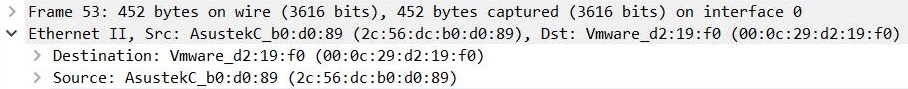
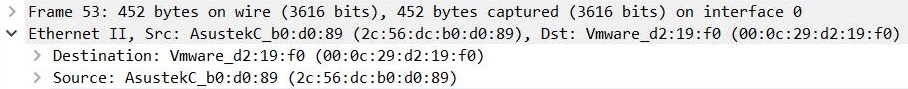
PARTE 1

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



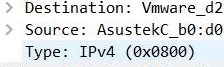
R: O nosso endereço MAC é 2c:56:dc:b0:d0:89.

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.



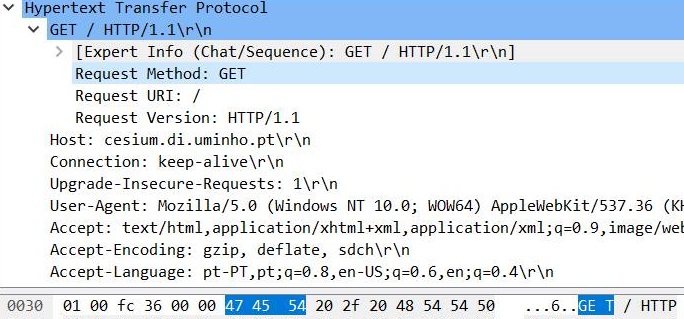
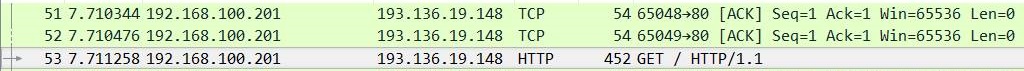
R: O endereço MAC destino da trama é 00:0c:29:d2:19:f0. A trama é destinada ao router que vai estar ligado à rede do departamento, acedendo ao http server e enviando a resposta.

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



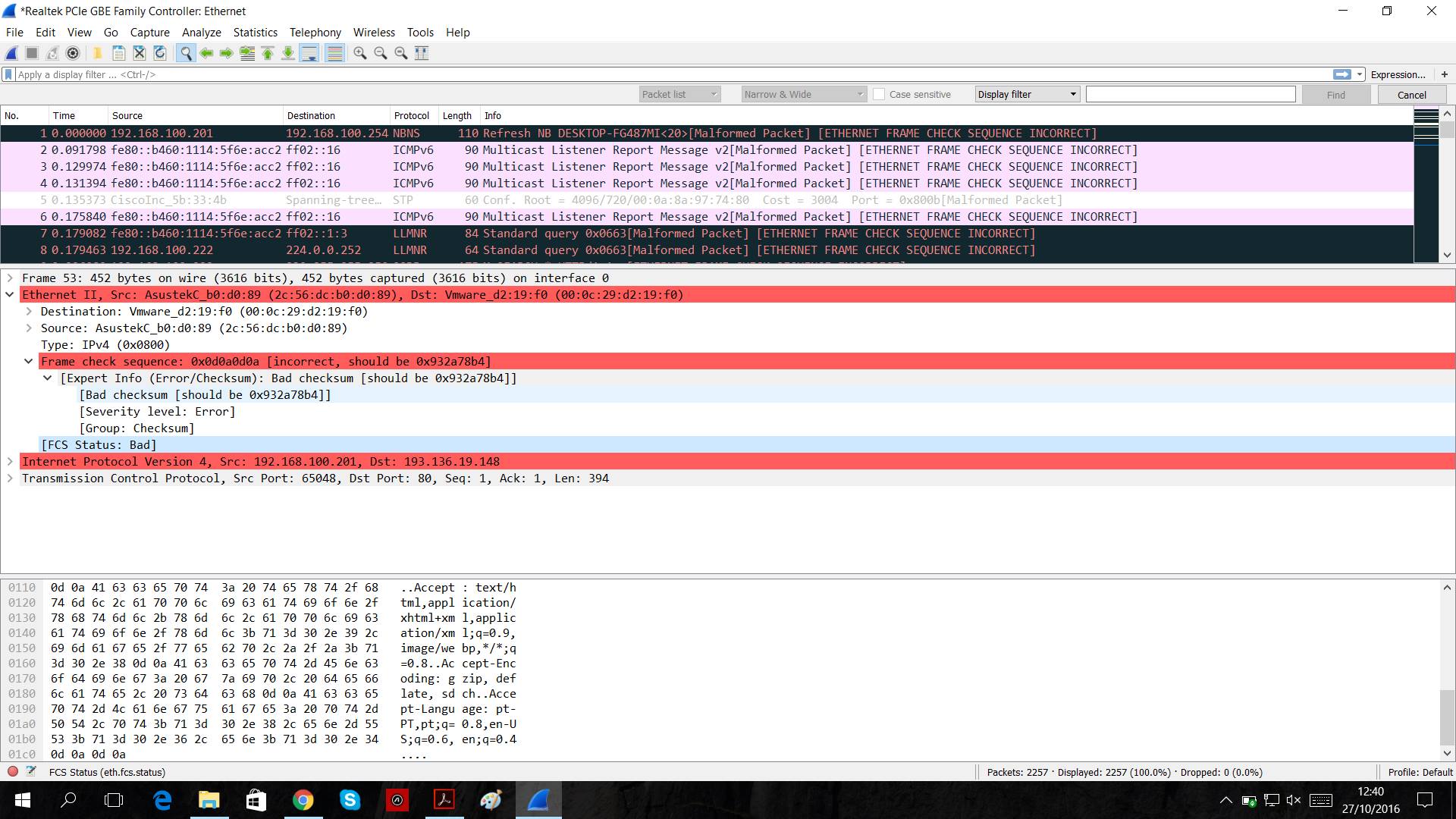
R: O valor hexadecimal do campo Type da trama Ethernet é 0x0800, o que corresponde ao tipo de dados do IP que vai ser encapsulado.

4. Quantos bytes são usados desde o ínicio 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.



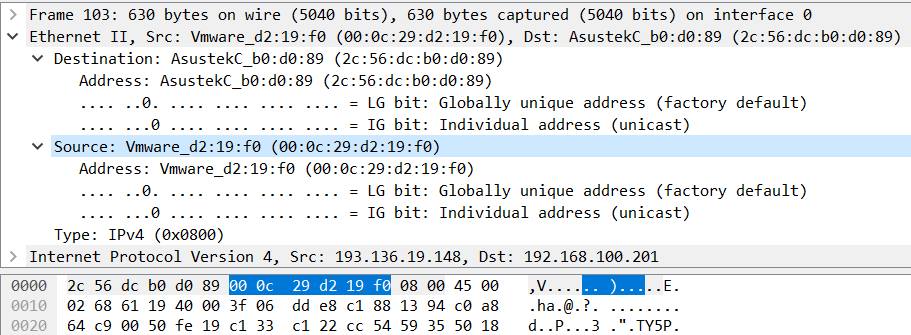
R: Desde o inicio da trama até ao caracter ASCII “G” do método HTTP GET, são usados 53 bytes. O tamanho da trama é 452, logo o overhead será dado por 53/452 = 0,117 = 11,7 %

5. Em ligações com fios pouco susceptíveis a erros, nem sempre as NICs geram o código de detecção 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 a configuração inicial.



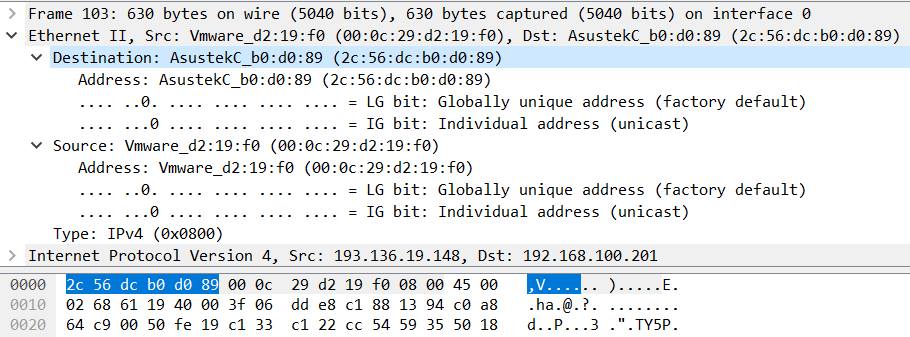
R: Não está a utilizar FCS, pois caso estivesse a utilizar a informação que corresponde a este iria aparecer a seguir à informação do tipo de nível 2. O valor que está na imagem corresponde aos 4 últimos bytes da trama. Concluimos que ao fazer a mudança vai dar como incorreto pois, como não foi utilizado FCS, não tem os bytes de verificação de erro como era suposto ter.

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

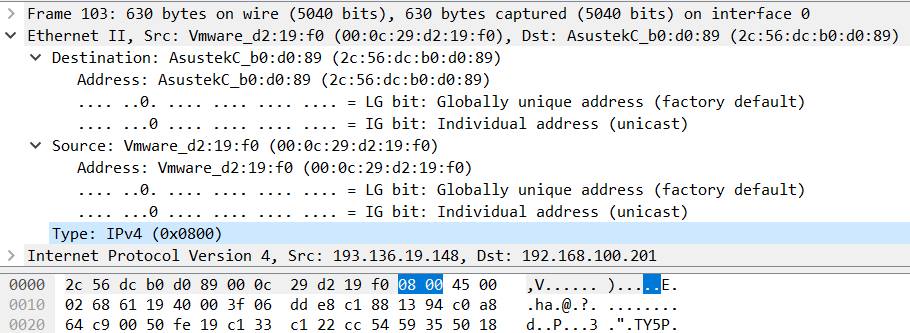


R: O endereço Ethernet da fonte é 00:0c:29:d2:19:f0. Este pertence à máquina virtual responsável pelo endereçamento da página, pois ao abrirmos a página cesium.uminho.pt, o pedido vai ter de ser enviado para a rede que suporta o site, e a resposta provém deste.

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

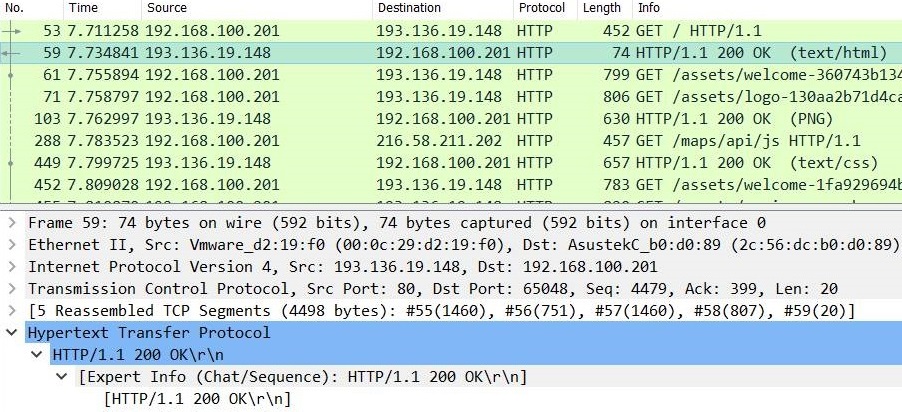


R: O endereço MAC do destino é 2c:56:dc:b0:d0:89, que vai corresponder ao endereço MAC do computador que efetuou o pedido anteriormente.

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

R: O valor hexadecimal do campo Type é 0X080.

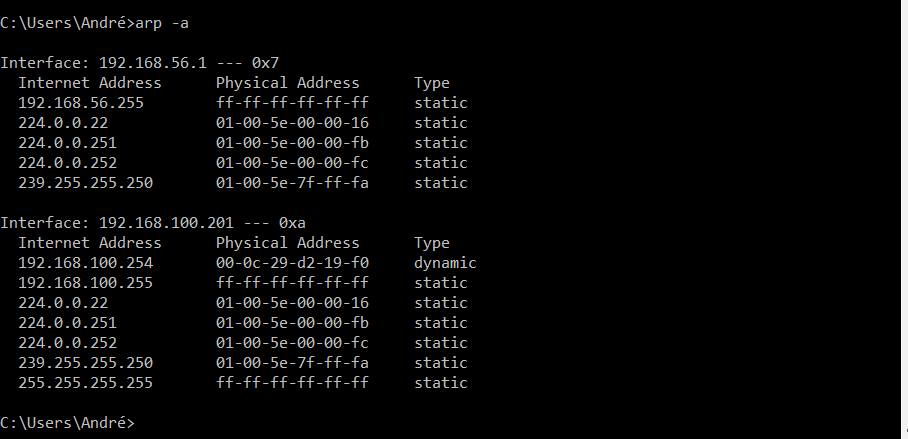
9. Que tipo de resposta foi enviada pelo servidor?



R: O tipo de resposta que foi enviado pelo servidor foi um ‘’OK’’.

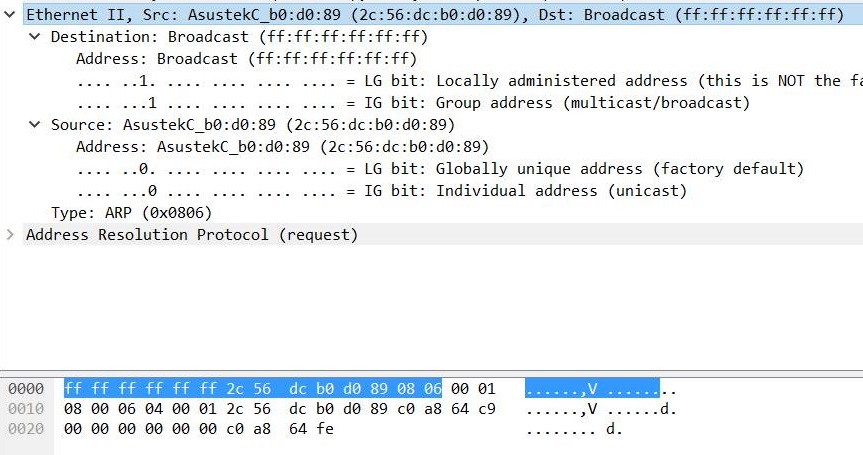
Protocolo ARP

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



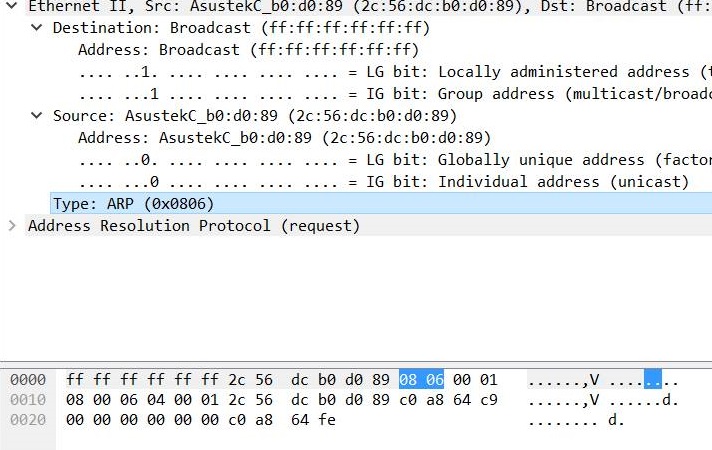
R: A primeira coluna (Internet Adress) corresponde ao endereço IP, a segunda coluna (Physical Adress) corresponde ao MAC Adress e a última coluna (Type) refere-se ao tipo, que pode ser estático ou dinâmico.

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?



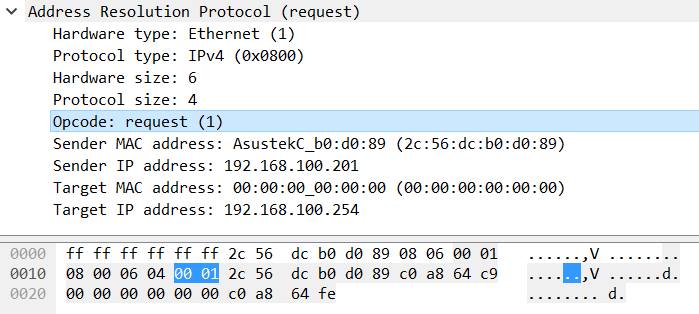
R: O valor hexadecimal do endereço de origem é 2c:56:dc:b0:d0:89 e o de destino é ff:ff:ff:ff:ff:ff. Isto indica que estamos a fazer um broadcast para a camada 2.

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

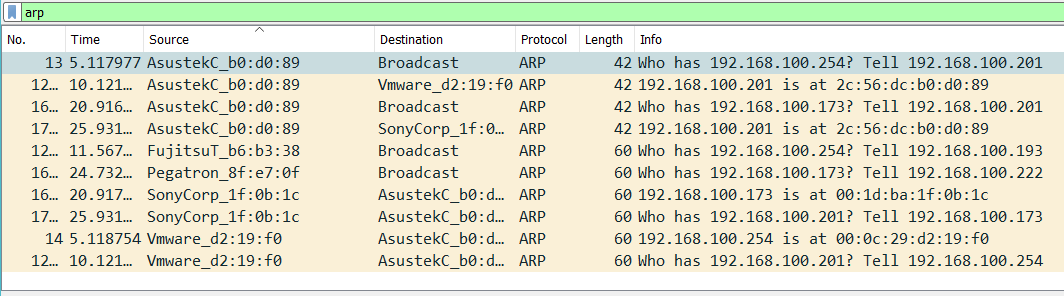


R: O valor hexadecimal do campo do tipo Ethernet é 0x0806, que significa que o ARP do tipo de Ethernet está associado a esse valor.

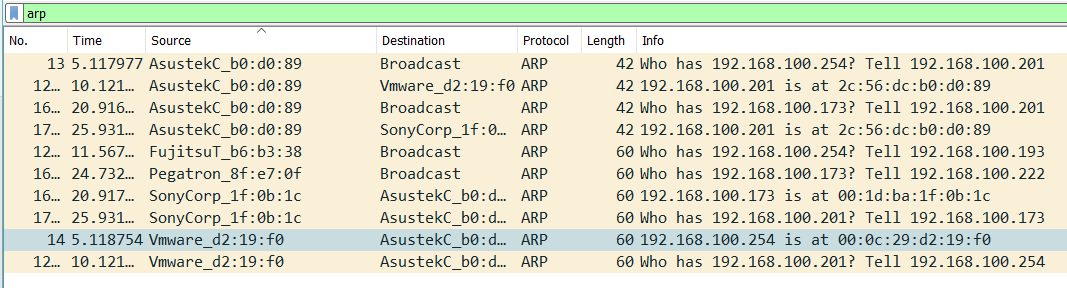
13. Qual o valor do campo ARP opcode? O que especifica? Se necessário, consulte a RFC do protocolo ARP <http://tools.ietf.org/html/rfc826.html>).

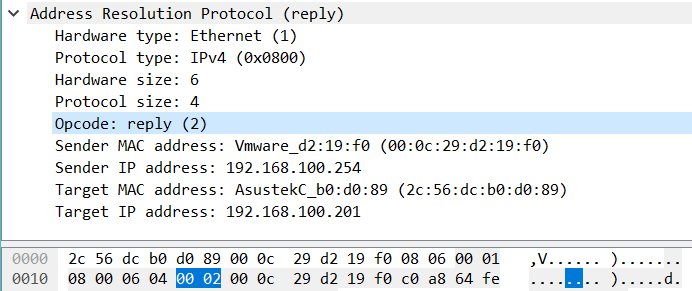


R: O valor do campo ARP opcode é 00 01, que nos diz que isto é relativo a um request ou a uma reply (ou seja, vai ser uma flag). Neste caso, vai ser um request como visto em cima [request (1)].

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

R: O nosso endereço IP está de facto contido na mensagem ARP, como podemos observar na imagem acima, estando este endereço a seguir a “Tell” (endereço IP da nossa máquina). Nós conectámos a nossa máquina a uma máquina dos nossos colegas. Para fazermos isso, enviamos um request (broadcast) a todas as máquinas que estão ligadas à nossa rede Ethernet a perguntar quem tem o IP 192.168.100.254 (“Who has 192.168.100.254?”), obtendo assim o seu endereço MAC para o conectarmos ao nosso.

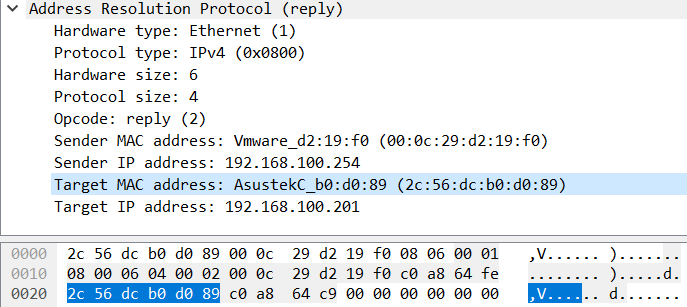
15. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

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

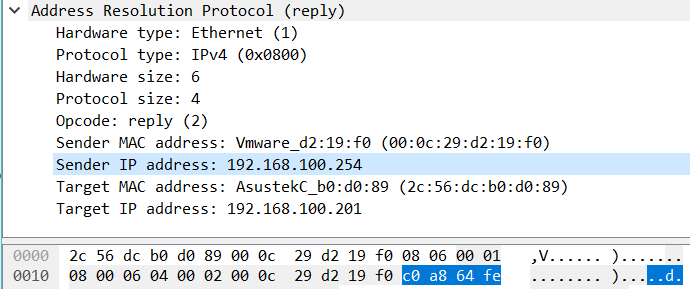
R: A resposta que nós procuramos é o endereço MAC relativo ao endereço IP procurado (“00:0c:29:d2:19:f0’’), como é possível observar na primeira imagem.

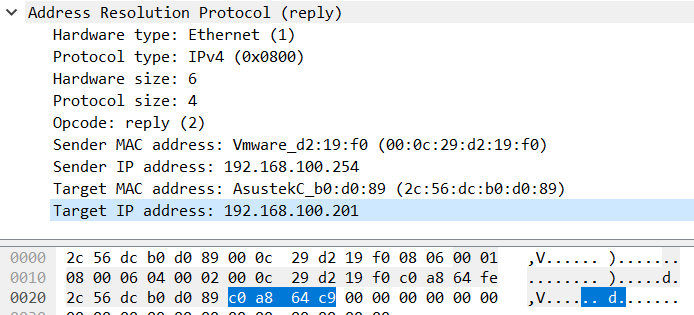
Relativamente ao valor do campo ARP opcode, vai ser 00 02. Ao estarmos a especificar o reply (2), estamos a ir buscar o valor do broadcast que fizemos.

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



R: A resposta ao pedido ARP vai estar no “Target MAC address” (2c:56:dc:b0:d0:89).

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

R: Os valores para os endereços origem que contém a resposta ARP são c0 a8 64 fe.

R: E os valores para o endereço destino da trama são c0 a8 64 c9.

Ou seja, é possível ligar diretamente a nossa máquina através do endereço IP.

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



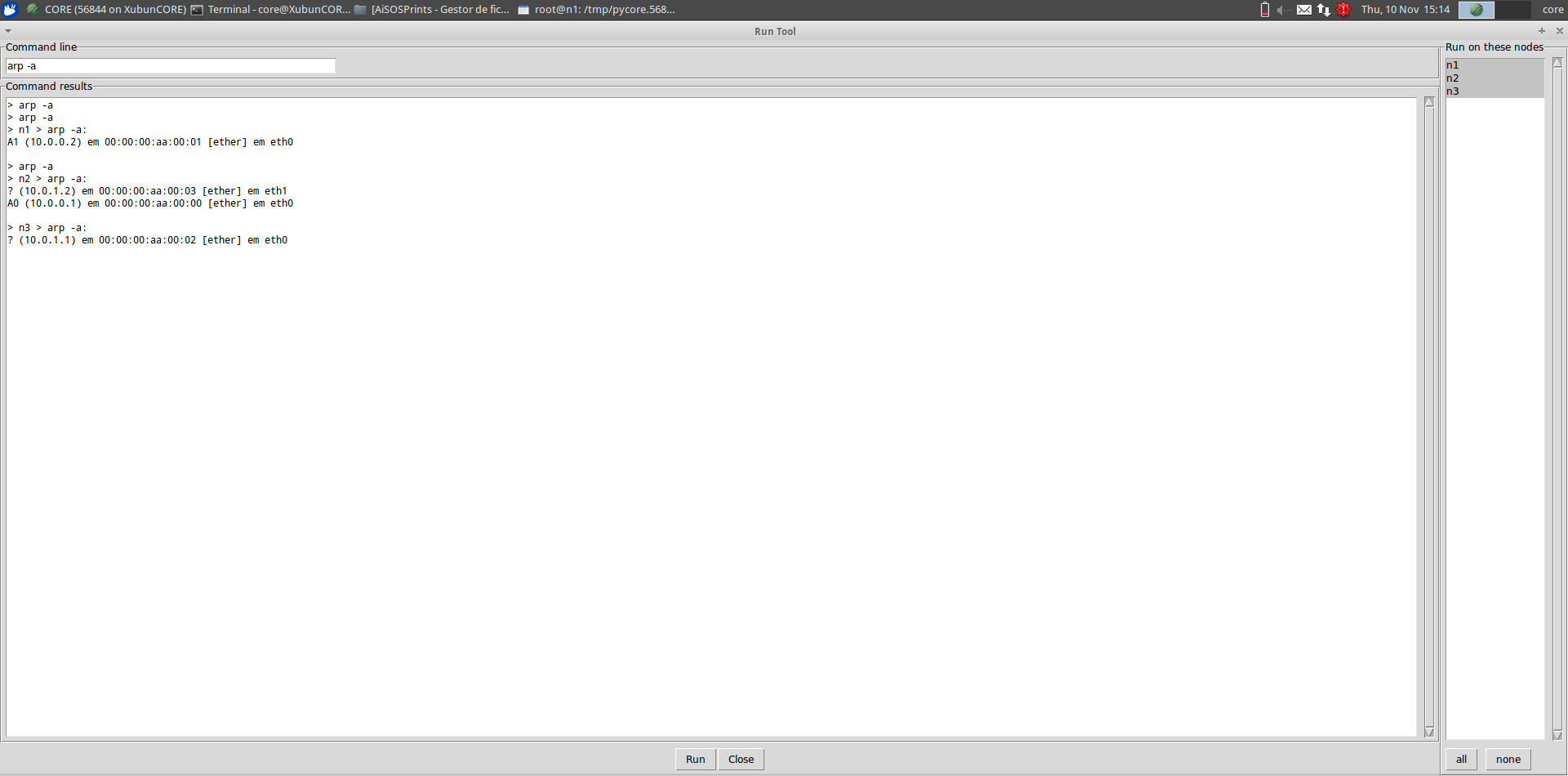
R: Os endereços Ethernet das interfaces dos diversos routers são:

n1: ee:aa:d8:c3:ce:b1

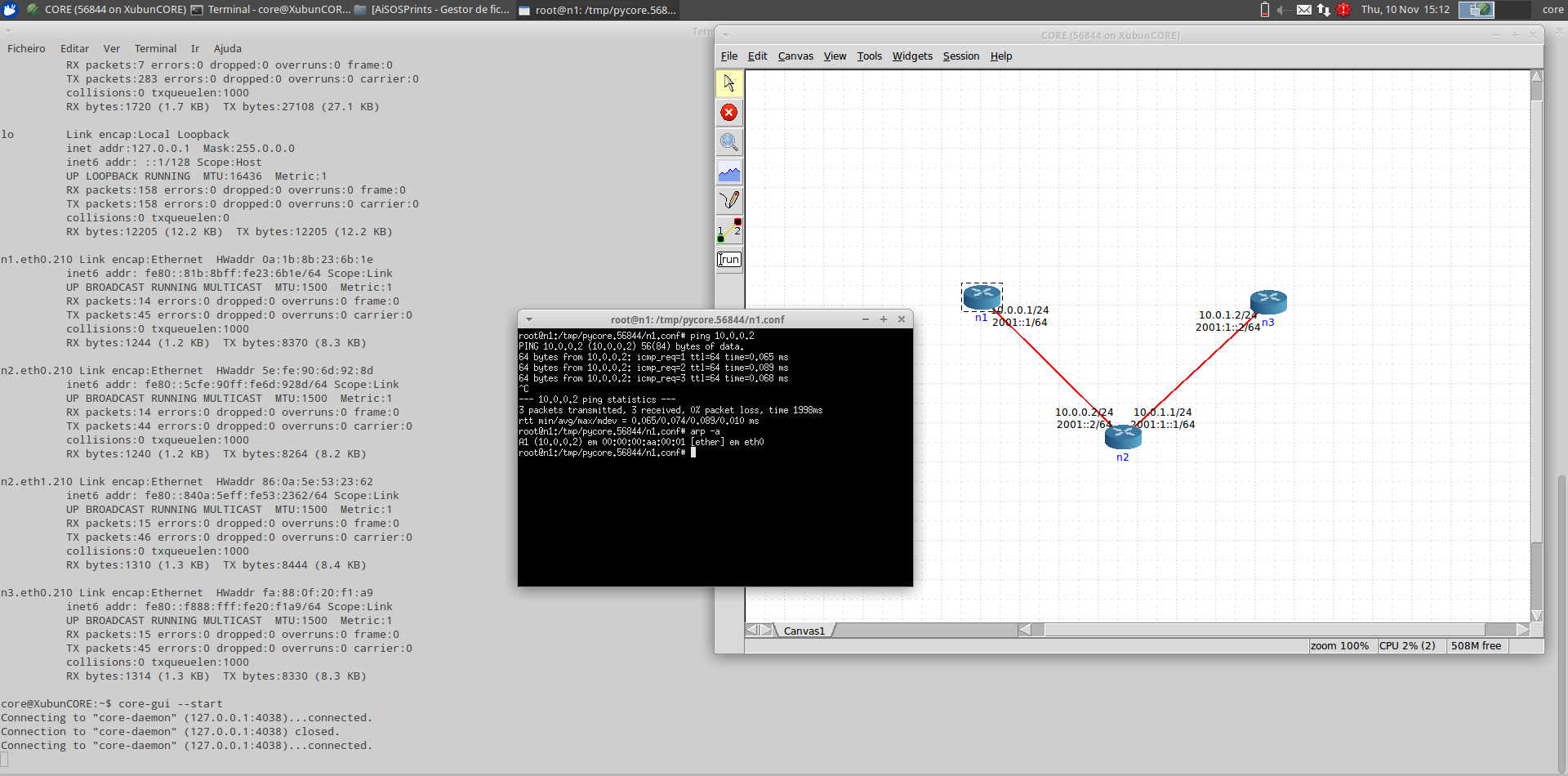
n2: 96:e8:b0:fb:27:e4 e a2:ba:cf:80:b3:2f

n3: ae:70:35:ce:0a:0d

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

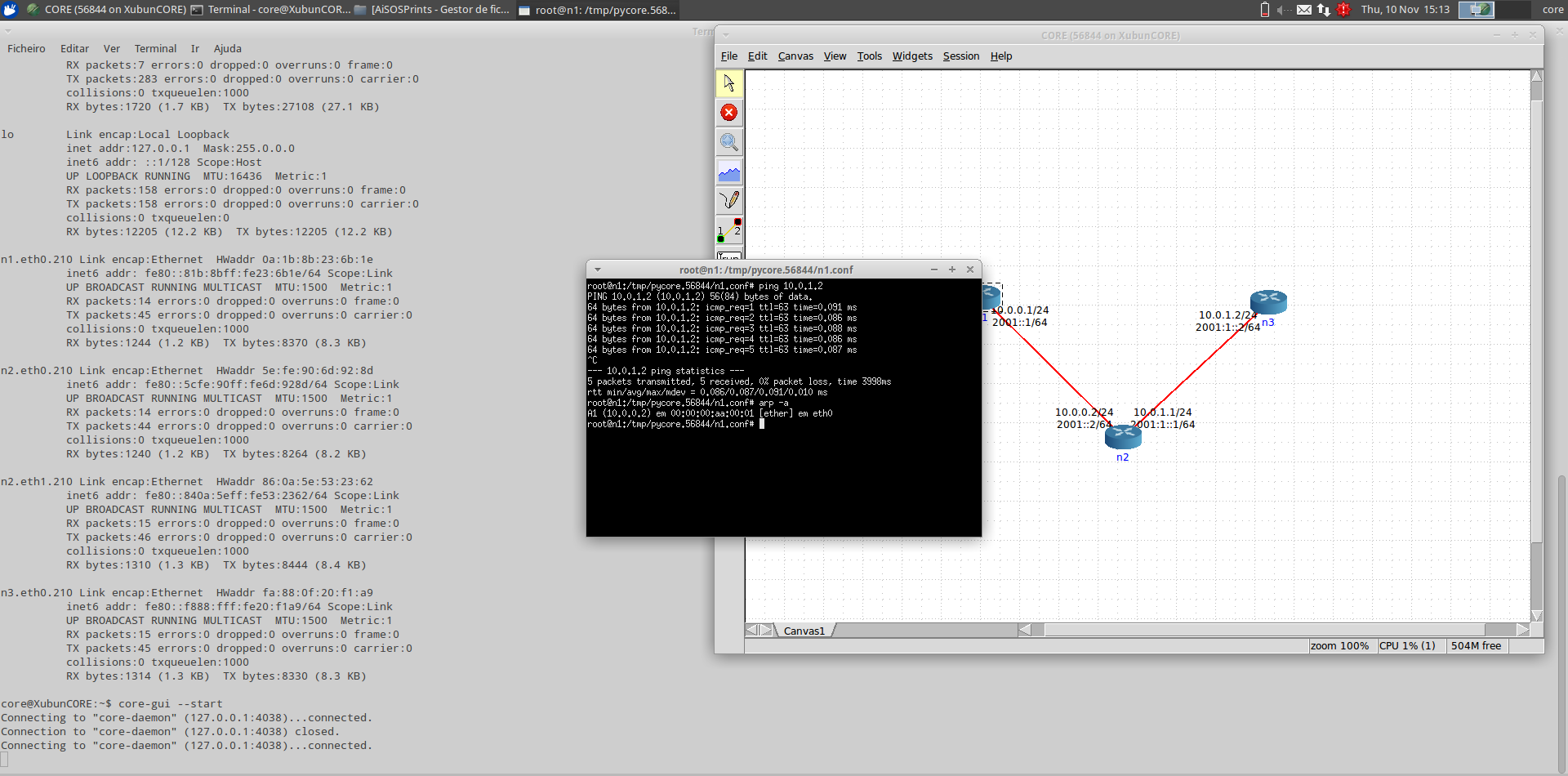


19. Faça ping de n1 para n2. Que modificações observa nas caches ARP desses sistemas? Faça ping de n1 para n3. Consulte as caches ARP. Que conclui?



R: n1 para n2

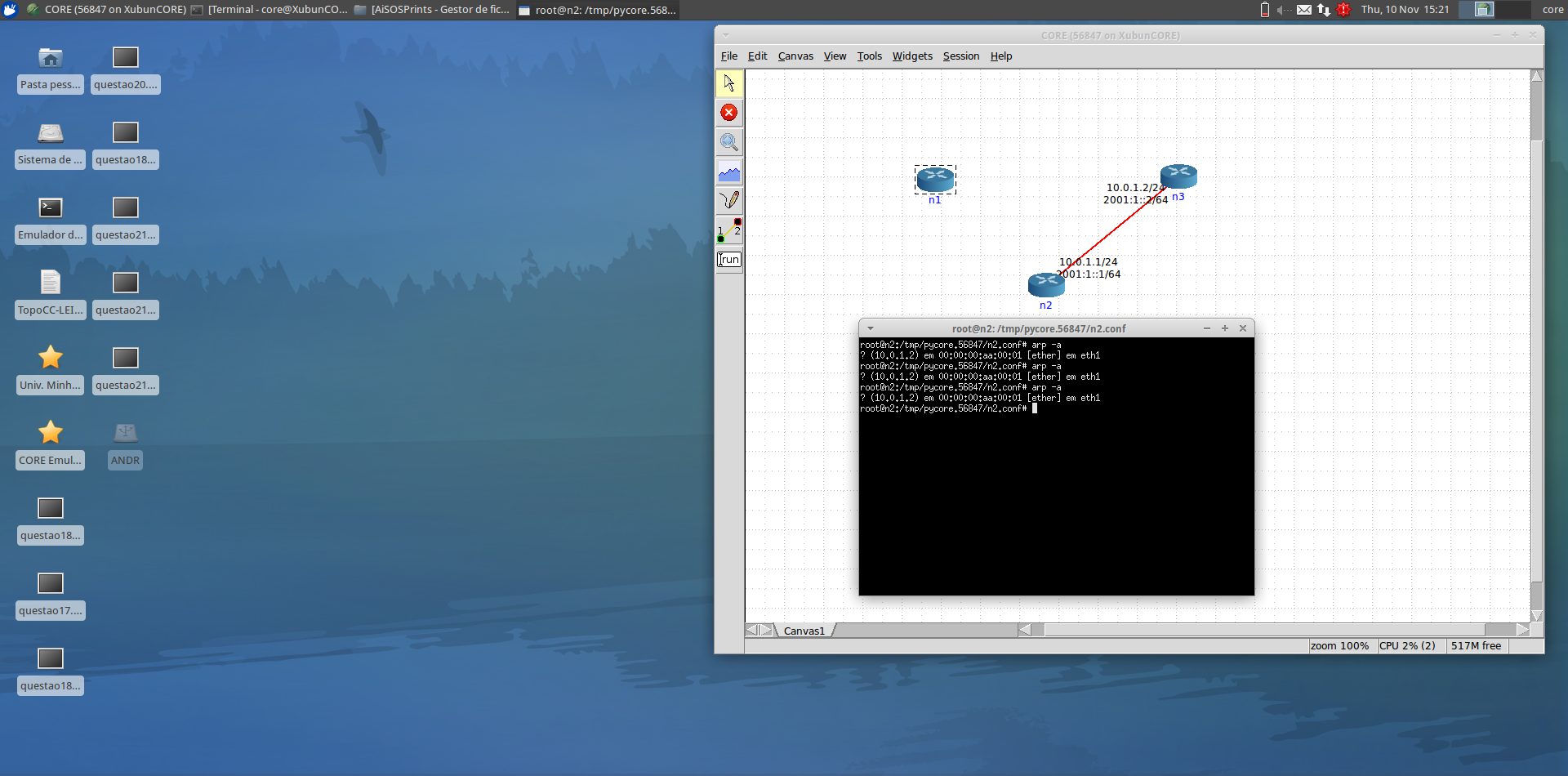
Pela análise da cache de n1, é possível reparar que o endereço 10.0.0.2 está ligado a 00:00:00:aa:00:01.



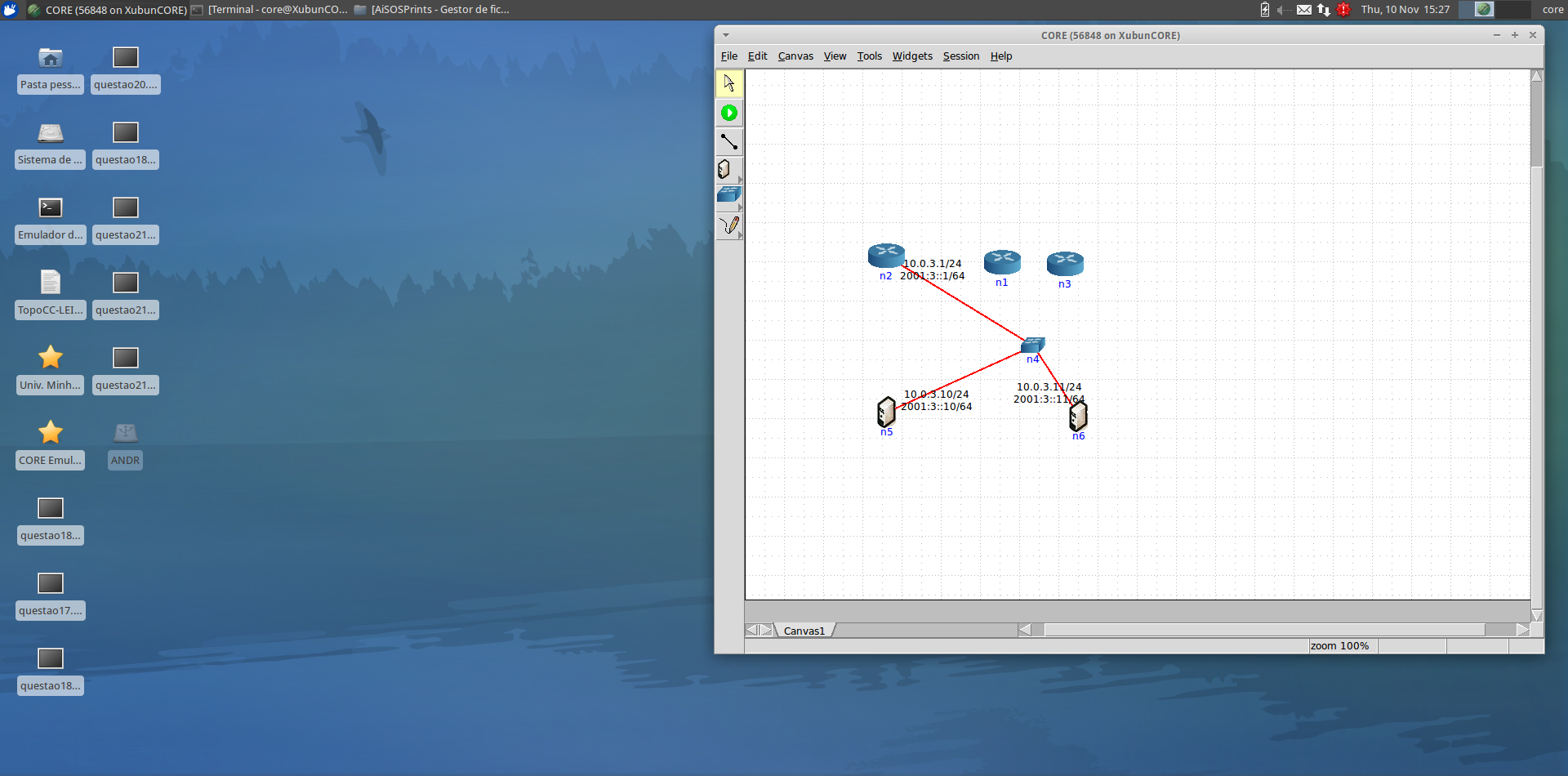
R: n1 para n3

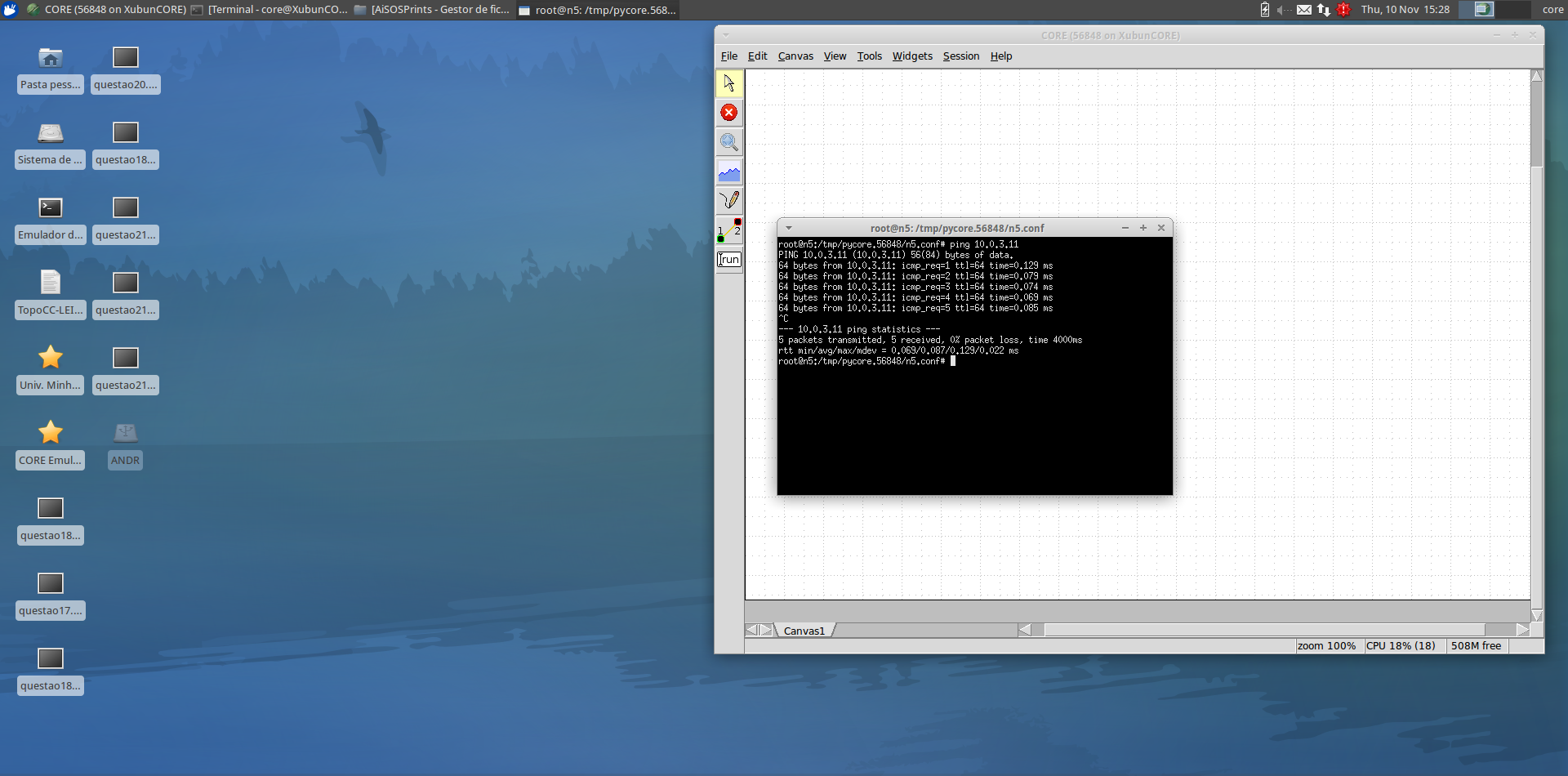
Pela análise da cache de n1, é possível reparar que o endereço 10.0.1.2 está ligado a 00:00:00:aa:00:01.

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

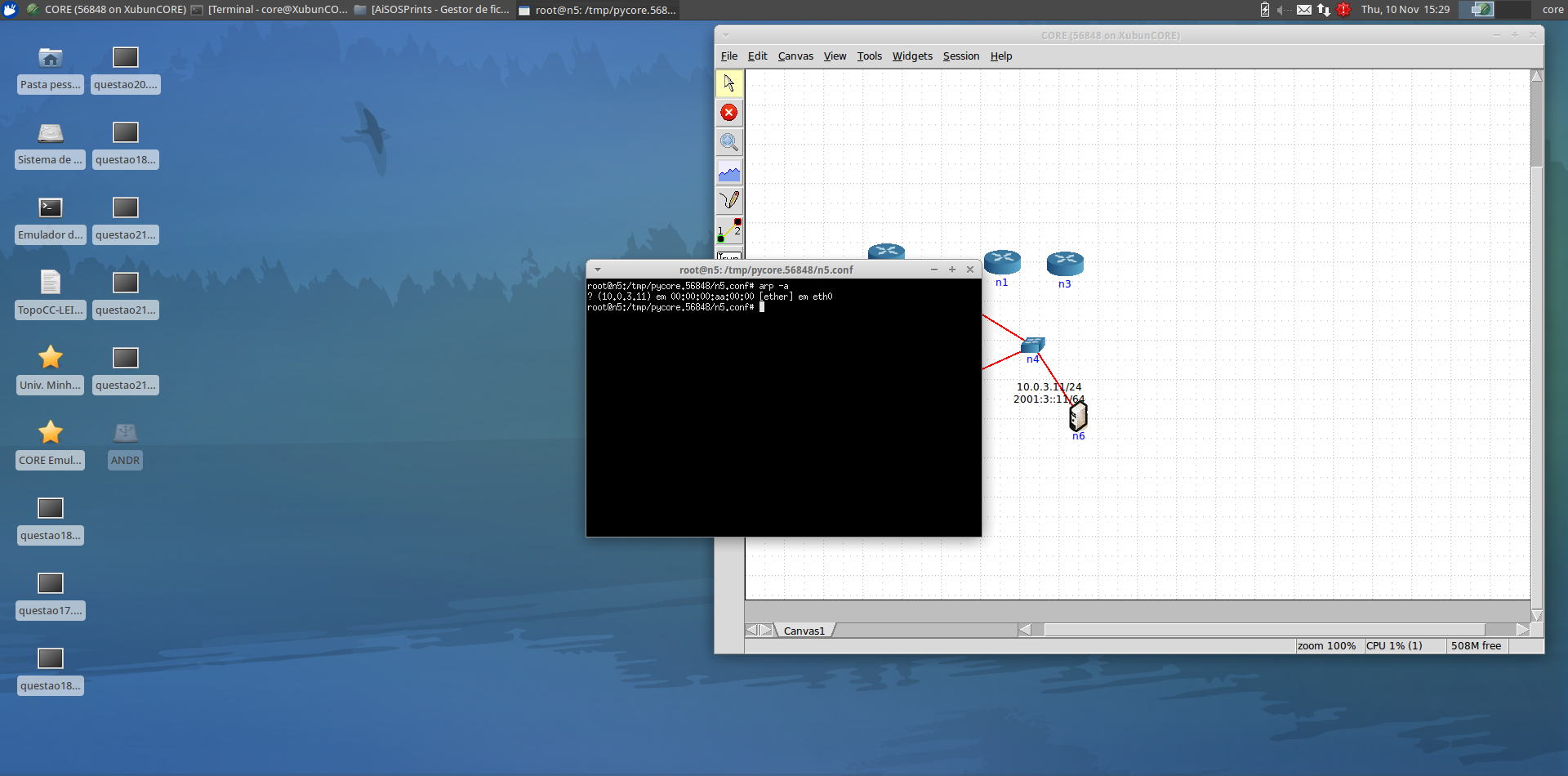


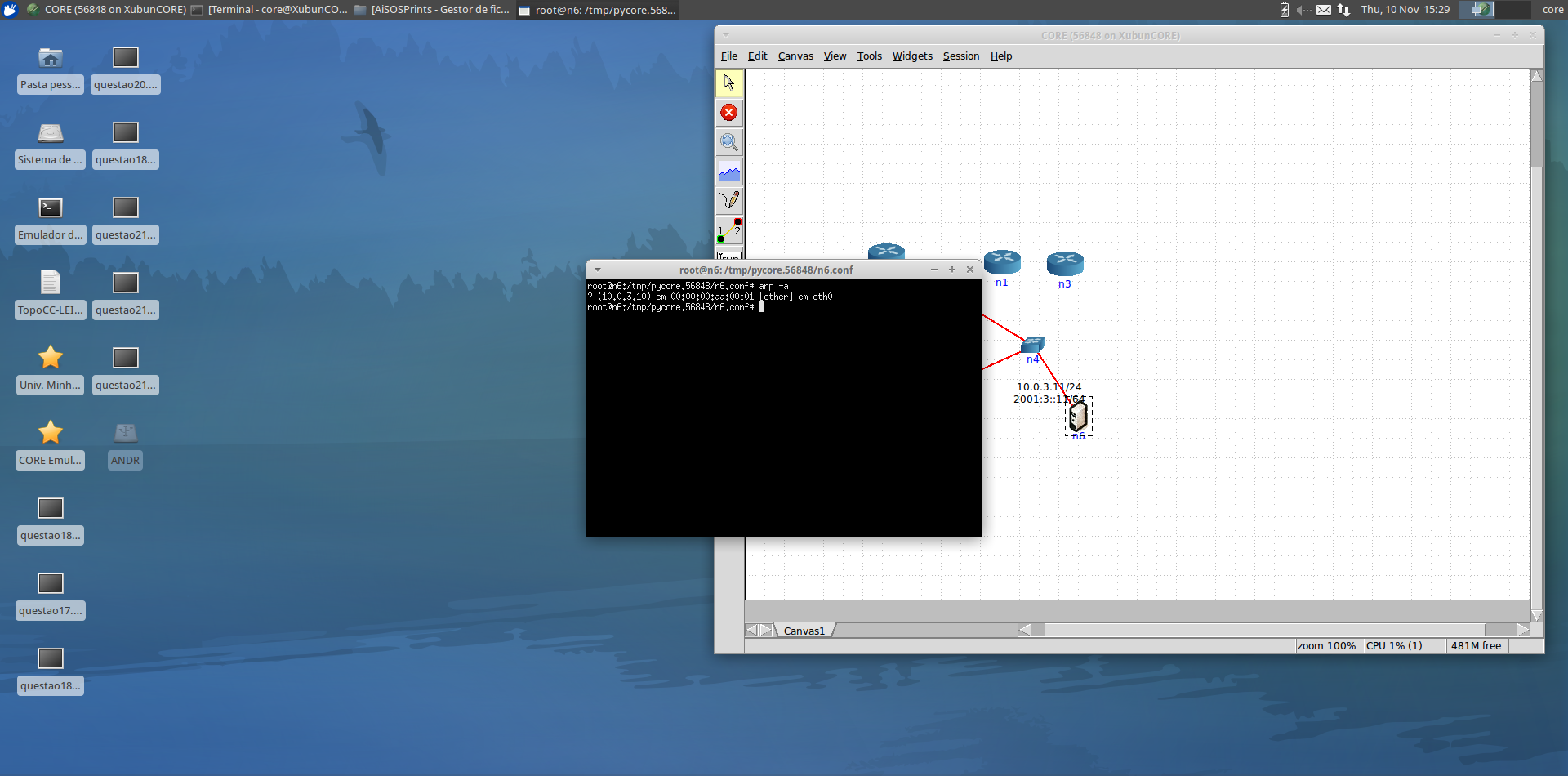
R: Pela imagem, podemos ver que apenas a interface n3 aparece, sendo o endereço que colocamos (ff:ff:ff:ff:ff:ff) ignorado.

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.



R: No ARP da bash de n5 deverá aparecer o IP de n6 e à frente o endereço MAC de n6.



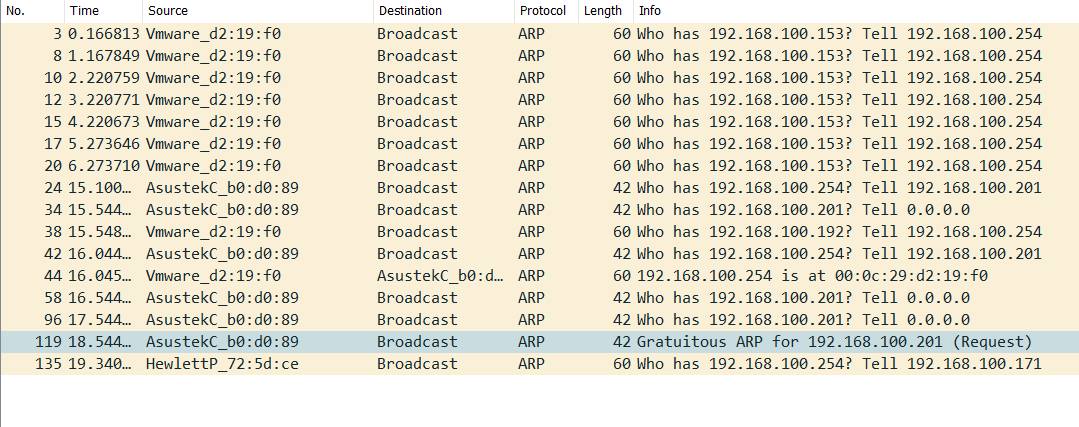


R: Pela imagem apresentada acima, é possível verificar que a nossa interpretação feita estava correta. Em n6, aparece também uma nova entrada com o IP de n5.

PARTE 2

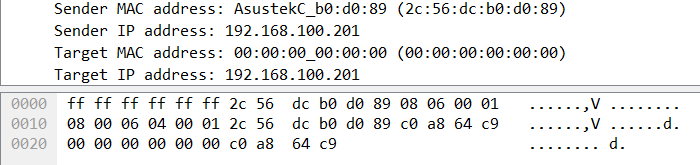
ARP Gratuito

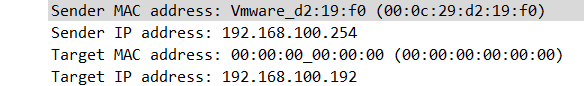
1. Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Verifique quantos pacotes ARP gratuito foram enviados e com que intervalo temporal?



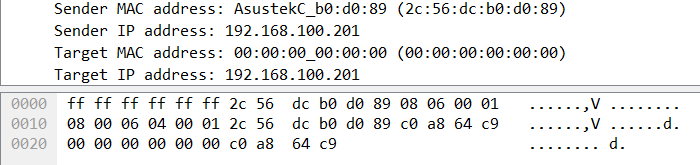
R: Foi enviado um pacote ARP gratuito que demorou 18.5s.

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?

**ARP Gratuito**

**ARP Normal**

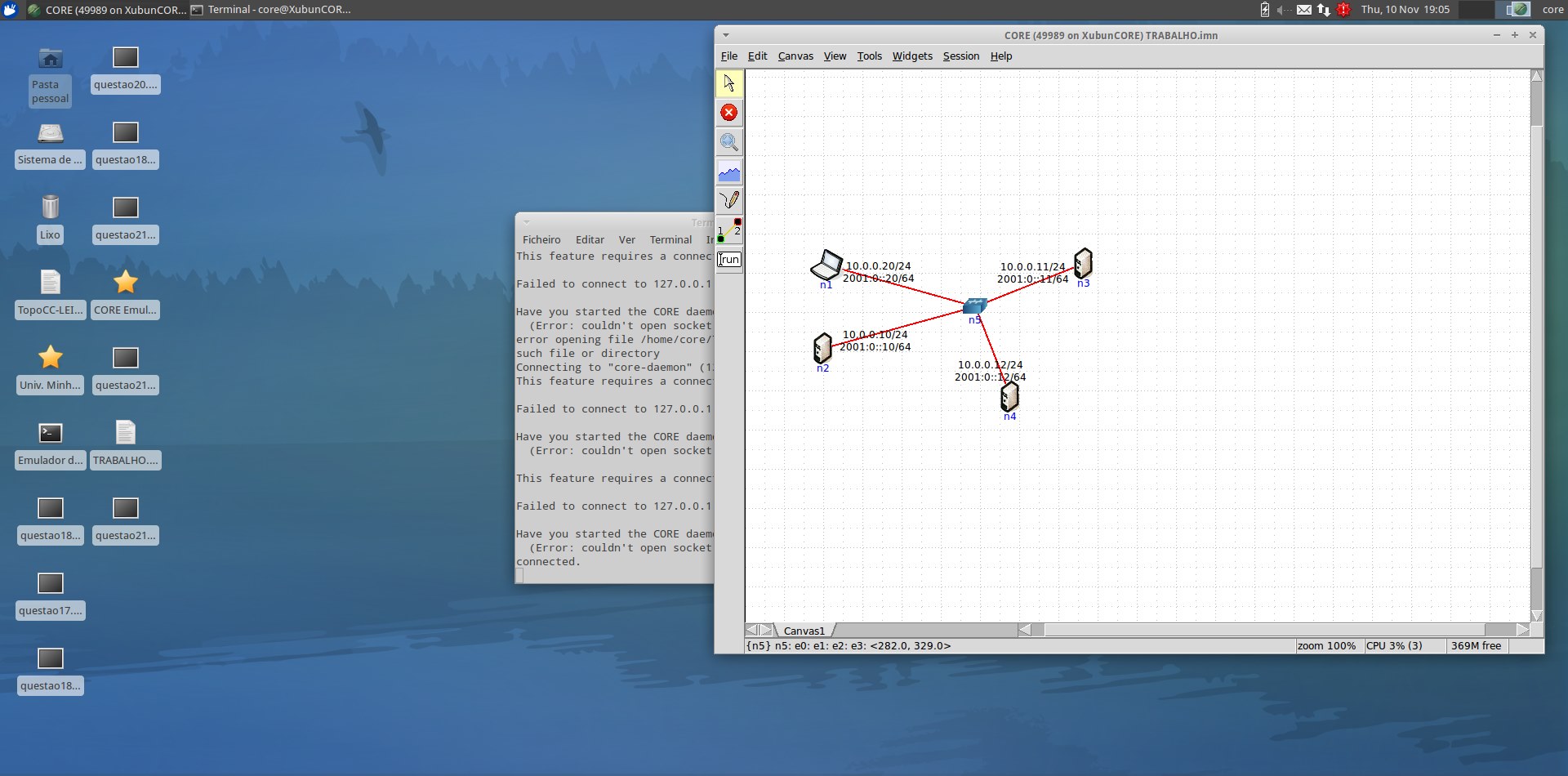
R: Num ARP Normal, é procurado o MAC correspondente a um certo IP. No Gratuito, a máquina questiona-se a si própria sobre qual o MAC que corresponde ao próprio IP, para descobrir se tem mais alguma máquina a usar o nosso IP.

A trama Ethernet que corresponde ao ARP Gratuito é a seguinte:

O resultado esperado face ao pedido ARP Gratuito enviado será “verdadeiro” se a nossa máquina for a única a utilizar este endereço IP.

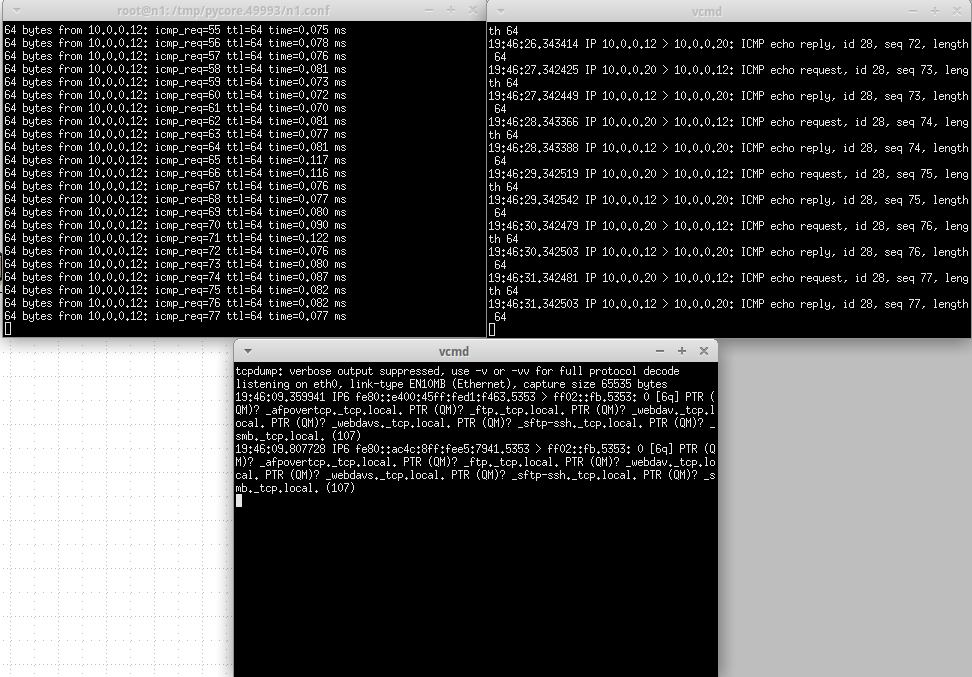
Domínios de Colisão

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





R: No terminal do canto superior esquerdo, está o ping do computador n1 para o host n2, no superior direito está o tcpdump de n2 e em baixo encontra-se o tcpdump de n3. Como temos um hub, há partilha de meio e o pedido vai fluir por todas as máquinas conectadas ao hub. O ping não foi para o servidor n3 mas este vai receber na mesma a trama enviada no meio. O pedido vai, por isso, fluir por todas as máquinas conectadas ao hub.

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.

R: No terminal do canto superior esquerdo, está o ping do computador n1 para o host n2, no superior direito está o tcpdump de n2 e em baixo encontra-se o tcpdump de n3. Como temos um switch, não há partilha de meio e o pedido vai apenas passar pelas máquinas envolvidas no ping. O ping não foi para o host n3, por isso, este não vai receber a trama. O pedido flui apenas pelas máquinas diretamente envolvidas nele.

Os switches eliminam as colisões, conectando cada dispositivo a uma porta do comutador, enquanto que os hubs permitem que estas colisões possam existir. Ao utilizar um hub para comunicar entre um computador e um host, também passava tráfego pelas outras máquinas do esquema, no entanto, ao mudarmos para o switch, observamos que apenas passava tráfego pelo computador e pelo host ao efetuar o ping, eliminando assim, o tráfego pelas outras máquinas e evitando colisões.

Conclusões