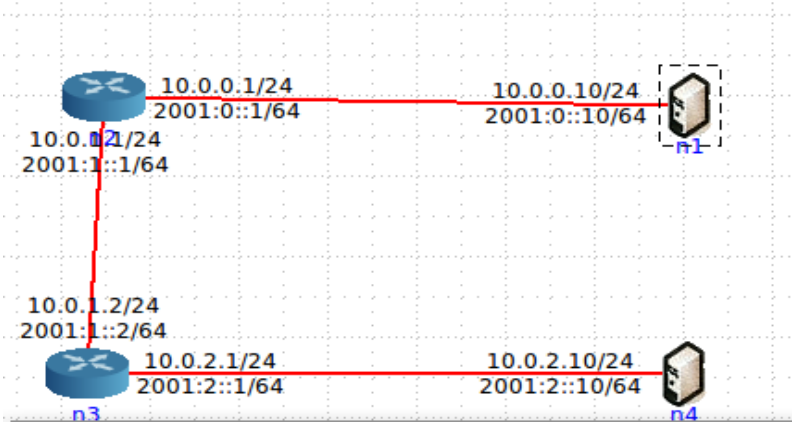
TP4

GRUPO 4.9

1ªParte

1. Prepare uma topologia CORE para verificar o comportamento do traceroute. Ligue um host n1 a um router n2; o router n2 a um router n3 que, por sua vez, se liga a um host n4.
    a. Active o *wireshark* ou o *tcpdump* no nó 1. Numa *shell* de n1, execute o comando *traceroute -I* para o endereço IP do *host* n4.



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

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:52:05.950944 IP (tos 0x0, ttl 1, id 15399, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 1, length 40
11:52:05.951001 IP (tos 0xc0, ttl 64, id 7020, offset 0, flags [none], proto ICMP (1), length 88)
    A0 > A9: ICMP time exceeded in-transit, length 68
        IP (tos 0x0, ttl 1, id 15399, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 1, length 40
11:52:05.953623 IP (tos 0x0, ttl 1, id 15400, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 2, length 40
11:52:05.953664 IP (tos 0xc0, ttl 64, id 7021, offset 0, flags [none], proto ICMP (1), length 88)
    A0 > A9: ICMP time exceeded in-transit, length 68
        IP (tos 0x0, ttl 1, id 15400, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 2, length 40
11:52:05.953744 IP (tos 0x0, ttl 1, id 15401, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 3, length 40
11:52:05.953764 IP (tos 0xc0, ttl 64, id 7022, offset 0, flags [none], proto ICMP (1), length 88)
    A0 > A9: ICMP time exceeded in-transit, length 68
        IP (tos 0x0, ttl 1, id 15401, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 3, length 40
11:52:05.953820 IP (tos 0x0, ttl 2, id 15402, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 4, length 40
11:52:05.953858 IP (tos 0xc0, ttl 63, id 59501, offset 0, flags [none], proto ICMP (1), length 88)
    10.0.1.2 > A9: ICMP time exceeded in-transit, length 68
        IP (tos 0x0, ttl 1, id 15402, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 4, length 40
11:52:05.954285 IP (tos 0x0, ttl 2, id 15403, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 5, length 40
11:52:05.954330 IP (tos 0xc0, ttl 63, id 59502, offset 0, flags [none], proto ICMP (1), length 88)
    10.0.1.2 > A9: ICMP time exceeded in-transit, length 68
        IP (tos 0x0, ttl 1, id 15403, offset 0, flags [none], proto ICMP (1), length 60)
    A9 > 10.0.2.10: ICMP echo request, id 75, seq 5, length 40
```

O tráfego ICMP enviado por n1 para 10.0.2.10 como não existe segurança na rede são enviados 3 datagramas com o mesmo TTL de cada vez, como podemos reparar pela figura só a partir do 6 (não incluído) é que este começa a receber resposta que foi possível encontrar, o que indica que usou no caso do 7 TTL = 3.

c. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o destino n4? Qual o tempo médio de ida-e-volta (RTT - round-trip time) obtido?

O tempo mínimo necessário para alcançar n4 será de 3.

Quanto ao RTT será a media dos tempos obtidos:

1: (0.078+0.058+0.025)/3 = 0.0536(6) ms

2: (0.043+0.053+0.061)/3 = 0.0523(3) ms

3: (0.060+0.090+0.048)/3 = 0.066 ms

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

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

```
Source: 192.168.100.187 (192.168.100.187)
Destination: 193.136.9.254 (193.136.9.254)
```

O endereço ip da interface do meu computador é o endereço “Source”, o 192.168.100.187

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

```
Protocol: ICMP (1)
```

O campo protocolo tem valor 1, que indica o tipo de protocolo, neste caso trata-se de ICMP.

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?

```
Header Length: 20 bytes
⊞ Differentiated Services Field:
Total Length: 112
```

O cabeçalho tem 20bytes. Se ao tamanho total (“Total Length”) retirarmos os bytes do cabeçalho ficamos com o payload. 112-20= 92 bytes de payload.

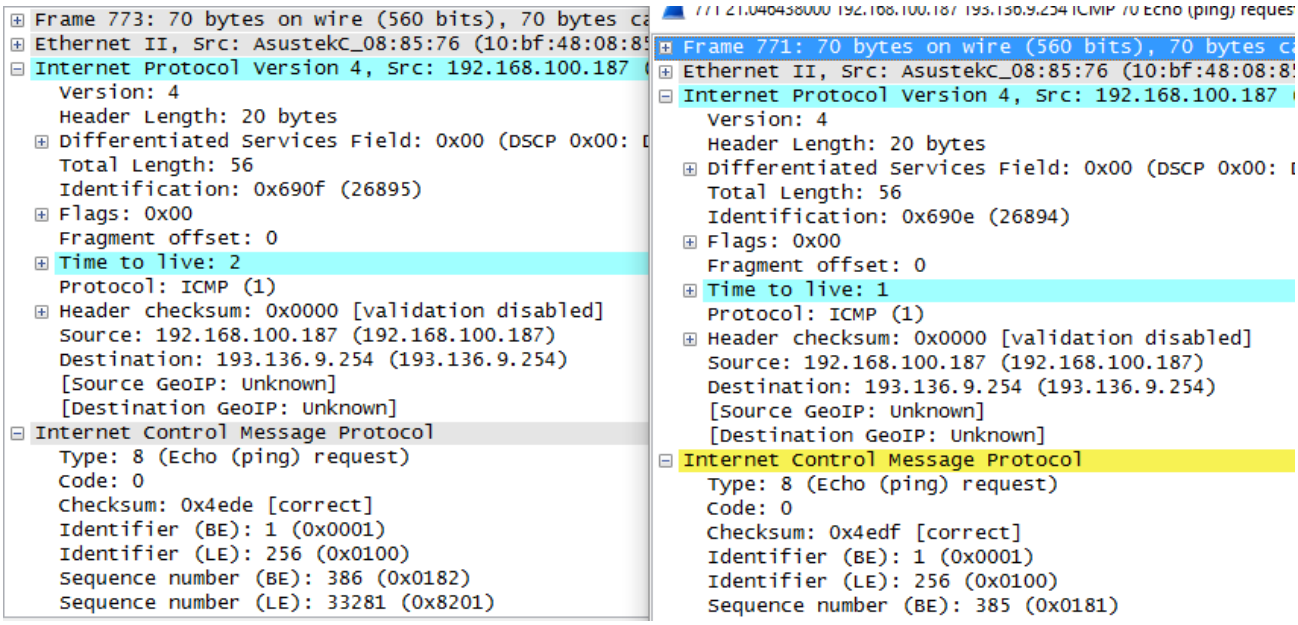
d. O datagrama IP foi fragmentado? Justifique

```
⊟ Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
```

A partir da informação das flags vemos que não foi fragmentado pois “More Fragmentes” = “Not set”, não havendo fragmentos. Para além disto temos o offset a 0.

e. Ordene os pacotes capturados de acordo com o endereço IP fonte (e.g., selecionando o cabeçalho da coluna Source), e analise a sequência de tráfego ICMP com base no IP gerado na sua máquina. Quais os campos do datagrama IP cujo valor muda sempre na série de mensagens ICMP enviadas pelo seu computador?

O “Time to live”, “Identification”, “Checkum” e o “Sequence Number” (BE e LE)



f. Que campos se mantêm constantes? Que campos se devem manter, preferencialmente, constantes? Justifique.

Ambos os Ips, de origem e de destino, o tipo, visto se tratar sempre do mesmo tipo de mensagem, o protocolo, sendo este sempre o mesmo, ICMP, e o header que conterá informação importante. Apesar de ser sempre 20, este poderá ser maior conforme as opções.

g. Observa algum padrão nos valores do campo de Identificação do datagrama IP?

Estes estão sequenciados.

h. A seguir (com os pacotes ordenados por endereço destino) encontre a série de respostas ICMP TTL exceeded enviadas ao seu computador pelo primeiro router. Qual é o valor dos campos Identificação e TTL?

O ttl é 1 pois o tempo de vida termina e a identificação vai corresponder com o request feito anteriormente

i. Esses valores permanecem constantes para todas as mensagens de resposta ICMP TTL exceeded enviados pelo primeiro router ao seu host? Porquê?

O identificador vai mudando conforme o request que enviou, o ttl é sempre 1 pois trata-se de replies.

3. Pretende-se agora analisar a fragmentação de pacotes IP. Reponha a ordem do tráfego capturado usando a coluna do tempo de captura.
   a. Localize a primeira mensagem ICMP depois do tamanho de pacote ter sido definido em 3072 bytes. A mensagem foi fragmentada? Porque é que houve (ou não) necessidade de o fazer?

```
[3 IPv4 Fragments (3052 bytes): #30(1480), #31(1480), #32(92)]
    [Frame: 30, payload: 0-1479 (1480 bytes)]
    [Frame: 31, payload: 1480-2959 (1480 bytes)]
    [Frame: 32, payload: 2960-3051 (92 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3052]
    [Reassembled IPv4 data: 0800dfb40001010530455069 6e67506c6f74746572342e31...]
```

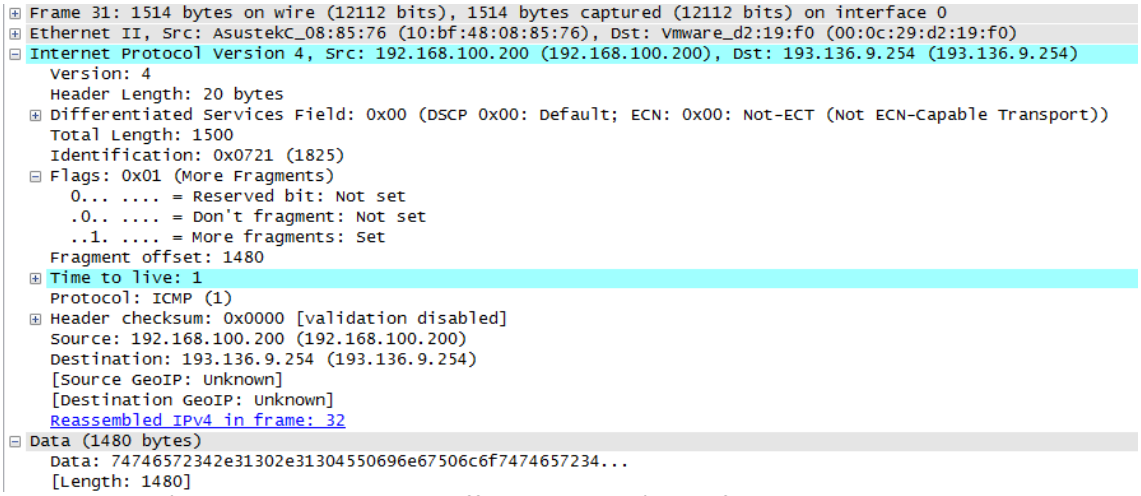
A mensagem foi fragmentada pois sendo demasiado grande teve de a dividir. Neste caso em 3 fragmentos.

   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?

```
Internet Protocol Version 4, Src: 192.168.100.200 (192.168.100.200), Dst: 193.136.9.254 (193.136.9.254)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 1500
    Identification: 0x0721 (1825)
  ⊟ Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 0
  ⊞ Time to live: 1
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 192.168.100.200 (192.168.100.200)
    Destination: 193.136.9.254 (193.136.9.254)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 32
⊟ Data (1480 bytes)
    Data: 0800dfb40001010530455069 6e67506c6f74746572342e31...
    [Length: 1480]
```

Temos a indicação “Reassembled IPv4 in frame: 32” ou seja, é um fragmento que vai ser reconstruído na trama 32. Como podemos ver temos o “More Frements” = set, ou seja existem mais fragmentos para além deste. Trata-se do primeiro fragmento pois tem o offset a 0, ou seja é o primeiro, o segundo vai ter o offset a 1480. Tem no total 1500, 1480 de dados e 20 de header.

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?



Não é o primeiro pois tem o offset a 1480. Há mais fragmentos pois conseguimos ver na flag que “More Fragments” = set.

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

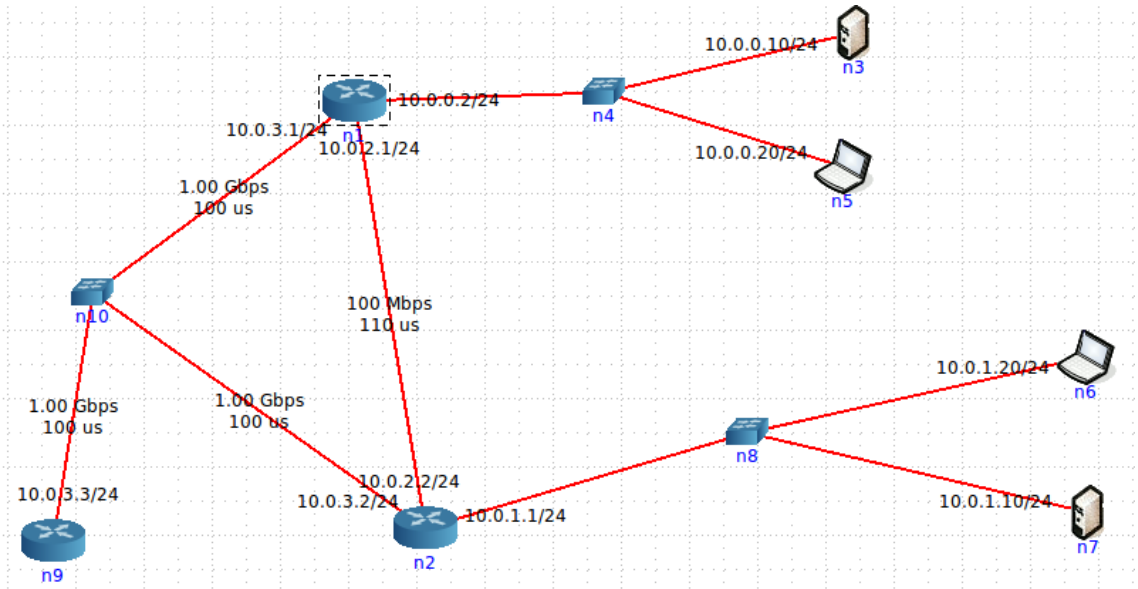
Como já explicado na alínea b), e na a), vamos ter 3 fragmentos que vão ser reconstruídos na trama 32, ou seja, a trama 32 vai ser o ultimo fragmento

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

Os campos que mudam são o offset dos fragmentos, e a identificação de cada. Através do offset vai-se reconstruir o datagrama, pois o offset fornece a posição de cada fragmento.

2ªParte

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 automaticamente pelo CORE a cada equipamento. (Pode incluir uma imagem que ilustre de forma clara a topologia e o endereçamento).



N1 to N4:	ip=10.0.0.2	Mascara de rede= 255.255.255.0
N2 to N8:	ip = 10.0.1.1	Mascara de rede= 255.255.255.0
N1 to N2:	ip=10.0.2.1	Mascara de rede= 255.255.255.0
N1 to N10:	ip=10.0.3.1	Mascara de rede= 255.255.255.0
N2 to N1:	ip=10.0.2.2	Mascara de rede= 255.255.255.0
N2 to N10:	ip=10.0.3.2	Mascara de rede= 255.255.255.0
N3:	ip= 10.0.0.10	Mascara de rede= 255.255.255.0
N5:	ip=10.0.0.20	Mascara de rede= 255.255.255.0
N6:	10.0.1.20	Mascara de rede= 255.255.255.0
N7:	10.0.1.10	Mascara de rede= 255.255.255.0

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

São endereçamentos privados pois foram endereços criados dentro de um espaço sem os deixar diretamente expostos a internet.

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

Trata-se de uma ethernet switch que troca pacotes ethernet. Ao nível dos pacotes ethernet não à necessidade de endereços IP.

d. Usando o comando *ping* certifique-se que existe conectividade total entre os sistemas em ligados em rede (basta certificar a conectividade para uma interface de cada rede).

```
root@n6:/tmp/pycore.55068/n6.conf# ping 10.0.1.10
PING 10.0.1.10 (10.0.1.10) 56(84) bytes of data.
64 bytes from 10.0.1.10: icmp_req=1 ttl=64 time=0.059 ms
64 bytes from 10.0.1.10: icmp_req=2 ttl=64 time=0.038 ms
64 bytes from 10.0.1.10: icmp_req=3 ttl=64 time=0.037 ms
64 bytes from 10.0.1.10: icmp_req=4 ttl=64 time=0.036 ms
64 bytes from 10.0.1.10: icmp_req=5 ttl=64 time=0.039 ms
```

```
root@n3:/tmp/pycore.55068/n3.conf# ping 10.0.0.20
PING 10.0.0.20 (10.0.0.20) 56(84) bytes of data.
64 bytes from 10.0.0.20: icmp_req=1 ttl=64 time=0.033 ms
64 bytes from 10.0.0.20: icmp_req=2 ttl=64 time=0.039 ms
64 bytes from 10.0.0.20: icmp_req=3 ttl=64 time=0.043 ms
64 bytes from 10.0.0.20: icmp_req=4 ttl=64 time=0.041 ms
64 bytes from 10.0.0.20: icmp_req=5 ttl=64 time=0.052 ms
```

2. Para o *router* e um *laptop* de um dos departamentos:
   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).

router:

```
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.0.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
10.0.1.0        10.0.2.2        255.255.255.0   UG        0 0          0 eth1
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth1
10.0.3.0        0.0.0.0         255.255.255.0   U         0 0          0 eth2
```

laptop:

```
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.0.1        0.0.0.0         UG        0 0          0 eth0
10.0.0.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

Como podemos ver pelas imagens acima indicadas, a ligação direta do n1 para o n3 vai ter o gateway direto, enquanto as outras ligações vamos ter o 0.0.0.0 que assumimos que corresponde ao endereço gateway de origem.

No laptop vamos ter o destino 0.0.0.0 que corresponde a todos os outros endereços, ou seja, qualquer endereço que não pertença a 10.0.0.0 é enviado pela porta 10.0.0.1.

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

O encaminhamento é Estático porque é um endereçamento baseado em rotas pré-definidas isto é rotas permanecem fixas.

c. Admita que, por questões administrativas, a rota por defeito (0.0.0.0 ou default) deve ser retirada das tabelas de encaminhamento dos *laptops* de cada departamento. Use o comando route delete para o efeito. Como é afectada a conectividade IP para cada um dos servidores. Justifique.

```
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.1.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
root@n6:/tmp/pycore.55070/n6.conf# ping 10.0.2.1
connect: Network is unreachable
```

A conetividade mantem-se com o servidor pois continua a ter a rota para 10.0.1.0 que corresponde à do servidor.

d. Adicione as rotas estáticas necessárias para repor a conectividade entre os departamentos. Utilize para o efeito o comando route add. Registe o comando completo que usou.

ip route add 10.0.0.0/24 via 0.0.0.0 dev eth0

e. Teste a nova política de encaminhamento garantindo que ambos os servidores estão acessíveis, utilizando para o efeito o comando *ping*. Inclua as novas tabelas de encaminhamento dos *laptops.*

A conexão entre o portátil de um andar e o servidor de outro não esta a ser feito, apenas tendo acesso ao servidor do seu próprio andar.

f. Que conclui face à atual conectividade externa e interna na empresa?

Apresenta algumas falhas internamente pois não é possível realizar a conexão. Quanto à externa, esta é realizada pelo router mais exterior, o N9.

3. Considere a topologia usada anteriormente. Assuma que o endereçamento entre os *routers* se mantém inalterado, contudo, o endereçamento em cada departamento deve ser redefinido.
   a. Assumindo que dispõe apenas de um único endereço de rede IP classe C 192.168.1.0/24, defina um novo esquema de endereçamento para as redes dos departamentos (mantendo a rede de core inalterada) e atribua endereços às interfaces dos vários sistemas envolvidos. Deve justificar as opções usadas.
   b. Qual a máscara de rede que usou (em formato decimal)?
   c. Com base no novo endereçamento, será possível ao encaminhador de saída anunciar um único prefixo de rede que agregue as redes dos departamentos?
   d. Que prefixo de rede pode ser anunciado para o exterior?
   e. Quantos *hosts* pode interligar em cada departamento?
   f. Garanta que conectividade IP entre as várias redes da filial é mantida.

Conclusão

Deparamos com alguns problemas ao longo do trabalho, bem como algumas dificuldades que foram posteriormente ultrapassadas com um bocado de aplicação. Mais uma vez aumentando o nosso grau de conhecimento no assunto.

Apesar disto, na parte da adição de rotas em que não foi possível realizar a mesmo com o comando route add, apenas com o ip route add. Apesar de a rota existir esta não parece estar a funcionar a 100% pois como mencionado no relatório, não se consegue fazer a conexão apesar de a rota existir.

Não conseguimos resolver o exercício 3 da parte 2, devíamos ter esforçado mais para o conseguir fazer, pois deparamos com o erro já referido em cima sobre não conseguirmos colocar o ping a funcionar entre os pisos, erro que não percebemos o porque de acontecer.

Com isto concluímos que não compreendemos bem a parte de remover, adicionar, e modificar os endereços das redes IP, como tal esperemos conseguir aprender o erro que fizemos de maneira a que no futuro não o voltemos a cometer, aprendo assim bem a matéria acerca do protocolo IP.