Redes de Computadores – TP2

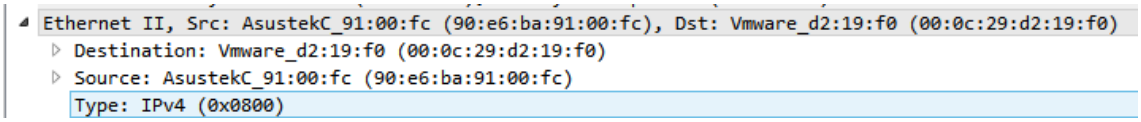
Parte 1

Neste relatório serão apresentadas as respostas ás questões presentes no TP2 e algumas conclusões tiradas no final das mesmas. O relatório apresenta cada uma das perguntas enumeradas, assim como as respostas ás mesmas, respostas estas com as devidas justificações, à base de texto e/ou de *prints, prints* estes que possuem a parte fulcral da justificação sublinhada a vermelho.

Captura e análise de tramas Ethernet

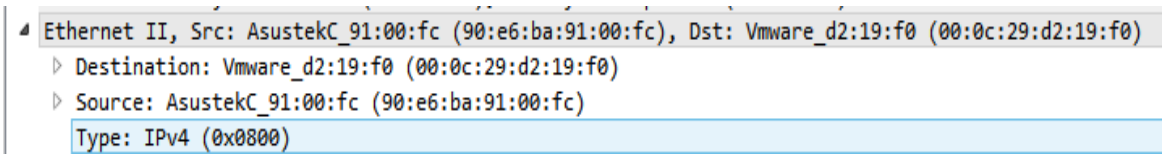
1 - Qual é o endereço MAC da interface ativa do seu computador?

O endereço MAC da interface ativa no nosso computador portátil Asus é: 90-E6-BA-91-00-FC



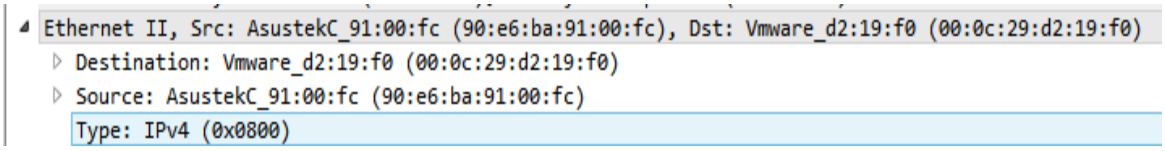
2 - Qual é o endereço MAC destino da trama? A que sistema é destinada essa trama, será o endereço Ethernet do servidor http para cesium.di.uminho.pt? Justifique.

O endereço MAC destino da trama é: 00:0c:29:d2:19:f0, e não é o endereço Ethernet do servidor http para cesium.di.uminho.pt, mas sim o endereço do dispositivo de onde saiu o pedido (neste caso, um portátil Asus).



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

O valor hexadecimal do campo Type da trama Ethernet é 0x0800. Este valor indica-nos qual o tipo de protocolo, sendo neste caso um protocolo IP (IPv4).



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

São usados 53 bytes até ao caractere ASCII "G". A sobrecarga (*overhead*) introduzida pela pilha protocolar no envio do HTTP GET é de:

$$x = \frac{nº\ de\ bytes\ do\ cabeçalho}{nº\ de\ bytes\ que\ chegaram\ em\ bruto} = \frac{53}{746} = 0.071 = 7.1\%$$

```
0000  00 0c 29 d2 19 f0 90 e6  ba 91 00 fc 08 00 45 00   ..)..... ......E.
0010  02 dc 2b 9b 40 00 80 06  00 00 c0 a8 64 a0 c1 88   ..+.@... ....d...
0020  13 94 c3 92 00 50 9e e6  b9 31 57 13 04 e3 50 18   .....P.. .1W...P.
0030  7f 98 fd 33 00 00 47 45  54 20 2f 61 73 73 65 74   ...3..GE T /asset
```

```
▷ Frame 28: 746 bytes on wire (5968 bits), 746 bytes
```

5 - Em ligações com fios pouco 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/Preferences/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.

O valor desse campo é de 0x0D0A0D0A, quando alterada a configuração. Até lá, o campo FCS não está a ser utilizado.

```
02d0  62 37 65 65 63 37 61 38 63 32 64 30 36 36 34 34   b7eec7a8c2d06644
02e0  39 38 35 35 65 62 0d 0a 0d 0a                     9855eb....
```

(A seguir responda às seguintes perguntas, baseado no conteúdo da trama Ethernet que contém o primeiro byte da resposta HTTP)

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

Endereço Ethernet da fonte → 00:0c:29:d2:19:f0

Corresponde ao sistema → Vmware_d2:19:fo

```
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0),
```

7 - Qual é o endereço MAC do destino? A que sistema corresponde?

Enderço MAC destino → 90-E6-BA-91-00-FC

Corresponde ao sistema → AsustekC_91:00:fc (Portátil)

```
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: AsustekC_91:00:fc (90:e6:ba:91:00:fc)
```

8 - Qual é o valor hexadecimal do campo tipo (*Type*)?

Type → 0x0800

```
Type: IPv4 (0x0800)
```

9 - Que tipo de resposta foi enviada pelo servidor?

O servidor dá uma resposta em que o que é transmitido passa pelo conteúdo textual e visual do website para onde foi mandado um pedido para lhe aceder

Protocolo ARP

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

A coluna Internet Address contém o endereço IP do nosso próprio Laptop, de onde sai o pedido (fonte). A coluna Physical Address mostra o endereço MAC do destino. A coluna Type mostra o tipo de protocolo que ocorre.

```
Interface: 192.168.100.160 --- 0xb
  Internet Address      Physical Address      Type
  192.168.100.254       00-0c-29-d2-19-f0     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
```

11 - Qual é o valor hexadecimal dos endereços origem e destino na trama Ethernet que contém a mensagem com o pedido ARP (*ARP Request*)? Como interpreta e justifica o endereço destino usado?

Endereço de origem na trama → 00:0c:29:d2:19:f0

Endereço de destino na trama → ff:ff:ff:ff:ff:ff

O endereço de destino usado consiste numa exceção, em que todos os nós recebem e processam a trama (endereço de difusão), ao invés de apenas um nó receber a informação.

```
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
```

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

O valor hexadecimal do campo Type da trama Ethernet é 0x0806. Este valor indica-nos que o protocolo da camada superior correspondente é ARP.

```
Type: ARP (0x0806)
```

13 - Qual o valor do campo ARP opcode? O que especifica? Se necessário, consulte a RFC do protocolo ARP http://tools.ietf.org/html/rfc826.html.

O valor do campo ARP opcode é 1 ou 0x0001. Este valor especifica que fizemos um request ao servidor do site.

```
Opcode: request (1)
```

14 - A mensagem ARP contém o endereço IP de origem? Que tipo de pergunta é feita?

Sim, a mensagem ARP contém o endereço IP 192.168.100.160, correspondente ao computador que envia o pedido.

```
    848 12.491589      AsustekC_91:00:fc     Vmware_d2:19:f0       ARP      42     192.168.100.160 is at 90:e6:ba:91:00:fc
Frame 848: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
    Interface id: 0 (\Device\NPF_{A881BC29-C43D-4ED6-941B-81B3B58A7EC5})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  7, 2016 15:50:07.197944000 Hora padr□o de GMT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1478533807.197944000 seconds
    [Time delta from previous captured frame: 0.000056000 seconds]
    [Time delta from previous displayed frame: 0.000056000 seconds]
    [Time since reference or first frame: 12.491589000 seconds]
    Frame Number: 848
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: AsustekC_91:00:fc (90:e6:ba:91:00:fc), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
    Destination: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
        Address: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: AsustekC_91:00:fc (90:e6:ba:91:00:fc)
        Address: AsustekC_91:00:fc (90:e6:ba:91:00:fc)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: AsustekC_91:00:fc (90:e6:ba:91:00:fc)
    Sender IP address: 192.168.100.160
    Target MAC address: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
    Target IP address: 192.168.100.254
```

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

a - Qual o valor do campo ARP opcode? O que especifica?

O valor do campo ARP opcode é 2 ou 0x0002. Este valor especifica que recebemos o reply do serviço ao qual fizemos ping.

b - Em que posição da mensagem ARP está a resposta ao pedido ARP?

A resposta ao pedido ARP está no Sender MAC Address.

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

Endereço de origem da trama -> 90:e6:ba:91:00:fc

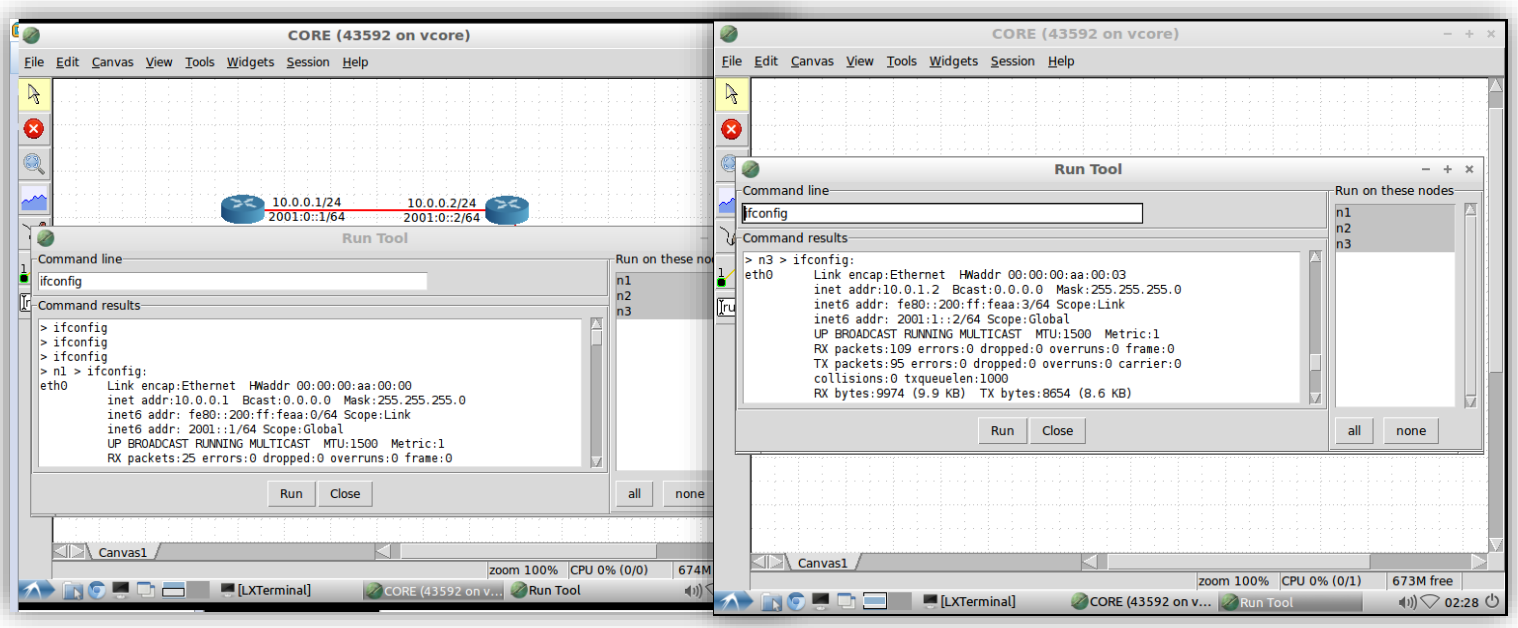
Endereço de destino da trama -> 00:0c:29:d2:19:f0

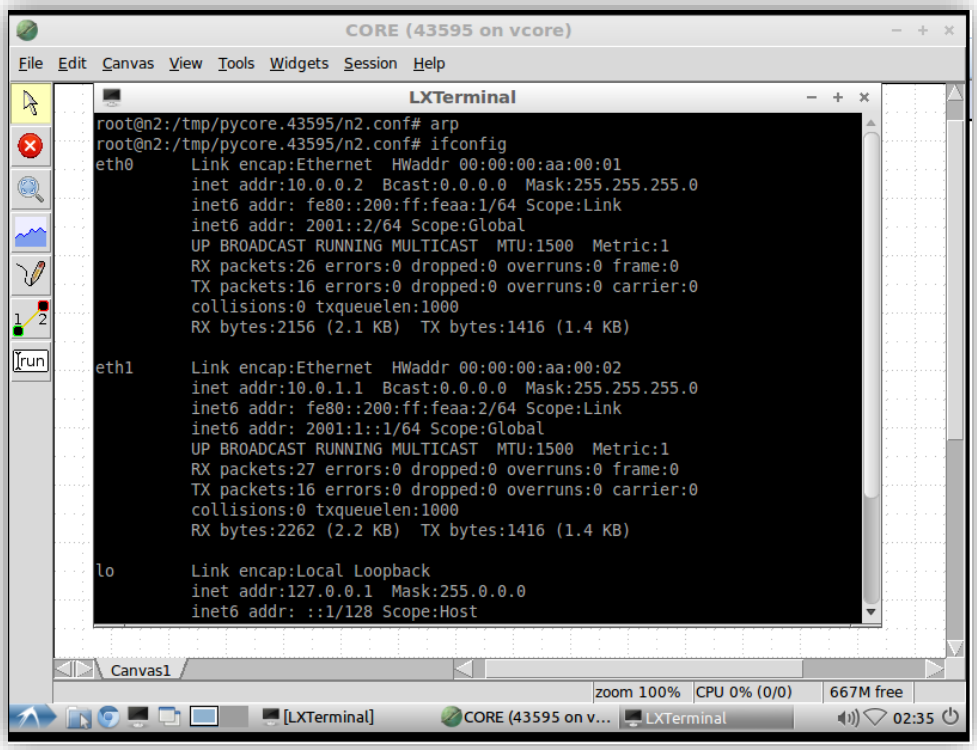
Podemos concluir que um deles, representa o endereço MAC da nossa máquina, de onde saiu o pedido, sendo que o outro representa o endereço ethernet de quem nos deu a resposta ao nosso pedido, nomeadamente, o serviço para o qual fizemos ping na sala de aula e não o próprio domínio “miei.di.uminho.pt”. Como o site não se encontra na rede local, seria impossível o mesmo enviar uma resposta.

ARP numa topologia CORE

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

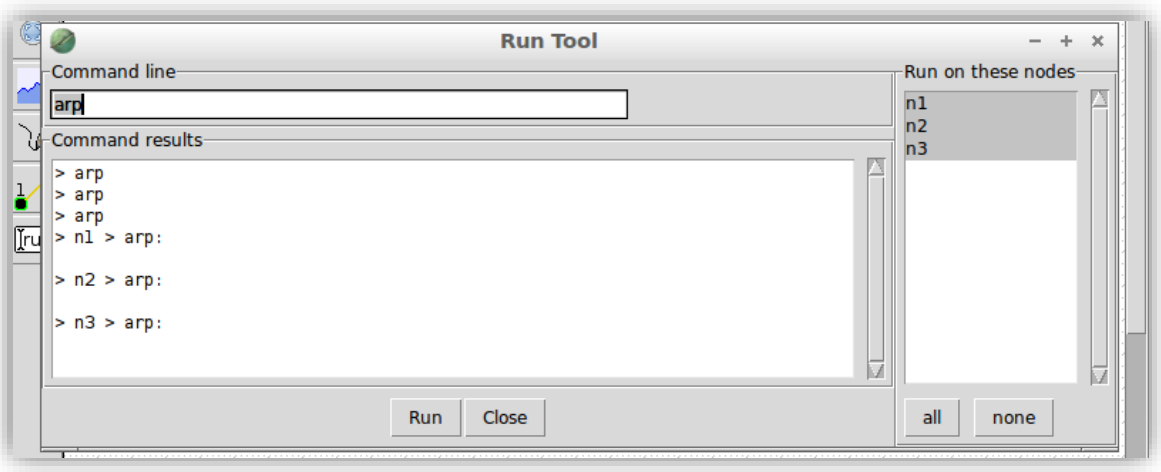
n1 Ethernet Address → 00:00:00:aa:00:00
n2 Ethernet Address 1 → 00:00:00:aa:00:01
n2 Ethernet Address 2 → 00:00:00:aa:00:02
n3 Ethernet Address → 00:00:00:aa:00:03





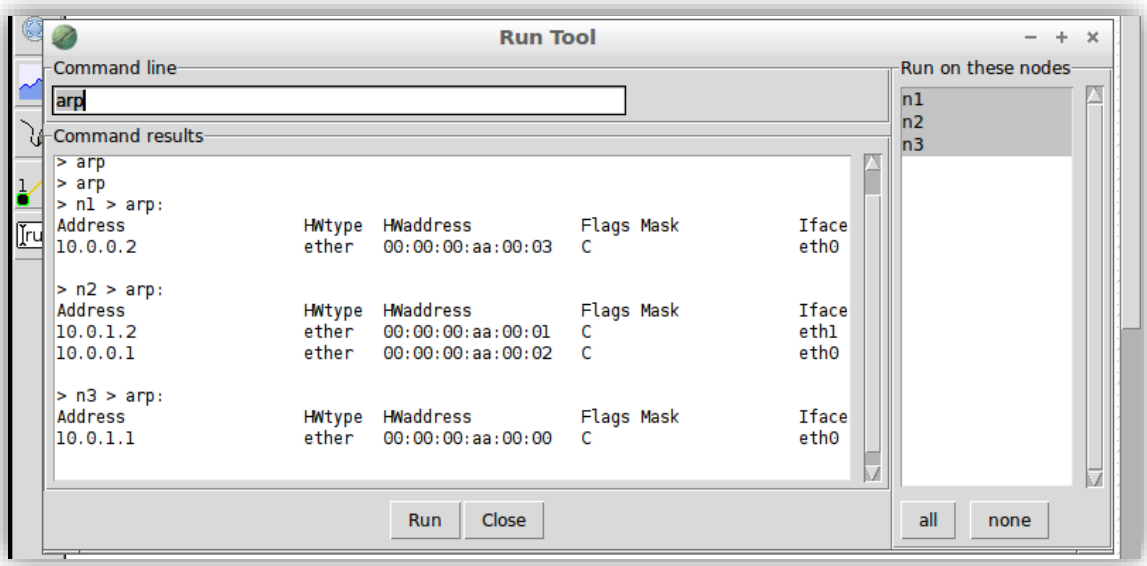
18 - Usando o comando arp obtenha as *caches* arp dos diversos sistemas.

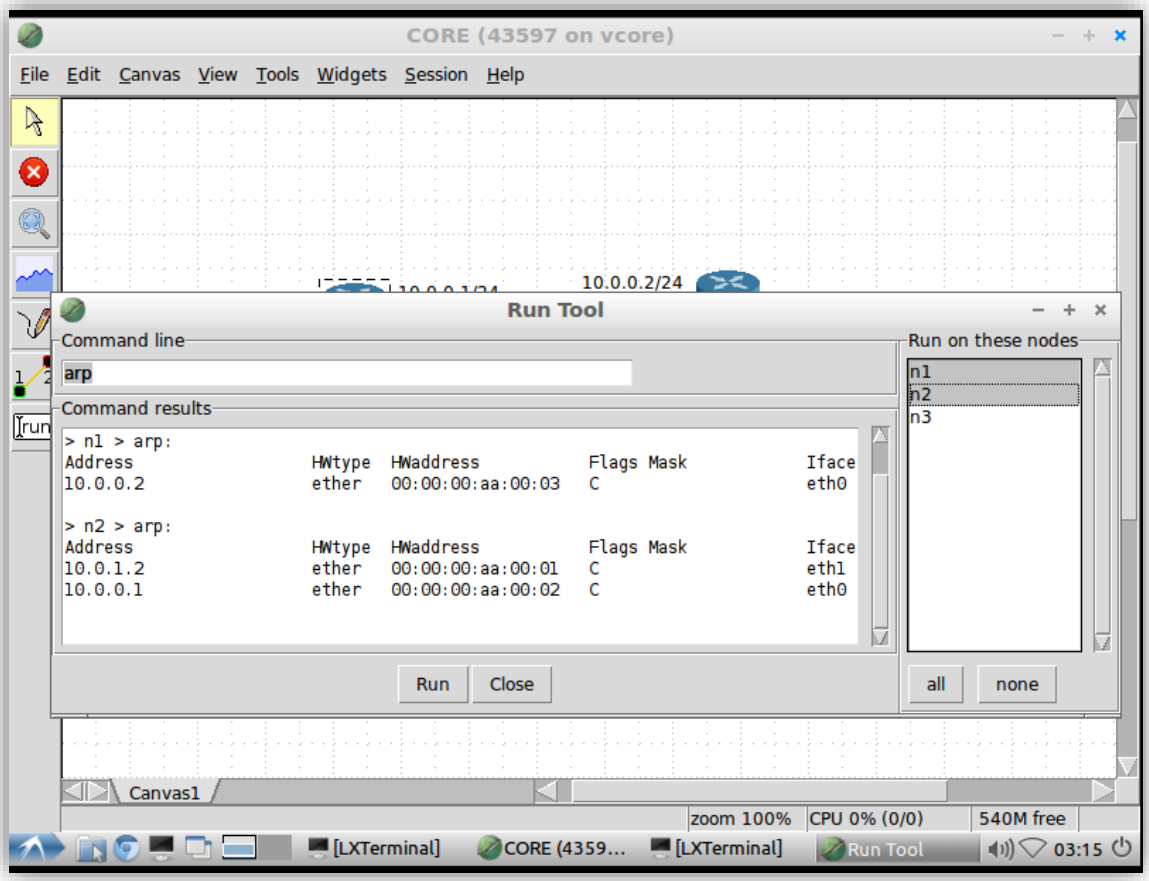
As caches de todos os sistemas estão vazias.



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?

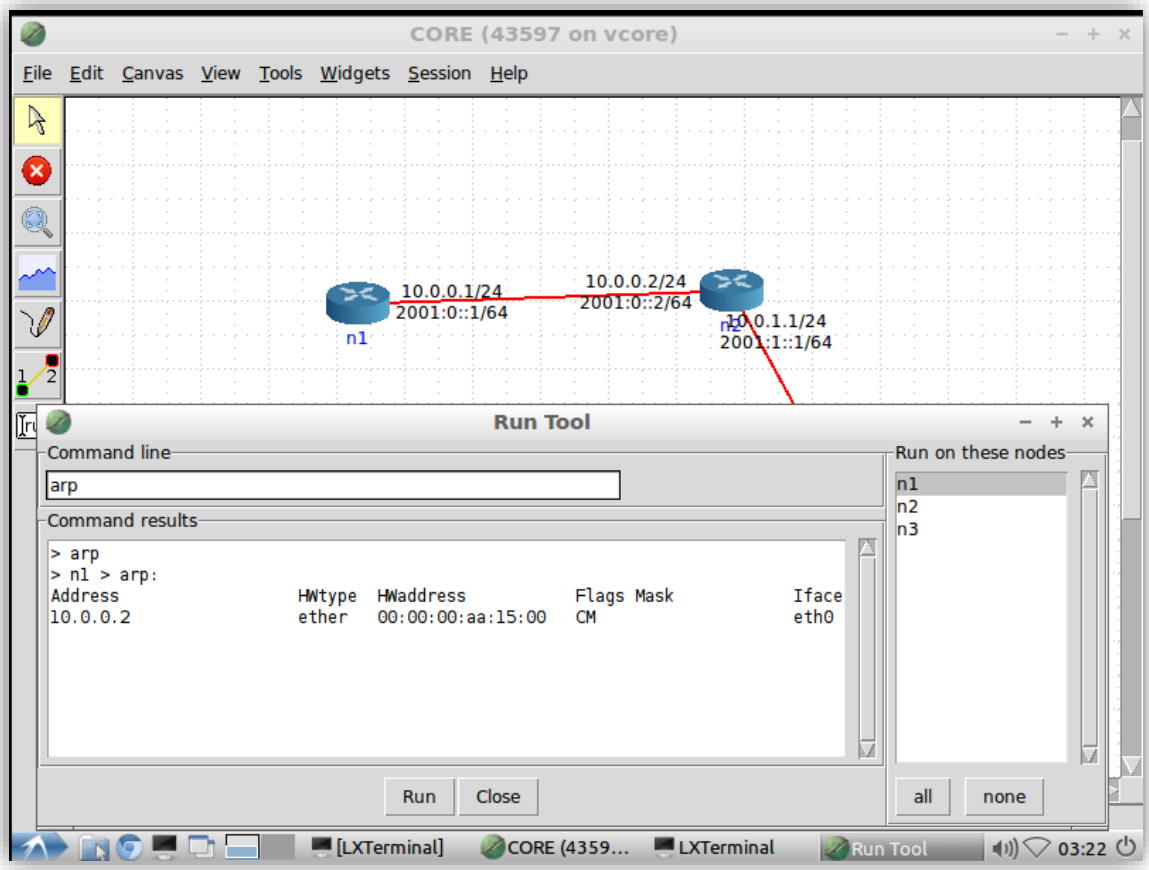
Passa a haver endereços referentes a n1 e n2 nas respetivas caches, visto que há comunicação entre os mesmos. Quando é feito ping de n1 para n3 passa de igual maneira a haver registo da comunicação entre os dois serviços, comprovado pelo preenchimento das caches dos serviços envolvidos.

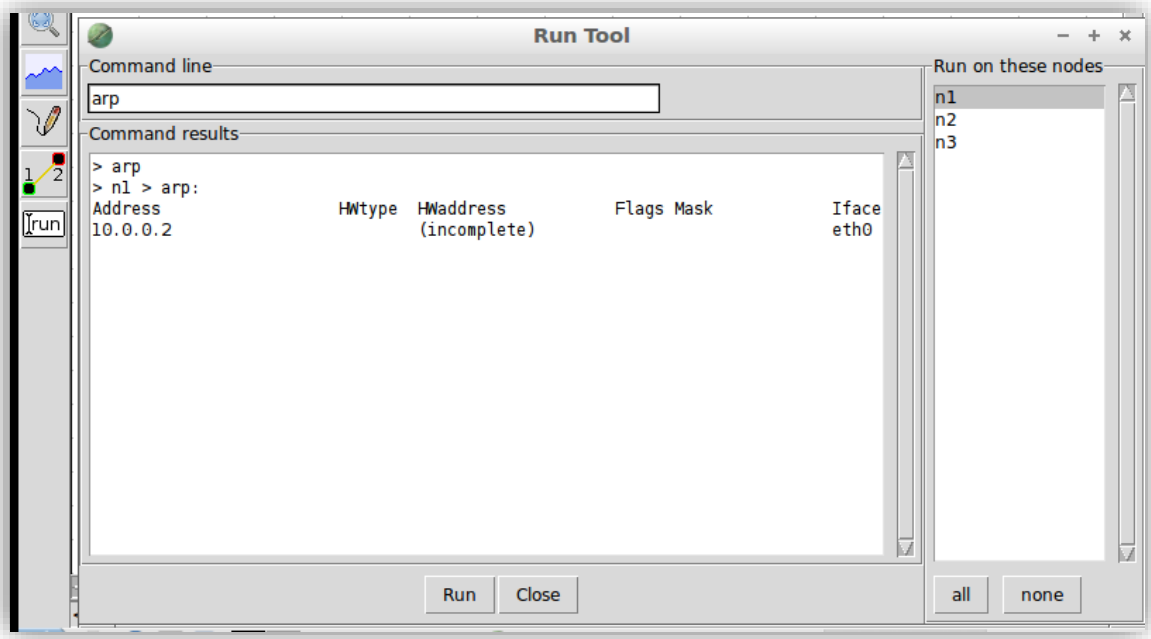




20 - Em n1 remova a entrada correspondente a n2. Coloque uma nova entrada para n2 com endereço Ethernet inexistente. O que acontece?

n1 deixa de comunicar com n2, visto que deixa de ter conhecimento acerca do seu endereço.

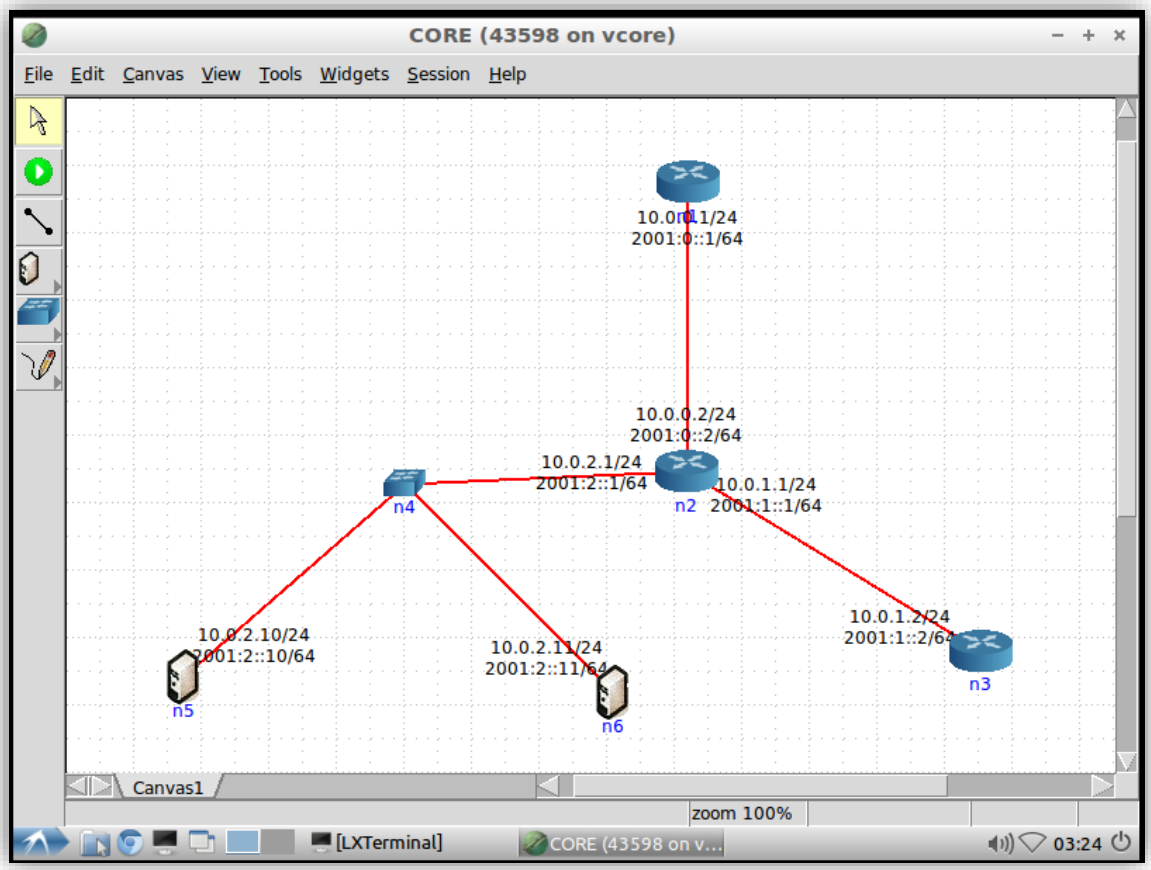


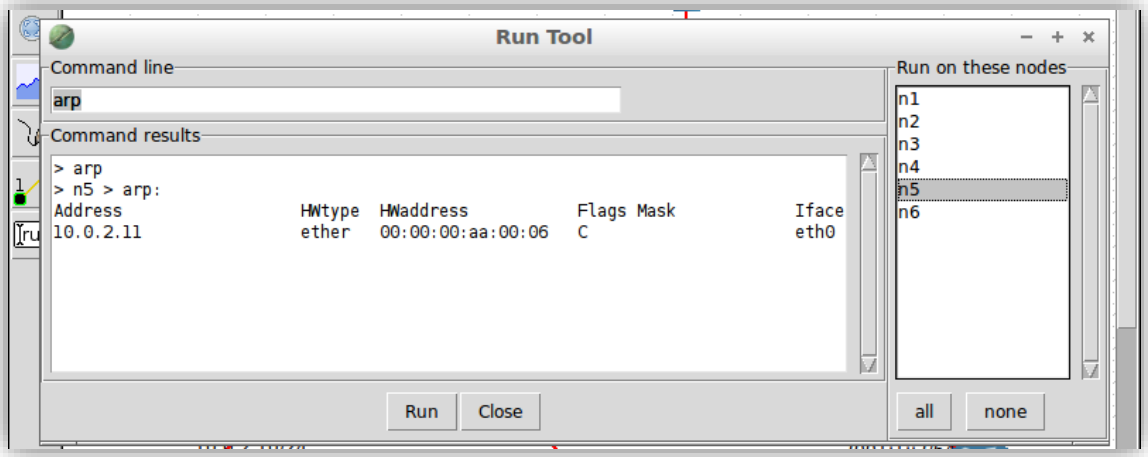


(Adicione agora um switch (n4) à rede e ligue o router n2, e os hosts n5 e n6 a esse switch.)

21 - Faça ping de n5 para n6. Sem consultar a tabela 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.

O que era natural aparecer na tabela ARP de n5 seria o endereço que diz respeito ao serviço 6. A nossa interpretação está correta, pois graças ao switch, é possível ocorrer a comunicação entre serviços que não estão ligados diretamente, mas passam a comunicar indiretamente graças à distribuição feita pelo switch, ao qual ambos os serviços estão ligados.





Parte 2

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?

Na nossa captura apenas conseguimos identificar 1 ARP gratuito ao longo de 18s.

```
    156 14.513003      AsustekC_91:00:fc     Broadcast             ARP      42     Gratuitous ARP for 192.168.100.160 (Request)
Frame 156: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
    Interface id: 0 (\Device\NPF_{A881BC29-C43D-4ED6-941B-81B3B58A7EC5})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov  7, 2016 15:34:48.985035000 Hora padr□o de GMT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1478532888.985035000 seconds
    [Time delta from previous captured frame: 0.191251000 seconds]
    [Time delta from previous displayed frame: 0.191251000 seconds]
    [Time since reference or first frame: 14.513003000 seconds]
    Frame Number: 156
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: AsustekC_91:00:fc (90:e6:ba:91:00:fc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
        Address: Broadcast (ff:ff:ff:ff:ff:ff)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: AsustekC_91:00:fc (90:e6:ba:91:00:fc)
        Address: AsustekC_91:00:fc (90:e6:ba:91:00:fc)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: AsustekC_91:00:fc (90:e6:ba:91:00:fc)
    Sender IP address: 192.168.100.160
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.100.160
```

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?

Uma das diferenças do ARP gratuito para o ARP regular, é que o IP de quem envia é igual ao de quem recebe. Supostamente, não devemos obter qualquer tipo de resposta, visto que o IP do sistema a quem queremos fazer um request é o nosso próprio IP. Sendo o IP algo único, será impossível a rede encontrar outro sistema com o nosso próprio IP para nos responder.

Domínios de colisão

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

Apesar de apenas fazermos ping para o serviço n2, todos os tcpdump mostram tráfego em todos os serviços. Era de se esperar tal comportamento, pois a topologia do hub faz com que o tráfego seja espalhado por todos os serviços a ele ligados.

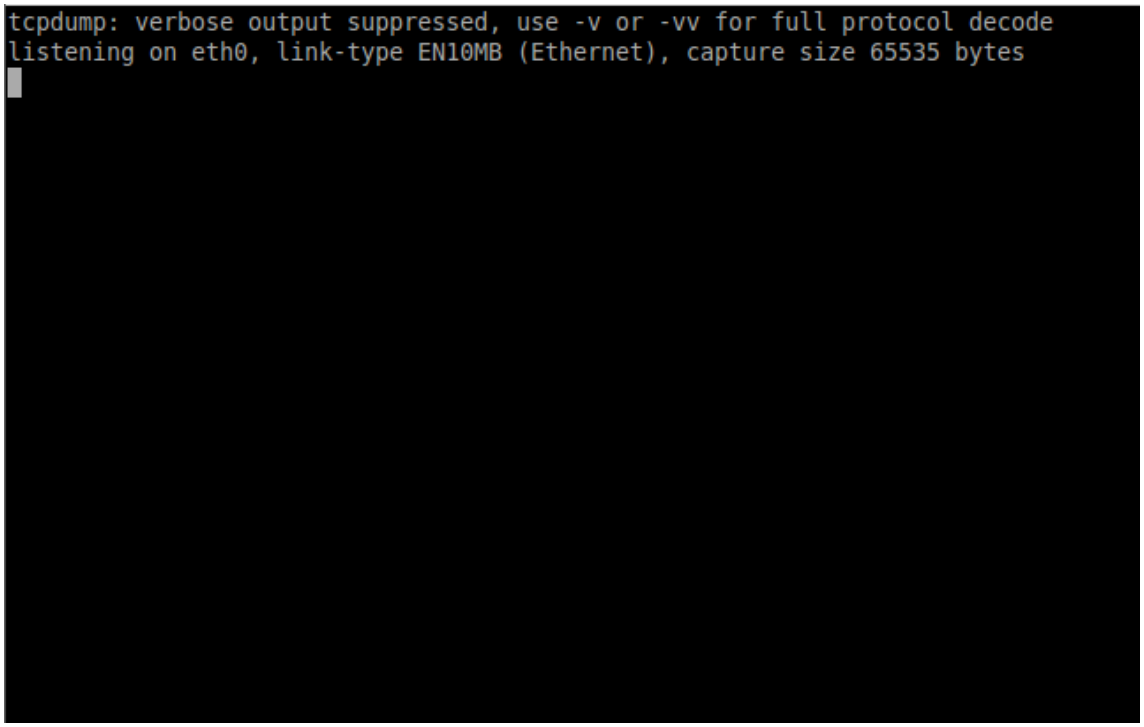
```
gth 64
09:21:09.212887 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 212, lengt
h 64
09:21:10.212581 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 213, len
gth 64
09:21:10.213391 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 213, lengt
h 64
09:21:11.212169 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 214, len
gth 64
09:21:11.212275 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 214, lengt
h 64
09:21:12.212321 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 215, len
gth 64
09:21:12.212500 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 215, lengt
h 64
09:21:13.212827 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 216, len
gth 64
09:21:13.212929 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 216, lengt
h 64
09:21:14.212428 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 217, len
gth 64
09:21:14.212551 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 217, lengt
h 64
```

2 - Na topologia de rede substitua 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 controlar ou dividir domínios de colisão. Documente as suas observações e conclusões com base no tráfego observado/capturado.

Com a substituição do hub por um switch, o tráfego apenas circula para o serviço a que fizemos ping, apesar do serviço que forneceu o tráfego ser o que está a receber, não serem os únicos ligados no switch. Não é surpresa, portanto, que uma análise do tcpdump mostre uma transferência de dados no serviço em que se fez ping e a inexistência dessa mesma transferência nos outros serviços, ao contrário do que acontecia anteriormente. Essa é a principal diferença do switch, para o hub, ou seja, o facto do primeiro apenas permitir a circulação de tráfego entre os nodos que interessam, dispensando assim os custos de ter de espalhar os dados por todos os serviços que estejam ligados a si, o que resultou num grande avanço a nível das redes. A partir do momento em que essa tecnologia foi implementada, apesar de haver situações em que o recurso a um hub ainda é vantajoso ou mesmo necessário.

```
root@n2:/tmp/pycore.35653/n2.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:23:03.552752 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 18, leng
th 64
09:23:03.552834 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 18, length
 64
09:23:04.552471 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 19, leng
th 64
09:23:04.552536 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 19, length
 64
09:23:05.552114 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 20, leng
th 64
09:23:05.552179 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 20, length
 64
09:23:06.552388 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 21, leng
th 64
09:23:06.552479 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 21, length
 64
09:23:07.552731 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 22, leng
th 64
09:23:07.552808 IP 10.0.0.12 > 10.0.0.20: ICMP echo reply, id 28, seq 22, length
 64
09:23:08.552259 IP 10.0.0.20 > 10.0.0.12: ICMP echo request, id 28, seq 23, leng
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```


tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

Conclusão

Após a realização deste trabalho podemos concluir que que os nossos conhecimentos iniciais sobre esta matéria eram escassos, tendo evoluído substancialmente.

Conseguimos na 1ª parte consolidar conhecimentos sobre análise e captura de tramas Ethernet com o Wireshark, aplicação que nos era desconhecida, ficando assim o nosso grupo a perceber como obter coisas como endereços MAC, campos Type, entre outros. Ficamos ainda a perceber os conceitos bases do protocolo ARP, assim como fazer a distinção entre tramas de pedidos ARP e as suas respetivas respostas. Por último, ainda nesta 1ª parte, aprendemos a utilizar o emulador CORE e a preparar diferentes topologias que nos permitissem obter várias informações sobre os sistemas em causa nas topologias criadas.

Na 2ª parte, apesar de ser mais simples, ficamos a perceber a diferença entre pedidos ARP regulares e pedidos ARP gratuitos, assim como a distinção entre hubs e switches.

Em suma, este foi sem dúvida um trabalho bastante benéfico para o alargar de conhecimentos do nosso grupo e esperamos poder no futuro aprofundar ainda mais no que diz respeito a esta matéria.

João Luís Amorim, A74806
João Miguel Araújo A75364
João Nuno Almeida A75209