

**Redes de Computadores:**

Camada de Ligação Lógica: Ethernet e Protocolo ARP

**Grupo de Trabalho 2**

Ana Esmeralda Fernandes A74321

Bárbara Nadine Freitas Oliveira A75614

Miguel Dias Miranda A74726

Novembro de 2016

**Conteúdo**

[Camada de ligação lógica: Ethernet e Protocolo ARP – Parte I 3](#_Toc466314023)

[Captura e análise de tramas Ethernet 3](#_Toc466314024)

[Protocolo ARP 7](#_Toc466314025)

[ARP numa topologia CORE 10](#_Toc466314026)

[Camada de ligação lógica: Ethernet e Protocolo ARP – Parte II 13](#_Toc466314027)

[ARP Gratuito 13](#_Toc466314028)

[Domínios de colisão 14](#_Toc466314029)

[Conclusão 16](#_Toc466314030)

# Camada de ligação lógica: Ethernet e Protocolo ARP – Parte I

## Captura e análise de tramas Ethernet

**1) Qual é o endereço MAC da interface ativa do seu computador?**

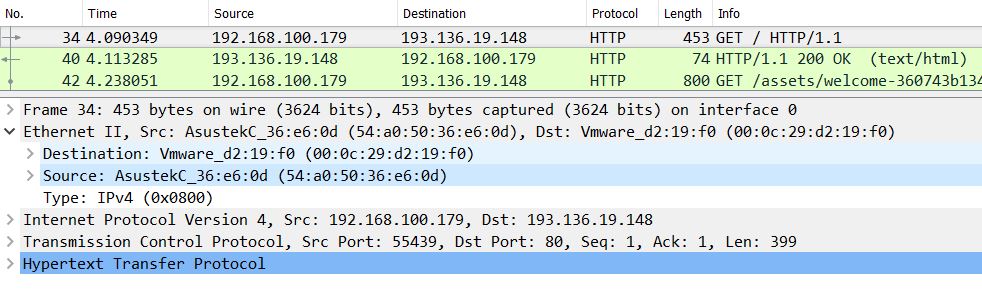
O endereço MAC da interface do computador é o 54:a0:50:36:e6:0d

Figura Endereço MAC origem frame 34

**2) Qual é o endereço MAC destino da trama? A que sistema é destinada essa trama, será o endereço Ethernet do servidor http para** *cesium.di.uminho.pt***? Justifique.**

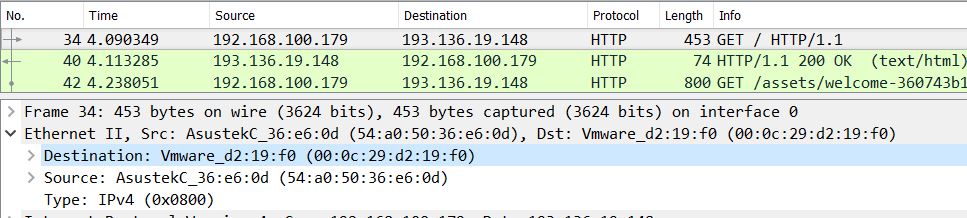
O endereço MAC do destino da trama é o 00:0c:29:d2:19:f0.

Figura Endereço MAC destino frame 34

A trama enviada é destinada ao sistema VmWare.

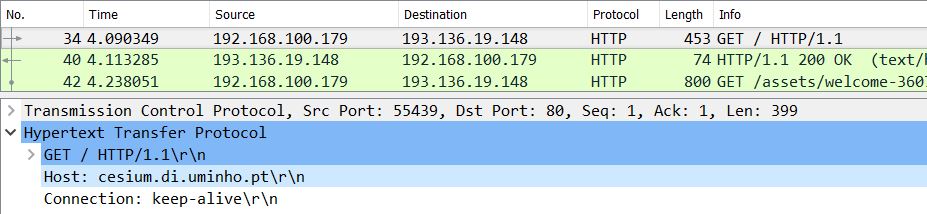
Como a informação listada na segunda linha da opção Hypertext Transfer Protocol, o Host da mensagem é o endereço *cesium.di.uminho.pt* então o destino desta trama é de facto o endereço MAC do router para cesium.di.uminho.pt.

Figura Host do endereço MAC frame 34

**3) Qual o valor hexadecimal do campo** *Type* **da trama Ethernet? O que significa?**

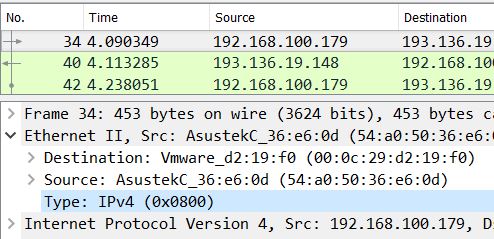
O valor hexadecimal *Type* da trama Ethernet apresenta o valor 0x0800 e identifica o tipo de dados que a frame enviada carrega (IPv4, IPv6, IPX, ARP, etc). Neste caso o valor 0x0800 indica que a frame tem nela um pacote de IPv4.

Figura Campo Type frame 34

**4) Quantos bytes são usados desde o inicio da trama até ao caracter ASCII “G” do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio HTTP GET.**

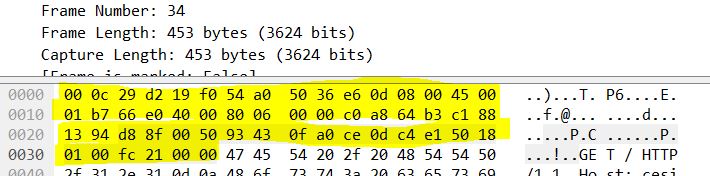
São usados, na nossa contagem, 54Bytes até ao caracter ASCII “G” do método HTTP GET.

Figura Bytes Controlo frame 34

Contamos 6 conjuntos de 8 pares + 6 pares. Cada par, por exemplo 00, 6c, 8f, tem 1Bytes porque cada valor isolado do par é um valor em hexadecimal que equivale a 4bits.

Logo 6x8 + 6 = 54Bytes.

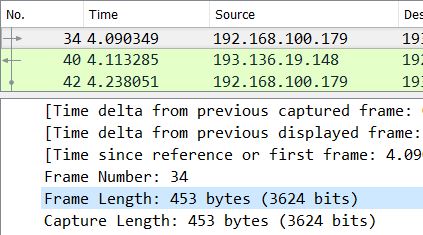
Na informação da opção Frame é possível ver que a Frame 34 (com o método HTTP GET em análise) tem como comprimento 453Bytes.

Figura Tamanho frame 34

Logo o

**5) Em ligações com fios suscetíveis a erros, nem sempre as NICs geram o código de deteção de erros. Verifique se o campo FCS está a ser utilizado. Aceda à opção Edit/Prefereces/Protocols/Ethernet e indique que é assumido o uso do campo FCS. Verifique qual o valor hexadecimal desse campo na trama capturada. Que conclui? Reponha a configuração original.**

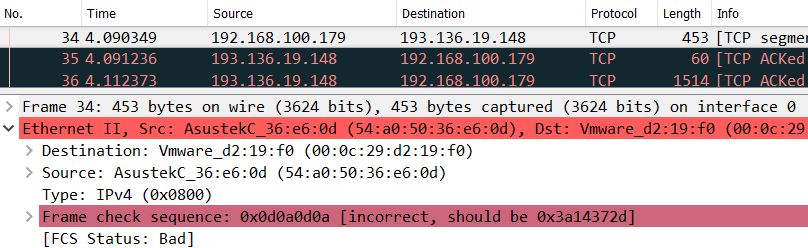
Selecionando o campo “Assume use of FCS”, na opção Ethernet II podemos ver que o valor da Fram check Sequence é 0x0d0a0d0a para a trama 34 (trama com o HTTP GET em estudo).

Figura Campo FCS da frame 34

Contudo, como surge sempre a mensagem “[ETHERNET FRAME CHECK SEQUENCE INCORRET]” e em frente á sequencia FCS da frame 34 “[incorrect: should be 0x3a14372d ] concluímos que este procedimento extra de deteção de erros não está a ser usado para validar os pacotes enviados, porque estes foram recebidos pelo recetor e o pedido gerado.

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

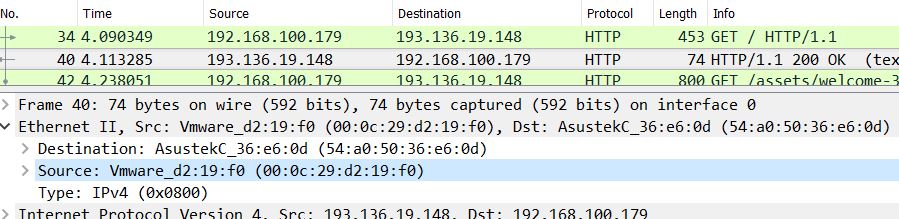
Analisando a trama 40, que contem o primeiro http response (ao pedido http get da trama 34 anterior) retiramos pelos dados do campo Ethernet II que o endereço MAC da fonte é 00:0c:29:d2:19:f0. Este endereço corresponde ao sistema VMware e é o mesmo que o endereço destino da trama 34 com o pedido http get.

Figura Endereço MAC origem frame 40

**7) Qual o endereço Ethernet da fonte? A que sistema corresponde?**

O endereço MAC do destino é 54:a0:50:36:e6:0d e corresponde ao sistema AsusTekc do utilizador que efetuou o pedido http get da trama 34.

**8) Qual o endereço MAC do destino? A que sistema corresponde?**

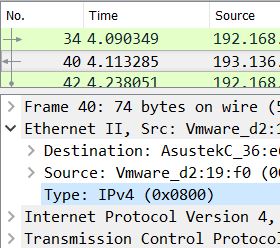
O campo Type da opção Ethernet II contem novamente o valor Hexadecimal 0x0800 o que indica que o pacote enviado na trama é IPv4.

Figura Campo Type frame 40

**9) Que tipo de resposta foi enviado pelo servidor?**

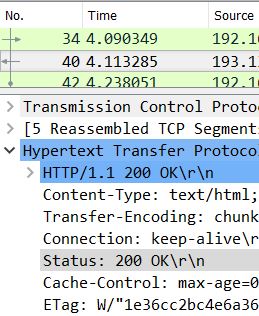
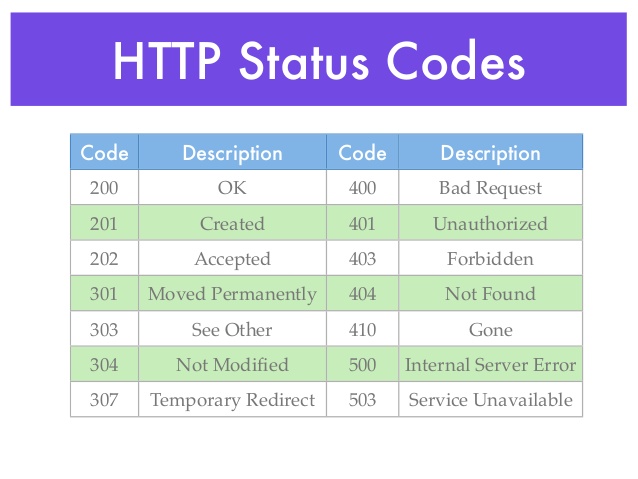
Observando o campo status da opção HyperText Transfer Protocol (e ainda na informação da tabela “info” da linha com a frame 40 ) vemos que a mensagem de resposta do servidor tem o código 200 que identifica que a requisição/pedido foi concluído com sucesso.

Figura 11 Códigos de Status HTTP

Figura 10 Campo Status frame 40

## Protocolo ARP

**10) Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas?**

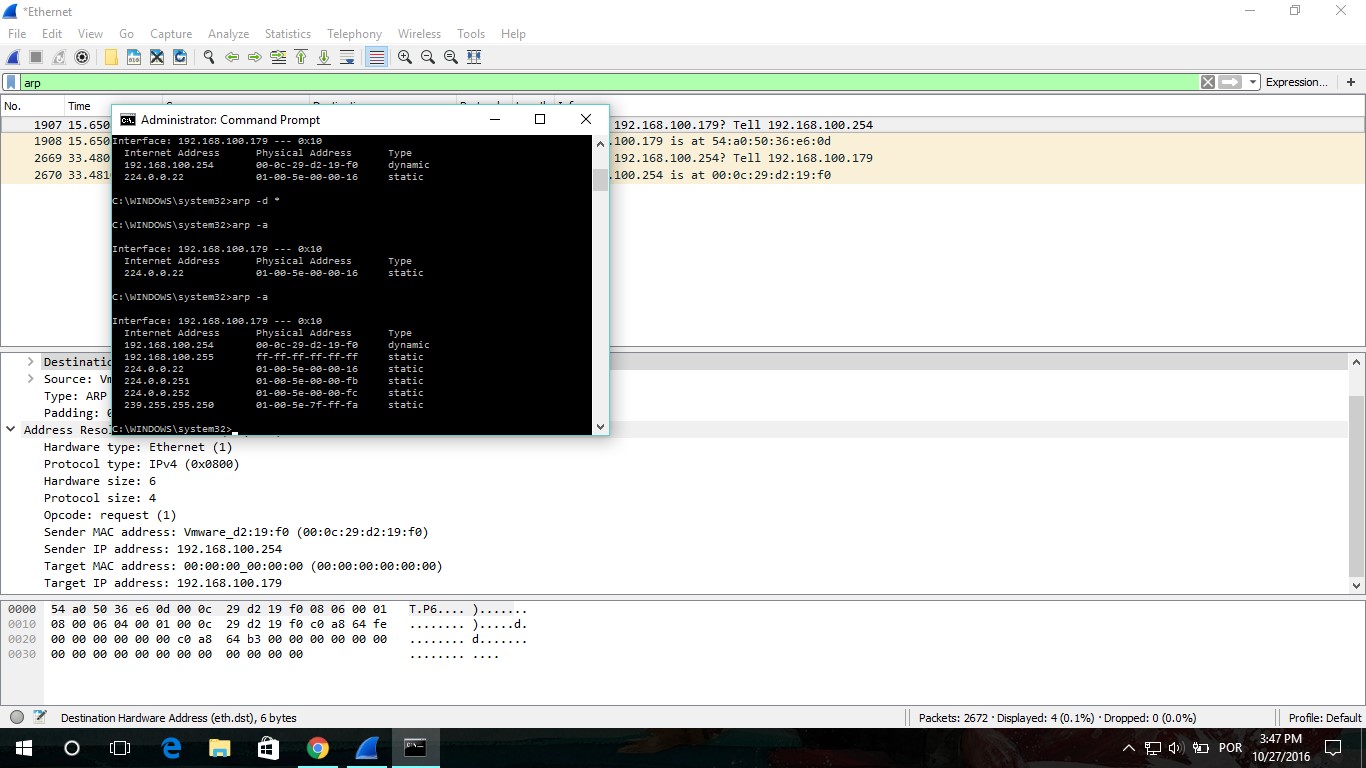
Na primeira coluna é possível ver os Internet Address (IP) e na segunda coluna os endereços físicos (Ethernet/MAC) associados aos endereços da primeira coluna. Na terceira e última coluna é listado o tipo de endereço, se dinâmico ou estático.

Figura 12 Comando "arp -a" no terminal Windows

**11) Qual o valor hexadecimal dos endereços origem e destino da trama Ethernet que contém a mensagem com o conteúdo ARP (ARP request)? Como interpreta e justifica o endereço destino usado?**

Considerando o nosso primeiro pedido ARP requisitado o valor hexadecimal do endereço de origem é 00:0c:29:d2:19:f0 e o endereço de destino é 54:a0:50:36:e6:0d.

Por algum motivo ou processo em segundo plano, o router da rede precisa de saber o nosso endereço MAC que não existe na sua tabela ARP. Nesta situação, o router envia um pacote de consulta ARP, perguntando a quem tem o endereço de IP 192.168.100.179 (portátil usado) que informe o seu endereço MAC para o IP 192.168.100.254 (do router).

Como este pedido ARP tem como endereço de destino MAC FF:FF:FF:FF:FF:FF é recebido por todos os portáteis, inclusive o nosso, daí o seu endereço Ethernet estar no destino deste pedido ARP. Com este pedido, o portátil com o endereço IP 192.168.100.179 envia um ARP reply ao router que fez a questão dizendo que o anterior IP está no endereço MAC 54:a0:50:36:e6:0d.

**12) Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?**

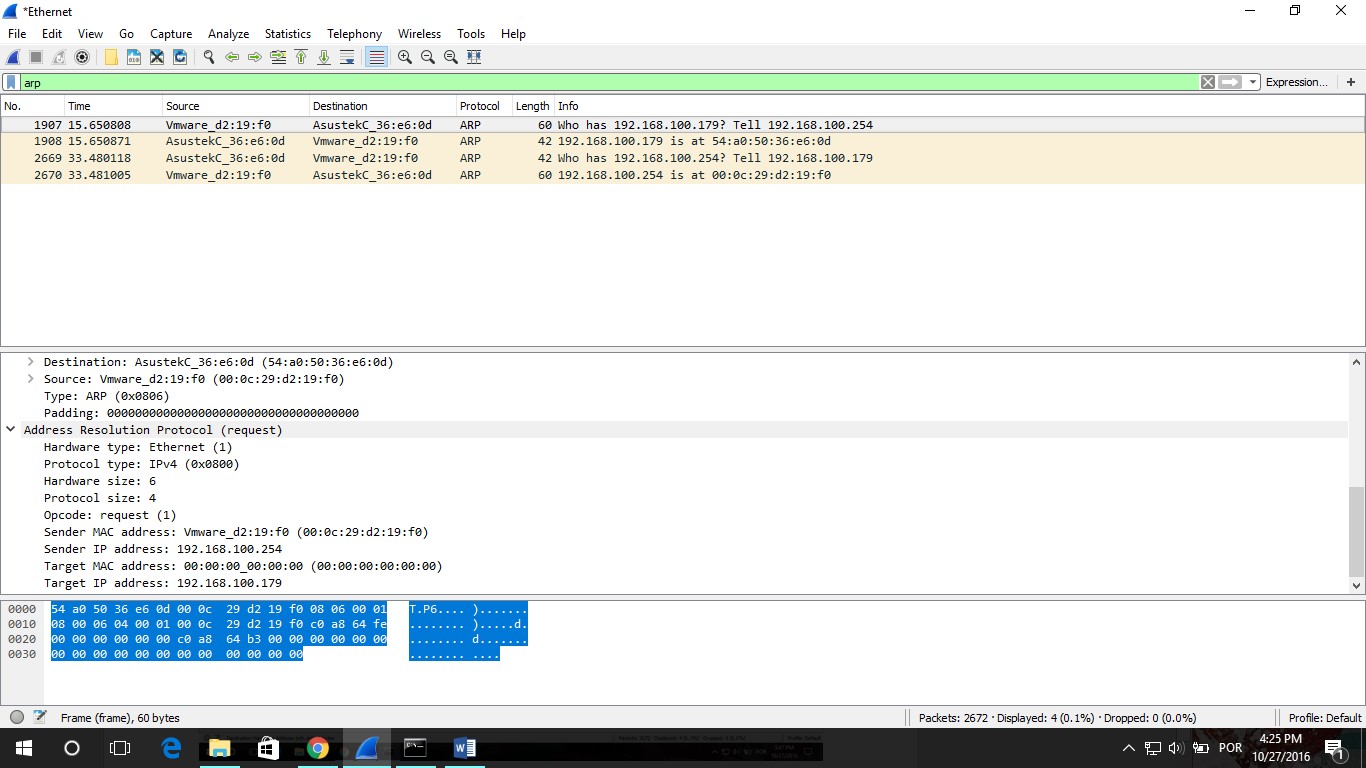
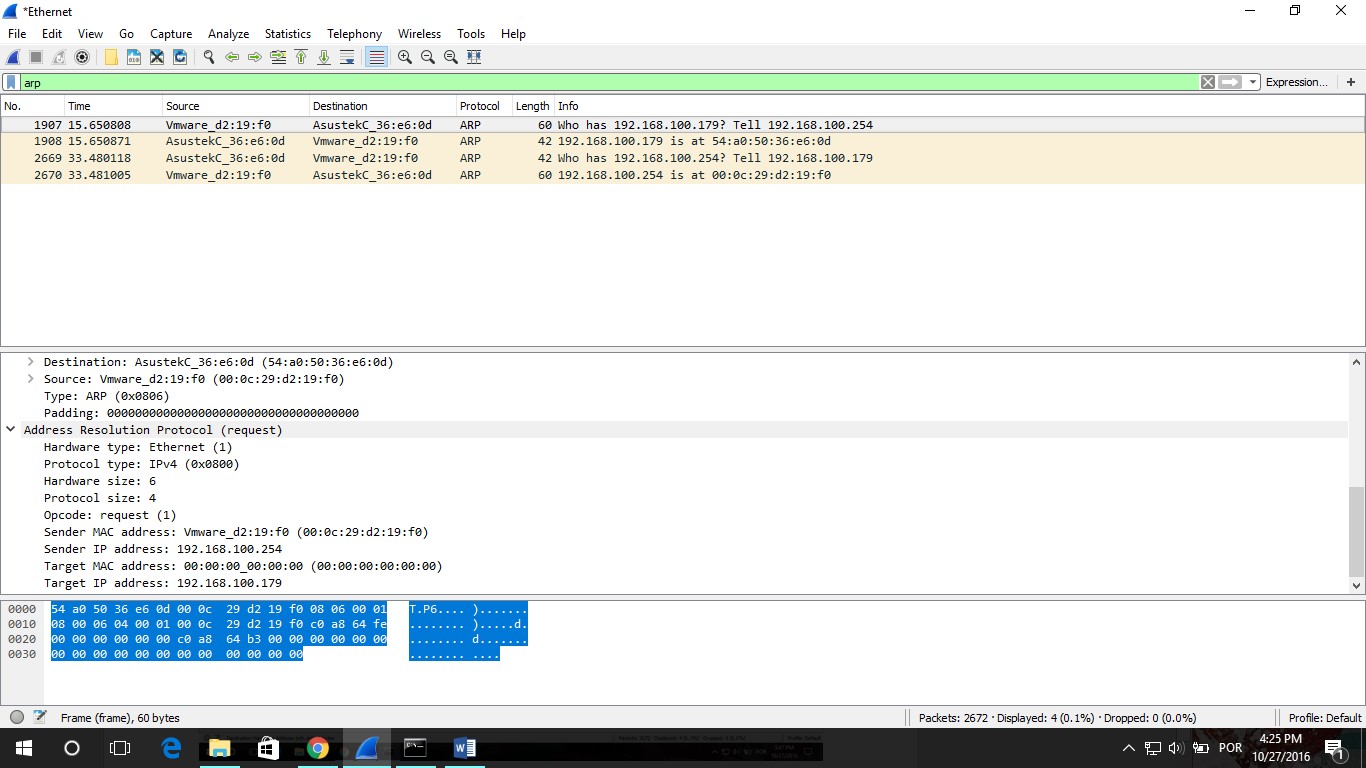
O valor hexadecimal do campo Type tem o valor 0x0806 e significa que o protocolo encapsulado na frame enviada é do tipo ARP .

Figura 13 Campo Type frame 1907 ARP request

Figura 14 Destino e origem da primeira frame ARP request

**13) Qual o valor do campo ARP opcode? O que especifica?**

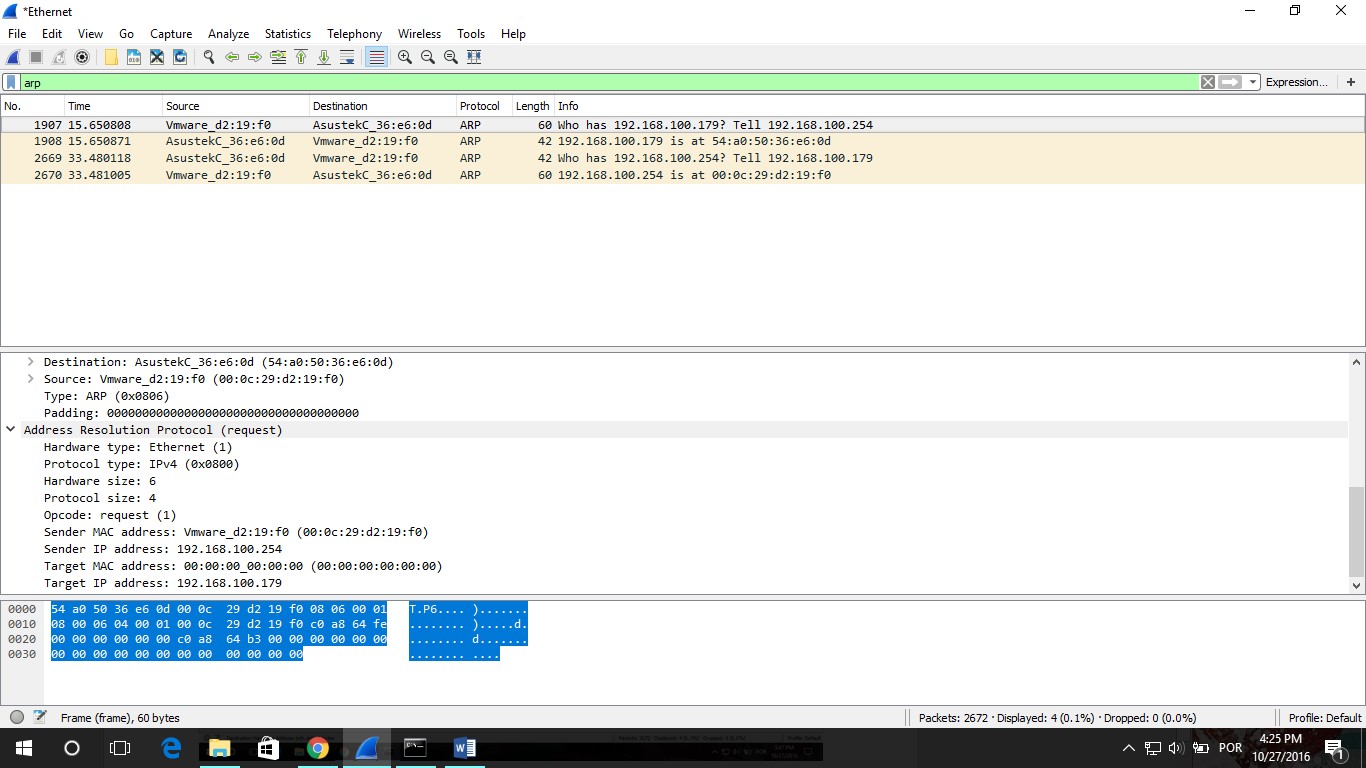
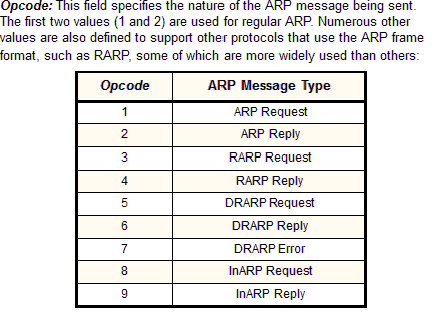
O campo opcode da opção Address Resolution Protocol (ARP) apresenta o valor 1 e especifica que se trata de um request (pedido ARP).

Figura 15 Campo opcode da frame ARP request e tabela com possíveis códigos para o campo opcode e seu significado

**14) A mensagem ARP contem o endereço IP de origem? Que tipo de pergunta é feita?**

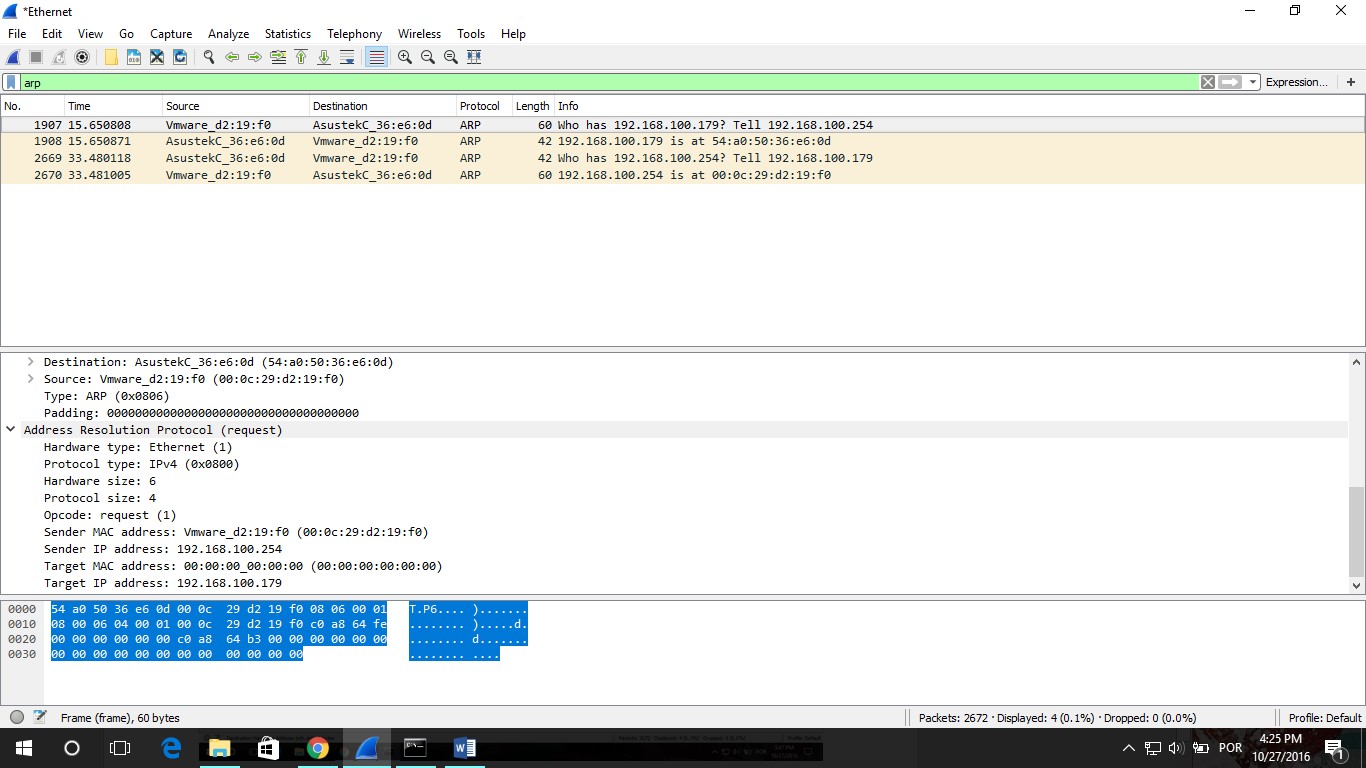
A mensagem ARP contem o endereço IP da origem, porque a fonte do pedido pergunta a quem tem o IP 192.168.100.179 (nosso portátil) e para lhe responderem para o seu IP 192.168.100.254.

Figura 16 Informação sobre o tipo de pergunta do ARP request

**15) Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.**

1. **Qual o valor do campo ARP opcode? O que especifica?**

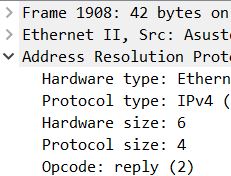
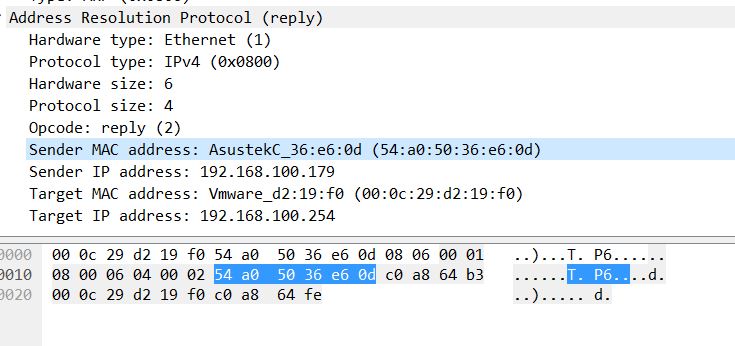
O valor do campo ARP opcode é 2 e especifica que a mensagem é um reply.

Figura 17 Campo opcode frame 1908 ARP reply

1. **Em que posição da mensagem ARP está a resposta ao pedido ARP?**

**16) Quais são os valores hexadecimais para os endereços origem e destino da trama que contém a resposta ARP? O que conclui?**

O valor hexadecimal do endereço de origem é 54:a0:50:36:e6:0d e o destino é 00:0c:29:d2:19:f0.

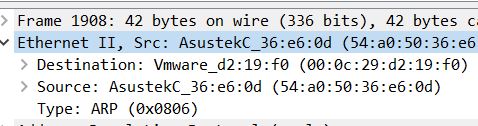
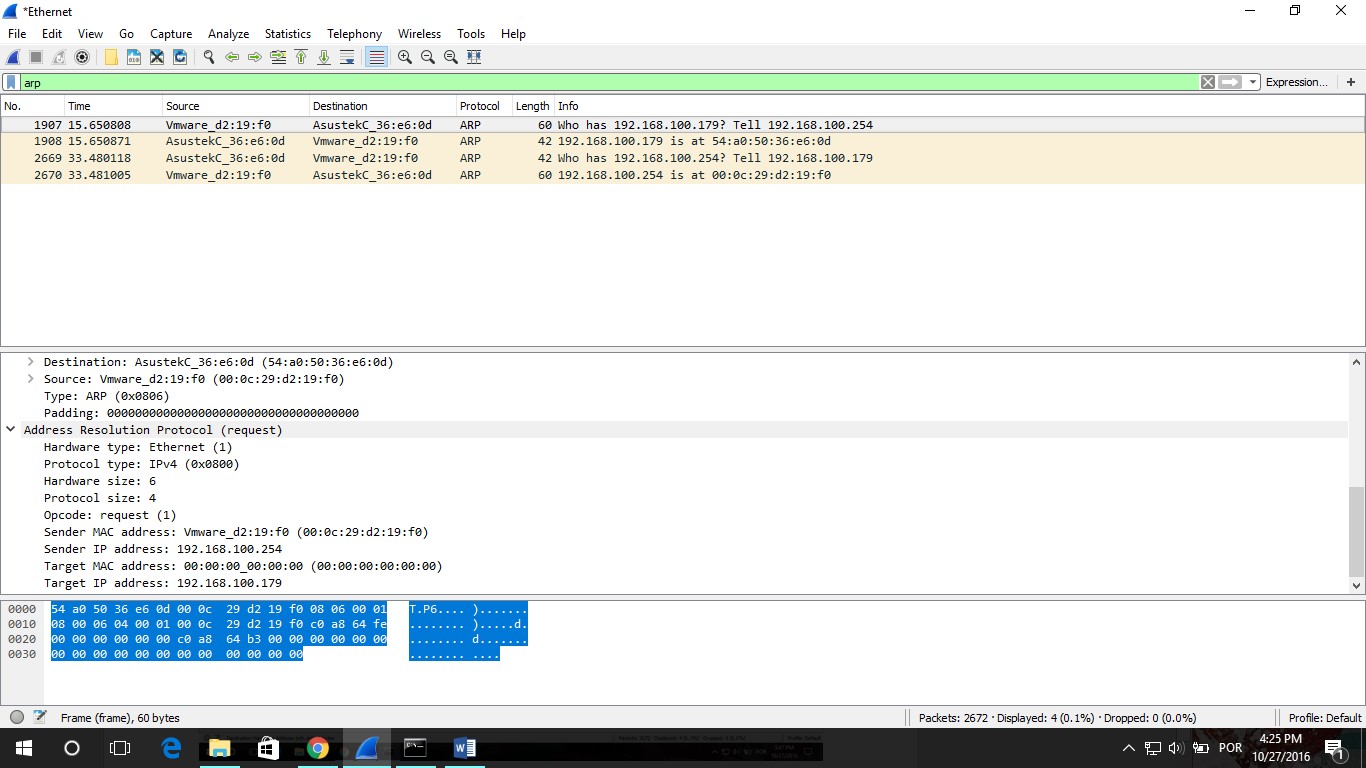
 O portátil responde ao pedido ARP recebido dizendo o endereço IP 192.168.100.179 tem a ele associado o endereço MAC 54:a0:50:36:e6:0d (ambos referentes ao nosso portátil, que efetua esta resposta).

Figura 19 Mensagem da frame ARP reply

Figura 18 Endereços de destino e origem frame ARP reply

## ARP numa topologia CORE

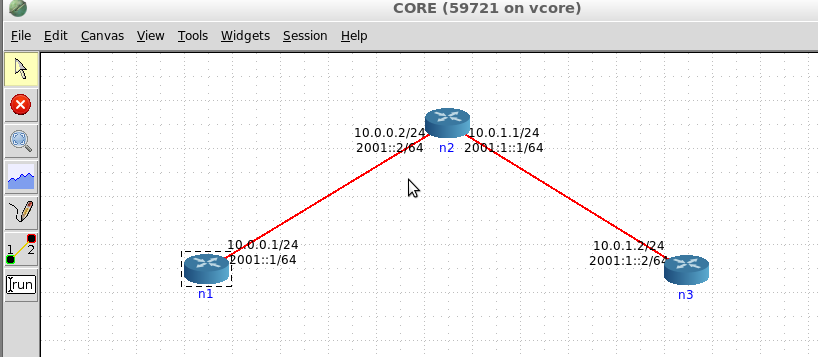
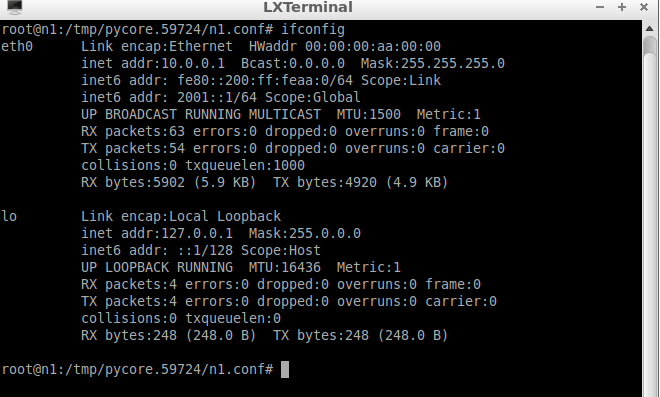
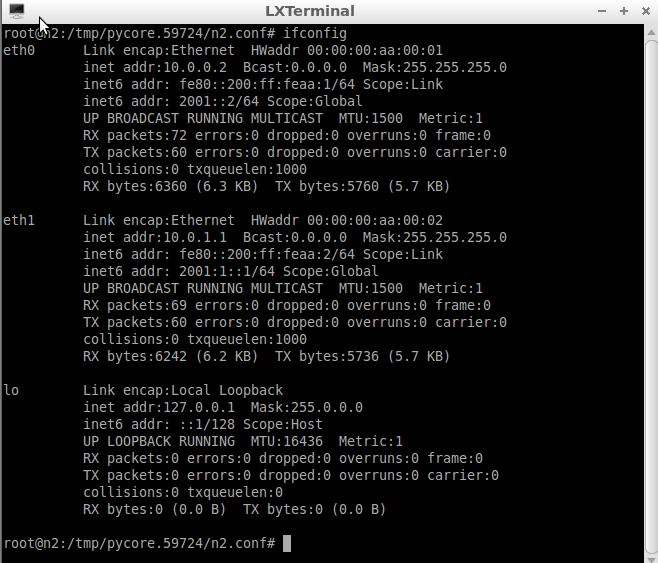
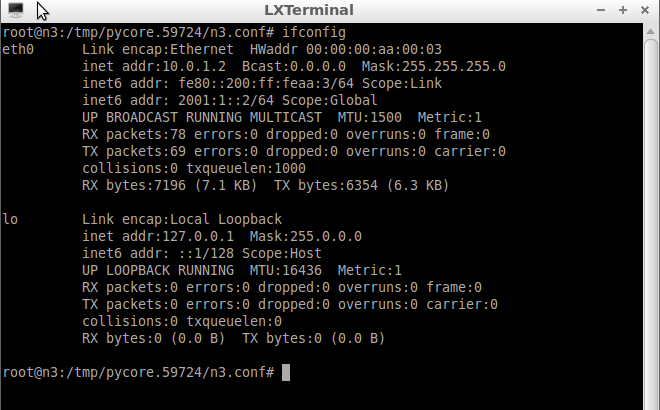
****

Figura 20 Esquema inicial da rede com três routers

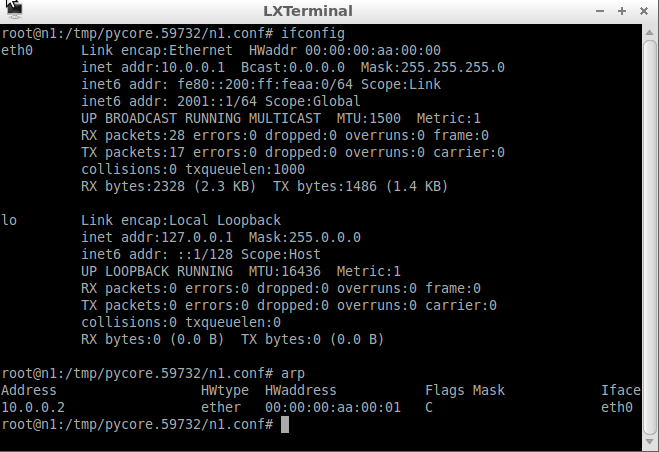
**17) Com auxílio do comando *ifconfig* obtenha os endereços Ethernet das interfaces dos diversos *routers*.**

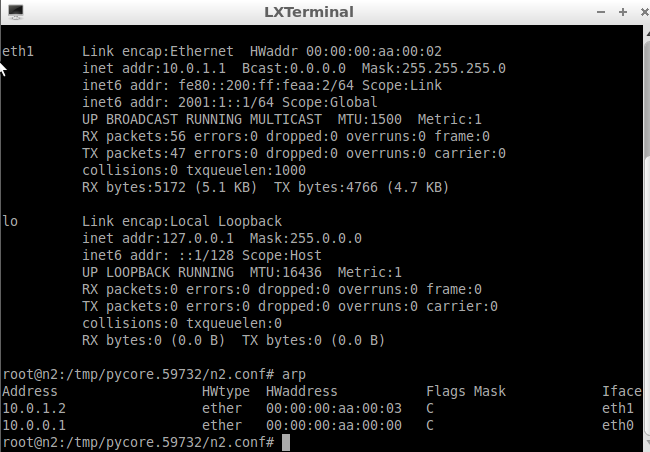
Router n1 tem endereço Ethernet 00:00:00:aa:00:00

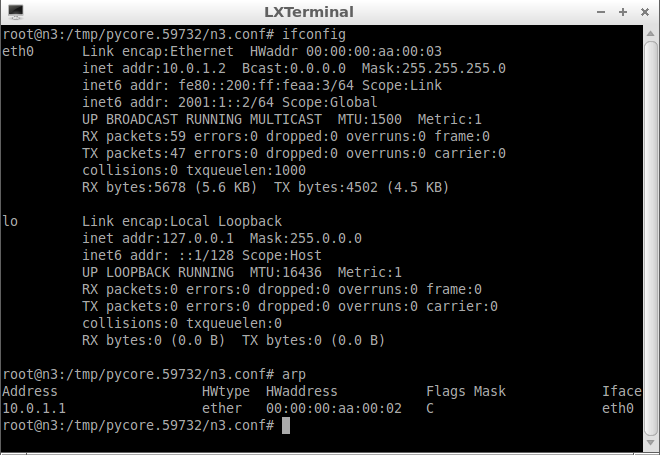
O router n2 tem como endereços os valores 00:00:00:aa:00:01 e 00:00:00:aa:00:02.

Por fim, o router n3 tem como endereço Ethernet 00:00:00:aa:00:03.

**18) Usando o comando arp obtenha as caches arp dos diversos sistemas.**

A cache ARP do router n1 tem registado o endereço Ethernet 00:00:00:aa:00:01 do router n2;

A cache ARP do router n2 tem registado o endereço Ethernet 00:00:00:aa:00:03 do router n3 e o 00:00:00:aa:00:00 do router n1;

A cache ARP do router n3 tem nela o endereço Ethernet 00:00:00:aa:00:02 do router n2.

**19) Faça ping de n1 para n2. Que modificações observa nas caches ARP desses sistemas? Faça ping de n1 para n3. Consulte as caches ARP. Que conclui?**

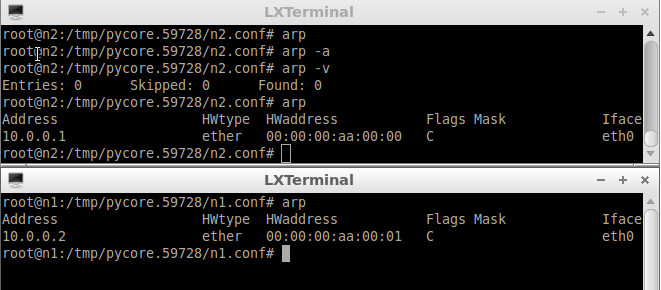
Após realizar o ping de n1 para n2, a cache ARP do router n1 não se alterou mas a do router n2 passou a ter só o endereço Ethernet 00:00:00:aa:00:00 que está associada ao router n1. Como para testar o ping de n1 para n2, o router n1 envia um pacote de teste para o router n2, então n2 terá na sua tabela ARP o endereço Ethernet de n1 e por sua vez, como o router n2 responde a n1 tem na sua tabela ARP o endereço Ethernet de n1.

Figura 21 Caches ARP do router n2 e n1 após ping de n2 para n1

Após realizar um ping de n1 para n3 só a cache ARP do n3 se alterou passando a ficar vazia. Concluímos que isto acontece porque o router n3 não tem ligação direta com o router n1 e, portanto, não consegue saber o seu endereço Ethernet.

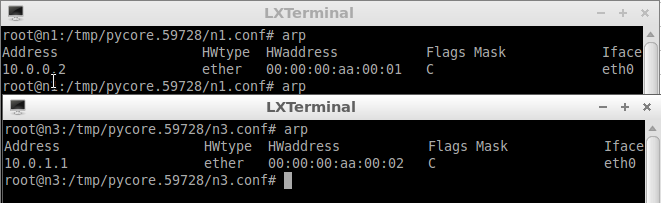


Figura 22 Caches ARP do royuter n1 e n3 após ping de n1 para n2

**20) Em n1 remova a entrada correspondente a n2. Coloque uma nova entrada para n2 com endereço Ethernet inexistente. O que acontece?**

Ao apagar a cache ARP do router n1 este não terá informações sobre o endereço Ethernet do router n2. Além disto, criando um endereço Ethernet inexistente no router n2, esta ligação não acontece porque o router n1 não tem informações em cache ARP sobre n2 e ao perguntar o endereço Ethernet de n2 a partir do seu endereço IP (de n2), como este é inexistente n1 nunca recebe resposta e, portanto, a ligação é impossível de se realizar.

**21) Faça ping de n5 para n6. Sem consultar a tabla ARP anote a entrada que, em sua opinião, é criada na tabela ARP de n5. Verifique, justificando, se a sua interpretação sobre a operação da rede Ethernet e protocolo ARP estava correto.**

Como é utilizado um switch, que interliga os dois sistemas n5 e n6, ao fazer ping do host n5 para n6 a cache ARP de n5 ficará com o endereço físico do host n6.

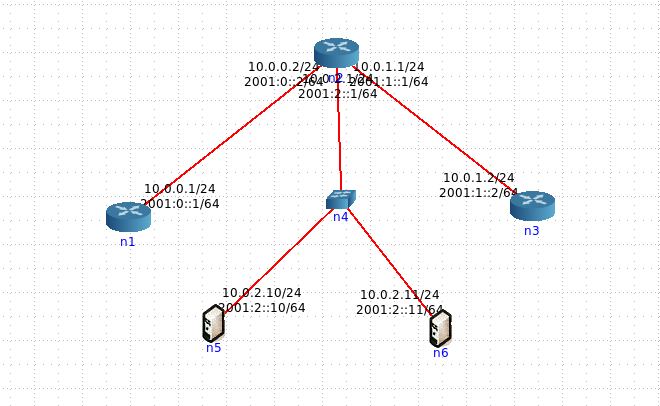
Este resultado é comprovado no conteúdo da cache ARP do n5 (após fazer o ping para n6) mas perdemos o registo em imagem dessa cache no decorrer do trabalho.

Figura 23 Esquema da rede com switch

# 

# Camada de ligação lógica: Ethernet e Protocolo ARP – Parte II

## 

## ARP Gratuito

**1) Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Verifique quantos pacotes ARP gratuito foram enviados e com que intervalo temporal?**

Como pacote ARP gratuito escolhemos a frame 937 que se volta a repetir na frame 2895. Assim, podemos concluir que foram enviados entre elas 1958 pacotes (2895 – 937).

O intervalo temporal, visto no campo “Time delta from previous captured frame” é de aproximadamente 45 segundos.

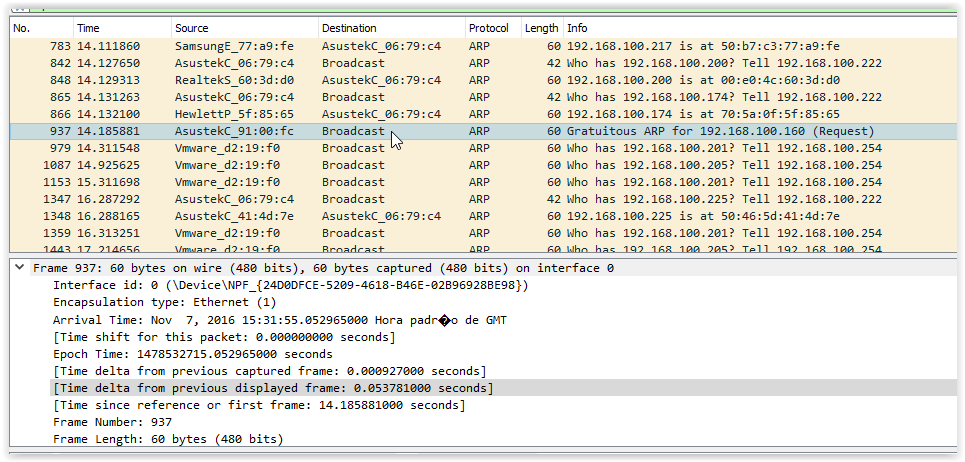
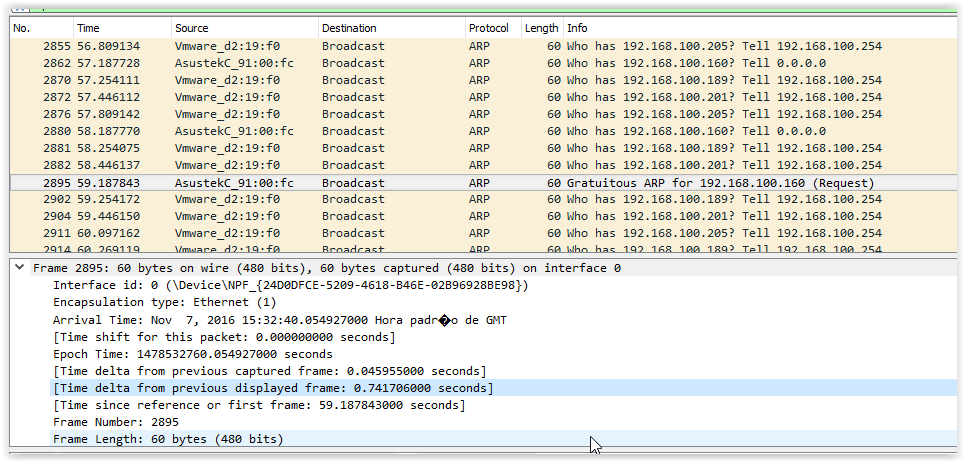
A frame 937 apareceu 14.185881 segundos após o inicio da captura e a frame 2895 apareceu no instante 59.187843

Figura 24 Registo das frames capturadas com ARP gratuitos

**2) Analise o conteúdo de um pedido ARP gratuito e identifique em que se distingue dos restantes pedidos ARP. Registe a trama Ethernet correspondente. Qual o resultado esperado face ao pedido ARP gratuito enviado?**

Analisando os ARPs normais que capturamos com os dois ARP gratuitos que analisamos, observamos que nos ARP gratuitos o seu endereço IP de origem e destino são os mesmos. Isto acontece porque o host faz um pedido ARP sem que este lhe seja solicitado por ninguém, para tentar determinar se existem anomalias nos endereços IP da rede local e para outros terminais atualizarem a sua cache ARP.

Se não houver nenhuma anomalia, só o host que enviou o pedido ARP irá responder ao mesmo. Se outro host qualquer responder àquele pedido, é porque haverão dois hosts (ou mais) com o mesmo endereço IP.

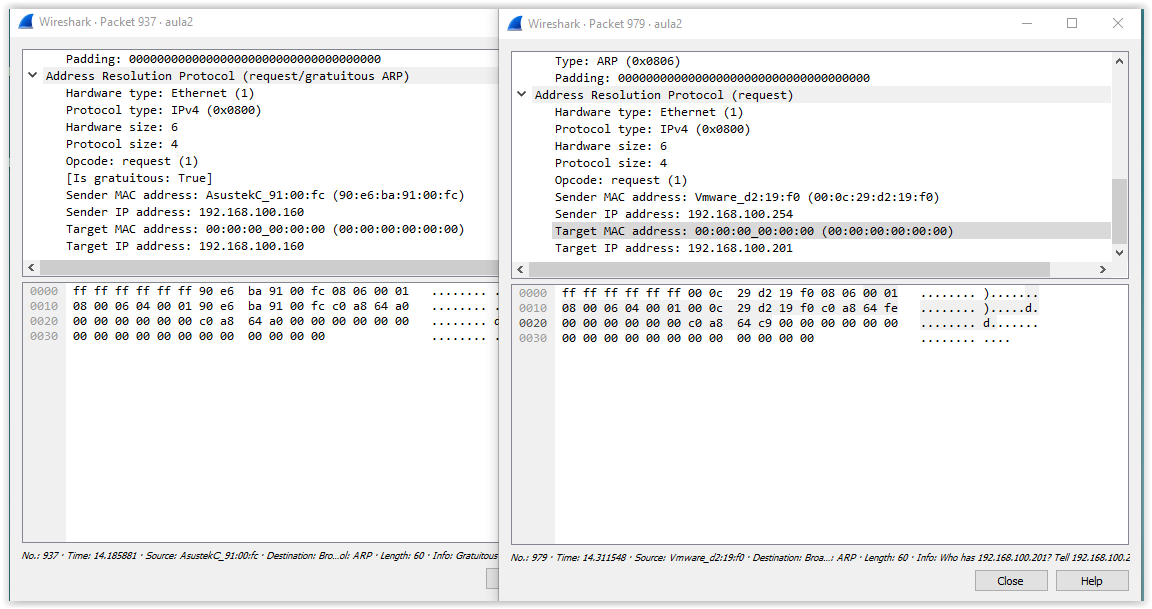
Na figura em baixo podemos observar que a nossa primeira frame com ARP gratuito tem destino e origem com o mesmo endereço IP e que uma frame genérica ARP feita por um host em contexto normal, tem endereços IP de destino e origem distintos.

Figura 25 Comparação entre destinos e origem de um ARP normal e um ARP gratiuto

# Domínios de colisão

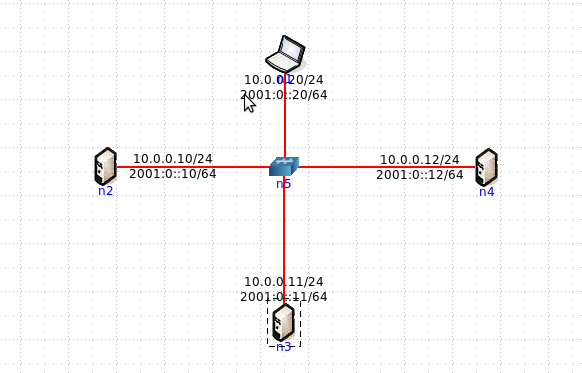


Figura 26 Esquema genérico da rede com um hub

**1) Faça ping de n1 para n2. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?**

Depois de abrir o terminal no portátil n1, fizemos um ping do mesmo para o host n2.

Deixando esta operação de ping a correr na Shell em segundo plano, abrimos uma nova janela de terminal no host n3 (poderia igualmente ter sido escolhido o host n4), onde efetuamos o comando tcpdump.

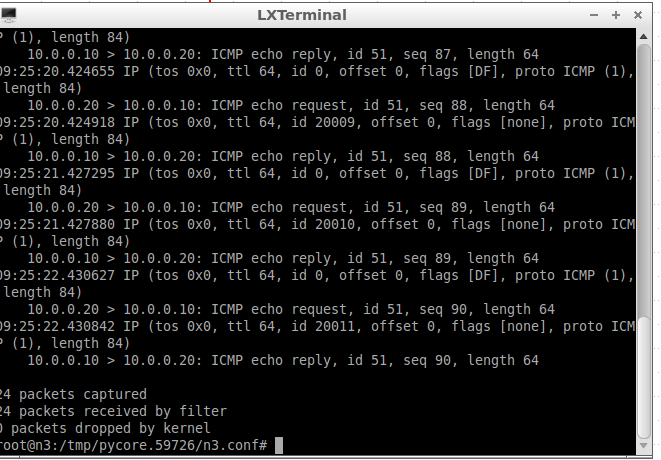
Com este processo, verificamos que com o uso de um hub a interligar os 4 sistemas, o host n3 que nada tinha a ver com o ping de n1 para n2, estava a receber todos os pacotes de echo request e reply que estavam partilhados pelos dois sistemas (n1 e n2).

Figura 27 O host 3 capta todos as mensagem echo do host n1 (10.0.0.10) e n2 (10.0.0.20)

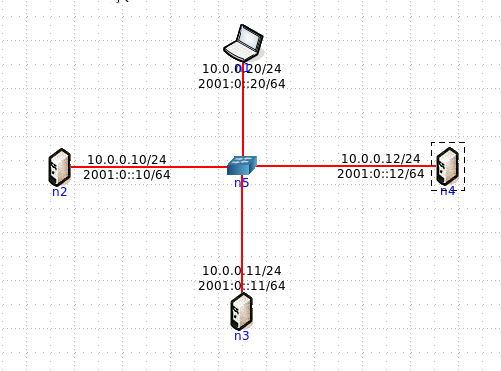
****

Figura 28 Esquema geral da rede com switch

**2) Na topologia de rede substitui o hub por um switch. Repita os procedimentos que realizou na pergunta anterior. Comente os resultados obtidos quanto à utilização de hubs e switches no contexto de controlador ou dividir domínios de tráfego de colisão. Documento as suas observações e conclusões com base no tráfego observado/capturado.**

Substituindo o hub por um switch e repetindo o processo da pergunta anterior, quer realizemos tcpdump no host n3 como no n4, estes não recebem nenhuma captura de pacotes partilhados entre n1 e n2. Isto acontece porque ao realizar o ping cada sistema envolvido tem a sua porta de entrada e, portanto, evitam-se as colisões ou que sistemas externos acedam aos pacotes trocados por outros sistemas.

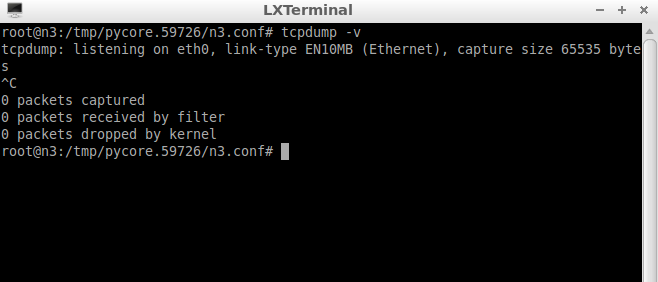
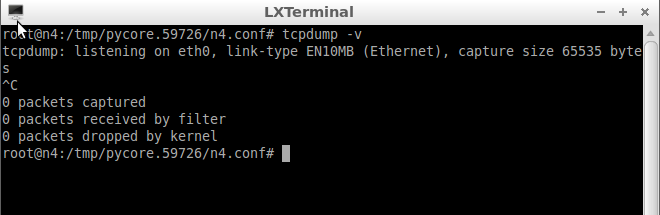
No sentido de controlar colisões ou dividir domínios de acesso, os switch são a melhor escolha para esses fins.

Figura 29 OS host n3 e n4 não capturam nenhum pacote do ping de n1 para n2 atravez de um switch

# Conclusão

Após a resolução deste trabalho ficamos a compreender o que ocorre durante o percurso de uma trama desde a sua origem até chegar ao destino, analisando todos os seus pontos de passagem até chegar ao recetor final, bem como alguns conceitos acerca da camada de ligação lógica. Nesta área focamos a abordagem nos pedidos e resposta HTTP e como funcionam as ligações através dos endereços lógicos e físicos de rede.

Ficamos ainda a perceber, com mais algum detalhe, como funciona o protocolo ARP e as suas caches, que mapeiam pares entre os endereços IP e endereços físicos conhecidos pela máquina ou host dessa memória cache. Quando esta informação do endereço MAC do destino não existe em cache ARP geram-se os pedidos ARP para que o sistema com o IP que conhecemos nos forneça o seu endereço Ethernet e nós guardemos estes dados na nossa cache.

Dentro do mesmo protocolo ARP focamos ainda o funcionamento dos ARP gratuitos, como uma forma de controlo para casos de duplicação de IPs -que levariam a anomalias e erros nas comunicações- ou meramente como forma de atualizar as caches ARP de outros sistemas da rede local.

Por fim, compreendemos e analisamos a grande diferença entre hubs e switches. Nos primeiros, sistemas alheios e externos a determinadas comunicações, mas ligados ao mesmo hub, podem ter acesso a todos os pacotes que passam pelo hub enquanto que com o uso de switches só os sistemas envolvidos explicitamente na ligação têm acesso aos pacotes trocados.

Os referidos processos foram explicados de forma mais cuidada no decorrer do relatório.

Ana Esmeralda Fernandes A74321

Bárbara Nadine Freitas Oliveira A75614

Miguel Dias Miranda A74726

Redes de Computadores

TP2: Camada de ligação lógica: Ethernet e Protocolo ARP

Novembro de 2016