

**Redes de Computadores:**

Protocolo IPv4

**Grupo de Trabalho 2**

Ana Esmeralda Fernandes A74321

Bárbara Nadine Freitas Oliveira A75614

Miguel Dias Miranda A74726

**Novembro de 2016**

**Conteúdo**

[Datagramas IP e fragmentação 3](#_Toc469578846)

[Captura de tráfego IP – Questão I 3](#_Toc469578847)

[Captura de tráfego IP - Questão II 5](#_Toc469578848)

[Captura de tráfego IP – Questão III 9](#_Toc469578849)

[Endereçamento e Encaminhamento IP 12](#_Toc469578850)

[Endereçamento e Encaminhamento IP – Questão I 12](#_Toc469578851)

[Endereçamento e Encaminhamento IP – Questão II 14](#_Toc469578852)

[Definição de Sub-Redes 19](#_Toc469578853)

[Conclusão 20](#_Toc469578854)

# Datagramas IP e fragmentação

## Captura de tráfego IP – Questão I

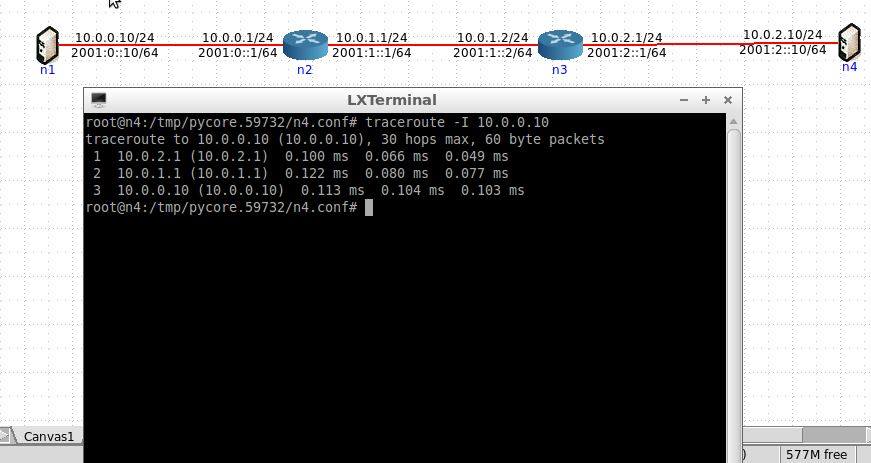


Figura 1- Topologia inicial do sistema

**a) Active o wireshark ou o tcpdump no host n4. Numa sheel de n4, execute o comando traceroute -I para o endereço IP do host n1.**

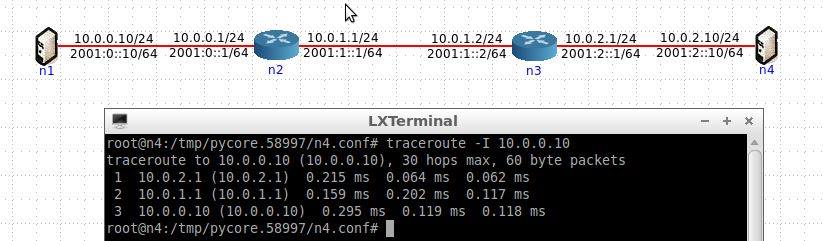
****

Figura 2 - Execução, numa shell de n4, do comando ´traceroute -I 10.0.0.10´, onde o endereço IP usado no comando é referente ao host n1

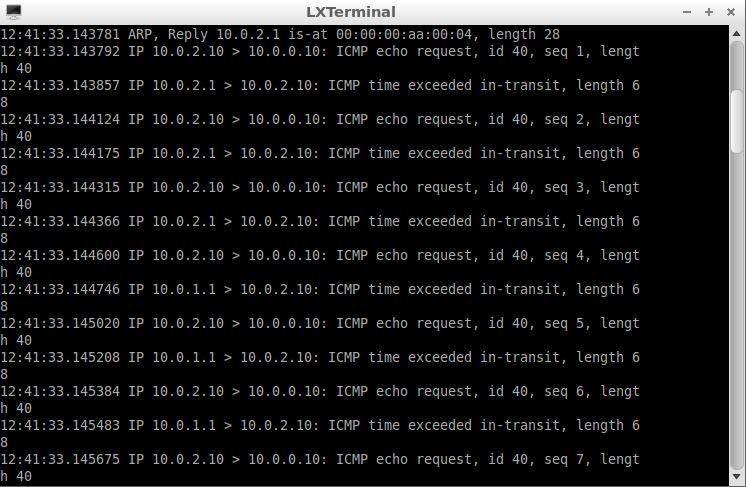
****

Figura 3 - Análise, numa shell de n4, do comando tcpdump

**b. Registe e analise o tráfego ICMP enviado por n4 e o tráfego ICMP recebido como resposta. Comente os resultados face ao comportamento esperado.**

Por parte do host n4 o trafego ICMP gerado caracteriza-se sempre por ser pedidos ‘ICMP request’ e o trafego ICMP recebido varia entre pacotes do tipo ‘ICMP time-exceeded’, quando o valor do campo TTL não é suficiente para que o pacote dê os “saltos” necessários até ao host destino, ou pacotes ICMP do tipo ‘ICMP Reply’ quando o pacote chega ao seu destino e este confirma a n4 a sua receção.

Quando o host n4 recebe pacotes do tipo ‘ICMP time exceeded’ o seu procedimento é enviar ao mesmo destino um novo ‘ICMP request’ mas com o valor do campo TTL incrementado em 1 unidade.

**c. Qual deve ser o valor inicial mínimo do campo TTL para alcançar o destino n1? Verifique na prática que a sua resposta está correta.**

O valor mínimo do campo TTL devia de ser 3 de forma a conseguir chegar até ao seu destino. Podemos verificar que este valor faz sentido, pois pelo sistema da rede que esboçamos no CORE vemos que existem 3 ligações/saltos que são necessários fazer para que o pacote enviado por n4 chegue a n1.

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

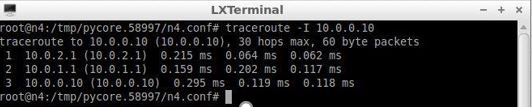
****

Figura 4 - Resultado Traceroute em n4

Como queremos analisar o tempo de ida-e-volta até ao host n1, cujo endereço IP é 10.0.0.10, usamos os valores registados na linha 3 do comando traceroute da imagem anterior.

Assim, o tempo médio será 0.1773.

## Captura de tráfego IP - Questão II

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

O endereço IP da interface ativa do computador usado é 192.168.100.158.

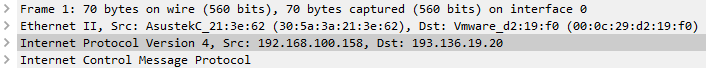


Figura 5 - O endereço IP da interface ativa do computador usado é 192.168.100.158.

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

O campo protocolo tem o valor 1 que identifica o ICMP foi usado via IP.

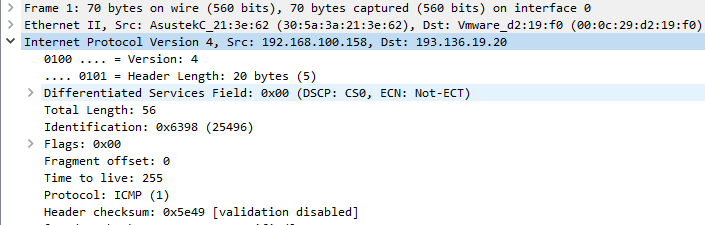
****

Figura 6 - O campo protocolo tem o valor 1 que identifica o ICMP foi usado via IP.

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?**

O cabeçalho do IPv4 tem 20 bytes.

Como nesta captura foi usado o tamanho do pacote definido por omissão pelo PingPlotter de 56 bytes, o campo de dados do datagrama tem 36 bytes.

Este payload calcula-se subtraindo-se ao tamanho do pacote os 20 bytes ocupados pelo header do IPv4 (56 –20=36).

C:\Users\Nadine\Pictures\My Screen Shots\RC4\2c).PNG

Figura 7 - Tamanho cabeçalho IPv4

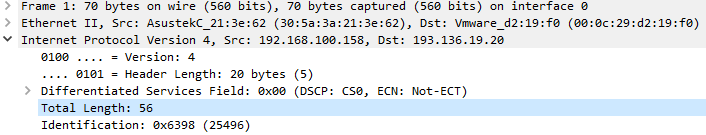


Figura 8 – Tamanho total do datagrama

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

O datagrama IP da frame 1 estudada não foi fragmentado. Pela análise do campo Flags da opção IPv4 vemos que o valor que contem é 0x00. Isto indica que a opção Don’t fragment está marcada como Not Set.

Alem disto, por analise da questão anterior, vemos que o datagrama IPv4 mais o cabeçalho deste protocolo tem exatamente o tamanho máximo de 56 bytes configurado por omissão no PingPlotter, logo, não existe razões para fragmentar este pacote.

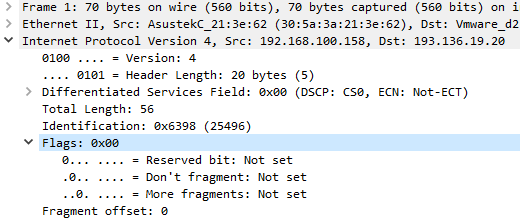


Figura 9 - Valor do campo Flags na opção IPv4

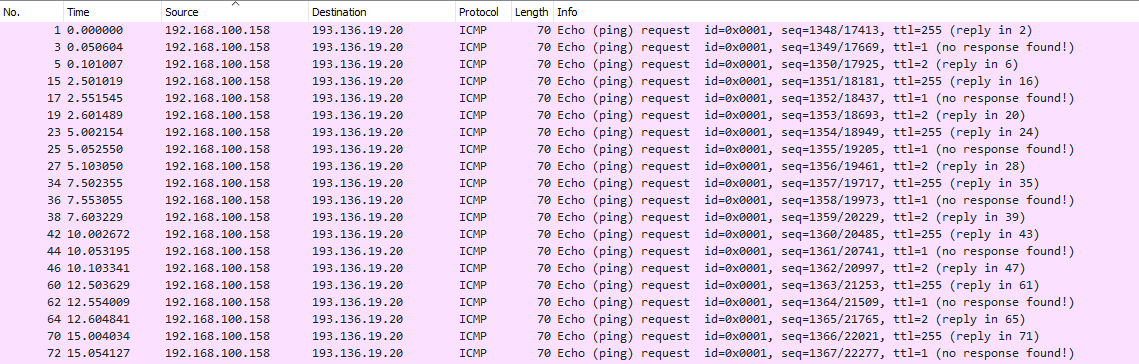
1. **Ordene os pacotes capturados de acordo com o endereço IP fonte e analise a sequencia de tráfego ICMP gerado a partir do endereço IP atribuído á sua máquina. Para a sequência de mensagens ICMP enviadas pelo seu computador, indique que campos do cabeçalho IP variam de pacote para pacote.**

Figura 10 - Vista geral dos pacotes capturados com origem no IP do portátil usado no estudo.

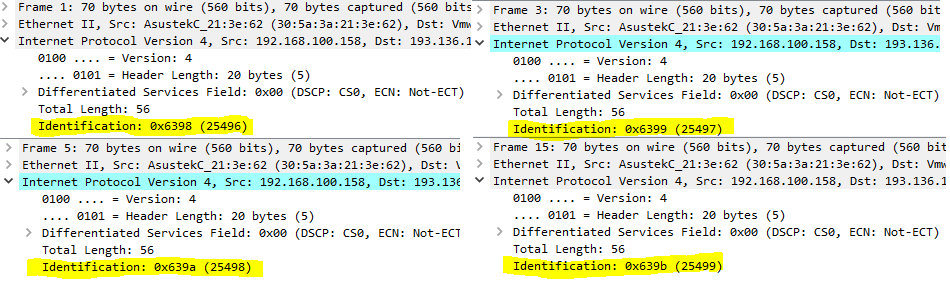


Figura 11 - Valores do campo Identification da opção IPv4 de diferentes pacotes ICMP

De algumas frames analisadas é possível ver que o campo identification varia de pacote para pacote, algo que faz sentido porque este ID deve ser único e ter o maior período de ‘vida’ possível. Quando este ID é especificado, juntamente com os valores do campo Flags acerca da possível fragmentação do pacote, é possível no destino ser feita a montagem dos pacotes fragmentados a partir do ID e do número do fragmento.

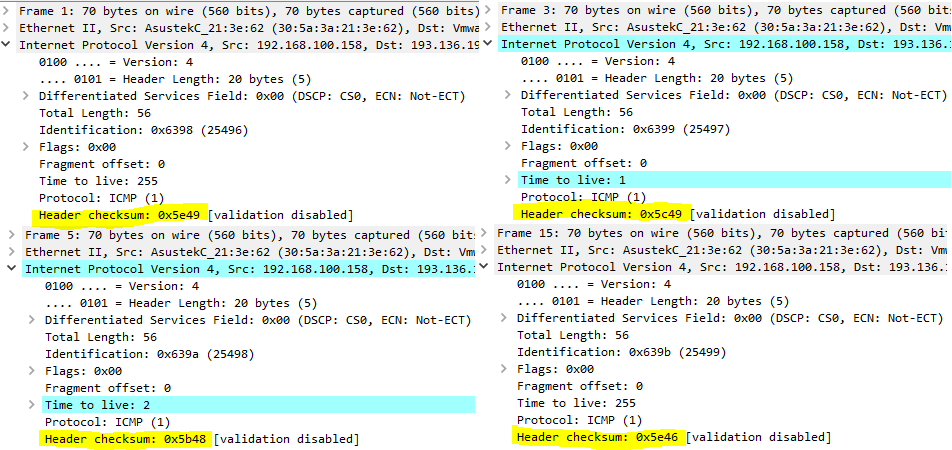


Figura 12 Valor do campo Header checkSum da opção IPv4 para diferentes pacotes ICMP

Ainda dentro da opção IPv4 é possível ver para diferentes frames que o campo Header Checksum é diferente. Este campo é usado para verificar a integridade ou existência de erros nos dados do pacote.

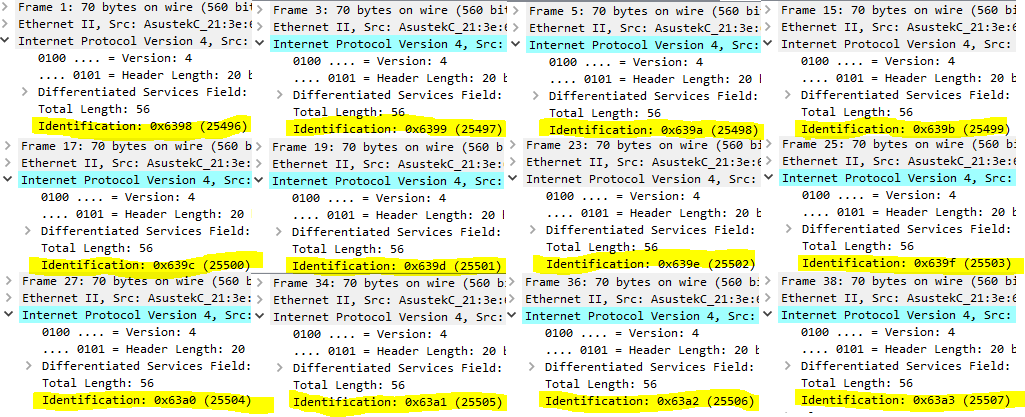
1. **Observa algum padrão nos valores do campo de Identificação do datagrama IP e TTL?** 

Figura - Valor do campo ID de algumas tramas ICMP com origem no computador usado para o estudo.

Pela observação de alguns frames do tipo ICMP e do valor do seu campo ID é possível concluir que estes são incrementados sequenciais de uma unidade face ao valor do mesmo campo no pacote anterior.

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 constante para todas as mensagens de resposta ICMP TTL exceeded enviadas ao seu host ? Porquê?**

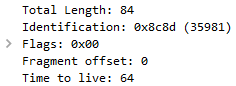
****

Figura 14 - Valor do campo TTL

O campo TTL apresenta o valor 64.

Sim, este valor permanece constante quando as frames têm como destino o endereço o computador usado. Isto acontece porque o router a que este está ligado é sempre o mesmo, logo, o número de passos até as mensagens chegarem até ele é o mesmo.

## Captura de tráfego IP – Questão III

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

Com o uso do PingPlotter definiu-se o tamanho do pacote ICMP para 4022Bytes. Com esta alteração, como o tamanho máximo do pacote por rede cablada Ethernet (usada para realizar a captura) é de 1500Bytes existe então a necessidade de fragmentar o pacote para que este possa ser enviado pelos protocolos usados na rede Ethernet.

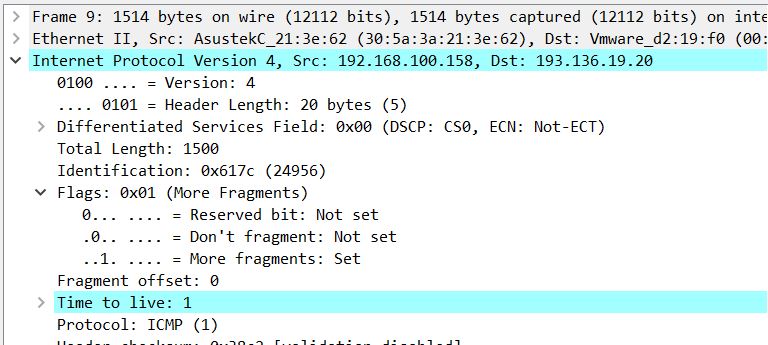
****

Figura 15 - análise do primeiro pacote fragmentado com origem no IP da maquina usada para a captura

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?**

Pela opção ´More fragments’ do campo ‘Flags’ é possível ver que este campo tem o valor 1, que indica que a opção de fragmentação está definida como ‘Set’.

Pelo valor do campo ‘Fragment offset’ é possível ver que se trata do primeiro fragmento, pois é colocado no offset 0, ou seja, na posição inicial quando se for reconstruir o pacote inicial.

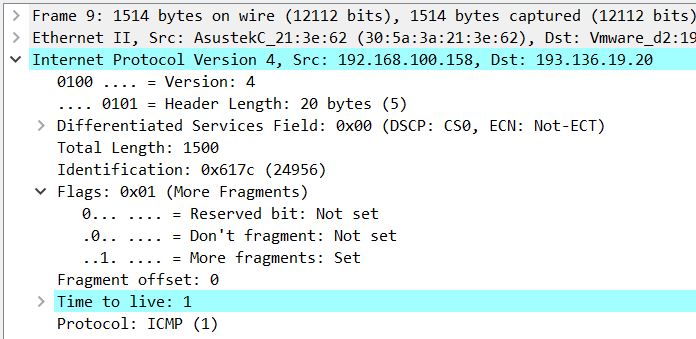
Sabemos que o datagrama tem 1500Bytes de tamanho, visto no campo ‘total length’ sendo que destes 20 Bytes são para o cabeçalho IP.

Figura 16 - Informações sobre o primeiro pacote fragmentado da nossa captura

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?**

Como o campo ‘Fragment offset’ tem o valor 1480, quando o pacote inicial for reconstruído, este datagrama em análise deve ser colocado na posição/offset 1480. Assim este não é o datagrama inicial porque esse vai ocupar desde a posição 0 até á posição 1480.

Embora os pacotes tenham um tamanho máximo de 1500Bytes, como 20butes são usados para o cabeçalho do protocolo, só 1480 é que são efetivamente dados para reconstrução do pacote original.

Existem mais fragmentos porque a opção ‘More Fragments’ volta a estar definida com o valor 1 e, portanto, existem mais fragmentos.

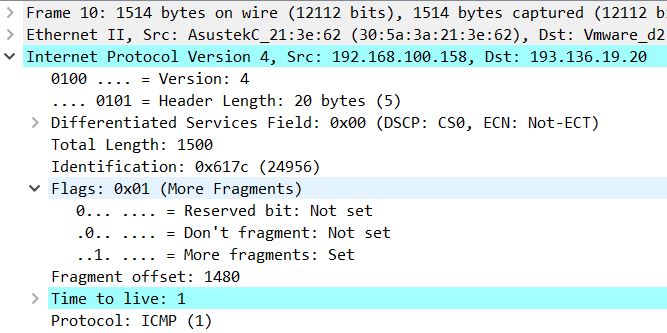
****

Figura 17 - informações sobre o segundo fragmento

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

Foram criados 3 fragmentos a partir do datagrama inicial. Alem da analise dos Datagramas que de facto irão compor o fragmento inicial, facilmente podíamos concluir isto porque sabendo que o tamanho máximo dos pacotes é de 1500 bytes e o nosso pacote tem 4022bytes, serão então precisos 3 fragmentos para o dividir.

O primeiro e o segundo fragmentos transportarão ambos 1480 bytes de dados e o ultimo fragmento, transportará apenas 1062.

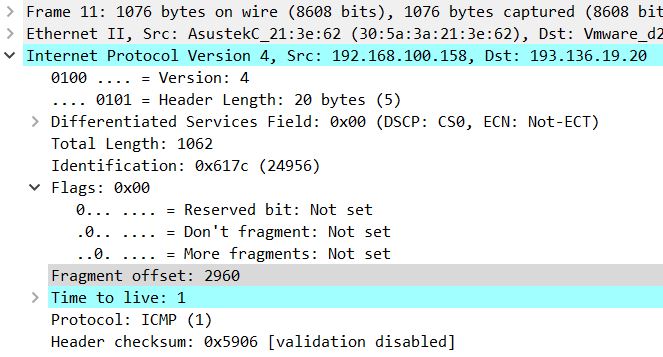


Figura 18 - informações sobre o ultimo datagrama do pacote em análise

Pelo valor do campo ‘More fragments’, que tem o valor 0, sabemos que já não vão haver mais fragmentos referentes a este Id.

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.**

O valor do campo ‘Total Length’ é diferente nos datagramas fragmentados de um mesmo pacote. Este valor não é sempre 1500Bytes (limite máximo da rede Ethernet) pois o ultimo fragmento, regra geral, tem sempre um tamanho inferior a 1500Bytes, com os últimos dados do pacote a reconstruir.

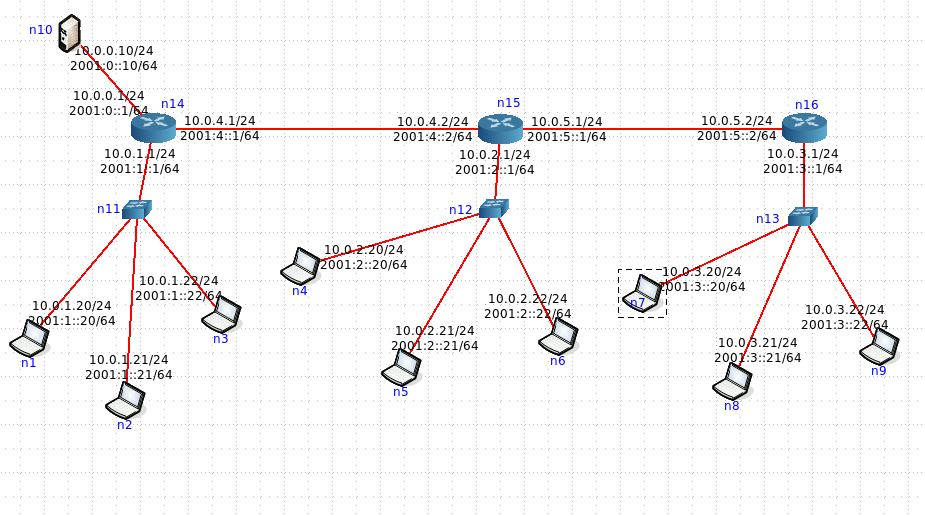
Exatamente por causa deste processo de reconstrução dos pacotes originais fragmentados para envio pela rede cablada, mudam também os campos ‘Fragment offset’ e ‘Flags’. O campo ‘Fragment offset’ muda porque cada datagrama corresponde a um fragmento que deve ser colocado numa posição especifica para reconstruir o pacote original e, portanto, aqui vai sempre surgir um valor diferente. O campo ‘Flags’ varia pois este indica se vão ou não existir mais fragmentos para aquele id.

Dentro do protocolo IP varia também o valor do campo Header Checksum pois este tem é usado para verificar a integridade dos dados e existência de erros.

# Endereçamento e Encaminhamento IP

## Endereçamento e Encaminhamento IP – Questão I

1. **Indique que endereços IP e máscaras de rede foram atribuídos pelo CORE a cada equipamento. Se preferir, pode incluir uma imagem que ilustre de forma clara a topologia e o endereçamento.**

****

Os router n14, n15 e n16 representam, respetivamente, os routers dos departamentos A, B e C.

De igual modo, os switches n11, n12 e n13 representam os switches que se ligam aos routers do seu departamento. Cada switch tem a si ligado três computadores.

De referir ainda o host (servidor) n10 que pertence ao departamento A e se liga ao router do referido departamento.

Os endereços de cada interface podem ser vistos no primeiro valor e o endereço da mascara no segundo endereço (em baixo do primeiro). Por exemplo, para o computador n1, o seu endereço é 10.0.1.20 e o seu endereço máscara é 2001.1::20

1. **Tratam‐se de endereços públicos ou privados? Porquê?**

Tratam-se de endereços privados porque se encontra na gama de endereços de 10.0.0.0 até 10.255.255.25 (redes com endereços 10.0.0.0/8).

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

Como os switches usados estão ligados a uma rede Ethernet estes apenas trocam e distribuem pacotes Ethernet entre os destinos finais e o router a que estão ligados. Neste nível de ligação não existem endereços IP e portanto, em geral os switches não apresentam endereços IP.

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

Por análise do resultado do comando ping, feito a partir de um computador de cada sistema (departamento) até ao Host (servidor) n10 vemos que todos os pacotes enviados são recebidos e, portanto, existem conectividade entre os computadores dos diferentes departamentos e o servidor do departamento A.

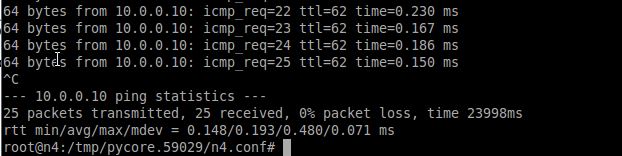
****

Figura 19 - comando ping do computador n4 (departamento B) para o host n10 do departamento A

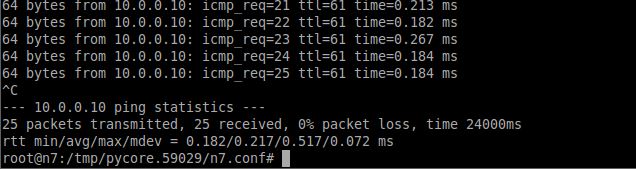
****

Figura 20- comando ping do computador n7 (departamento C) para o host n10 do departamento A

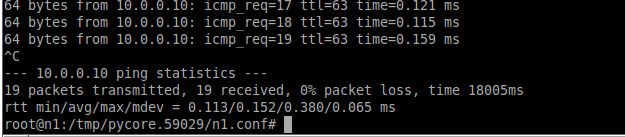
****

Figura 21- comando ping do computador n1 (departamento A) para o host n10 do departamento A

## Endereçamento e Encaminhamento IP – Questão II

1. **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).**

Para a atual questão usamos como objeto de estudo o computador representado por n1 e o router do departamento A representado pelo router n14.

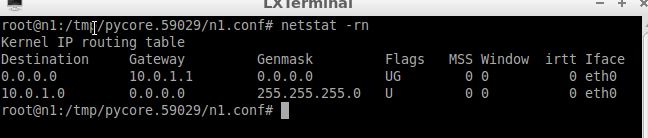


Figura 22 - Tabela de encaminhamento do computador n1 da rede do Departamento A

Na primeira linha representa-se o procedimento a tomar quando o portátil recebe um pacote com IP default (0.0.0.0). Quando não existe encaminhamento definido na tabela, o caminho por defeito do pacote é ir para o router da rede, com o endereço 10.0.1.1 (endereço da interface do router a que o portátil está ligado) e este trata de encaminhar o pacote conforme o encaminhamento da sua tabela.   
Quando o destino é o endereço 10.0.1.0 não é especificado nenhum encaminhamento porque o destino é o próprio computador.

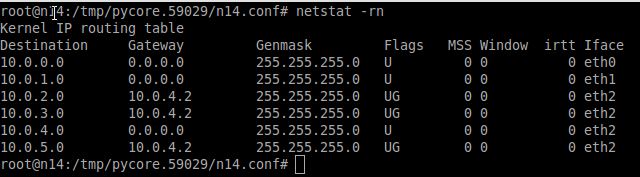


Figura 23 - Tabela de encaminhamento do router do Departamento A

Quando o router do departamento A recebe pacotes cujo destino têm como endereço os endereços das suas interfaces ( IPs 10.0.0.0, 10.0.1.0, 10.0.4.0 ) não é feito nenhum encaminhamento porque o destino é o próprio router.

Quando o destino é o IP 10.0.2.0 (endereços dos computadores da rede do departamento B) os pacotes são enviados para a interface que liga o router B ao router A, neste caso com o endereço 10.0.4.2. Será depois o router B, com a sua tabela de distribuição que encaminhará os pacotes até ao destino final.

Quando o destino é o endereço 10.0.5.0 ( endereço da interface que liga o router B ao router C) ou os endereços 10.0.3.0 (endereços dos computadores que compõe a rede do router C) o encaminhamento é feito para a interface do router B com o endereço 10.0.4.2 (interface que liga o router A ao router B). Será depois, de forma semelhante, o router B a encaminhar os pacotes até ao router C e este, por sua vez, a encaminhar os pacotes para o seu destino final na sua rede.

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

Pela análise dos processos que o router e o computador executam concluímos que o router apresenta encaminhamento dinâmico, quer pela sua tabela de encaminhamento quer pelo número de processo que executa e o computador, pelo trafego mais especifico que recebe e por não ter processos a correr, apresenta encaminhamento estático.

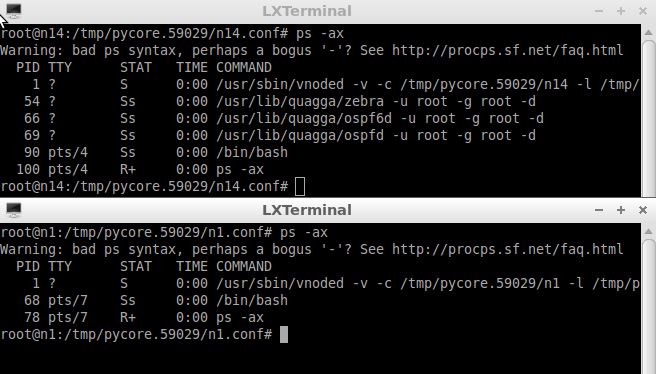


Figura 24- Execução do comando 'ps -ax' no router n14 do departamento A e no computador n1 da rede do departamento A, respetivamente

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 localizado no departamento A. Use o comando route delete para o efeito. Que implicações tem esta medida para os utilizadores da empresa que acedem ao servidor. Justifique.**

Ao apagar a linha que indicava o encaminhamento a tomar para todos os endereços IP marcados como default (ou não conhecidos pelo host), o host perde a ligação com a interface do router do departamento A que estava ligado (e a quem encaminhava estes pacotes), e portanto, não consegue comunicar com nenhum router ou computador de qualquer um dos departamentos.

Ao realizar um ping do host n10 para um computador escolhido aleatoriamente de cada uma das redes dos diferentes departamentos, vemos que a mensagem não chega ao destino e é marcada com a mensagem “Network is unreachable”. De igual modo, fazer ping a partir de um dos computadores das várias redes para o host n10, apesar de serem enviados nenhum pacote é recebido de volta na origem do ping.

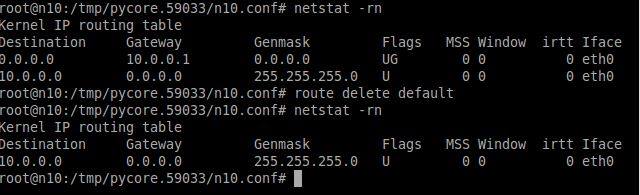
****

Figura 25 - Remoção da linha que continha o procedimento de encaminhamento para a rota por defeito

****

Figura 26 - Realização do comando ping no servidor n10 do departamento A para os computadores n4 (na rede do departamento B), n9 (na rede do departamento C) e n2 (na rede do departamento A). Todos os pedidos recebem a mensagem 'Network is unreachable' porque o router não saber para onde encaminhar estes endereços que vão para um destino que não o seu endereço.

1. **Adicione as rotas estáticas necessárias para restaurar a conectividade para o servidor, por forma a contornar a restrição imposta em c). Utilize para o efeito o comando route add e registe os comandos que usou.**

Para reestabelecer o encaminhamento do servidor n10 foi usado o comando ‘route add -net [endereço\_dest] netmask 255.255.255.0 gw [endereço\_gw]’.

Como o host n10 só está ligado a uma interface, em especifico a uma do router do departamento A, o endereço do campo gateway será sempre o endereço 10.0.0.1 dessa mesma interface do router, que posteriormente encaminhara o trafego até ao destino.

Como estamos a trabalhar com endereços do tipo x/24, a mascara de rede é o endereço 255.255.255.0 pois só o último octeto é que caracteriza o host.

Criaram-se assim três rotas, que definem o encaminhamento a realizar quando o endereço destino é, respetivamente, as redes 10.0.1.0 (do departamento A), 10.0.2.0 (do departamento B) e 10.0.3.0 (do departamento C).

Comandos usados:

‘route add 10.0.1.0 netmask 255.255.255.0 gw 10.0.0.1’ – encaminha o trafego destinado para a rede do departamento A.

‘route add 10.0.2.0 netmask 255.255.255.0 gw 10.0.0.1’ - – encaminha o trafego destinado para a rede do departamento B.

‘route add 10.0.3.0 netmask 255.255.255.0 gw 10.0.0.1’ - – encaminha o trafego destinado para a rede do departamento C.

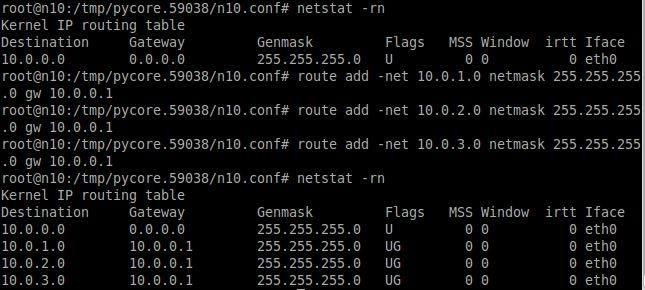


Figura 27 - comandos usados para restaurar a conectividade do servidor com o router e a rede

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.**

Para testar se o servidor estava novamente acessível, realizamos neste o comando ping para um computador na rede de cada um dos departamentos. Pelos resultados vimos que o ping foi bem-sucedido e portanto o servidor está novamente acessível.

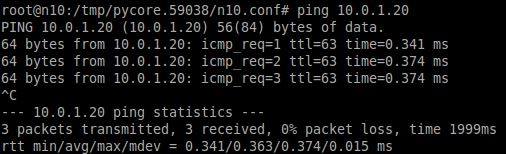


Figura 28 - Ping do servidor para o computador n1 (na rede do departamento A)

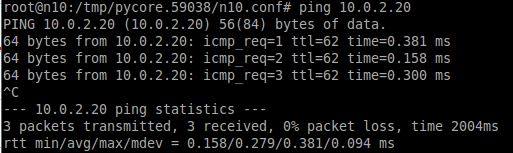


Figura 29 - Ping do servidor para o computador n4 (na rede do departamento B)

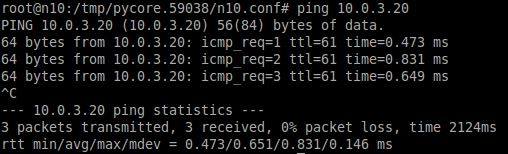


Figura 30 - Ping do servidor para o computador n7 (na rede do departamento C)

## Definição de Sub-Redes

1. **Assumindo que dispõe apenas de um único endereço de rede IP classe C 1 192.168.128.0/24, 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.**

Com o endereço 192.168.128.0/24 que nos foi atribuído temos à nossa responsabilidade a gestão de um octeto, por forma a ter endereços suficientes para as interfaces dos router e para os utilizadores ou hosts do sistema.

No nosso esquema CORE, identificamos 6 redes e, portanto, precisamos de uma divisão do octeto que permita identificar 6 endereços de subrede.

Dividir o octeto em 3 bits para a mascara de subrede e 5 bits para a identificação do host, permite ter exatamente 6 subredes e cerca de 30 dispositivos ligados a cada subrede. Como na eventualidade de ser necessária uma nova subrede, esta divisão já estaria no seu limite, seria necessária uma nova gestão e reimplementação de todos os endereços da rede. Assim, optamos por uma divisão do octeto em 4 bits para a subrede e 4 bits para identificar as interfaces. Apesar de isto só permitir cerca de 14 ligações em cada subrede, permite que novas subredes sejam criadas e estruturadas no futuro, sem alterar a implementação atual.

192.168.128.0/24 -> 8bits livres para gestão

192.168.128. \_ \_ \_ \_ | \_ \_ \_ \_

**Identificar subrede**

**Identificar subrede**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 |
| Reservado | Subrede 1 | Subrede 2 | Subrede 3 | Subrede 4 | Subrede 5 | Subrede 6 | Subrede 7 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 0111 |
| Subrede 8 | Subrede 9 | Subrede 10 | Subrede 11 | Subrede 12 | Subrede 13 | Subrede 14 | Reservado |

Ás subredes do nosso sistema atribuímos os 6 primeiros valores da tabela apresentada anteriormente. Os endereços são do tipo x/28 porque dos 24 que anteriormente identificavam a rede, existem mais 4 reservados para identificar as subredes.

Subrede 1 – 192.168.128.16/28

Subrede 2 – 192.168.128.32/28

Subrede 3 – 192.168.128.48/28

Subrede 4 – 192.168.128.64/28

Subrede 5 – 192.168.128.80/28

Subrede 6 – 192.168.128.96/28

A subrede 1 terá a gama de endereços uteis para interfaces desde 192.168.128.17 até 192.168.128.31;

A subrede 2 terá a gama de endereços uteis para interfaces desde 192.168.128.33 até 192.168.128.47;

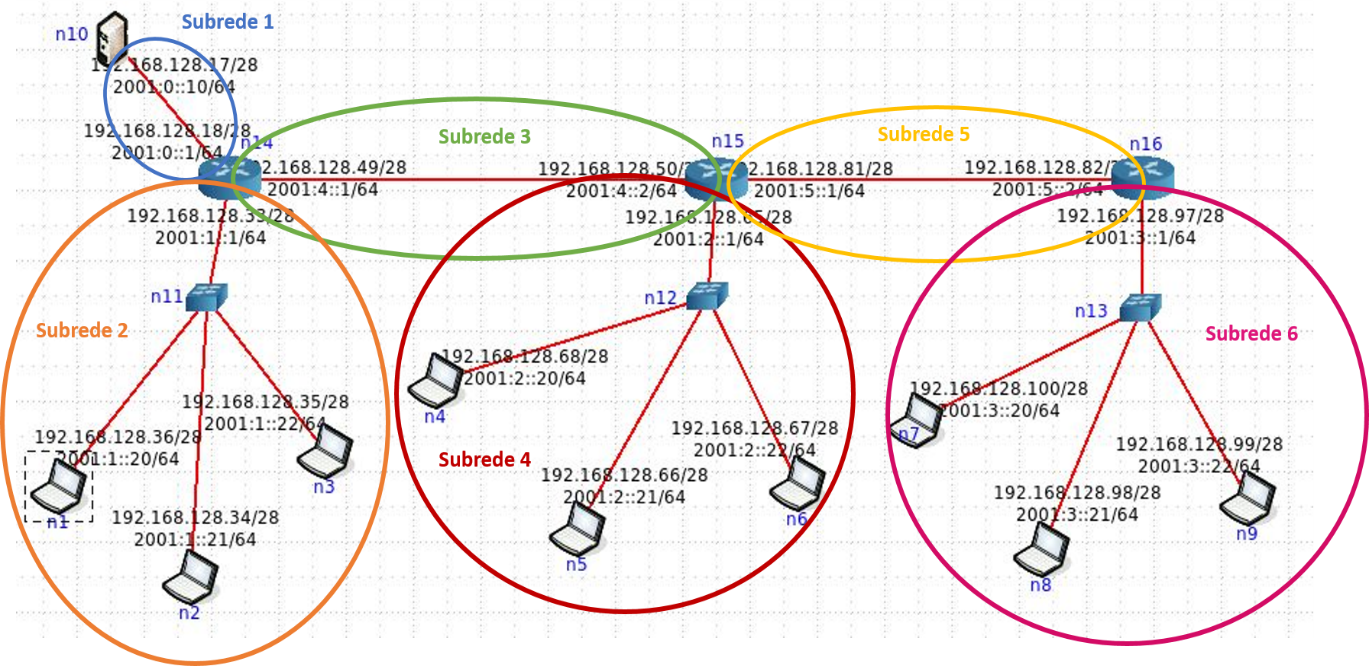
A subrede 3 terá a gama de endereços uteis para interfaces desde 192.168.128.48 até 192.168.128.63;

A subrede 4 terá a gama de endereços uteis para interfaces desde 192.168.128.65 até 192.168.128.79;

A subrede 5 terá a gama de endereços uteis para interfaces desde 192.168.128.81 até 192.168. 128.95;

A subrede 6 terá a gama de endereços uteis para interfaces desde 192.168.128.97 até 192.168.128.111;

A distribuição das redes é ilustrada pela seguinte figura com o modelo CORE



1. **Qual a máscara de rede que usou (em formato decimal)? Justifique.**

Como os endereços são do tipo x/28 (explicado na questão 1 deste grupo) os endereços máscara da rede são 255.255.255.240.

Como existem 4 bits do ultimo octeto a definir as subredes

1. **Quantos *hosts* IP pode interligar em cada departamento? Justifique.**

Para cada interface dos router dos departamentos, que terão a sua própria subrede, podem ser ligados até 14 hosts.

Por isso, um departamento pode ter no máximo 14\*N, onde N é o numero de interfaces do router ativas e a ser usadas num dado departamento.

1. **Garanta que conectividade IP entre as várias redes locais da empresa MIEInet é mantida.**

# Conclusão

Com a realização da parte I deste trabalho, foi possível compreender o processo de fragmentação para o envio de Datagramas de grades dimensões sobre a rede Ethernet, onde o tamanho por pacote é limitado a 1500Bytes.

De forma sucinta, apreendemos que neste processo de fragmentação de Datagramas os fragmentos do mesmo pacote original são identificados pelo mesmo ID (valor do campo Identification do protocolo IPv4) e irão ter no máximo 1480Bytes de dados, pois 20Bytes são ocupados pelo cabeçalho do protocolo referido.

O processo de reconstrução é feito de forma correta recorrendo ás informações do campo ‘Identification’: para juntar todos os fragmentos do mesmo pacote original, sem misturar fragmentos de diferentes Datagramas iniciais; do campo ‘Flags’: que indica se existem mais fragmentos ou se o fragmento em análise é o último e do campo ‘Fragmente offset’: que indica onde deve ser a posição a encaixar o fragmento para reconstruir o pacote original.

Para uma configuração do tamanho de mensagem padrão (no nosso caso de estudo 56Bytes mas podia ser qualquer valor que não exceda o limite de 1500Bytes ) não existe a necessidade de realizar fragmentação porque o datagrama pode circular na rede sem problemas.

Ana Esmeralda Fernandes A74321

Bárbara Nadine Freitas Oliveira A75614

Miguel Dias Miranda A74726

Redes de Computadores

TP4: Protocolo IPv4

Novembro de 2016