**3. Captura e análise de Tramas Ethernet**

1. **Anote os endereços MAC de origem e de destino da trama capturada. Identifique a que sistemas se referem. Justifique.**

**R:**

Figura 1 - Endereços MAC (origem destino)

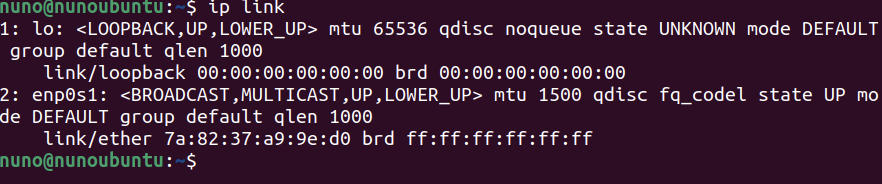
****Os sitemas referidos na imagem acima são o da interface do computador que utilizou o Wireshark “Src”, e o do servidor do website <https://alunos.uminho.pt> representado com o endereço “Dst”.Sabemos que os ips estão corretos, uma vez que com o comando “ip link” conseguimos aceder ao ip link do sistema que estamos utilizar que, por sua vez, é coincidente com o endereço MAC de “source” capturada no Wireshark.

Figura 2 - Output após a utilização do comando “ip link”

1. **Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?**

**R:** O valor do campo “Type” em hexadecimal é o que está rodeado na imagem mencionada em baixo e representa o protocolo da camada superior utilizada.

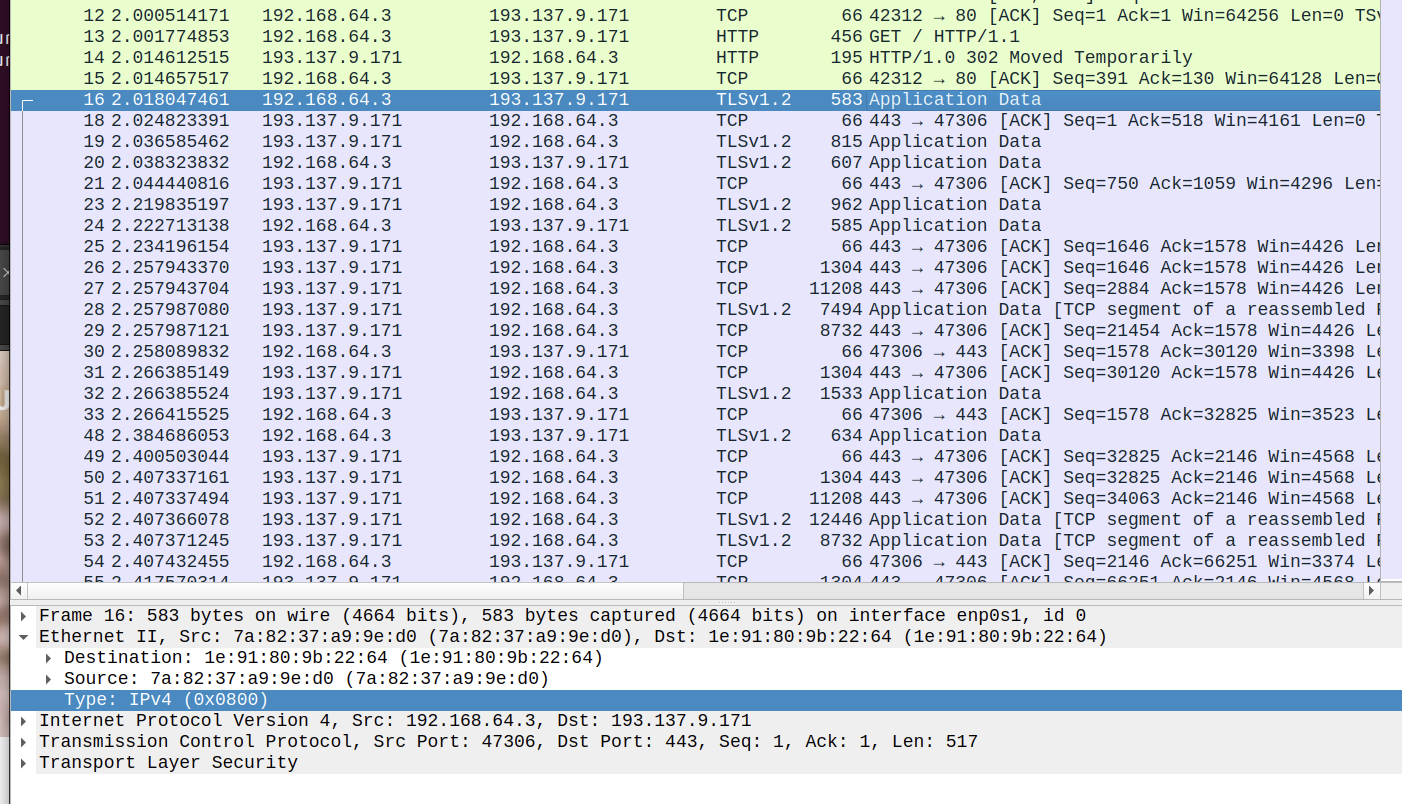
****

Figura 3 – Campo “Type” em hexadecimal

1. **Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional (Application Data Protocol: http-over-tls, no caso de HTTPS)? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.**

Bytes do cabeçalho:

74 + 74 + 66 + 583 + 66 + 6212 + 66 + 224 + 66 + 117 + 66 = 7614 bytes

Bytes do “Aplication Data”:

542+66+815+66+576+66+962+544+66+1304+15241+205+66+1304+13462+66+543 = 35884 bytes

⬄ Resultado: 0,175 (17,5%)

1. **Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.**

**Uma imagem com texto

Descrição gerada automaticamente**

Figura 4 – Trama que contêm o primeiro byte da resposta HTTP

O endereço da Ethernet da fonte é 1e:91:80:9b:22:64 e corresponde ao default gateway da rede local. Uma vez que o servidor do website se encontra fora das ligações diretas à interface de rede do nosso computador, é necessário recorrer ao “default gateway” para realizar uma conexão.

1. **Qual é o endereço MAC do destino? A que sistema (host) corresponde?**

O endereço MAC do destino está presente na Figura 4 com Dst: 7a:82:37:a9:9e:d0, que por sua vez, corresponde à interface ethernet do computador utilizado

1. **Atendendo ao conceito de encapsulamento protocolar, identifique os vários protocolos contidos na trama recebida. Justifique, indicando em que campos dos cabeçalhos capturados se baseou.**

Tendo em conta as figuras apresentadas anteriormente, os protocolos que surgem na trama recebida são os seguintes: Ethernet, IPv4, TCP.

**Uma imagem com gráfico

Descrição gerada automaticamente4. Protocolo ARP**

Figura 5 – Printscreen da topologia utilizada

1. **Abra uma consola no PC onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando arp -a.**
2. **Com a ajuda do manual ARP (man arp), interprete o significado de cada uma das colunas da tabela.**

**R:**

Figura 6 - Output após o comando arp -a

O endereço 192.168.15.1 corresponde apenas ao gateway da rede local e o endereço MAC que este está a utilizar é o 00:00:00:aa:00:00 que está conectado à interface eth0.

1. **Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.**

Tendo em contas as conexões que cada equipamento da intranet possui, podemos concluir que, o que terá uma tabela ARP com mais entradas será o “switch layer 2”.

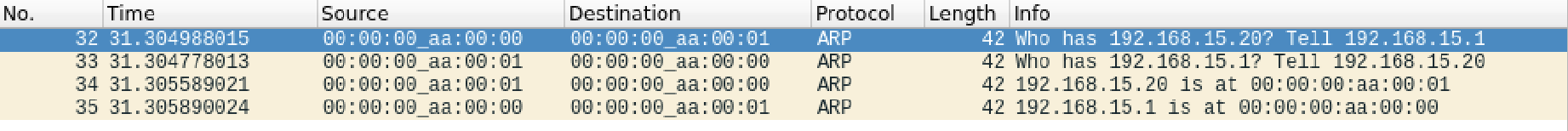
1. **Observe a trama Ethernet que contém a mensagem com o pedido ARP (ARP Request).**
2.  **Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?**

Figura 7 – Printscreen do Wireshark com a informação com o pedido

O valor hexadecimal do Endereço MAC de destino é o 00:00:00\_aa:00:01 que corresponde ao endereço do computador utilizado e o 00:00:00\_aa:00:00 corresponde ao pc “n5”. Dado que o computador volta a receber mensagem o endereço de destino tem de ser desse mesmo computador.

1. **Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?**

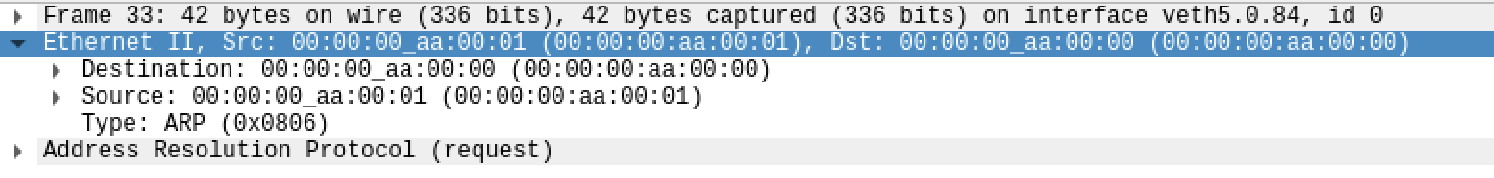
****



Figura 8 - Campo “Type” em hexadecimal

O valor em hexadecimal está rodeado no ficheiro em cima e indica que se trata de um protocolo ARP.

1. **Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.**

Uma das formas para conseguirmos concluir que se trata de um pedido ARP é através do opcode com o valor de “Request (1) ” indicando que se trata de uma mensagem de pedido. Uma outra forma de sabermos que se trata de uma mensagem de pedido é através da coluna de informação, presente na Figura 6.

1. **Explicite, em linguagem comum, que tipo de pedido ou pergunta é feita pelo host de origem à rede?**

A pergunta que é feita pelo “host” à rede é a seguinte: Quem é o 192.168.15.20? Pergunta ao 192.168.15.1.

Estas perguntas são feitas dada à associação que o endereço MAC tem com o endereço IP que permite que os dispositivos de rede comuniquem entre si em uma rede local usando o protocolo Ethernet.

1. **Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.**
2. **Qual o valor do campo ARP opcode? O que especifica?**

Uma imagem com texto, carta

Descrição gerada automaticamente

Figura 9 – Printscreen do valor do Opcode

Podemos observar o valor do campo ARP opcode na imagem em cima, “Reply (2)” e, este representa a operação que foi realizada.

1. **Uma imagem com texto, carta

   Descrição gerada automaticamenteEm que posição da mensagem ARP está a resposta ao pedido ARP efetuado?**

Figura 10 – Printscreen da posição da mensagem ARP

A posição da mensagem ARP, está presente no campo “Sender MAC adress” tal como mostra a figura 10.

1. **Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos ifconfig, netstat -rn e arp executados no PC selecionado.**

Depois de executados os comandos, “ifconfi” e “arp”, tal como demonstrado na figura em cima, obtivemos os seguintes resultados. Através dos mesmos, podemos concluir que o endereço de destino corresponde ao router do departamento A e o de origem corresponde ao do computador n5.

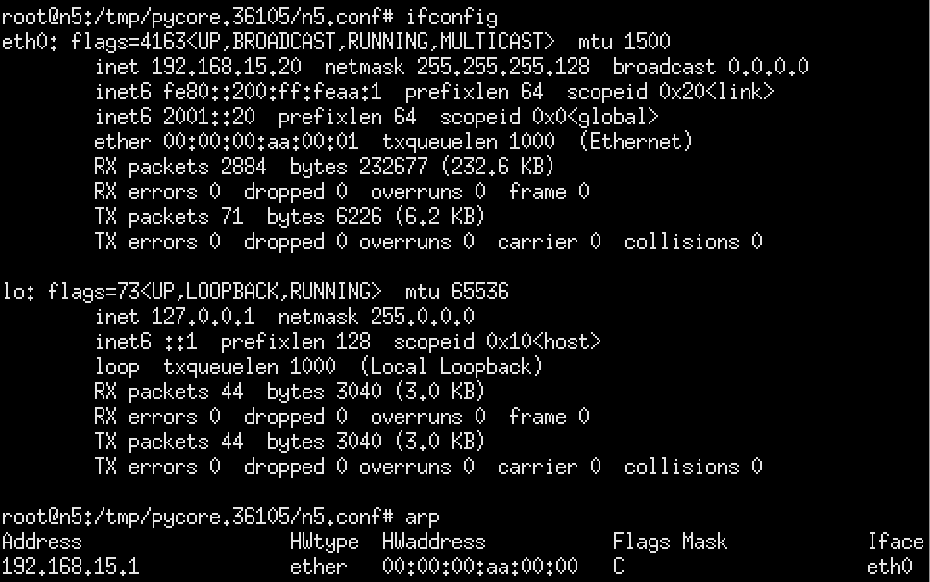


Figura 11 – Resultados após a utilização dos comandos “ifconfi” e “arp” no computador n5.

1. **Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).**

A comunicação usada no envio da resposta ARP é determinada pelo endereço MAC de destino incluído na mensagem ARP. A solicitação ARP é enviada como uma mensagem de Broadcast para o endereço (FF:FF:FF:FF:FF:FF) garantindo que todos os dispositivos na rede local recebem a solicitação. O dispositivo que tiver o endereço IP correspondente irá responder com uma mensagem unicast para o dispositivo que solicitou o endereço MAC correspondente. Isso minimiza o tráfego da rede desnecessário e garante que a reposta ARP seja entregue apenas ao dispositivo que solicitou.

1. **Verifique se o ping feito ao segundo PC originou pacotes ARP. Justifique a situação observada**

**Uma imagem com mesa

Descrição gerada automaticamente**

Figura 12 – Printscreen do wireshark do segundo pc

Analisando a figura em cima é possível perceber que foram originados pacotes ARP dado pelo envio dos pedidos em Broadcast. Isto deve se ao facto de uma vez que o sistema tem as caches dos routers limpas, é necessário estabelecer pelo menos uma vez a associação entre IPv4 e MAC de uma respetiva interface. Desta forma, se lhes voltássemos a enviar os pedidos já não haveria pacotes ARP visto que estes seriam enviados em “unicast”.

1. **Identifique na mensagem ARP os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica que se pretendem mapear. Justifique os valores apresentados nesses campos.**

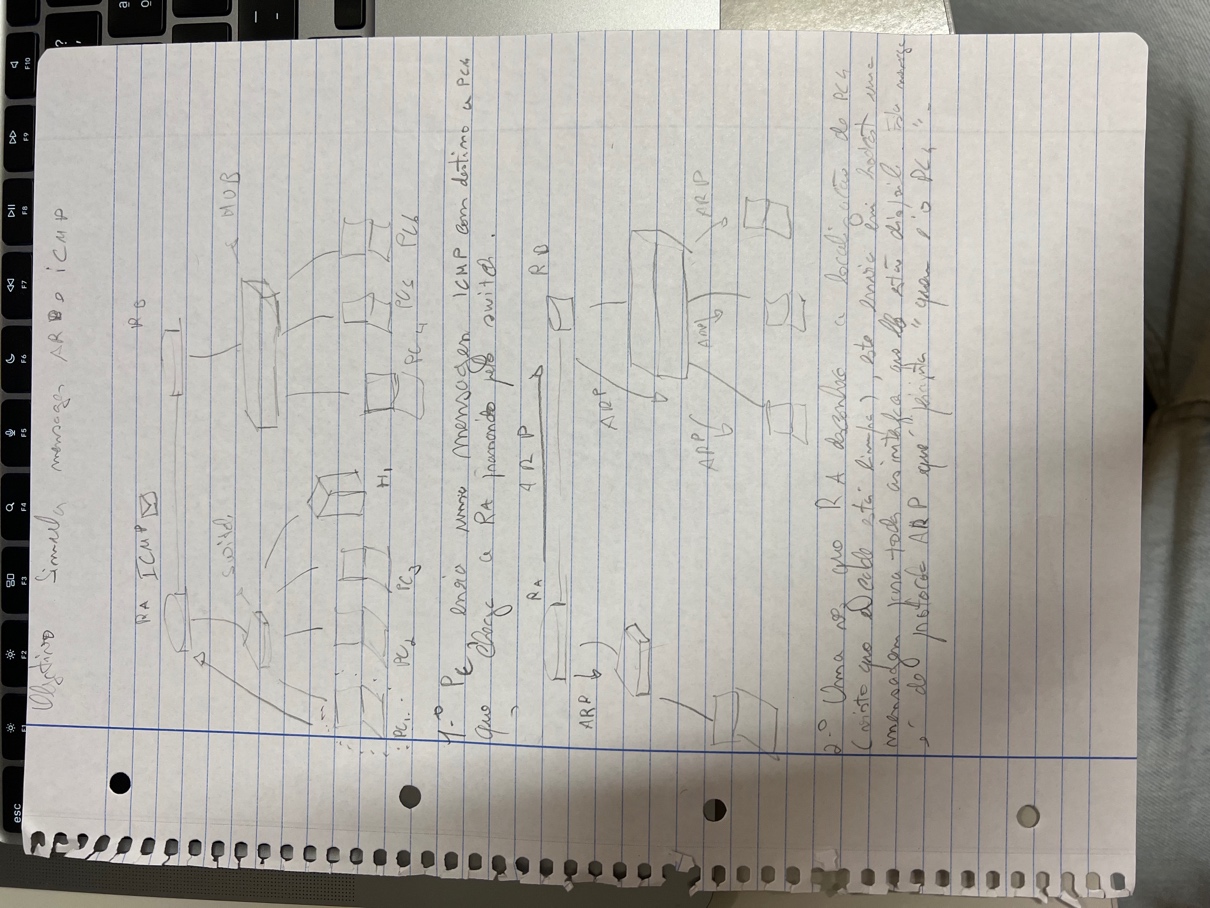
Uma imagem com texto

Descrição gerada automaticamente

Analisando a figura em cima, podemos observar que os tipos e os tamanhos dos endereços das camadas de rede.

Já o tipo e o tamanho do endereço de ligação lógica estão presentes no endereço MAC e tem geralmente 48 bytes.

1. **Na situação em que efetua um ping a um PC não local à sua sub-rede, esboce um diagrama em que indique claramente, e de forma cronológica, todas as mensagens ARP e ICMP trocadas, até à recepção da resposta ICMP do sistema destino (represente apenas os nós intervenientes). Assuma que todas as tabelas ARP se encontram inicialmente vazias.**

****

**Uma imagem com texto

Descrição gerada automaticamente**

**5. Domínios de colisão**

**1. Através da opção tcpdump, verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando é gerado tráfego intra-departamento (por exemplo, através do comando ping). Que conclui? Comente os resultados obtidos quanto à utilização de hubs e switches no contexto de controlar ou dividir domínios de colisão. Documente as suas observações e conclusões com base no tráfego observado/capturado.**

**Uma imagem com texto

Descrição gerada automaticamenteDepartamento A**

**Uma imagem com texto

Descrição gerada automaticamenteUma imagem com texto

Descrição gerada automaticamenteDepartamento B**

Figura 13 – Printscreens dos comandos tcpdump e ping no departamento A e B respetivamente

Como é possível ver na figura, no departamento B a rede é partilhada, devido ao recurso de um hub, o qual permite aos diferentes elementos do departamento visualizar as tramas enviadas pelos restantes dispositivos (tal como é o caso dos echo request/reply). Inicialmente o switch apresenta um comportamento semelhante ao hub, isto é, são enviados pacotes em “brodcast” até ao switch conhecer os dispositivos da rede. Depois de conhecer os endereços, o departamento A deixa de apresentar o mesmo comportamento, visto que neste a rede é comutada, devido ao procedimento de um switch, e, consequentemente, não é possível aos elementos que a ele pertencem capturar as tramas enviadas por outros dispositivos da mesma rede local.

**2. Construa manualmente a tabela de comutação do switch do Departamento A, atribuindo números de porta à sua escolha.**

|  |  |  |
| --- | --- | --- |
| **Porta** | **Endereço MAC** | **TTL** |
| **E1** | **00:00:00:aa:00:01** | **20** |
| **E2** | **00:00:00:aa:00:02** | **20** |
| **E3** | **00:00:00:aa:00:03** | **20** |
| **E4** | **00:00:00:aa:00:04** | **20** |