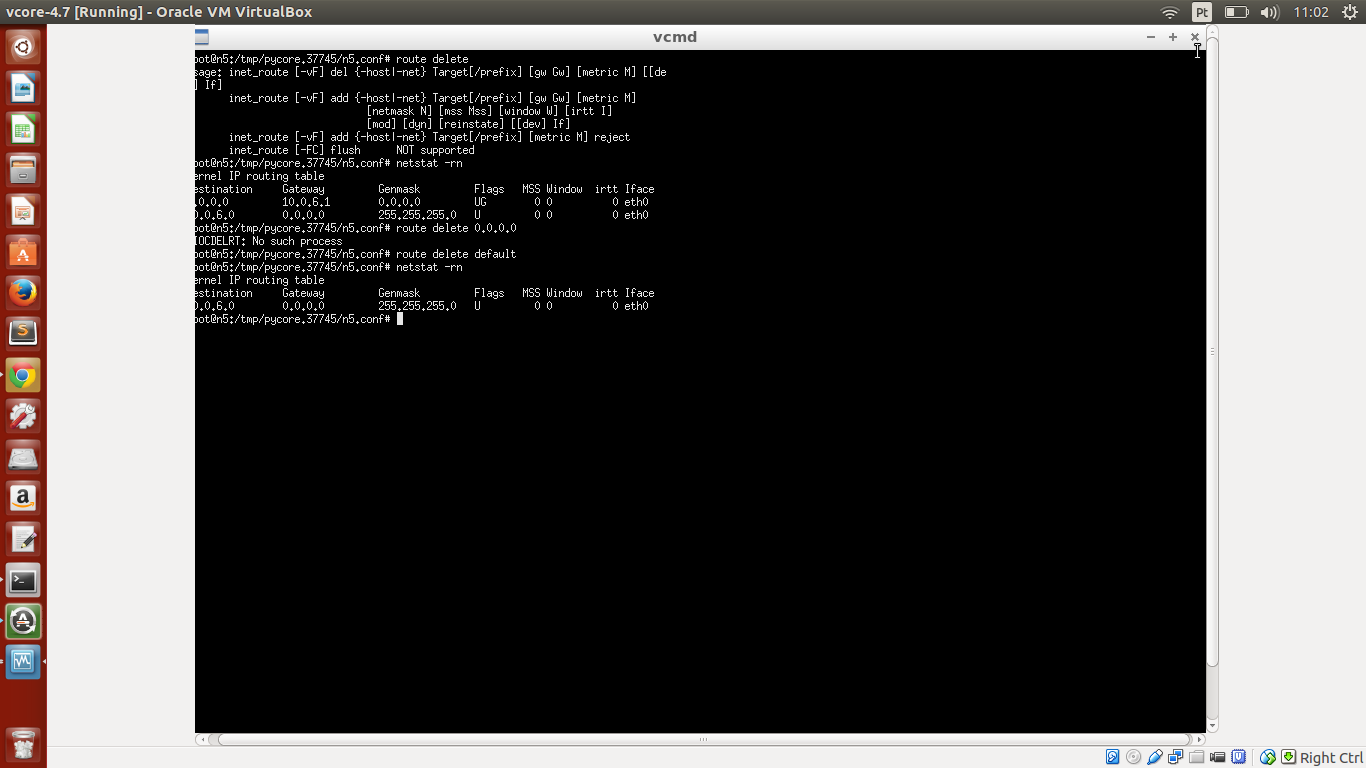
Relativamente ao laptop:Para a primeira entrada da tabela de encaminhamento, a rede destino é a rota por defeito (0.0.0.0) e o próximo salto vai corresponder ao *router* Ra (10.0.4.1).

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

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

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

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



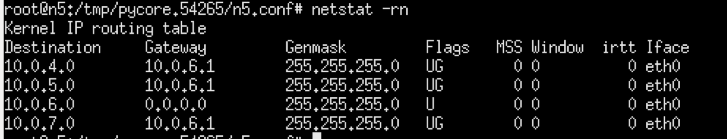
**R:** A implementação desta medida não tem nenhuma implicação para os utilizadores que acedem ao servidor pois continua a existir a rota para a rede [10.0.6.0](http://l.facebook.com/l.php?u=http%3A%2F%2F10.0.3.0%2F&h=fAQEAfHBl) a partir do servidor.

1. C:\Users\Daniel Vieira\AppData\Local\Microsoft\Windows\INetCache\Content.Word\23718320_1906934606013817_359499918_n.pngAdicione as rotas estáticas necessárias para restaurar a conectividade para o servidor S1, por forma a contornar a restrição imposta em c). Utilize para o efeito o comando route add e registe os comandos que usou.

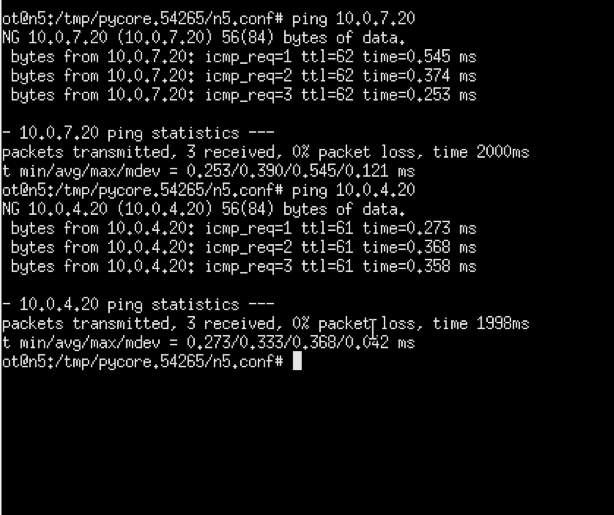
**R:** Em que 10.0.4.0 corresponde a sub-rede do departamento A,10.0.5.0 corresponde a B e a 10.0.7.0 corresponde a C.

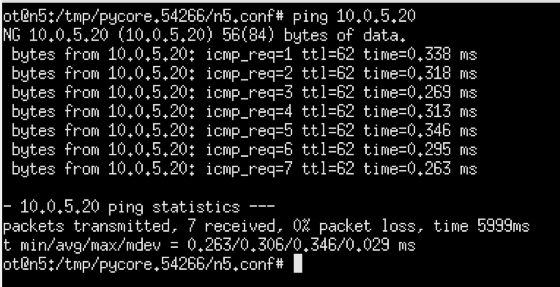
1. Teste a nova política de encaminhamento garantindo que o servidor está novamente acessível, utilizando para o efeito o comando ping. Registe a nova tabela de encaminhamento do servidor.

**R:** A nova tabela de encaminhamento é a seguinte:



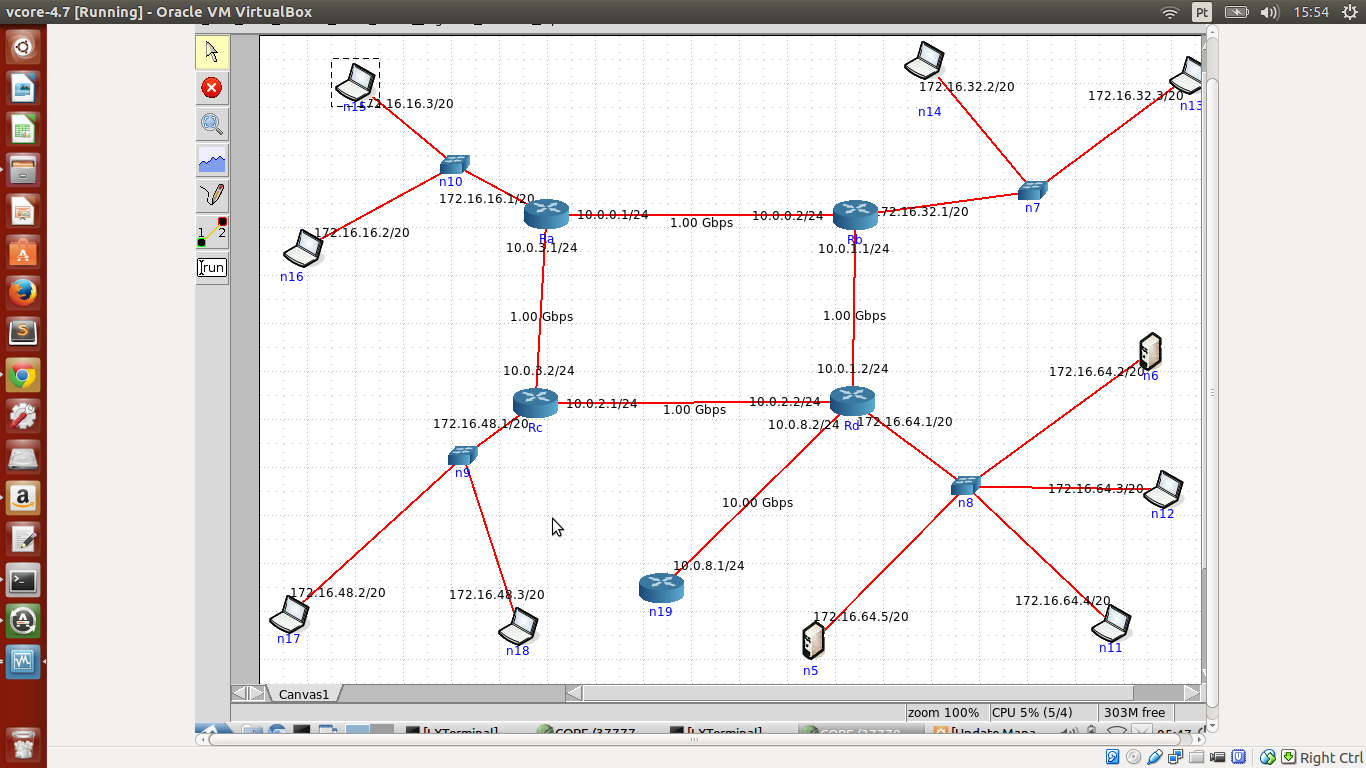
De seguida são novamente verificadas as ligações dos laptops com os departamentos:



****

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

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

**R:**

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

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

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

NetMask:

255.255.240.0 11111111.11111111.11110000.00000000 /20 16 Class C's

Sub-rede A:

N15-172.16.16.3/20

N16-172.16.16.2/20

Ra-172.16.16.1/20

Sub-rede B:

N14-172.16.32.2/20

N13-172.16.32.3/20

Rb-172.16.32.1/20

Sub-rede C:

N17-172.16.48.2/20

N18-172.16.48.3/20

Rc-172.16.48.1/20

Sub-rede D:

N5-172.16.64.5/20

N11-172.16.64.4/20

N12-172.16.64.3/20

N6-172.16.64.2/20

Rd-172.16.64.1/20

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

**R:**  255.255.240.010. Existem 16 bits para identificar a rede, sendo 4 destes usados para especificar a sub-rede. Por isso, e como para criar a máscara de rede é necessário colocar todos os bits identificadores da rede a 1, o número obtido em decimal foi 255.255.240.010. Os 12 bits restantes são para os *hosts* -> 212 = 4096. Há dois endereços reservados, logo há 4096-2 = 4094 endereços possíveis para *hosts.* Assim, é possível interligar 4094 *hosts* em cada departamento, assumindo que apenas vamos ligar *hosts*.

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

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

