**eTP2: Protocolo IPv4 (Parte I)**

Filipa Correia Parente, José André Martins Pereira, Ricardo André Gomes Petronilho

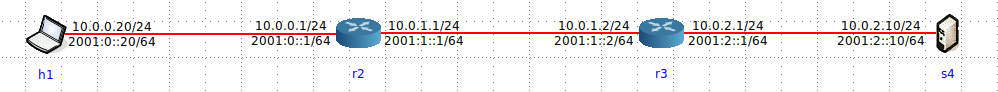
University of Minho, Department of Informatics, 4710-057 Braga, Portugal e-mail: {a82145,a82880,a81744}@alunos.uminho.pt

**Exercício 1:**

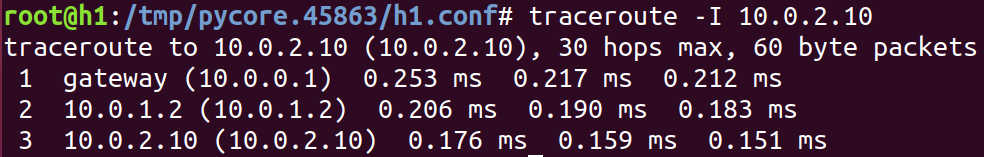
a) Active o wireshark ou o tcpdump no pc h1. Numa shell de h1, execute o comando traceroute -I para o endereço IP do host s4.

**Resposta:**

Através do emulador de redes CORE foi montada uma topologia envolvendo 1 pc, 2 routers, e 1 host tal como a seguinte figura ilustra.



De seguida é executado um traceroute no dispositivo h1 (pc) para o s4 (host).

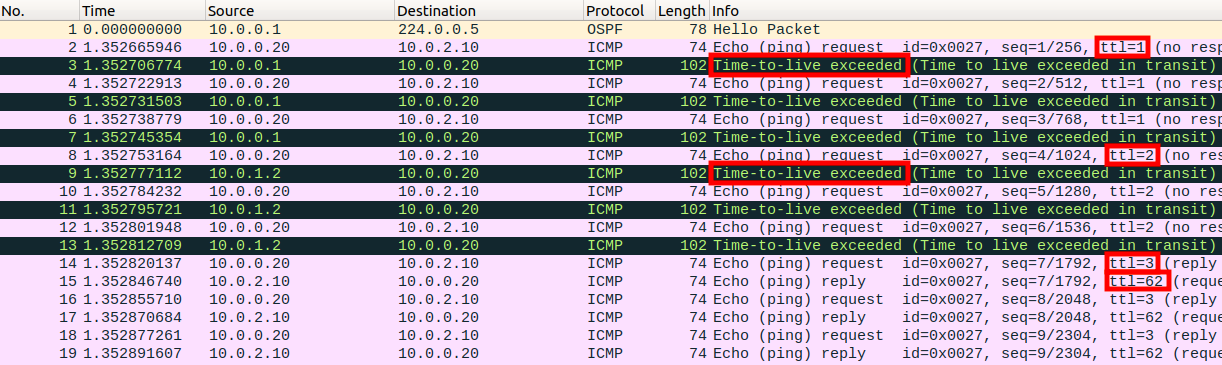


Como se pode observar no output obtido, é possível verificar a rota dos pacotes envidados pelo h1 para o s4 através do comando traceroute.

b) Registe e analise o tráfego ICMP enviado por h1 e o tráfego ICMP recebido como resposta. Comente os resultados face ao comportamento esperado.

**Resposta:**

Assim é feito o registo do tráfego gerado pelo comando traceroute, e analisado através do software wireshark.



Os resultados obtidos na prática são coerentes com os resultados téoricos esperados.

**Explicação teórica:**

Inicialmente, o traceroute envia 3 datagramas com o campo TTL (time-To-Live) igual a 1, o TTL é decrementado em cada gateway intermédio, caso o TTL atinga o valor 0 é enviado uma mensagem ICMP - Time-To-Live exceeded - no sentido contrário, permitindo assim, registar o endereço IP do gateway intermédio. De seguida são enviados novamente 3 pacotes com o TTL a 2 e assim sucessivamente até que o TTL inicial seja suficiente para o pacote atingir o destino.

No final obtêm-se a rota completa que os pacotes seguiram desde a origem até ao destino.

**Análise prática:**

Como é possível observar na imagem acima, inicialmente, é enviado um pacote com TTL = 1, desde a origem h1 (10.0.0.20) com destino a s4 (10.0.2.10).

Ao passar pelo primeiro gateway r2 (10.0.0.1) o TTL é decrementado atingindo assim TTL = 0, desta forma, o dispositivo r2 envia uma mensagem ICMP á origem (h1) a informar que o TTL foi excedido.

Na figura a baixo são filtrados os dois pacotes referidos anteriormente.



De seguida, o traceroute envia mais 2 pacotes com o TTL = 1, para assegurar a fiabilidade da informação recolhida.

O mesmo procedimento é feito para pacotes com TTL inicialmente a 2, no entanto quando chegam a r3 (10.0.1.2) o TTL é igual a 0, por isso são enviadas novamente 3 mensagens ICMP a informar que o TTL foi excedido.



Finalmente, são enviados 3 pacotes com TTL = 3, desta forma os mesmo conseguem alcançar o destino (s4) antes do TTL tomar o valor de 0.



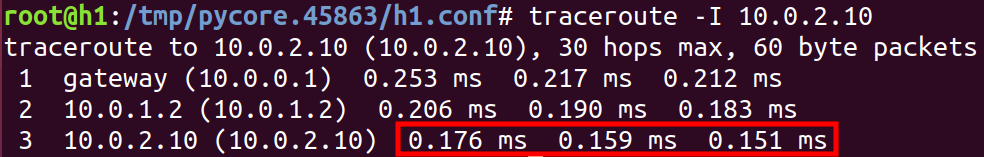
Note-se que a mensagem ICMP reply chega ao destino com TTL = 62 pois inicialmente o pacote é enviado com TTL = 64 passando em 2 nodos intermédidos, decrementando o TTL duas vezes, ficando no fim com TTL = 62.

c) Qual deve ser o valor inicial mínimo do campo TTL para alcançar o destino s4? Verifique na prática que a sua resposta está correta.

**Resposta:**

Conlui-se que o **TTL = 3** inicial, é suficiente para os pacotes alcançarem o destino, este resultado confirma-se com a análise prática efetuada na alínea b).

O traceroute também informa o valor de ida-e-volta (Round-Trip Time) para cada um dos 3 pacotes em cada percurso.



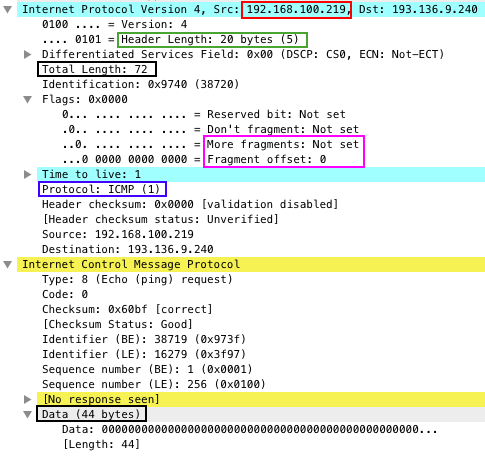
d) Qual o valor médio do tempo de ida-e-volta (Round-Trip Time) obtido?

**Resposta:**

Verifica-se que o tempo médio de ida-e-volta no percurso total (3) é **0.162 ms**.

**Exercício 2:**

No exercício 2 é feita a análise de tráfego num abiente de redes real, sendo analisado o tráfego ICMP gerado pelo comando traceroute com tamanho dos pacotes padrão.



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

**Resposta:**

O endereço IP da interface ativa do computador é 192.168.100.219 tal como se pode observar na região a vermelho.

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

**Resposta:**

O valor do campo protocolo é **1.** Identifica o protocolo **ICMP**. Tal é possível ser observado na região a azul.

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?

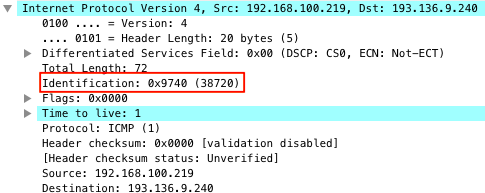
**Resposta:**

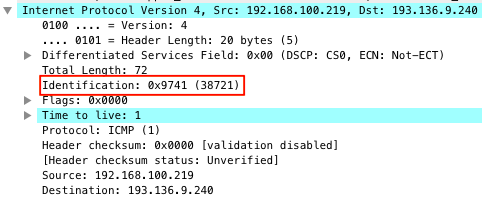
O cabeçalho tem 20 bytes como é verificado na região a verde. O campo payload tem 44 bytes como é possível verificar na região a preto no campo denominado “**Data”**. Este valor é obtido excluindo o tamanho do header do IPv4 e do ICMP ao tamanho total: **44 = 72 (tamanho total) – 20 (header do IPv4) – 8 (header do ICMP)**

d) O datagrama IP foi fragmentado? Justifique.

**Resposta:**

Como o campo **“More fragments”** não está inicializado (not set) e o campo **“Fragment offset”** tem o valor 0 siginifica que corresponde ao primeiro pacote e não está fragmentado. Tal é possível observar na região a rosa.





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.

**Resposta:**

É possível verificar que o campo **“Identification”** do IPv4altera **sequencialmente** consoante o pacote, no entanto apesar de não ser possível verificar no tráfego analisado, o **“Header checksum“** tambem é alterado.

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

**Resposta:**

Podemos observar que o TTL muda sequencialmente a cada grupo de 3 pacotes (3 a TTL = 1, 3 a TTL = 2, etc) e os identificadores são sequenciais, ou seja, aumentam 1 a cada pacote enviado/recebido.

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?

**Resposta:**

Cada grupo de 3 pacotes enviados para o nosso computador têm todos o mesmo TTL visto que são enviados do memo router.

O primeiro grupo foi enviado com valor inicial TTL = 64 e alcançou o nosso computador com TTL = 64 pois não passou por nenhum nó intermédio.

O segundo grupo foi enviado com valor inicial TTL = 255 e alcançou o nosso computador com TTL = 254 pois passou por 1 nó intermédio.

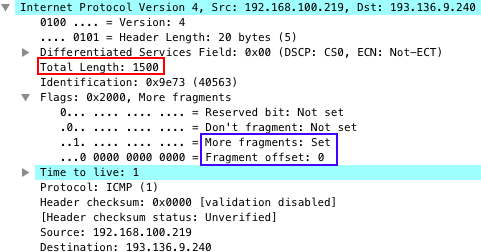
O terceiro grupo foi enviado com valor inicial TTL = 64 e alcançou o nosso computador com TTL = 62 pois passou por 2 nós intermédios.

**Exercício 3:**

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

**Resposta:**

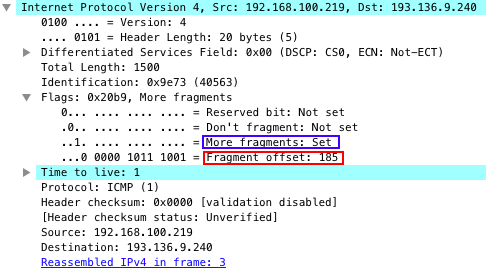
Como o tamanho da fonte (3521 bytes) excede o MTU, 1500 bytes (capacidade máxima de um datagrama) é necessário recorrer ao processo de fragmentação dos dados.



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?

**Resposta:**

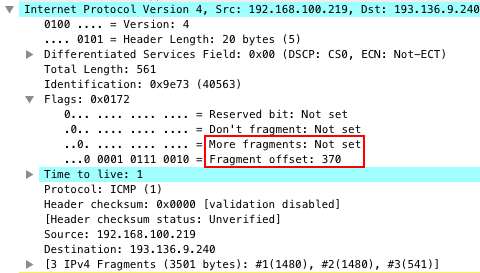
Como se pode observar na região a azul, este datagrama é fragmentado (**“More fragments: Set”**) e corresponde ao primeiro fragmento (**“Fragment offset: 0”**). O tamanho total do pacote é 1500 como se verifica na região a vermelho.



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?

**Resposta:**

O datagrama não se trata do 1º fragmento como se pode comprovar com o valor do **“Fragment offset”** na região a vermelho. Existem mais fragmentos como se pode constatar com o valor de **“More fragments”** na região a azul.



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

**Resposta:**

Foram criados 3 fragmentos a partir do datagrama original. O último fragment o tem o **“Fragment offset”** diferente de 0 e **“More fragements”** sem atribuição. Tal é possível constatar na região a vermelho.

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.

**Resposta:**

Entre os diferentes fragmentos mudam 2 campos , o campo **“More fragments”** e o **“Fragment offset”**. O último pacote geralmente tem **dimensão** menor que os anteriores.

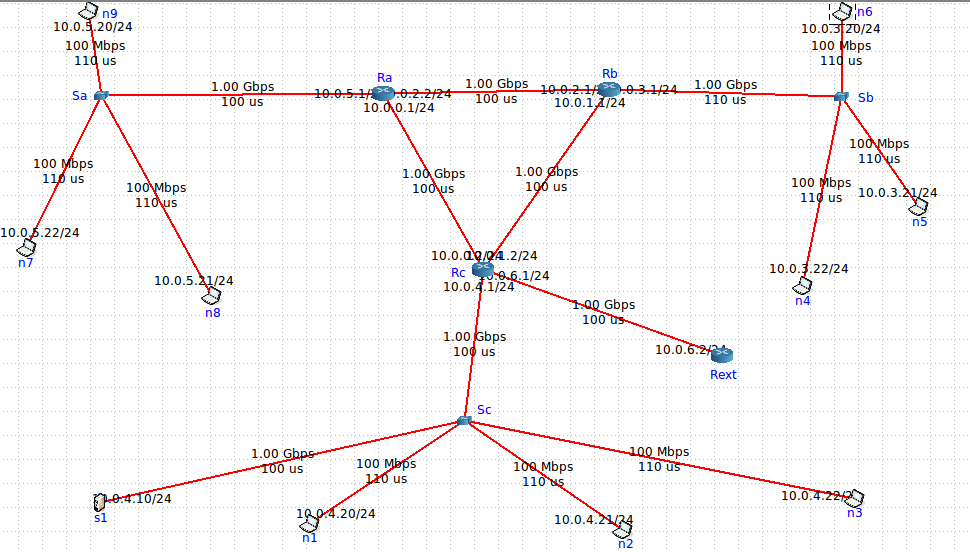
A resconstrução cronológica dos fragmentos é possível uma vez que o primeiro fragmento tem o **“More fragments: set”** e o **“Fragment offset: 0”** os sucessores têm o **“More fragments: set”** e o **“Fragment offset”** com valores incrementais, o último fragmento tem o **“More fragments: not set”** e o **“Fragment offset”** com o valor máximo.

**eTP2: Protocolo IP (Parte II)**

**Exercício 1:**

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.

**Resposta:**



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

**Resposta:**

Tratam-se de endereços privados uma vez que não são visíveis para o exterior da rede, o próprio padrão do endereço de IP é indicativo que é privado isto é, começa com 10.0.0.0 até 10.255.555.555.

c) Porque razão não é atribuído um endereço IP aos *switches*?

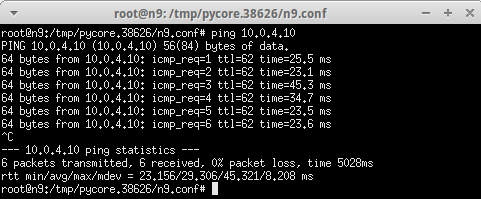
**Resposta:**

Os switches não atuam em nível 3 (IP), apenas em nível 2 (ethernet).

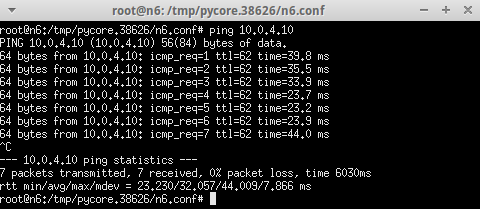
d) Usando o comando ping certifique-se que existe conectividade IP entre os laptops dos vários departamentos e o servidor do departamento C (basta certificar-se da conectividade de um laptop por departamento).

**Resposta:**

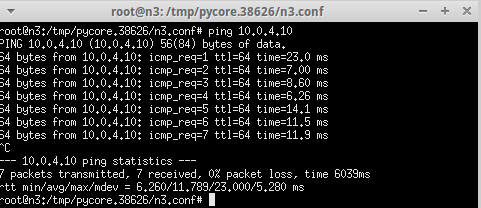
Laptop no depeartamento A para o servidor S1.



Laptop no depeartamento B para o servidor S1.



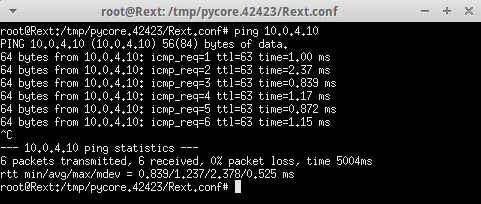
Laptop no depeartamento C para o servidor S1.



Conclui-se que existe concectividade entre todos os laptops dos vários departamentos e o servidor S1.

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

**Resposta:**

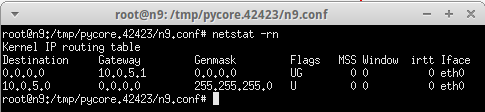


Como se verifica na imagem existe conectividade entre o router externo e o servidor S1.

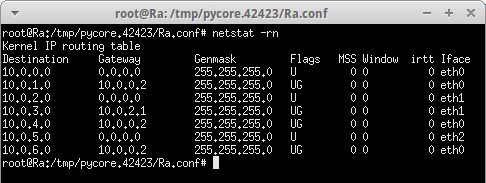
**Exercício 2:**

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).

**Resposta:**

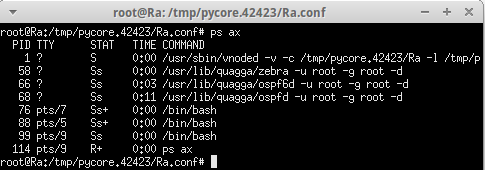


O comando netstat (network status) apresenta informações sobre o estado atual da rede. A opção -rn apresenta as tabelas de encaminhamento, **–r (route)**, sobre a forma de IP’s numéricos , -**n (numeric host)**. Como podemos ver na tabela existe encaminhamento do laptop (dispostivo atual - 0.0.0.0) para o router (10.0.5.0).



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

**Resposta:**

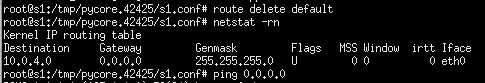


Como se pode verificar na imagem acima, estão a correr 3 processos do **Quagga**, este software é responsável por fazer encaminhamento dinâmico das rotas. Ainda é possível observar que está a ser usado encaminhamento dinâmico tanto para IPv4 (ospfd que implementa o algorimto OSPF - Open Shortest Path First) como para IPv6 (ospfd6d que implementa o mesmo algoritmo numa versão diferente).

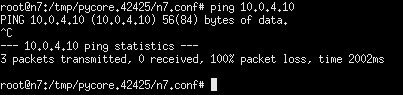
c) Admita que, por questões administrativas, a rota por defeito (0.0.0.0 ou *default*) deve ser retirada definitivamente da tabela de encaminhamento do servidor S1 localizado no departamento C. Use o comando route delete para o efeito. Que implicações tem esta medida para os utilizadores da empresa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

**Resposta:**

Após ser retirada da tabela de encaminhamento do servidor S1 a rota por defeito (0.0.0.0 ou default) a mesma encontra-se da seguinte forma.



A tentativa de conexão entre um laptop (n7) do departamento A para o servidor S1 foi falhada como a seguinte imagem evidencia.

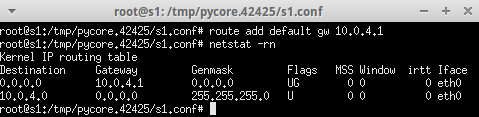


Ao eleminar a rota por defeito no servidor S1, o mesmo deixa de poder enviar pacotes para outras redes ou seja, existe caminho de ida entre os outros dispositivos fora da rede e o servidor mas não existe caminho de volta.

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.

**Resposta:**

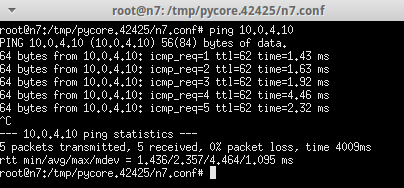
A tabela de encaminhamento restaurada é a seguinte.



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.

**Resposta:**

Como a seguinte imagem demostra o servidor S1 está de novo acessível, visto que temos conectividade, conexão (“caminho”) de ida e volta.



**Exercício 3:**

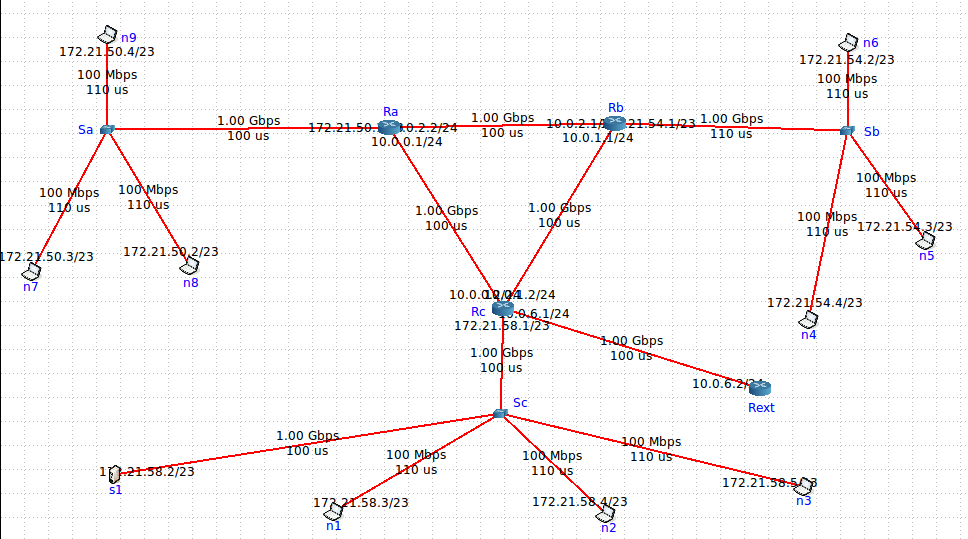
1) Considere que dispõe apenas do endereço de rede IP 172.XX.48.0/20, em que XX é o decimal correspondendo ao seu numero de grupo (PLXX). Defina um novo esquema de endereçamento para as redes dos departamentos (mantendo a rede de acesso e core inalteradas) e atribua endereços às interfaces dos vários sistemas envolvidos. **Deve justificar as opções usadas**.

**Resposta:**

O endereço IP inicial da rede proposto é o 172.21.48.0/20. Com base no número de departamentos existentes, neste caso são 3, é necessário definir pelo menos 3 sub-redes distintas. Assumimos que são reservados os dois endereços extremos (x.x.x.0) e o (x.x.x.255). Deste modo necessitamos de pelo menos 3 bits para identificar a sub-rede. Usando 3 bits conseguimos identificar 8 sub-redes distintas, no entanto excluindo os 2 endereços reservados, resta-nos 6 sub-redes. Assim ficamos com um novo endereço /23 variando entre **172.21.48.0**, **172.21.50.0**, 172.21.52.0, **172.21.54.0**, 172.21.56.0, **172.21.58.0**, 172.21.60.0, **172.21.62.0**, sendo que os endereços IP a vermelho são os reservados.

Os endereços IP a azul são os escolhidos para cada departamento, uma vez que pensamos numa possível expansão.

Desta forma propomos a seguinte topologia.



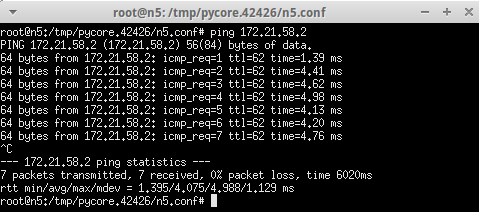
2) Qual a máscara de rede que usou (em formato decimal)? Quantos *hosts* IP pode interligar em cada departamento? Justifique.

**Resposta:**

Visto que o endereço de IP é **/23** temos uma máscara de rede **1111 1111 . 1111 1111 . 1111 111**0 . 0000 0000 que em decimal é **255.255.254.0**. Em cada departamento é possível interligar **510** dispositivos, por exemplo a sub-rede C (172.21.58.0) varia entre 172.21.58.0 e 172.21.59.255, assumindo que se exclui o IP de identificação de rede e o de broadcast, ficamos com 256 \* 2 – 2 = 510 endereços de IP possíveis de associar aos dispositivos na rede.

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

**Resposta:**



Como se pode observar na imagem a conectividade verifica-se após a implementação do sub-neting.

**Conclusão:**

Relativamente à realização da primeira parte, surgiram alguns desafios, nomeadamente no estabelecimento do “routing” no emulador de rede utilizado (CORE), e na interpretação dos resultados retirados do Wireshark, uma vez que existiam valores de TTL (time to live) que não correspondiam ao habitual. Por exemplo, numa rede com 2 routers e um host o time to live deveria ter decrementado no máximo 3, contudo decrementou a mais. Posteriormente, verificou-se que era um erro do emulador.

No que diz respeito à realização da segunda parte, o principal desafio foi o estabelecimento do routing dinâmico no CORE, uma vez que aconteciam momentos em que o “ping” funcionava, e outras em que não funcionava. Mais uma vez se verificou que o problema estava no delay no estabelecimento do “routing” no CORE.

Contudo, é de destacar a importância que este trabalho prático teve no aprofundamento dos conhecimentos acerca da forma como o protocolo IPv4 atua ao nível do “Network layer”, bem como na influência que o sub-neting tem na organização de uma rede, apesar da diminuição de endereços válidos disponíveis.