Universidade do Minho
Mestrado Integrado em Engenharia Informática

Redes de Computadores
2019/2020

TP2: Protocolo IPv4
Grupo 05

Ana Afonso
A85762

João Diogo Mota
A80791

Márcia Teixeira
A80943

1. Parte I: Datagramas IP e Fragmentação

1. Questões e Respostas

Questão 1

Prepare uma topologia no CORE para verificar o comportamento do traceroute. Ligue um host (servidor) s1 a um router r2; o router r2 a um router r3, o router r3 a um router r4, que por sua vez, se liga a um host (pc) h5. (Note que pode não existir conectividade IP imediata entre s1 e h5 até que o routing estabilize). Ajuste o nome dos equipamentos atribuídos por defeito para a topologia do enunciado.

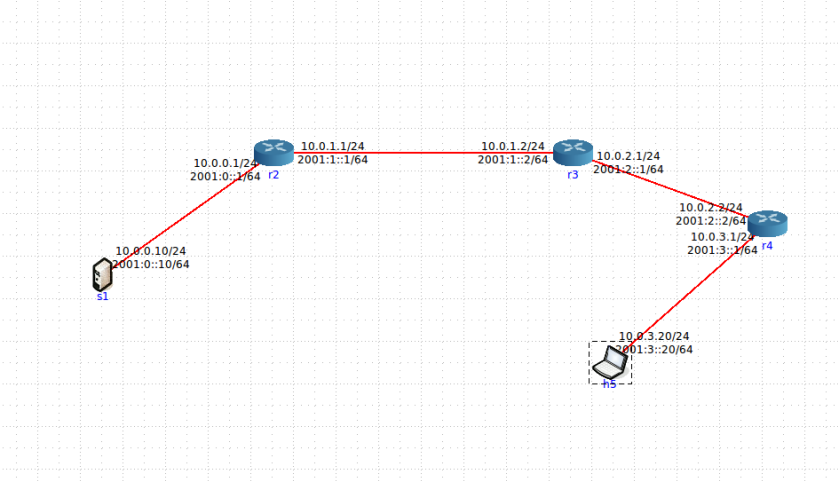


Figura 1: Implementação da topologia no CORE

a. Ative o wireshark ou o tcpdump no pc s1. Numa shell de s1, execute o comando traceroute -I para o endereço IP do host h5.

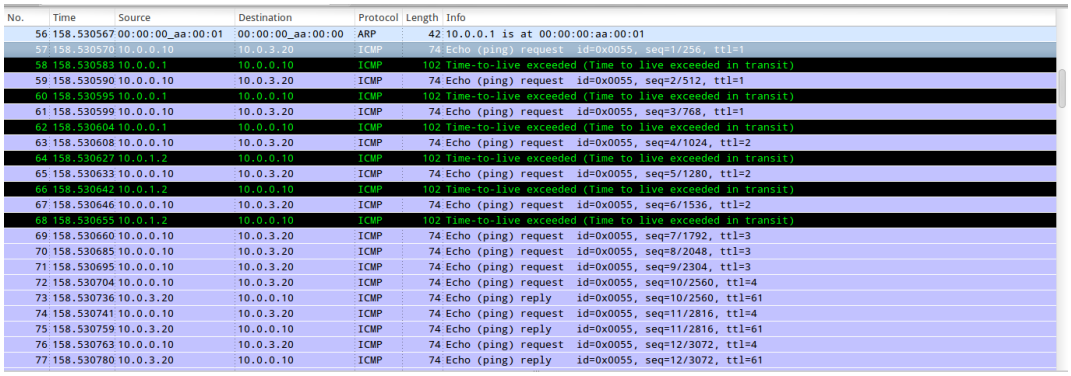
```
root@s1:/tmp/pycore.33223/s1.conf# traceroute -I 10.0.3.20
traceroute to 10.0.3.20 (10.0.3.20), 30 hops max, 60 byte packets
 1  A0 (10.0.0.1)  0.045 ms  0.007 ms  0.007 ms
 2  10.0.1.2 (10.0.1.2)  0.021 ms  0.012 ms  0.011 ms
 3  * * *
 4  10.0.3.20 (10.0.3.20)  0.033 ms  0.019 ms  0.020 ms
root@s1:/tmp/pycore.33223/s1.conf#
```

Figura 2: Execução do comando "traceroute -I" para o endereço IP do host h5

b. Registe e analise o tráfego ICMP enviado por s1 e o tráfego ICMP recebido como resposta. Comente os resultados face ao comportamento esperado.

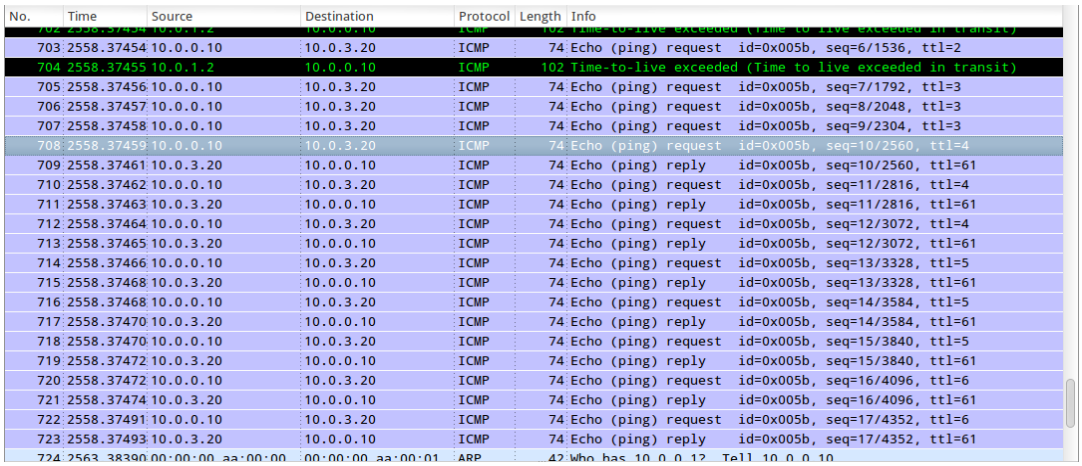
Através do comando *traceroute -I*, espera-se que sejam enviados um ou mais datagramas com o campo TTL (*Time to live)* = 1. Posteriormente, prevê-se que o mesmo suceda para valores incrementais do TTL na tentativa de obter a identificação dos routers durante o percurso até ao *host* h5.

Com a análise do tráfego ICMP enviado pelo servidor s1, foram enviados três datagramas com a mensagem "*Echo Request"* com TTL = 1, recebendo como resposta a mensagem "*Time To Live Exceeded*", o que indica que o servidor não conseguiu que o datagrama chegasse até ao host. Seguidamente, este processo repetiu-se para TTL = 2 e para TTL = 3, sendo que neste último, não foi obtido um "*Echo Reply"* para os respetivos "*Echo Request"*, sendo este ignorado por aconselhamento do docente. Por fim, a partir de TTL = 4, não é recebida a mensagem de controlo "*Time To Live Exceeded"*.



No.	Time	Source	Destination	Protocol	Length	Info
56	158.530567	00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	42	10.0.0.1 is at 00:00:00:aa:00:01
57	158.530570	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=1/256, ttl=1
58	158.530583	10.0.0.1	10.0.0.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
59	158.530590	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=2/512, ttl=1
60	158.530595	10.0.0.1	10.0.0.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
61	158.530599	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=3/768, ttl=1
62	158.530604	10.0.0.1	10.0.0.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
63	158.530608	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=4/1024, ttl=2
64	158.530627	10.0.1.2	10.0.0.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
65	158.530633	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=5/1280, ttl=2
66	158.530642	10.0.1.2	10.0.0.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
67	158.530646	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=6/1536, ttl=2
68	158.530655	10.0.1.2	10.0.0.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
69	158.530660	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=7/1792, ttl=3
70	158.530685	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=8/2048, ttl=3
71	158.530695	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=9/2304, ttl=3
72	158.530704	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=10/2560, ttl=4
73	158.530736	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x0055, seq=10/2560, ttl=61
74	158.530741	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=11/2816, ttl=4
75	158.530759	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x0055, seq=11/2816, ttl=61
76	158.530763	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x0055, seq=12/3072, ttl=4
77	158.530780	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x0055, seq=12/3072, ttl=61

Figura 3: Tráfego ICMP (1/2)



No.	Time	Source	Destination	Protocol	Length	Info
703	2558.37454	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=6/1536, ttl=2
704	2558.37455	10.0.1.2	10.0.0.10	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
705	2558.37456	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=7/1792, ttl=3
706	2558.37457	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=8/2048, ttl=3
707	2558.37458	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=9/2304, ttl=3
708	2558.37459	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=10/2560, ttl=4
709	2558.37461	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x005b, seq=10/2560, ttl=61
710	2558.37462	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=11/2816, ttl=4
711	2558.37463	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x005b, seq=11/2816, ttl=61
712	2558.37464	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=12/3072, ttl=4
713	2558.37465	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x005b, seq=12/3072, ttl=61
714	2558.37466	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=13/3328, ttl=5
715	2558.37468	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x005b, seq=13/3328, ttl=61
716	2558.37468	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=14/3584, ttl=5
717	2558.37470	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x005b, seq=14/3584, ttl=61
718	2558.37470	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=15/3840, ttl=5
719	2558.37472	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x005b, seq=15/3840, ttl=61
720	2558.37472	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=16/4096, ttl=6
721	2558.37474	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x005b, seq=16/4096, ttl=61
722	2558.37491	10.0.0.10	10.0.3.20	ICMP	74	Echo (ping) request id=0x005b, seq=17/4352, ttl=6
723	2558.37493	10.0.3.20	10.0.0.10	ICMP	74	Echo (ping) reply id=0x005b, seq=17/4352, ttl=61

Figura 4: Tráfego ICMP (2/2)

c. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o destino h5? Verifique na prática que a sua resposta está correta.

O valor inicial mínimo do campo TTL para que seja possível alcançar o destino h5 deve ser TTL = 4, o que se verifica uma vez que, a partir deste valor de TTL, são recebidas mensagens de controlo "*Echo Reply*".

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

O valor médio de ida-e-volta obtido foi de 0.024ms, sendo este alcançado a partir do cálculo da média aritmética entre os três valores obtidos.

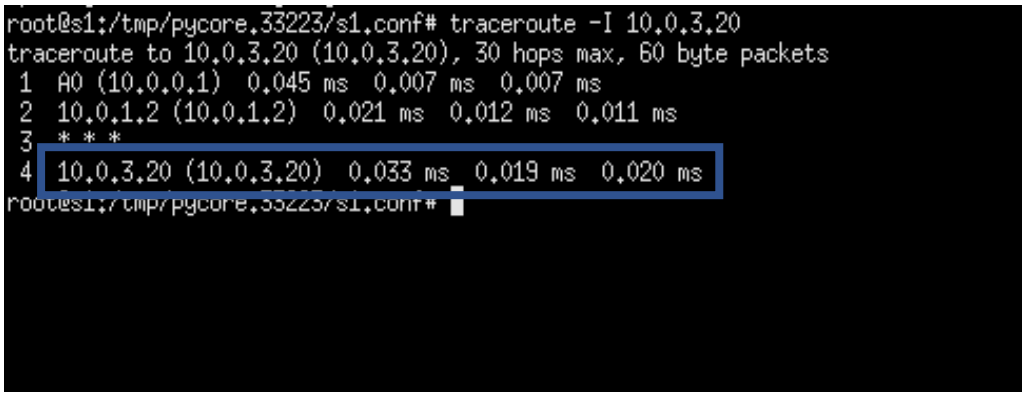


Figura 5: Round-Trip-Time

Questão 2

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

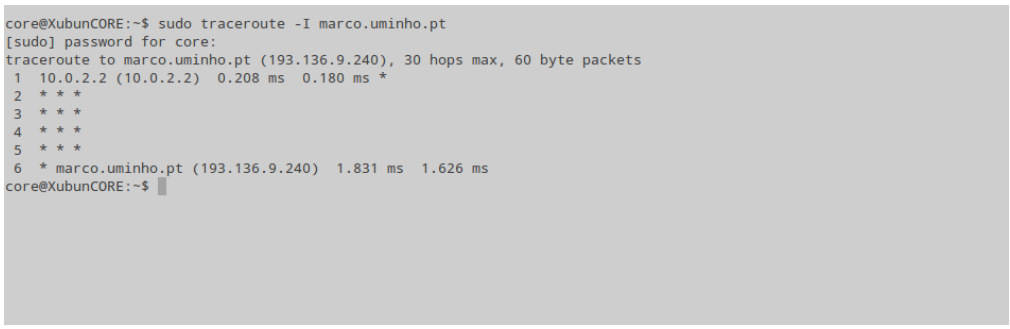


Figura 6: Comando "traceroute" para a máquina nativa

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

O endereço IP da interface ativa do computador usado é 10.0.2.15

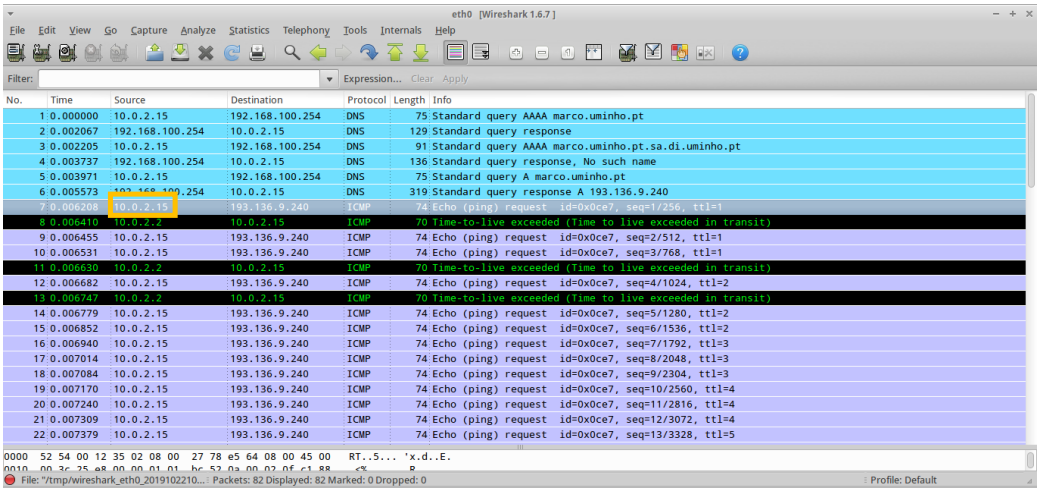


Figura 7: Tráfego capturado com o Wireshark

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

O valor do campo protocolo é "ICMP (1)". Este valor permite identificar de que protocolo procede o datagrama.

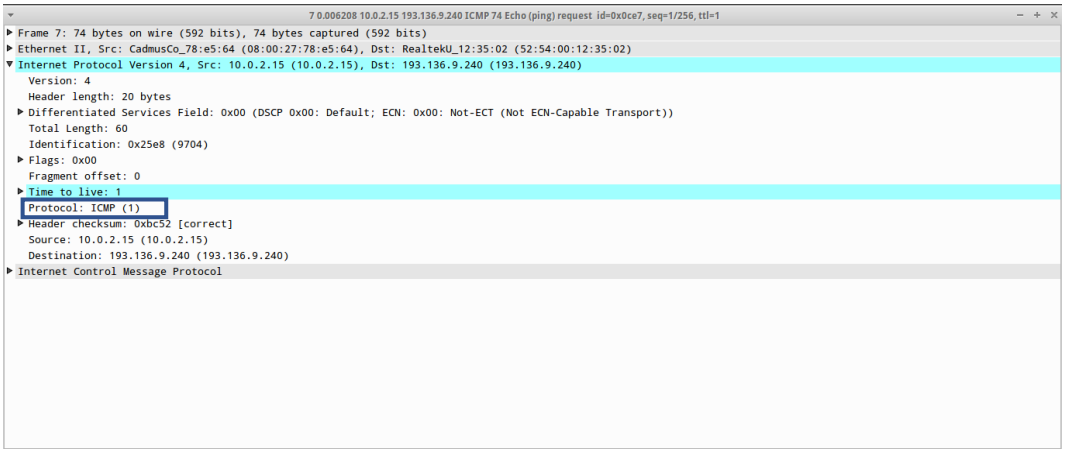


Figura 8: Informações sobre o datagrama-Campo Protocolo

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

O cabeçalho IP(v4) tem 20 bytes.

O tamanho do campo de dados (payload), foi calculado através da diferença entre o tamanho total do datagrama (60 bytes) e o tamanho do cabeçalho (20 bytes), concluindo-se assim que tem como tamanho 40 bytes.

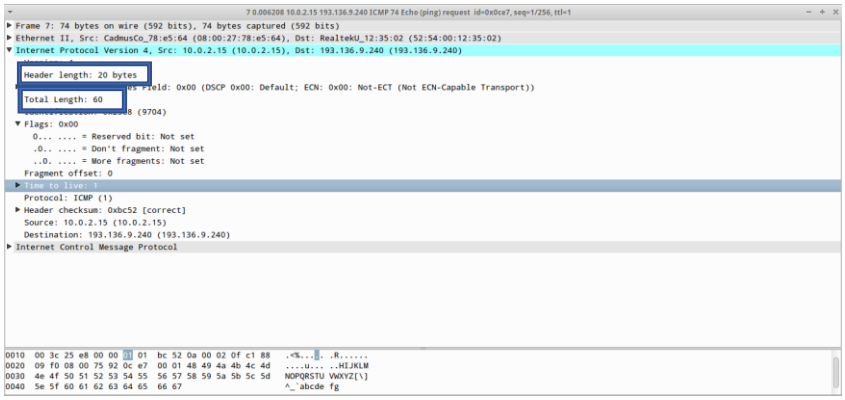


Figura 9: Informações sobre o datagrama-Campos Header length & Total Length

d. O datagrama IP foi fragmentado? Justifique.

Através da análise das *flags* concluiu-se que o datagrama IP não foi fragmentado, dado que "*Fragment offset=0"* e "*More fragments = Not set"*.

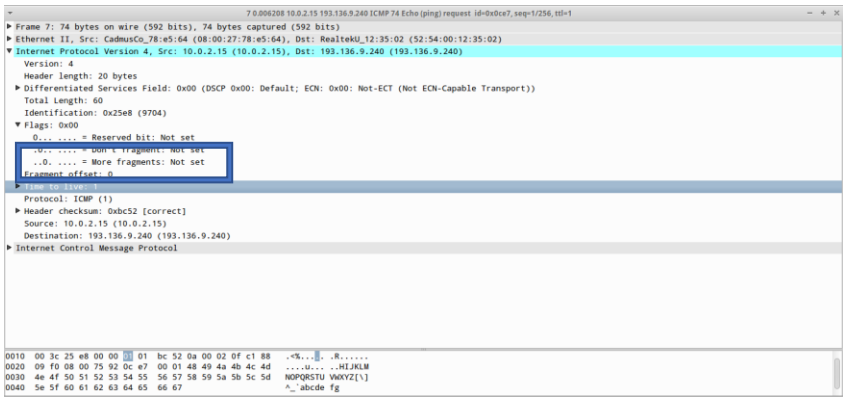


Figura 10: Informações sobre o datagrama-Análise das Flags

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.

Com a análise de três datagramas aleatórios de mensagens ICMP enviadas pelo computador em que foi feita a análise, foi verificado que, além da sua identificação e do *header checksum*, o campo TTL varia entre eles.

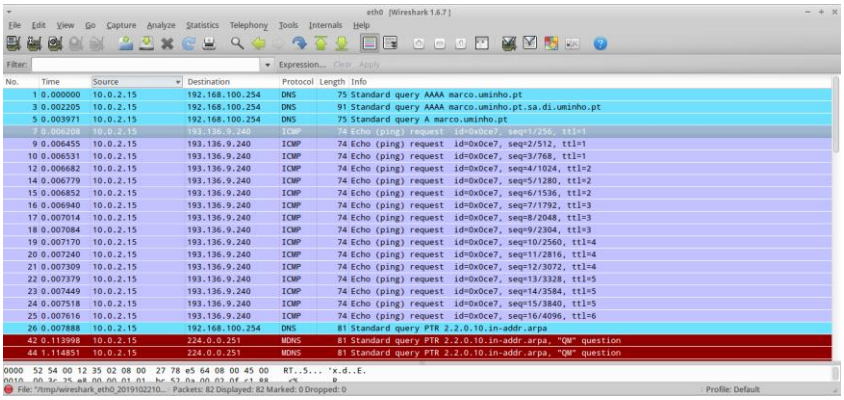


Figura 11: Análise do tráfego ordenado por Source

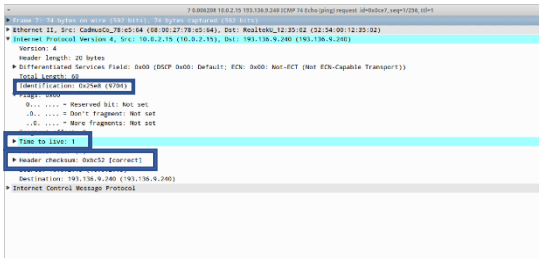


Figura 12: Informações sobre o datagrama (1/3)

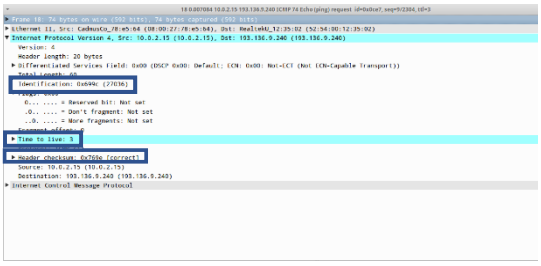


Figura 13. : Informações sobre o datagrama (2/3)

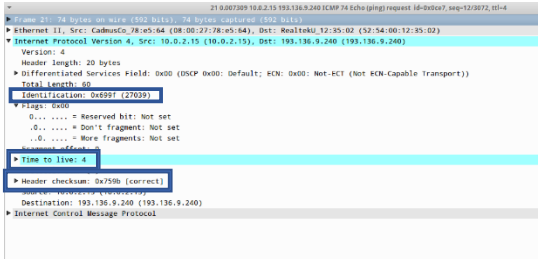


Figura 14: : Informações sobre o datagrama (3/3)

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

Ao ser feita a análise do tráfego no wireshark, concluiu-se que o TTL incrementa de três em três datagramas e o campo de identificação incrementa a cada datagrama.

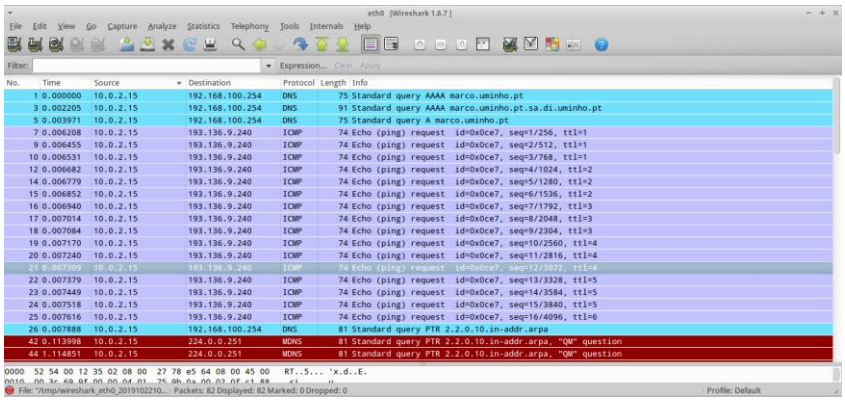


Figura 15: Análise de Trafego

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

O valor do campo TTL varia de acordo com a *source* da qual foi recebido o datagrama, logo se os datagramas corresponderem à mesma *source* o campo TTL permanecerá constante. Caso contrário, esse valor não permanecerá constante, irá variar.

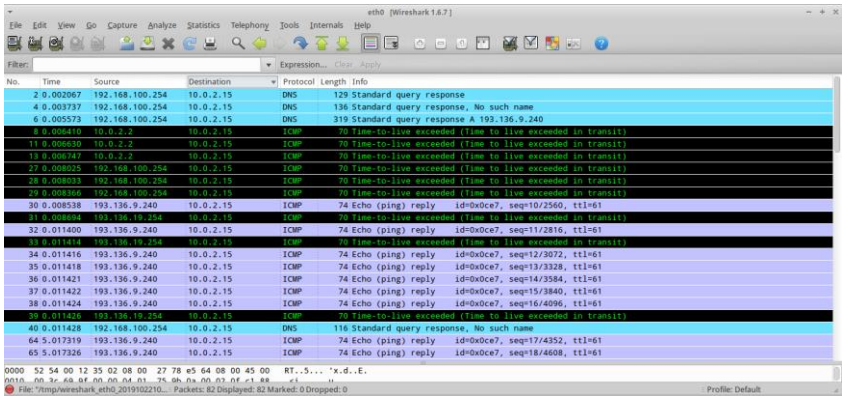


Figura 16: Tráfego ordenado por Destination

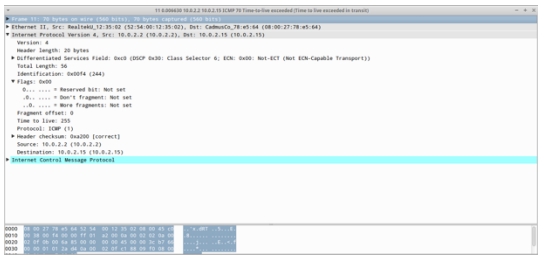


Figura 17: Informações sobre o datagrama (1/3)

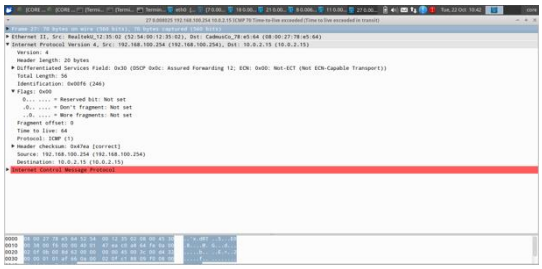


Figura 18: Informações sobre o datagrama (2/3)

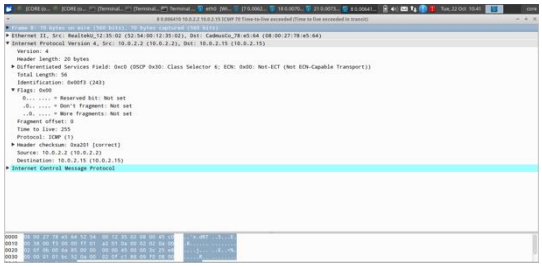


Figura 19: Informações sobre o datagrama (3/3)

Questão 3

Pretende-se agora analisar a fragmentação de pacotes IP. Reponha a ordem do tráfego capturado usando a coluna do tempo de captura. Observe o tráfego depois do tamanho de pacote ter sido definido para 42XX bytes.

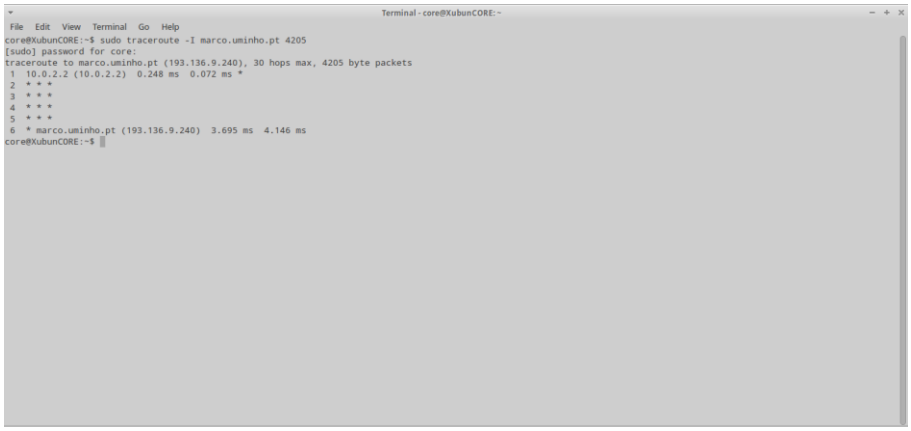


Figura 20: Comando "traceroute" para tamanho de pacote = 4205 bytes

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

Houve necessidade de fragmentar o pacote inicial pois o tamanho original do pacote é mais pequeno do que o *maximum transmission unit* (MTU), o que não permite que o pacote original, como um todo, consiga ser enviado.

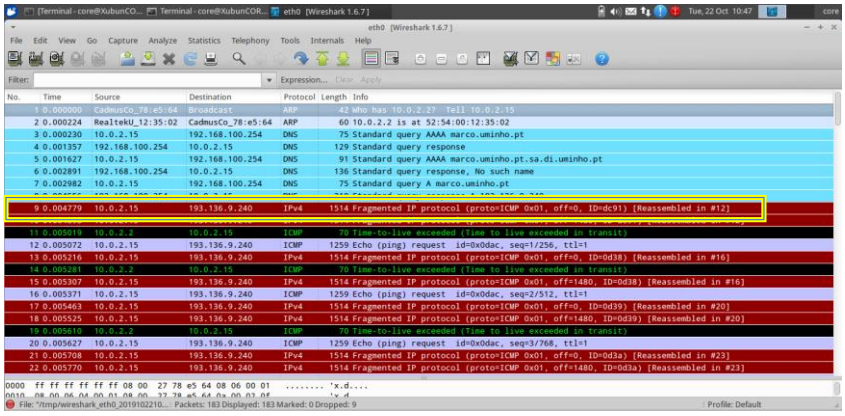


Figura 21: Verificação da fragmentação da primeira mensagem ICMP

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

A informação presente no cabeçalho permitiu a conclusão de que o datagrama foi fragmentado, uma vez que a *flag* "*More fragments*" se encontra a "*Set*", o que indica que existem outros fragmentos desse datagrama. É possível afirmar que se trata do primeiro fragmento, visto que o valor de "*Fragment offset"* é zero.

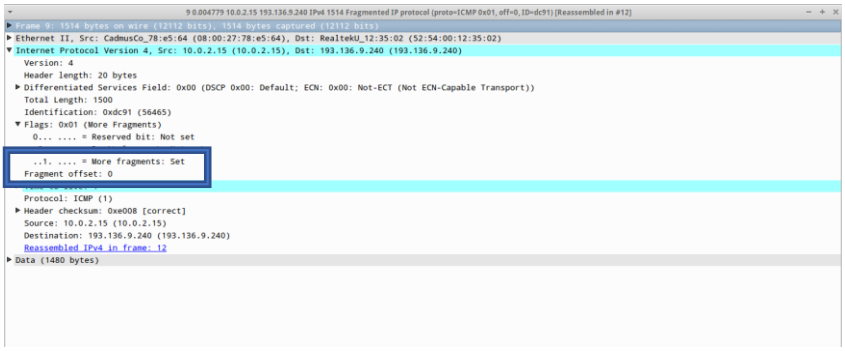


Figura 22: Análise do primeiro fragmento do datagrama

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

O que permite concluir que não se trata do primeiro fragmento é o campo "*Fragment offset"* se encontrar diferente de zero, neste caso, 1480. Existem mais fragmentos, uma vez que o campo "*More fragments"* se encontra a "*Set*".

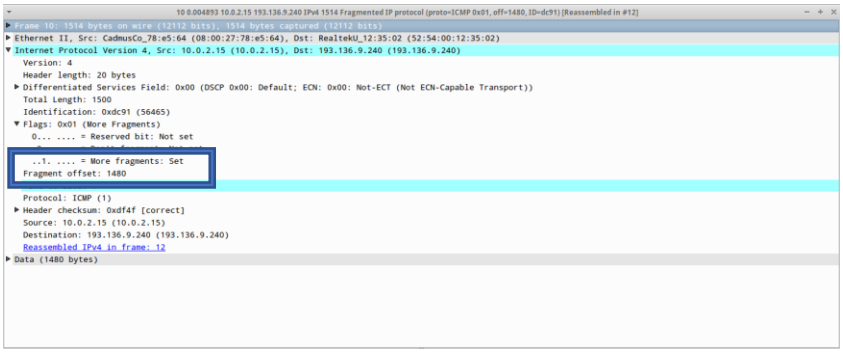


Figura 23: Análise do segundo fragmento do datagrama

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

A partir do datagrama original foram criados três fragmentos. Além dos especificados nas figuras 22 e 23, também o fragmento impresso na figura 24. Neste é possível concluir que é o último fragmento, pois os campos "*Fragments offset"* é diferente de zero, indicando que não é o primeiro fragmento e "*More fragments"* se encontra a "*Not set",* indicando que não existem mais fragmentos após este.

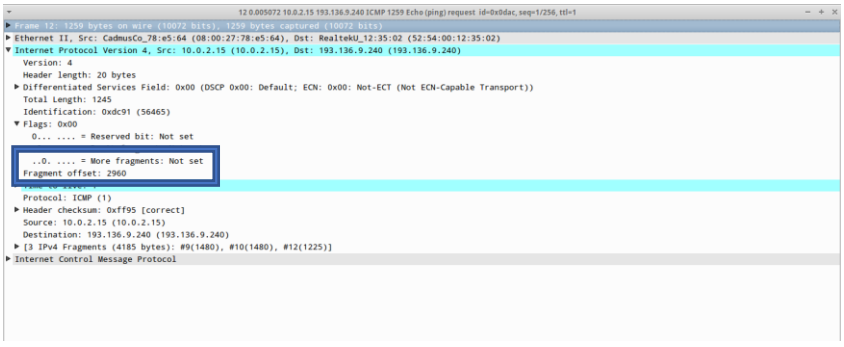


Figura 24: Análise do último fragmento do datagrama

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

Para que seja possível a reconstrução do datagrama original é preciso ter em atenção a ordem dos fragmentos. Essa ordem pode ser desvendada através da análise das *flags*.

Quanto ao primeiro fragmento, observa-se que o campo "*More fragments"* se encontra a "*Set",* indicando que existem mais fragmentos para além do atual e o "*Fragment offset"* toma o valor de zero, mostrando que é o primeiro fragmento.

Quanto ao último fragmento, verifica-se que o campo "*More fragments*" se encontra a "*Not set"*, o que indica que não há mais fragmentos após este, e "*Fragment offset"* diferente de zero.

Entre estes dois limites, podem ser encontrados mais fragmentos, cujos valores do campo "*Fragment offset"* são progressivamente maiores, entre zero e "*Fragment offset"* do último fragmento e o campo "*More Fragments"* encontra-se a "*Set".*

2. Parte II: Endereçamento e Encaminhamento IP

2. Questões e Respostas

Questão 1
Atenda aos endereços IP atribuídos automaticamente pelo CORE aos diversos equipamentos da topologia.

a. Indique que endereços IP e máscaras de rede foram atribuídos pelo CORE a cada equipamento. Para simplificar, pode incluir uma imagem que ilustre de forma clara a topologia definida e o endereçamento usado.

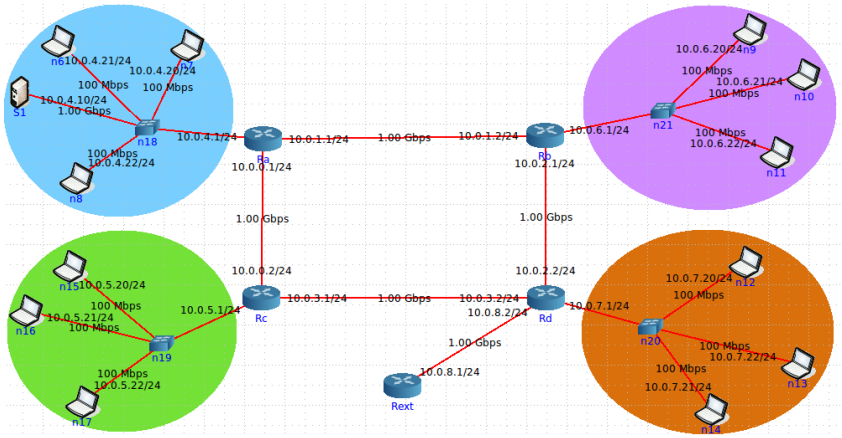


Figura 25: Endereços IP - Topologia Core

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

Tratam-se de endereços privados, uma vez que se encontram no intervalo 10.0.0.0 a 10.255.255.255.

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

Não são atribuídos endereços IP aos switches dado que se tratam de *ethernet switches* pelo que estes, ao se encontrarem na camada "*Link Layer"*, utilizam os endereços MAC dos datagramas recebidos em vez dos endereços IP.

d. Usando o comando ping certifique-se que existe conectividade IP entre os laptops dos vários departamentos e o servidor do departamento A.

Com a utilização do comando "*ping"* foi possível comprovar que existe conectividade entre os laptops dos quatro departamentos com o servidor do departamento A.

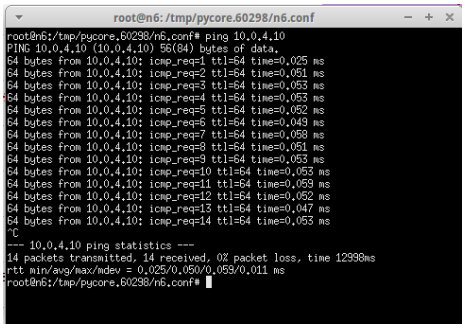


Figura 26: Execução do comando ping (Laptop n6-Servidor)

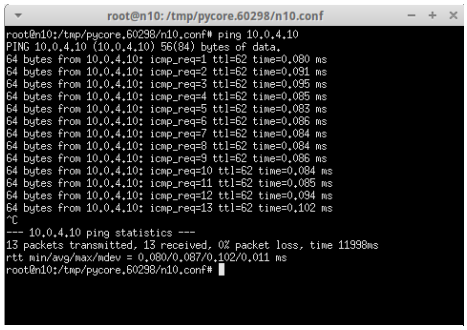


Figura 27: Execução do comando ping (Laptop n10-Servidor)

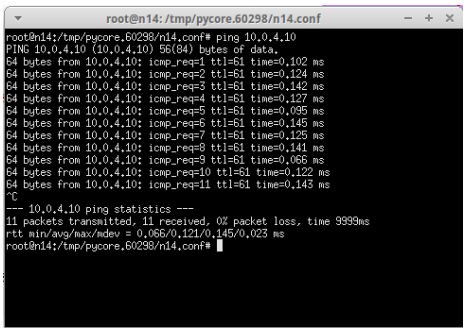


Figura 28: Execução do comando ping (Laptop n14-Servidor)

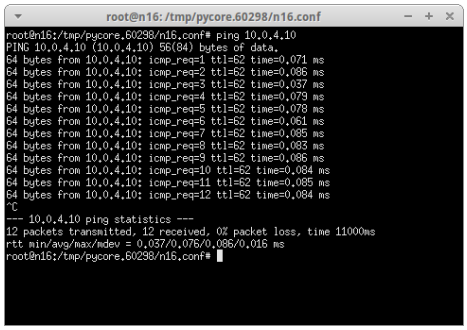


Figura 29: Execução do comando ping (Laptop n16-Servidor)

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

Através do comando "*ping*" foi possível verificar a conectividade IP do router de acesso Rext para o servidor S1.

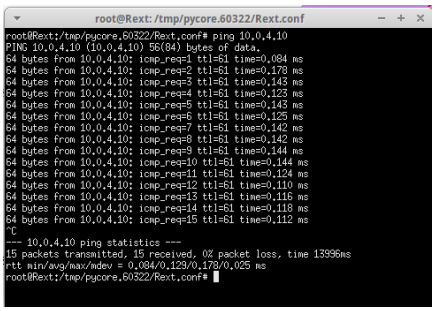


Figura 26: Execução do comando ping (Router de acesso Rext-Servidor)

Questão 2

Para o router e um laptop do departamento B:

a. Execute o comando netstat –rn por forma a poder consultar a tabela de encaminhamento unicast (IPv4). Inclua no seu relatório as tabelas de encaminhamento obtidas; interprete as várias entradas de cada tabela. Se necessário, consulte o manual respetivo (man netstat).

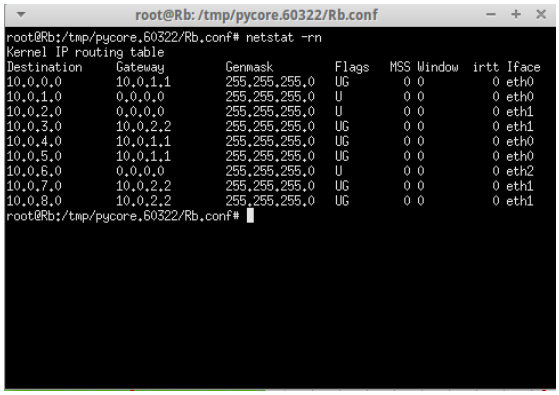


Figura 31: Tabela de encaminhamento - Router Rb

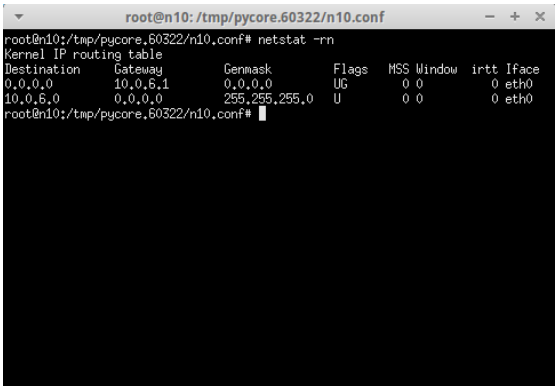


Figura 32: Tabela de encaminhamento - Laptop n10

- ***Destination:*** Indica a sub-rede de destino.
- **Gateway:** Indica o caminho a percorrer pelo tráfego até este chegar ao destino.
- **Genmask:** Indica o tipo de máscara da sub-rede utilizada.
- **Flags:**
  - **U:** *Flag* que indica rota válida.
  - **UG:** *Flag* que indica rota válida e ligação a um *Gateway.*
- **MSS:** Sigla para "*Maximum Segment Size",* parâmetro que especifica a maior quantidade de dados (em *bytes)* que um dispositivo pode receber num único segmento TCP.
- **Iface:** Tipo de interface para onde os pacotes irão ser enviados.

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

Através da análise dos processos obtidos através do comando "ps ax" foi possível concluir-se que está a ser usado encaminhamento dinâmico, uma vez que é possível encontrar o protocolo de roteamento OSPF (*"Open Shortest Path First").* Este protocolo indica que as rotas são atualizadas ao longo do tempo.

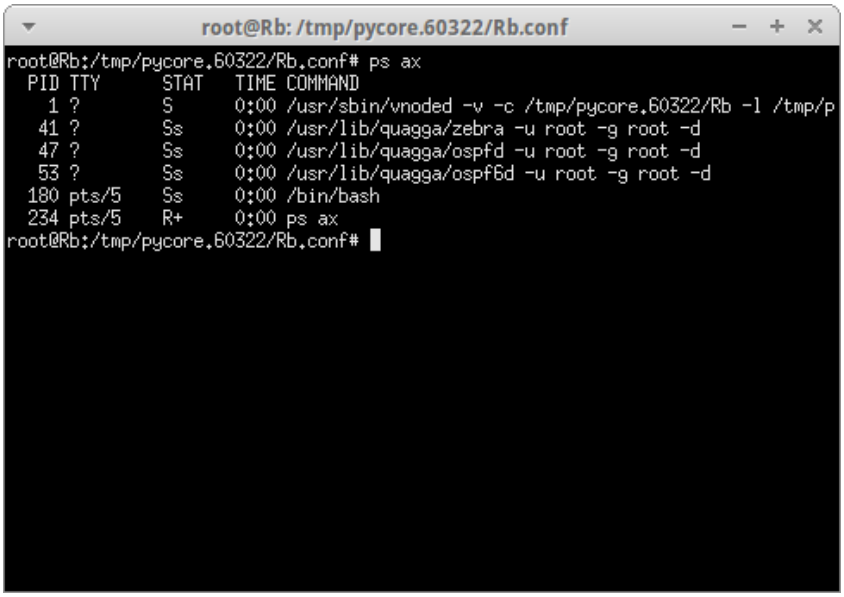


Figura 27: Execução do comando "ps ax" para análise de processos

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

De modo a eliminar a rota por defeito executou-se o comando "route delete default". Para testar as implicações que esta ação traz, realizamos novamente o comando "ping" para testar a conectividade entre o servidor S1 e um laptop de cada departamento.

Com a análise dos resultados concluiu-se que para o laptop que se encontra na mesma sub-rede do servidor S1 continuou a existir conectividade entre ambos, enquanto que laptops fora dessa rede local deixaram de conseguir comunicar com S1. Essa impossibilidade deve-se à ausência da rota a seguir no caso de não existir uma entrada especifica na tabela para a rede destino.

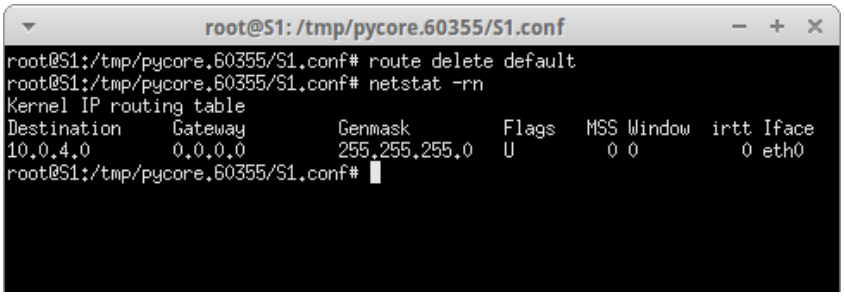


Figura 28: Execução do comando "Route delete" para eliminar a rota por defeito

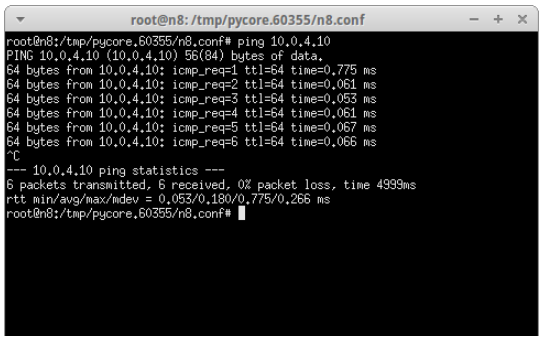


Figura 35: Comando ping (Laptop n8 - Servidor S1)

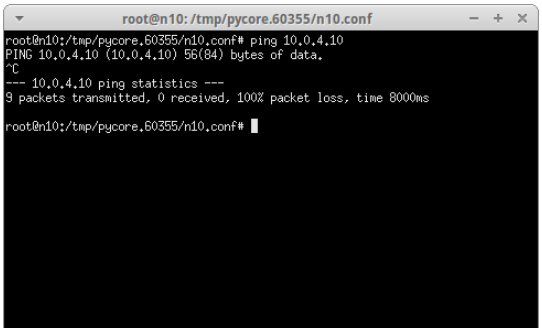


Figura 36: Comando ping (Laptop n10 - Servidor S1)

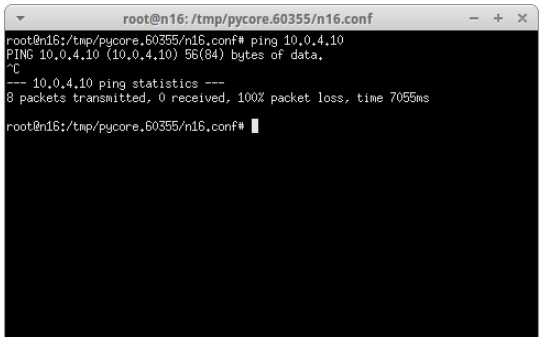


Figura 37: Comando ping (Laptop n16 - Servidor S1)

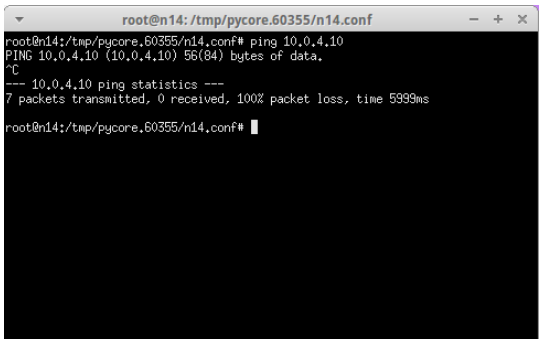


Figura 38: Comando ping (Laptop n14 - Servidor S1)

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

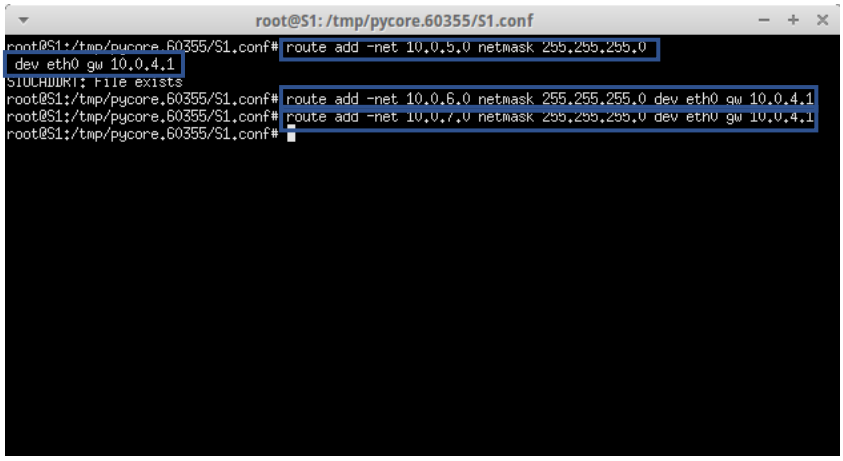


Figura 39: Execução do comando "route add" para os diferentes sub-redes

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

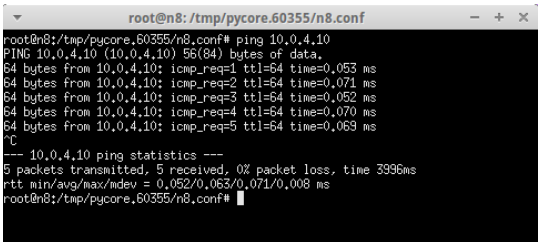


Figura 40: Comando ping (Laptop n8 - Servidor S1)

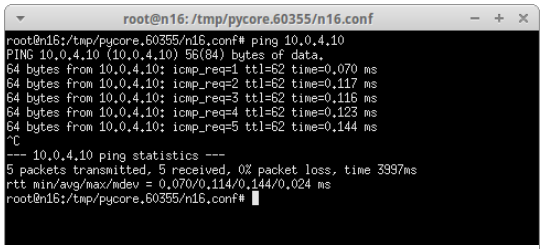


Figura 41: Comando ping (Laptop n16 - Servidor S1)

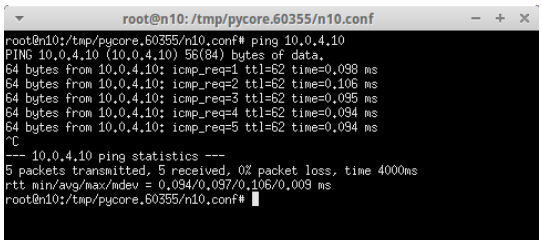


Figura 42: Comando ping (Laptop n10 - Servidor S1)

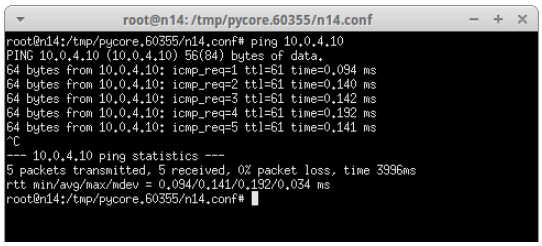


Figura 43: Comando ping (Laptop n14 - Servidor S1)

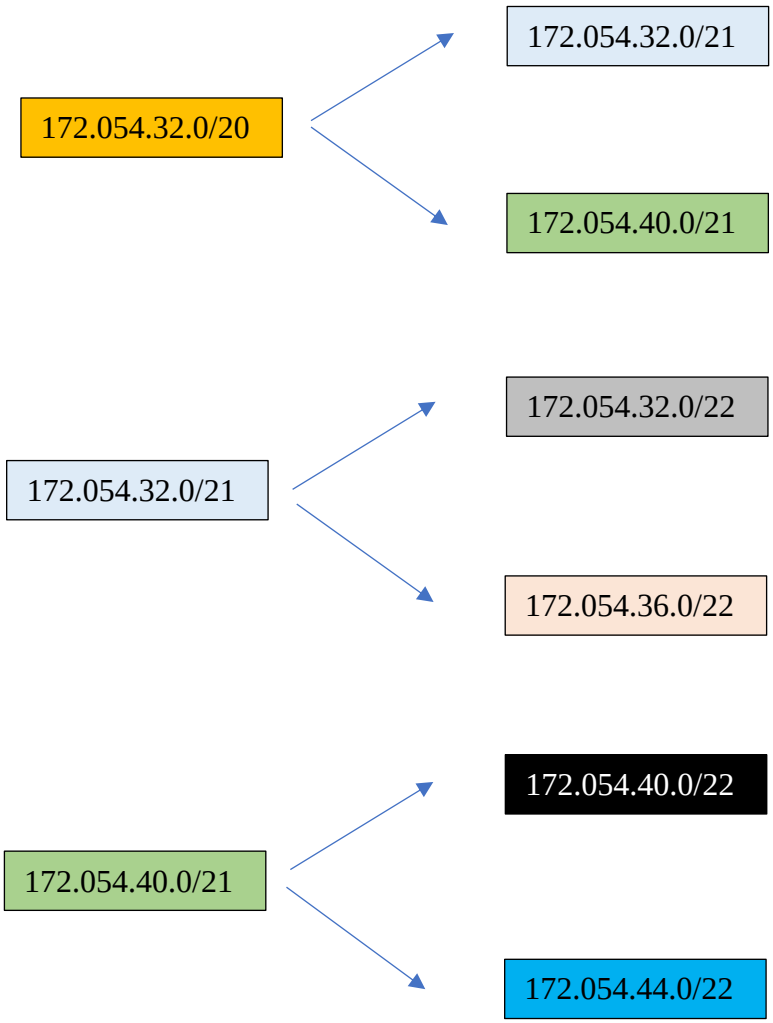
Figura 44: Nova tabela de encaminhamento do servidor S1

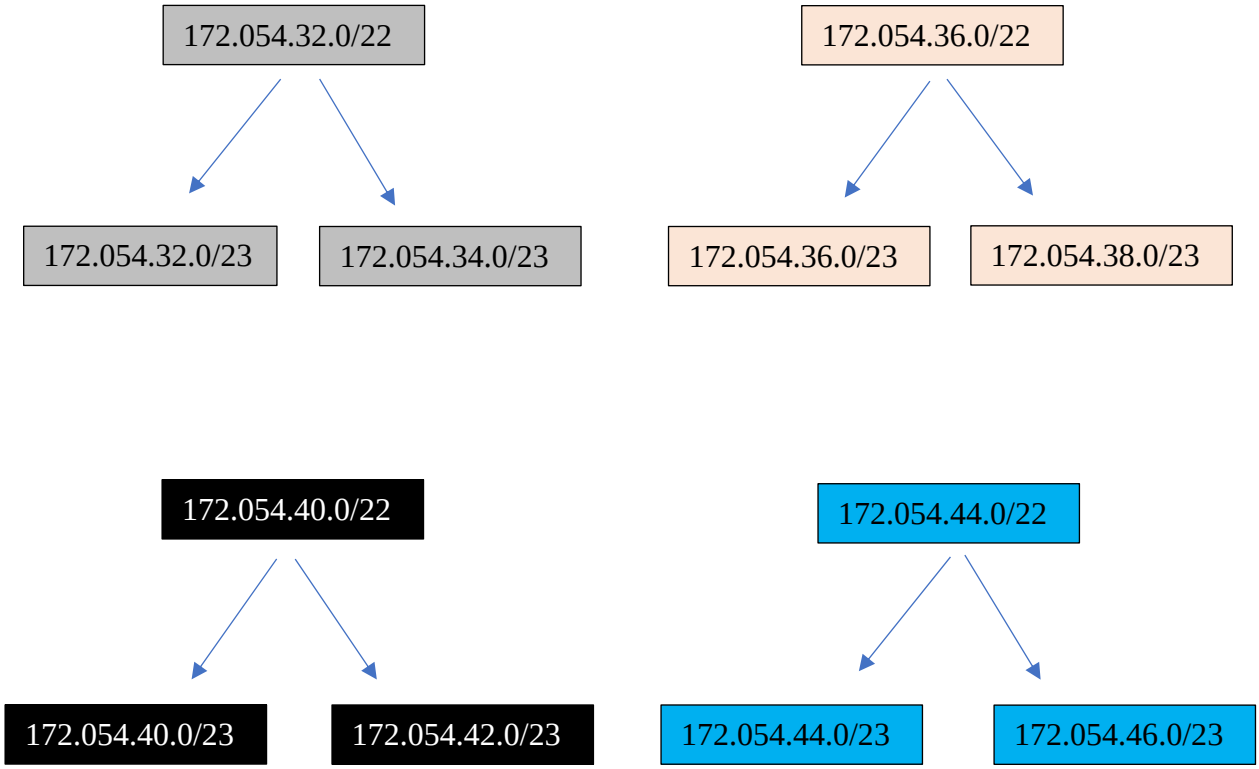
2.1. Parte II: Definição de Sub-redes

Questão 1

Considere que dispõe apenas do endereço de rede IP 172.yyx.32.0/20, em que "yy" são os dígitos correspondendo ao seu número de grupo (Gyy) e "x" é o dígito correspondente ao seu turno prático (PLx). 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.

Sendo o endereço inicial 172.054.32.0/20, tem-se:





O processo realizado anteriormente deve-se ao facto de ser necessário atribuir uma sub-rede a cada um dos quatro departamentos, ou seja, uma totalidade de quatro sub-redes.

Inicialmente, dividiu-se o endereço de rede IP inicial (172.054.32.0/20) em dois endereços, visto que ainda não era suficiente para endereçar os quatro departamentos, continuou-se a divisão e ficou-se com quatro endereços. No entanto, como os endereços tudo a 1´s e o tudo a 0´s são reservados, continua-se com a problemática referida anteriormente, por isso houve necessidade de se voltar a dividir.

Por fim, obteve-se oito endereços e apesar de dois destes se encontrarem reservados, ainda se consegue usufruir de seis, embora só seja preciso quatro para endereçar os departamentos (escolheu-se aleatoriamente o endereço 172.054.36.0/23 para o departamento A, o 172.054.44.0/23 para o departamento B, o 172.054.40.0/23 para o departamento C e 172.054.48.0/23 para o departamento D).

Relativamente à parte do host do endereço foram mantidos os valores atribuídos na topologia inicial realizada no CORE.

A topologia CORE após as alterações referidas encontra-se representada na figura 45.

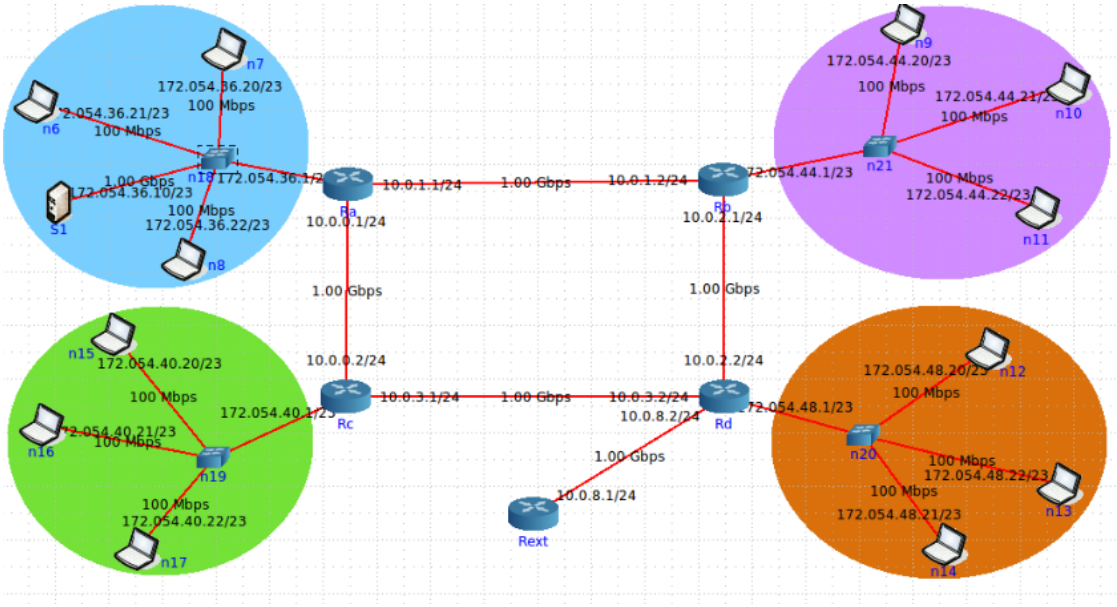


Figura 45: Topologia CORE atualizada com subnetting

Questão 2

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

A máscara de rede usada (em notação decimal) foi 255.255.254.0.

11111111 11111111 11111110 00000000

Dado que em notação CIDR: /23

Questão 3

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

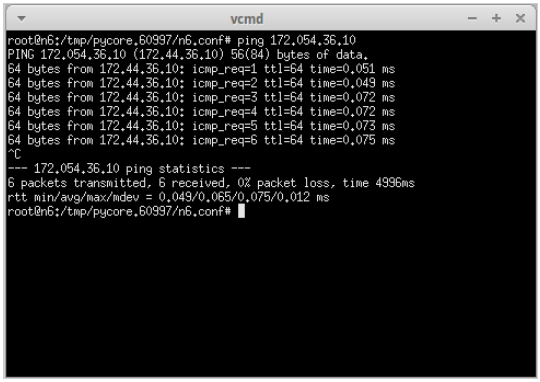


Figure 46: Comando ping (Laptop n6 - Servidor S1)

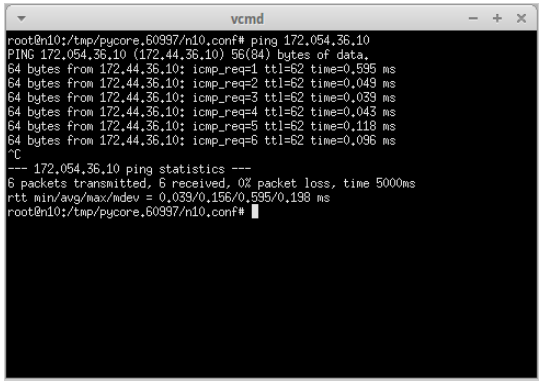


Figure 47: Comando ping (Laptop n10 - Servidor S1)

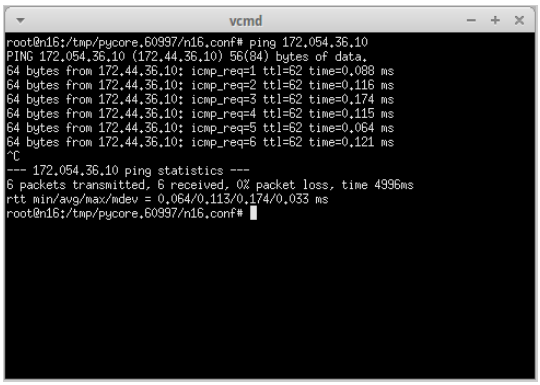


Figure 48: Comando ping (Laptop n16 - Servidor S1)

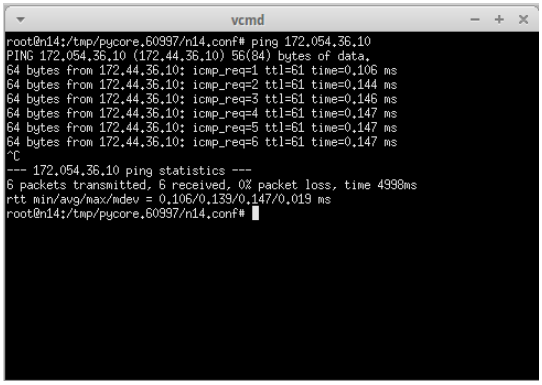


Figure 49: Comando ping (Laptop n14 - Servidor S1)

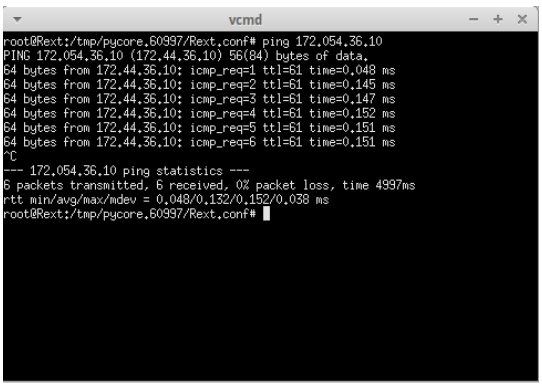


Figure 50: Comando ping (Router Rext - Servidor S1)

3. Conclusões

A realização do presente trabalho permitiu ao grupo aprender a utilizar ferramentas de simulação, nomeadamente o CORE e de captura de tráfego, o WIRESHARK.

Numa primeira etapa, analisou-se o tráfego de rede utilizando o comando "traceroute" de forma a conseguir descobrir a rota desde uma origem IP até um destino IP, em que para isto foram dados vários valores de TTL para a análise. Seguidamente observou-se as várias características dos datagramas, como por exemplo, o seu tamanho total e do cabeçalho IP (em bytes), o protocolo a ele associado e ainda se verificou o funcionamento da fragmentação nestes pacotes.

Numa segunda etapa, foi realizado um protótipo no CORE constituído por routers ligados a alguns departamentos com diversos laptops, um servidor localizado num dos departamentos, switches e um router externo que assegura a conetividade externa. A partir desta topologia, observou-se tabelas de encaminhamento, nas quais foi possível verificar as diferentes rotas e o tipo de encaminhamento associado. Foi também constatado o impacto de remover a rota existente por defeito na tabela, para contornar esta situação, adicionou-se as rotas necessárias para repor a conectividade. Para definir o novo esquema de endereçamento aplicaram-se os conceitos de subnetting lecionados, o que inicialmente se mostrou um desafio para os integrantes do grupo, no entanto com a ajuda do docente e posteriores pesquisas tornou-se uma barreira ultrapassada com sucesso.

Por fim, o grupo adquiriu conhecimentos análogos ao funcionamento do protocolo IP e a forma como estes endereços estão atribuídos em todo o protótipo, concluindo assim, que estes foram alcançados e o conteúdo programático bem cimentado e compreendido.