Camada de Ligação Lógica

Hugo Manuel Cunha, Marcos Daniel Teixeira da Silva, Susana Vitória Sá Silva Marques

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
Email:{a84656,a78566,a84167} @alunos.uminho.pt

1 Captura e análise de tramas Ethernet

1.1 Questões

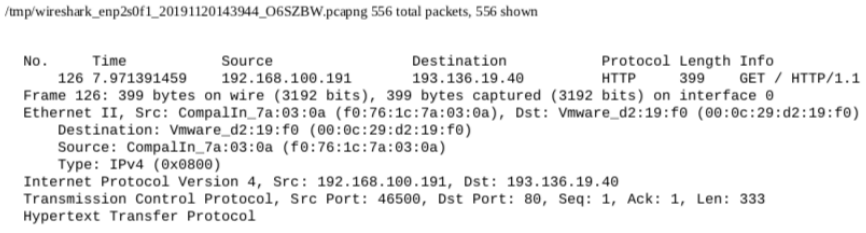

Fig. 1.

Pergunta 1

Anote os endereços MAC de origem e de destino da trama capturada.

Resposta

Destino: 00:0C:29:D2:19:F0
Source: F0:76:1C:7A:03:0A

Pergunta 2

Identifique a que sistemas se referem. Justifique.

Resposta

Destino: VMWare D2:19:F0
Source: CompalIn 7A:03:0A
Os primeiros 3 bytes do endereço MAC referem-se ao fabricante do equipamento.

Pergunta 3

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

Resposta

O Type é 0X0800. Isto significa que o payload da trama Ethernet é um protocolo IPv4.

Pergunta 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.

Resposta

399(tamanho total da trama) - 333 (tamanho total do payload do protocolo TCP: request HTTP) = 66
O tamanho de tudo o que está acima do início do método HTTP GET é 66.
66/399 *100= 17 %
O overhead introduzido por todos os protocolos onde o HTTP está inserido é de 17 %

Pergunta 5

Através de visualização direta de uma trama capturada, verifique que, possivelmente, o campo FCS (Frame Check Sequence) usado para deteção de erros não está a ser usado. Em sua opinião, porque será?

Resposta

O FCS é calculado pela placa de rede e é desnecessário numa ligação Ethernet por ser fiável. O equipamento descarta automaticamente todos os pacotes com o checkSum errado.

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

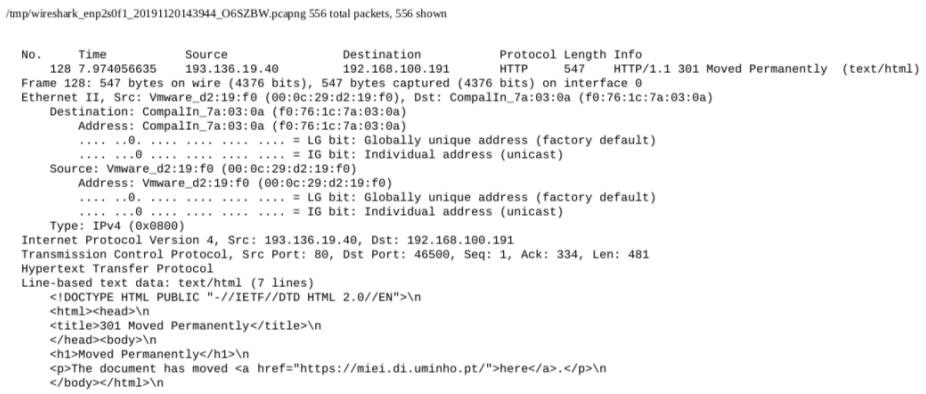

Fig. 2.

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

Resposta

Source: 00:0C:29:D2:19:F0
VMWare D2:19:F0

Pergunta 7

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

Resposta

Destino: F0:76:1C:7A:03:0A
CompalIn 7A:03:0A

Pergunta 8

Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.

Resposta

A trama recebida contém um protocolo HTTP (camada de aplicação) encapsulado num protocolo TCP (camada de transporte) encapsulado num protocolo IPv4 (camada de rede) encapsulado num protocolo Ethernet (camada de rede/física).

2 Protocolo ARP

2.1 Questões

Pergunta 9

Observe o conteúdo da tabela ARP. Explique o significado de cada uma das colunas.

Resposta

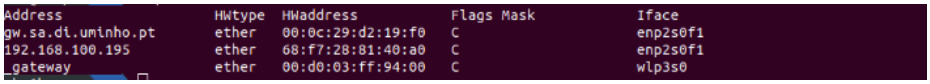

Fig. 3.

A primeira coluna indica-nos o endereço ip do host, a segunda coluna indica-nos o tipo de ligação(Ethernet), na terceira encontramos o endereço de destino(MAC address), a quarta coluna tem a indicação da flag e na quinta encontramos a interface(neste caso é nos mostrada a interface do host).

Pergunta 10

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?

Resposta

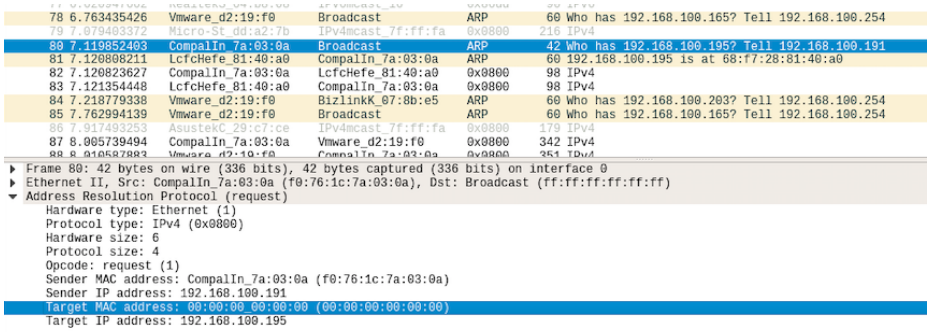

Fig. 4.

Destino:ff:ff:ff:ff:ff:ff
Source:f0:76:1c:7a:03:0a
É usado um endereço ethernet do broadcast (camada 2) para poder ser recebido por todos os hosts da rede.

Pergunta 11

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

Resposta

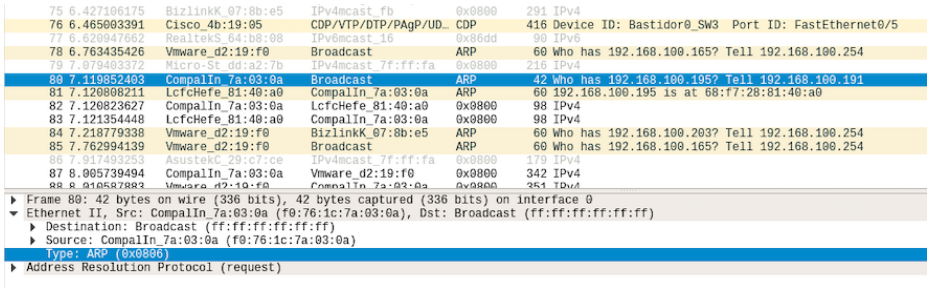

Fig. 5.

ARP (0X0806) indica que o protocolo Ethernet tem nos seus dados um protocolo ARP encapsulado.

Pergunta 12

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).

Resposta

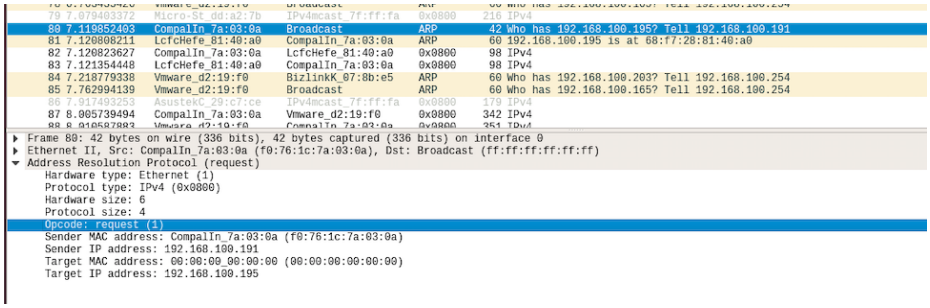

Fig. 6.

Opcode: request (1), que nos indica que é um request que espera um reply. Percebemos isso através do valor 1 especificado(se fosse o valor 2 seria um reply).

Pergunta 13

Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?

Resposta

Na mensagem ARP estão contidos endereços IP e MAC de origem e IP de destino. O MAC de destino ainda é um broadcast porque o objetivo é ainda descobrir qual é o MAC correspondente ao IP do destino.

Pergunta 14

Explicite que tipo de pedido ou pergunta é feito pelo host de origem?

Resposta

"Who has 192.168.100.195? Tell 192.168.100.191"
Perguntamos aos hosts da rede qual o mac de quem tem o ip 192.168.100.195, e pedimos para enviar a resposta para o 192.168.100.191.

Pergunta 15

Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.
a. Qual o valor do campo ARP opcode? O que especifica?
b. Em que posição da mensagem ARP está a resposta ao pedido ARP?

Resposta

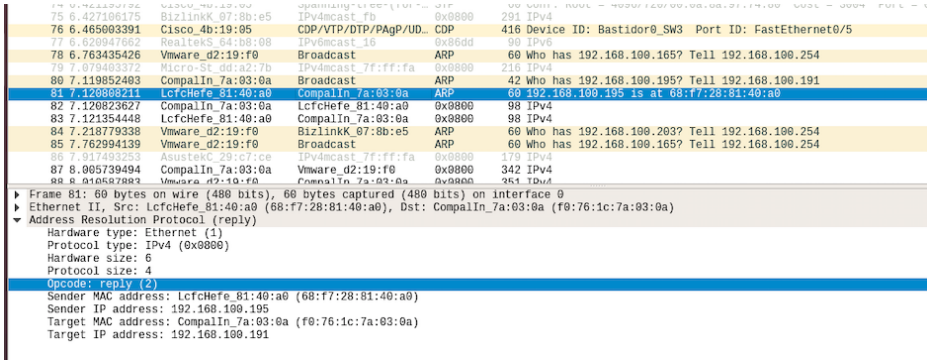

Fig. 7.

a) Opcode: reply(2) , que nos indica que é um reply. Percebemos isso através do valor 2 especificado.
b) A resposta encontra-se no Sender MAC address e no Sender IP address:

Pergunta 16

Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. 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?

Resposta

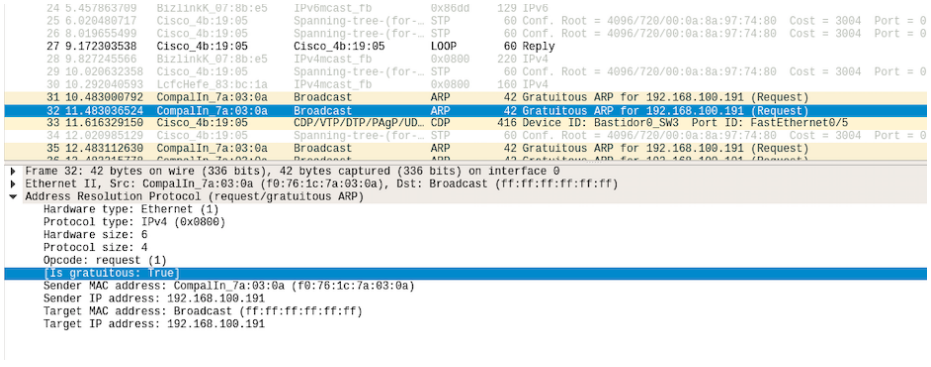

Fig. 8.

Distingue-se através da adição de um campo: Is gratuitous: True O resultado esperado é não obter resposta uma vez que o endereço de IP testado é único.

3 Domínios de colisão

3.1 Questões

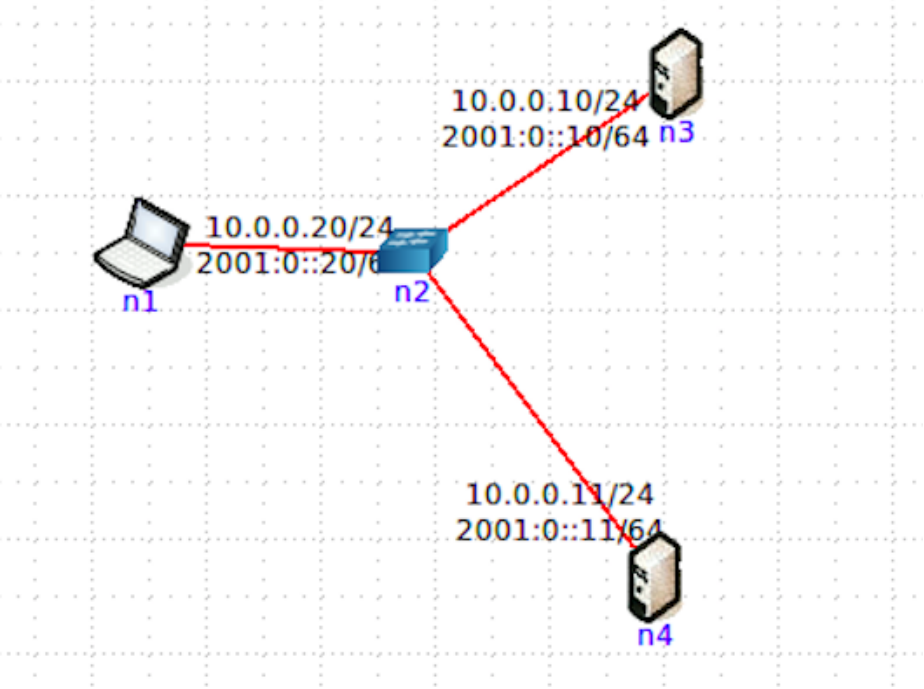

Fig. 9.

Pergunta 17

Faça ping de n1 para n3. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?

Resposta

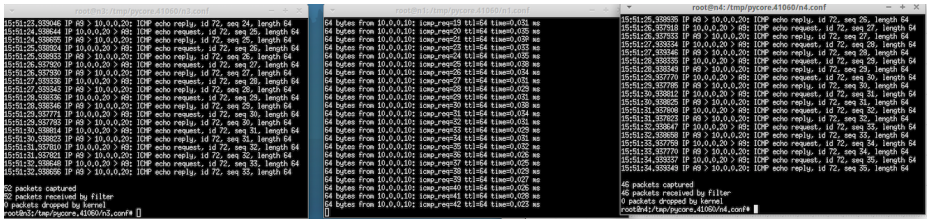

Fig. 10.

Depois de fazer o ping de n1 para n3, analisando o tráfego num host não envolvido na comunicação, por exemplo, n4, verificamos que apesar de o pedido não lhe ser destinado ele recebe mesmo assim essa comunicação.

Pergunta 18

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.

Resposta

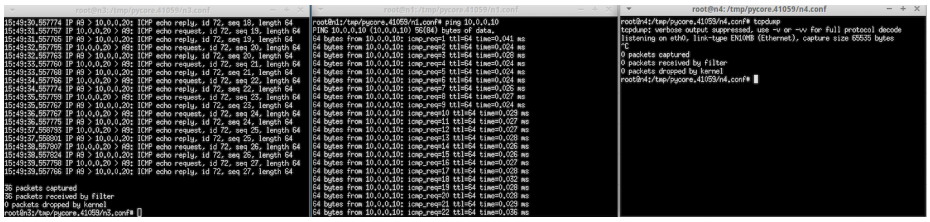

Fig. 11.

Com a utilização do switch o problema analisado na pergunta anterior fica resolvido, isto porque se analisarmos mais uma vez o tráfego que flui para n4 verificamos que com o switch ele já não recebe a ping que n1 faz para n3.

4 Conclusão

Com este trabalho prático aprendemos como funciona a conexão de redes locais baseado no envio de pacotes.

Abordamos o funcionamento da partilha de endereços MAC, nestas mesmas redes, usando o protocolo ARP e com a ferramenta CORE analisamos o funcionamento dos domínios de colisão e o modo de como são corrigidos (através de um switch de rede, por exemplo).

Assim, ao realizarmos este trabalho conseguimos consolidar melhor toda a matéria que abrange a camada de Ligação Lógica dada nas aulas teóricas.