

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

/tmp/wireshark_enp2s0f1_20191120143944_O6SZBW.pcapng 556 total packets, 556 shown

No.	Time	Source	Destination	Protocol	Length	Info
126	7.971391459	192.168.100.191	193.136.19.40	HTTP	399	GET / HTTP/1.1

Frame 126: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface 0
Ethernet II, Src: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a), Dst: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
Destination: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
Source: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.100.191, Dst: 193.136.19.40
Transmission Control Protocol, Src Port: 46500, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
Hypertext Transfer Protocol

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

Quanto 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

$399(\text{tamanho total da trama}) - 333(\text{tamanho total do payload do protocolo TCP: request HTTP}) = 66$

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:

/tmp/wireshark_enp20f1_20191120143944_O6SZBW.pcapng 556 total packets, 556 shown

```
No.      Time            Source                Destination            Protocol Length Info
 128 7.974956635    193.136.19.40         192.168.100.191        HTTP      547      HTTP/1.1 301 Moved Permanently (text/html)
Frame 128: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface 0
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a)
  Destination: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a)
    Address: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
    Source: 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)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 193.136.19.40, Dst: 192.168.100.191
  Transmission Control Protocol, Src Port: 80, Dst Port: 46500, Seq: 1, Ack: 334, Len: 481
  Hypertext Transfer Protocol
  Line-based text data: text/html (7 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>301 Moved Permanently</title>\n
    </head><body>\n
    <h1>Moved Permanently</h1>\n
    <p>The document has moved <a href="https://miei.di.uminho.pt/">here</a>.</p>\n
    </body></html>\n
```

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

Address	Hwtype	Hwaddress	Flags	Mask	Iface
gw.sa.di.uninho.pt	ether	00:0c:29:d2:19:f0	C		enp2s0f1
192.168.100.195	ether	68:f7:28:81:40:a0	C		enp2s0f1
gateway	ether	00:d0:03:ff:94:00	C		wlp3s0

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

Time	Source	Destination	Protocol	Length	Info
78.6763435426	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.165? Tell 192.168.100.254
79.7.079483372	Micro-St_dd:a2:7b	IPv4mcast_7f:ff:fa	0x0800	216	IPv4
80.7.119525493	Compalln_7a:03:0a	Broadcast	ARP	42	Who has 192.168.100.195? Tell 192.168.100.191
81.7.120800211	LcfcHefe_81:40:a0	Compalln_7a:03:0a	ARP	60	192.168.100.195 is at 68:f7:28:81:40:a0
82.7.120823627	Compalln_7a:03:0a	LcfcHefe_81:40:a0	0x0800	98	IPv4
83.7.121354448	LcfcHefe_81:40:a0	Compalln_7a:03:0a	0x0800	98	IPv4
84.7.218779338	Vmware_d2:19:f0	BizlinkK_07:8b:e5	ARP	60	Who has 192.168.100.203? Tell 192.168.100.254
85.7.762994139	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.165? Tell 192.168.100.254
86.7.917493253	AsustekC_29:c7:ce	IPv4mcast_7f:ff:fa	0x0800	178	IPv4
87.8.005739494	Compalln_7a:03:0a	Vmware_d2:19:f0	0x0800	342	IPv4
88.9.010823903	Vmware_d2:19:f0	Compalln_7a:03:0a	0x0800	254	TxD
▶ Frame 80: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0					
▶ Ethernet II, Src: Compalln_7a:03:0a (f0:76:1c:7a:03:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)					
▼ Address Resolution Protocol (request)					
Hardware type: Ethernet (1)					
Protocol type: IPv4 (0x0800)					
Hardware size: 6					
Protocol size: 4					
Opcode: request (1)					
Sender MAC address: Compalln_7a:03:0a (f0:76:1c:7a:03:0a)					
Sender IP address: 192.168.100.191					
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)					
Target IP address: 192.168.100.195					

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

75	6.427106175	BizlinkK_07:8b:e5	IPv4mcast_fb	0x0800	291	IPv4
76	6.465003391	Cisco_4b:19:05	CDP/VTP/DTP/PAGP/UDL	CDP	416	Device ID: Bastidor0_SW3 Port ID: FastEthernet0/5
77	6.620947662	RealtekS_64:b8:08	IPv6mcast_16	0x86dd	90	IPv6
78	6.763435426	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.165? Tell 192.168.100.254
79	7.079403372	Micro-St_dd:a2:7b	IPv4mcast_7f:ff:fa	0x0800	216	IPv4
80	7.116552103	CompalIn_7a:03:0a	Broadcast	ARP	42	Who has 192.168.100.195? Tell 192.168.100.191
81	7.120008211	LcfcHefe_81:40:a0	CompalIn_7a:03:0a	ARP	60	192.168.100.195 is at 08:00:27:00:00:00
82	7.120823627	CompalIn_7a:03:0a	LcfcHefe_81:40:a0	0x0800	98	IPv4
83	7.121354448	LcfcHefe_81:40:a0	CompalIn_7a:03:0a	0x0800	98	IPv4
84	7.218779338	Vmware_d2:19:f0	BizlinkK_07:8b:e5	ARP	60	Who has 192.168.100.203? Tell 192.168.100.254
85	7.762994139	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.165? Tell 192.168.100.254
86	7.907492203	AsustekC_20:07:ce	IPv4mcast_7f:ff:fa	0x0800	179	IPv4
87	8.005730494	CompalIn_7a:03:0a	Vmware_d2:19:f0	0x0800	342	IPv4
88	8.016587882	Vmware_d2:19:f0	CompalIn_7a:03:0a	0x0800	351	IPv4
▶ Frame 80: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
▼ Ethernet II, Src: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)						
▶ Source: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a)						
▶ Type: ARP (0x0806)						
▶ Address Resolution Protocol (request)						

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

70 7.013403372	Micro_S1_01:a2:7b	IPv4broadcast_7f:ff:fa	0x0800	215 IPv4	
80 7.119852493	CompalIn_7a:03:0a	Broadcast	ARP	42 Who has 192.168.100.195? Tell 192.168.100.191	
81 7.120808211	LcfChefe_81:40:a0	CompalIn_7a:03:0a	ARP	60 192.168.100.195 is at 68:f7:28:81:40:a0	
82 7.120823627	CompalIn_7a:03:0a	LcfChefe_81:40:a0	0x0800	98 IPv4	
83 7.121354448	LcfChefe_81:40:a0	CompalIn_7a:03:0a	0x0800	98 IPv4	
84 7.218779338	Vmware_d2:19:f0	BizlinkK_07:0b:e5	ARP	60 Who has 192.168.100.203? Tell 192.168.100.254	
85 7.762994139	Vmware_d2:19:f0	Broadcast	ARP	60 Who has 192.168.100.165? Tell 192.168.100.254	
86 7.917493253	AsustekC_29:c7:c8	IPv4broadcast_7f:ff:fa	0x0800	179 IPv4	
87 8.005739494	CompalIn_7a:03:0a	Vmware_d2:19:f0	0x0800	342 IPv4	
88 8.010607982	Vmware_d2:19:f0	CompalIn_7a:03:0a	0x0800	361 IPv4	
▶ Frame 80: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0 ▶ Ethernet II, Src: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff) ▼ Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (1)					
Sender MAC address: CompalIn_7a:03:0a (f0:76:1c:7a:03:0a) Sender IP address: 192.168.100.191 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.100.195					

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

Explicita 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.

- Qual o valor do campo ARP opcode? O que especifica?
- Em que posição da mensagem ARP está a resposta ao pedido ARP?

Resposta

75	6.427196175	BizlinkK 07:8b:e5	IPv4mcast fb	0x0800	291	IPv4
76	6.465003391	Cisco_4b:19:05	CDP/VTP/DTP/PagP/UD...	CDP	416	Device ID: Bastidor0_SW3 Port ID: FastEthernet0/5
77	6.629947682	RealtekS 84:b8:08	IPv6mcast 16	0x86dd	99	IPv6
78	6.763435426	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.165? Tell 192.168.100.254
79	7.079403772	Micro-S 8d:a2:7d	IPv6mcast ff:ff:fa	0x8000	216	IPv4
80	7.11952493	Compalln_7a:03:0a	Broadcast	ARP	42	Who has 192.168.100.195? Tell 192.168.100.191
81	7.120808211	LcfcHefe 81:40:a0	Compalln_7a:03:0a	ARP	60	192.168.100.195 is at 68:f7:28:81:40:a0
82	7.120823627	Compalln_7a:03:0a	LcfcHefe 81:40:a0	0x0800	98	IPv4
83	7.121354448	LcfcHefe 81:40:a0	Compalln_7a:03:0a	0x0800	98	IPv4
84	7.218779338	Vmware_d2:19:f0	BizlinkK 07:8b:e5	ARP	60	Who has 192.168.100.203? Tell 192.168.100.254
85	7.762994139	Vmware_d2:19:f0	Broadcast	ARP	60	Who has 192.168.100.165? Tell 192.168.100.254
86	7.917493253	AsustekC_29:c7:ce	IPv4mcast 7f:ff:fa	0x0800	179	IPv4
87	8.005739494	Compalln_7a:03:0a	Vmware_d2:19:f0	0x0800	342	IPv4
88	8.010087981	Vmware_d2:19:f0	Compalln_7a:03:0a	0x0800	261	IPv4
▶ Frame 81: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0						
▶ Ethernet II, Src: LcfcHefe 81:40:a0 (68:f7:28:81:40:a0), Dst: Compalln_7a:03:0a (f0:76:1c:7a:03:0a)						
▼ Address Resolution Protocol (reply)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: reply (2)						
Sender MAC address: LcfcHefe 81:40:a0 (68:f7:28:81:40:a0)						
Sender IP address: 192.168.100.195						
Target MAC address: Compalln_7a:03:0a (f0:76:1c:7a:03:0a)						
Target IP address: 192.168.100.191						

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

24	5.457863709	BizlinkK 07:8b:e5	IPv6mcast fb	0x86dd	129	IPv6
25	6.020480717	Cisco_4b:19:05	Spanning-tree (for-...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 3004 Port = 0
26	6.010555499	Cisco_4b:19:05	Spanning-tree (for-...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 3004 Port = 0
27	9.17299538	Cisco_4b:19:05	Cisco_4b:19:05	LOOP	60	Reply
28	9.027245596	BizlinkK 07:8b:e5	IPv4mcast fb	0x0800	228	IPv4
29	10.020632358	Cisco_4b:19:05	Spanning-tree (for-...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 3004 Port = 0
30	10.202040593	LcfcHefe 83:bc:1a	IPv4mcast fb	0x0800	160	IPv4
31	10.483080792	Compalln_7a:03:0a	Broadcast	ARP	42	Gratuitous ARP for 192.168.100.191 (Request)
32	11.483095324	Compalln_7a:03:0a	Broadcast	ARP	42	Gratuitous ARP for 192.168.100.191 (Request)
33	11.616329150	Cisco_4b:19:05	CDP/VTP/DTP/PagP/UD...	CDP	416	Device ID: Bastidor0_SW3 Port ID: FastEthernet0/5
34	12.020985129	Cisco_4b:19:05	Spanning-tree (for-...	STP	60	Conf. Root = 4096/720/00:0a:8a:97:74:80 Cost = 3004 Port = 0
35	12.483112630	Compalln_7a:03:0a	Broadcast	ARP	42	Gratuitous ARP for 192.168.100.191 (Request)
36	12.483095324	Compalln_7a:03:0a	Broadcast	ARP	42	Gratuitous ARP for 192.168.100.191 (Request)
▶ Frame 32: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
▶ Ethernet II, Src: Compalln_7a:03:0a (f0:76:1c:7a:03:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
▼ 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: Compalln_7a:03:0a (f0:76:1c:7a:03:0a)						
Sender IP address: 192.168.100.191						
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)						
Target IP address: 192.168.100.191						

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

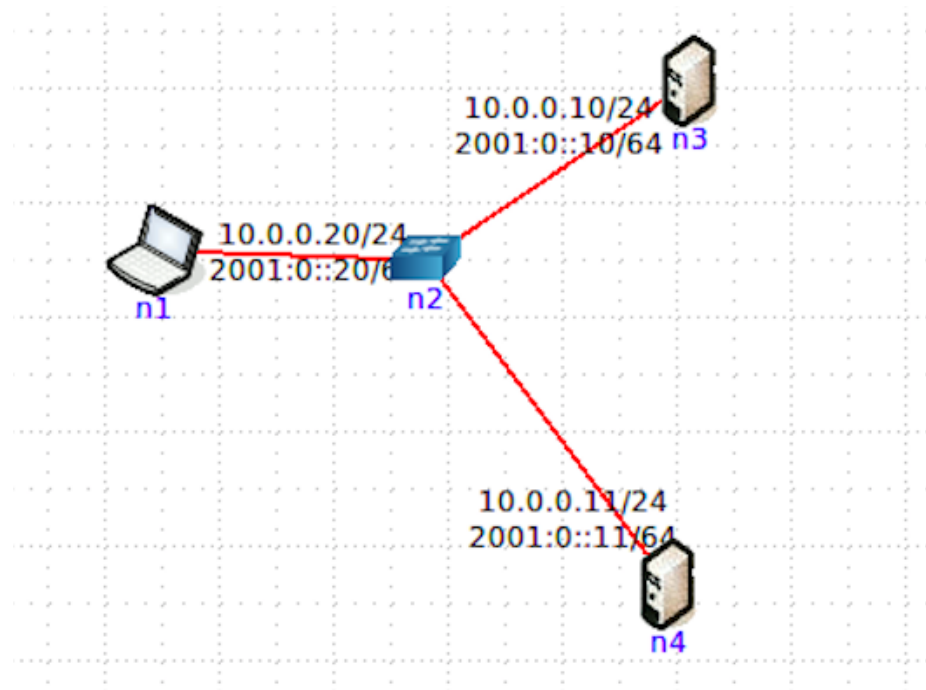


Fig. 9.

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

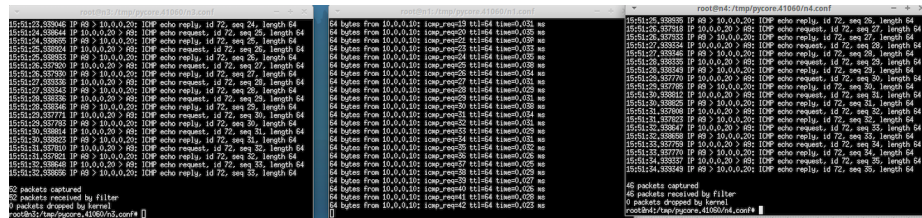


Fig. 10.

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

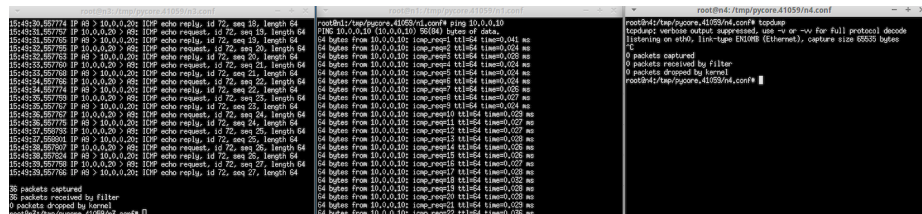


Fig. 11.

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.