Universidade do Minho

Licenciatura em Ciências da Computação

Sistemas de Comunicações e Redes

Ensaio Escrito

Nível de Ligação Lógica - Ethernet e Protocolo ARP; Redes Sem Fios (IEEE 802.11)

Grupo 28

Davide Santos (A102938)

Edgar Araújo (A102946)

Pedro Augusto Camargo (A102504)

Outubro 2023

Contents

1 Parte 1

Analise da fragmentação de pacotes I

Foi capturado o tráfego gerado pelo comando: ping -s 6328 marco.uminho.pt

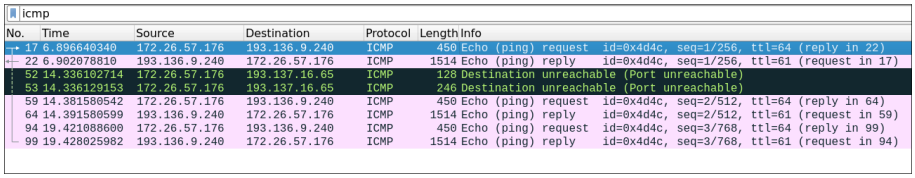

Figure 1: Ping

a. Localize a primeira mensagem ICMP.

i) Porque é que houve necessidade de fragmentar o pacote inicial?

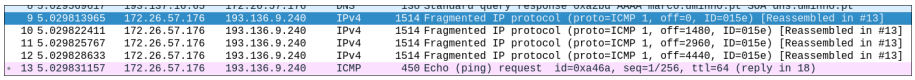

Figure 2: Fragment

A necessidade surge de o facto de o tamanho do pacote ser superior ao MTU da rede, ou seja, não cabe num único pacote. O MTU da rede é de 1500 bytes, e o tamanho do pacote é de 6328 bytes, logo é necessário fragmentar o pacote.

ii) Em que equipamento da rede ocorreu essa fragmentação?

A fragmentacao ocorreu no computador que enviou o pacote.

b. Imprima o primeiro fragmento do datagrama IP.

i) Que informação no cabeçalho indica que o datagrama foi fragmentado?

A opcao MF, que indica que o pacote foi fragmentado, pode ser observada no wireshark, dentro do campo Flags, no cabeçalho IP.

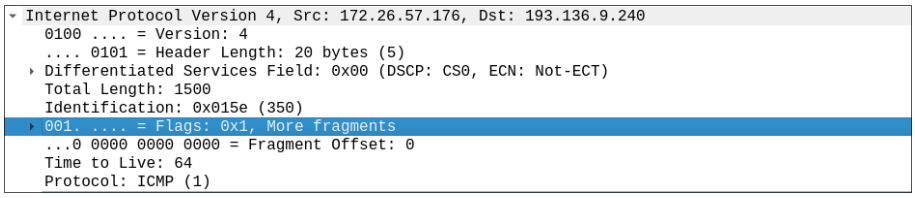

Figure 3: More Fragments

ii) Que informação no cabeçalho IP indica que se trata do primeiro fragmento?

O campo Fragment Offset indica que se trata do primeiro fragmento, uma vez que o seu valor é 0.

iii) Qual é o tamanho deste fragmento?

O tamanho do fragmento é de 1500 bytes, tal como indica o campo Total Length.

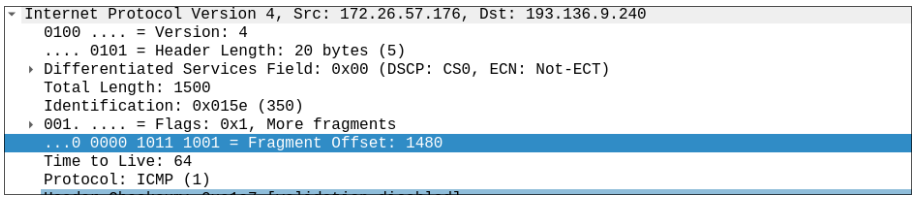

Figure 4: More Fragments Com Offset

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

O campo Fragment Offset indica que não se trata do primeiro fragmento, uma vez que o seu valor é 1480. O campo MF indica que há mais fragmentos, uma vez que o seu valor é 1. Logo basta que: Fragment Offset != 0 $\wedge$ MF == 1 para sabermos que não se trata do primeiro fragmento.

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

Os campos que mudam sao:

- Flag More Fragments (MF)
- Fragment Offset
- Total Length

Os campos que permitem reconstruir o datagrama original, sao o Fragment Offset, e a flag MF, pois estes permitem saber a ordem exata dos fragmentos, de forma a reconstruir tal e qual como antes de ser fragmentado.

e. Como se deteta o último fragmento correspondente ao datagrama original? Estabeleça um filtro no Wireshark que permita listar o último fragmento do primeiro datagrama IP segmentado.

ip.flags.mf == 0

f. Identifique o equipamento onde o datagrama IP original é reconstruído a partir dos fragmentos. A reconstrução poderia ter ocorrido noutro equipamento diferente do identificado? Porquê?

O equipamento onde o datagrama IP original é reconstruído é o servidor de IP: 193.136.9.240, ou seja, o servidor de marco.uminho.pt. A reconstrução poderia ter ocorrido noutro equipamento desde que a MTU fosse superior a MTU da ligacao anterior, ou seja maior que 1500 bytes, e que o equipamento tivesse a capacidade de reconstruir o datagrama original.

g. Por que razão apenas o primeiro fragmento de cada pacote é identificado como sendo um pacote ICMP?

Apenas o primeiro fragmento de cada pacote é identificado como sendo um pacote ICMP, pois o conceito de ICMP tem por base os cabecalhos IP, e o conceito de fragmentacao de datagramas IP e relativo ao cabecalho IP.

h. Determine o valor máximo de SIZE sem que ocorra fragmentação do pacote? Justifique o valor obtido, relacionando-o com o MTU (Maximum Transmission Unit) da rede.

Apos observar o output do comando ping no linux: Reparei que houve um acrescimo de 28 bytes na informacao enviada, para acomodar todos os cabecalhos essenciais na trasnmissao do pacote.

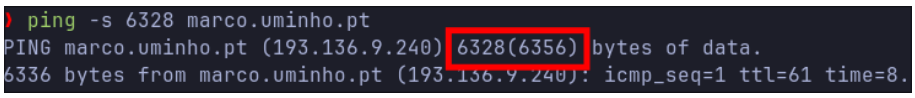

Figure 5: Comando Ping no Linux

Logo o valor maximo de SIZE sem que ocorra fragmentacao do pacote e de 1472 bytes, pois 1472 + 28 = 1500 bytes, que e o MTU da rede.

2 Parte 2

2.1 Endereçamento e Encaminhamento IP

2.1.1 Atribua um conjunto de endereços IP válidos (públicos) aos diversos sistemas da GEO, devendo o seu nº de grupo estar presente em pelo menos um octeto da componente de rede. Use máscaras (prefixos) de rede que respeitem a divisão clássica de endereçamento por classes (ver a tabela em anexo).

2.1.2 Diga, justificando, se na rede está a ser usado encaminhamento estático ou dinâmico (e.g. baseado no protocolo OSPF - Open Shortest Path First). (Sugestão: analise os processos que estão a correr em cada sistema (hosts, routers) usando, por exemplo, o comando ps -ax).

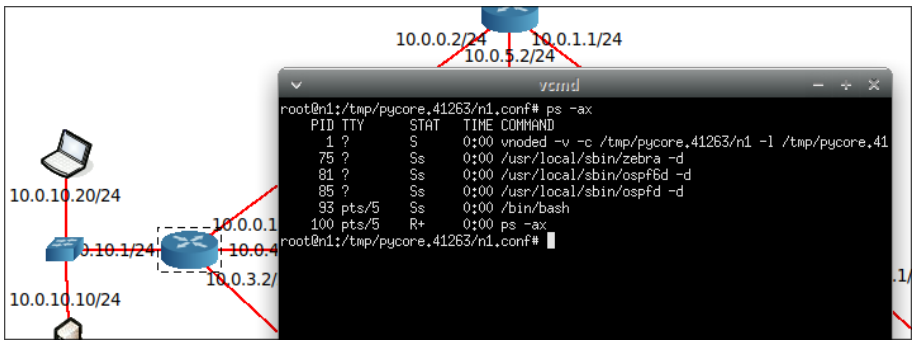

Figure 6: OSPF no router

Conforme a figura acima demonstra, o router esta a usar o protocolo OSPF, logo esta a usar encaminhamento dinamico, pois nao foi necessario especificar as rotas manualmente, e o protocolo ficou responsavel por isso.

2.1.3 Apague na tabela de encaminhamento do router de cada departamento e do router central a entrada respeitante à rede da interface wireless do router RISP. Confirme que os sistemas da GEO deixaram de ter acesso à interface wireless do router RISP. Usando apenas rotas por defeito, altere as tabelas de encaminhamento desses routers de forma a tornar novamente acessível o acesso à Internet através da interface wireless do router RISP.

Apos apagar a entrada respeitante a rede da interface wireless do router RISP, os sistemas da GEO deixaram de ter acesso a interface wireless do router RISP, pois nao sabem para onde encaminhar os pacotes.

Para retormar o acesso a interface wireless do router RISP, foi necessario adicionar 2 rotas manualmente.

- No router 1 foi executado o comando: ip route add default via 10.0.4.2
- No router 2 foi executado o comando: ip route add default via 10.0.9.1

Mas de forma a retornar a conexao de cada departamento a internet, foi necessario adicionar uma rota por defeito no router de cada departamento em direcao ao router central, seguindo o mesmo esquema: ip route add default via "ip do router central".

Apos testar, todos os departamentos conseguiram aceder a internet.

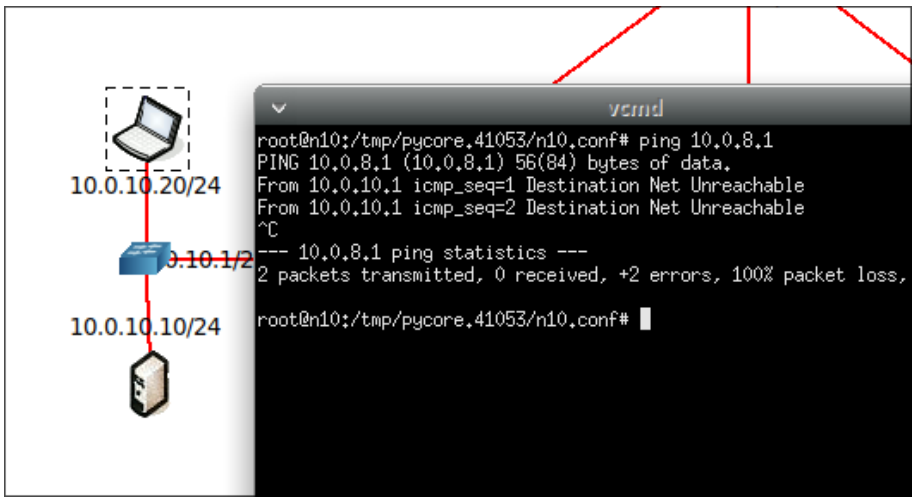

Figure 7: Antes de routing manual

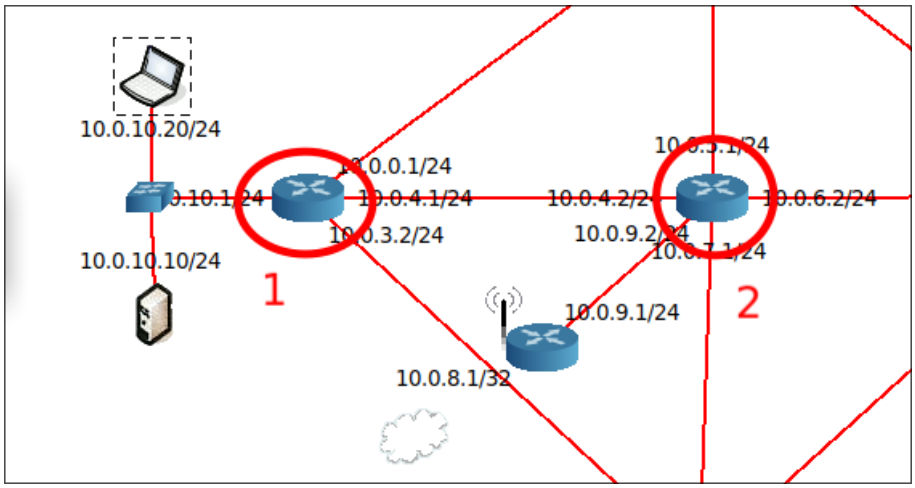

Figure 8: Routing manual

2.2 Definição de Sub-redes

2.2.1 Apresente uma imagem que mostre claramente o esquema de endereçamento de subredes adotado. Deve justificar as opções tomadas.

Tem em conta que existem 4 departamentos, apenas seriam necessarios 2 bits para representar as 4 subredes, mas como o enunciado pede que seja reservada pelo menos uma rede para uso futuro, foram reservados 3 bits para representar as subredes, ou seja, 8 subredes.

Logo as subredes seguem o seguinte formato de endereçamento, tendo por base o endereco 10.0.10.xx/24:

- Subrede 1 - 10.0.10.0/27 - sendo .0 o valor do ultimo octeto, com o bit

$$2^7 = 0 \wedge 2^6 = 0 \wedge 2^5 = 0$$

- Subrede 2 - 10.0.10.64/27 - sendo .64 o valor do ultimo octeto, com o bit

$$2^7 = 0 \wedge 2^6 = 1 \wedge 2^5 = 0$$

- Subrede 3 - 10.0.10.128/27 - sendo .128 o valor do ultimo octeto, com o bit

$$2^7 = 1 \wedge 2^6 = 0 \wedge 2^5 = 0$$

- Subrede 4 - 10.0.10.192/27 - sendo .192 o valor do ultimo octeto, com o bit

$$2^7 = 1 \wedge 2^6 = 1 \wedge 2^5 = 0$$

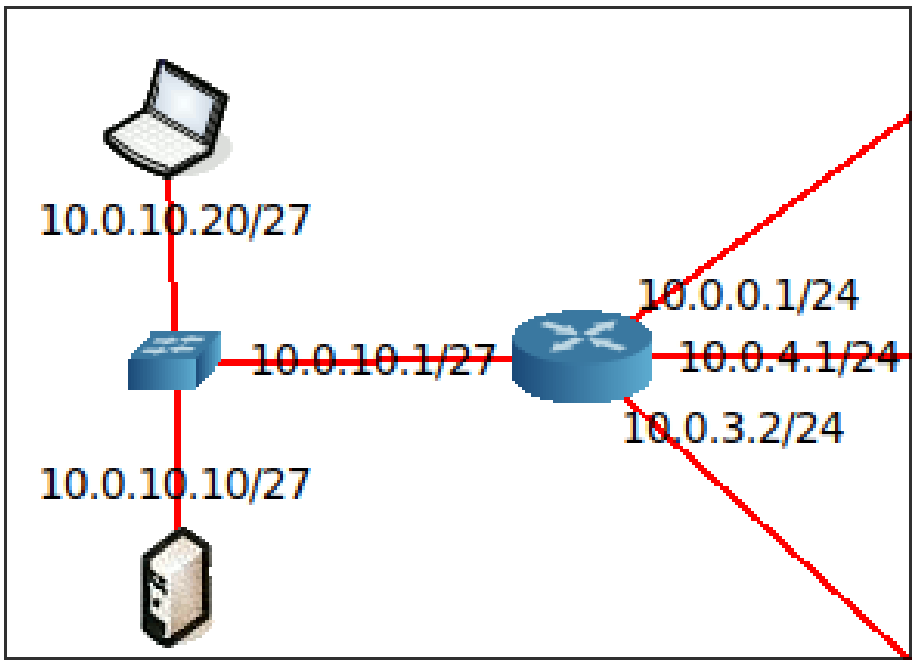

Figure 9: Subnetting

2.2.2 Qual a máscara de rede que usou? Quantos hosts IP pode interligar no máximo em cada departamento? Quantos endereços de sub-rede ficam disponíveis para uso futuro? Justifique.

A mascara de rede usada foi 255.255.255.192, em formato CIDR /27 pois foram reservados 3 bits para representar as subredes, dos ja reservados 24 bits para representar a rede principal. Sobram-nos 5 bits para representar os hosts, logo temos 32 enderecos disponiveis para hosts, mas como o endereco de rede e o endereco de broadcast nao podem ser usados, ficam disponiveis 30 enderecos para hosts. A nivel das subredes, ficam disponiveis 4 subredes para uso futuro, pois das 8 subredes possiveis, apenas foram usadas 4.

2.2.3 Garanta e verifique que a conectividade IP entre os vários departamentos é mantida. Explique como procedeu.

Para verificar a conectividade, foi feito ping de cada departamento para cada departamento, e todos os pings foram bem sucedidos.