

Atividade Pratica: Analise de Protocolo com Wireshark

-Bernardo Rizzone (232013194)

PARTE 3:

Meu computador:

```
      Sufixo DNS específico de conexão.
      :

      Descrição.
      :
      :
      Realtek PCIe GbE Family Controller #2

      Endereço Físico.
      :
      9C-6B-00-10-E8-47

      DHCP Habilitado.
      :
      Sim

      Configuração Automática Habilitada.
      :
      Sim

      Endereço IPv6.
      :
      2804:14c:6584:4d58::1000(Preferencial)

      Concessão Obtida.
      :
      :
      terça-feira, 2 de setembro de 2025 16:45:34

      Concessão Expira.
      :
      :
      quarta-feira, 3 de setembro de 2025 15:28:35

      Endereço IPv6.
      :
      2804:14c:6584:4d58:383d:cab5:d324:bd0b(Preferencial)

      Endereço IPv6 Temporário.
      :
      2804:14c:6584:4d58:78bb:d824:e11b:98f3(Preferencial)

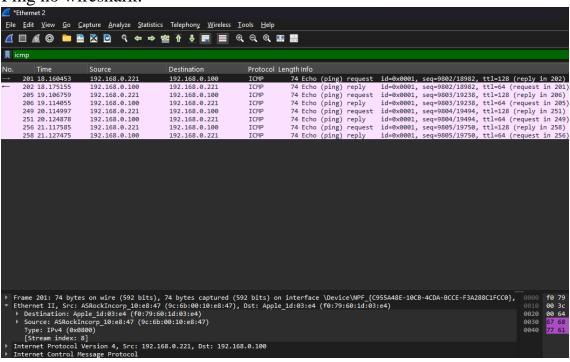
      Endereço IPv6 de link local
      :
      fe80::37db:7233:48fb:17aa%18(Preferencial)

      Endereço IPv4.
      :
      192.168.0.221(Preferencial)
```

Computador Analisado:

```
options=400<CHANNEL_10>
ether f0:79:60:1d:03:e4
inet6 fe80::1c7b:41ee:bb79:8631%en0 prefixlen 64 secured scopeid 0x4
inet6 2804:14c:6584:4d58:18bc:44fe:f51c:c23f prefixlen 64 autoconf secured
inet6 2804:14c:6584:4d58:ad00:ca60:14f2:2be9 prefixlen 64 autoconf temporary
inet6 2804:14c:6584:4d58::1000 prefixlen 64 dynamic
inet 192.168.0.100 netmask 0xffffff00 broadcast 192.168.0.255
```

Ping no wireshark:

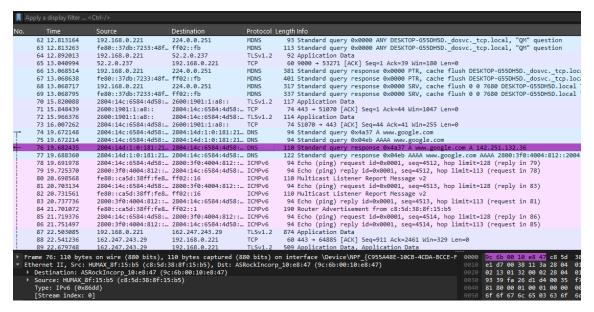


Ambos os endereços MAC correspondem aos devidos computadores.

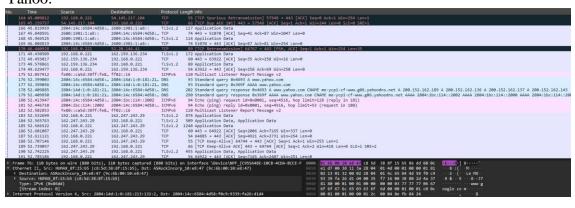
PARTE 3:

Local	Endereço de IP de Destino	Endereço Mac de Destino		
Yahoo	200.152.162.189	c8:5d:38:8f:15:b5		
Cisco		c8:5d:38:8f:15:b5		
Google	142.251.132.36	c8:5d:38:8f:15:b5		

Imagens de analise: Google



Yahoo:



Cisco:

No.		Source		Protocol Ler	
	236 62.761955	192.168.0.221	162.247.243.29	TCP	54 64922 → 443 [FIN, ACK] Seq=8359 Ack=2803 Win=255 Len=0
3	237 62.762577	162.247.243.29		TLSv1.2	78 Application Data
			162.247.243.29	TCP	54 64922 + 443 [RST, ACK] Seq=8360 Ack=2827 Win=0 Len=0
		162.247.243.29	192.168.0.221	TCP	60 443 → 64922 [ACK] Seq=2828 Ack=8360 Win=342 Len=0
		192.168.0.221	52.2.0.237	TLSv1.2	92 Application Data
		52.2.0.237	192.168.0.221	TCP	60 9000 + 53271 [ACK] Seq=77 Ack=115 Win=180 Len=0
			2804:14d:1:0:181:21		93 Standard query 8xd276 A www.cisco.com
			2804:14d:1:0:181:21		93 Standard query 0x453b AAAA www.cisco.com
			2804:14c:6584:4d58:		315 Standard query response 0x453b AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.com.edgekey.net.globalredir.
_	245 63.111557		2804:14c:6584:4d58:		275 Standard query response 0xd276 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME wwwds.cisco.com.edgekey.net classes
	246 63.115441		2600:1419:3600:1b4:		94 Echo (ping) request id=0x0001, seq=4520, hop limit=128 (reply in 247)
	247 63.146900		2804:14c:6584:4d58:		94 Echo (ping) reply id=0x0001, seq=4520, hop limit=55 (request in 246)
	248 64.132454		2600:1419:3600:1b4:		94 Echo (ping) request id=0x0001, seq=4521, hop limit=128 (reply in 249)
	249 64.173661		2804:14c:6584:4d58:		94 Echo (ping) reply id=0x0001, seq=4521, hop limit=55 (request in 248)
	250 65.136657		2600:1419:3600:1b4:		94 Echo (ping) request id-0x0001, seq-4522, hop limit-128 (reply in 251)
	251 65.147833		2804:14c:6584:4d58:		94 Echo (ping) reply id=0x0001, seq=4522, hop limit=55 (request in 250)
	252 66.143158		2600:1419:3600:1b4:		94 Echo (ping) request id=0x0001, seq=4523, hop limit=128 (reply in 253)
			2804:14c:6584:4d58:		94 Echo (ping) reply id=0x0001, seq=4523, hop limit=55 (request in 252)
		192.168.0.221	52.20.144.41	TLSv1.2	89 Application Data
		192.168.0.221	52.20.144.41		89 [TCP Retransmission] 64788 + 443 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=35
					89 [TCP Retransmission] 64788 + 443 [PSH, ACK] Seq-1 Ack-1 Win-254 Len-35
				TCP	89 [TCP Retransmission] 64788 + 443 [PSM, ACK] Seq=1 Ack=1 Win=254 Len=35
		HUMAX_8f:15:b5	ASRockIncorp_10:e8:		60 Who has 192.168.0.221? Tell 192.168.0.1
_		ASRockIncorp_10:e8:		ARP	42 192.168.0.221 is at 9c:6b:00:10:e8:47
		192.168.0.221	52.20.144.41	TCP	89 [TCP Retransmission] 64788 → 443 [PSM, ACK] Seq-1 Ack-1 Win-254 Len-35
		192.168.0.221	52.86.188.173		93 Application Data
		52.86.188.173			93 Application Data
					54 51231 + 443 [ACK] Seg=118 Ack=118 Win=255 Len=0
					interface \Device\NPF_[C955A48E-10CB-4CDA-BCCE-F 0000 9c 6b 00 10 e8 47 c8 5d 38 8f 15 b5 86 dd 60 0c -k····C-] 8·····
				tockIncorp_	00:00 e1 d7 00 38 11 3a 28 04 01 4d 00 01 00 00 01 818.:(M
		ockIncorp_10:e8:47 (90			0020 02 13 01 32 00 02 28 04 01 4c 65 84 4d 58 f0 c9 ···2··(··Le·MX··
> Source: HUMAX_8f:15:b5 (c8:5d:38:8f:15:b5)					
	Type: IPv6 (0x86d				0040 81 80 00 01 00 01 00 00 00 00 03 77 77 77 06 67 · · · · · · · · · · · · · · · · · ·
	[Stream index: 0]				0050 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c oogle co m · · · · ·

Ping do cisco no DNS não apareceu o ipv4 nem o ipv6.

Questões dissertativas:

1. Na Parte 2, como o seu computador descobriu o endereço MAC do outro computador?

R: Meu computador descobriu o endereço MAC do outro computador usando o Protocolo ARP. Ao tentar enviar o ping, ele primeiro enviou uma mensagem ARP em broadcast para toda a rede loca, perguntando: "Quem tem este endereço IP?". O outro computador respondeu diretamente com seu endereço MAC. Após receber essa resposta, meu computador armazenou essa informação e utilizou o endereço MAC recebido para enviar os pacotes de ping.

2. Na parte 3, os endereços MAC de destino que você anotou pertencem aso servidores da Cisco, Google, e Yahoo? Se não, a qual dispositivo eles pertencem? Qual a importância dessa informação?

R: Não, esse endereço MAC não pertence aos servidores do google, yahoo e cisco. Ele pertence ao meu roteador, que atua como o gateway padrão da rede local para a internet. A importância dessa informação demonstra a diferença entre o endereçamento local e o endereçamento global. O endereço MAC e usado para a entrega local, ou seja, para encontrar o próximo dispositivo no caminho dentro da sua propia rede. No caso, para sair para a internet, o roteador e usando como "Ponte".

3. Comparando os resultados da parte 2 e da parte 3, explique por que o wireshark exibe o endereço MAC real do host de destino para pings locais, mas não para pings remotos.

R: Para os pings locais (Parte 2), o computador de destino está na mesma rede que o meu. Isso significa que eles podem se comunicar diretamente. Meu computador utiliza o protocolo ARP para obter o endereço MAC específico do host de destino e, em seguida, cria um quadro Ethernet endereçado diretamente do meu MAC para o MAC do

outro computador. Para os pings remotos (Parte 3), o host de destino (como o Google) está em uma rede externa. O endereço MAC só tem validade dentro da nossa rede local e não pode ser usado para roteamento na internet. Meu computador, ao perceber que o IP de destino é externo, envia o pacote para o seu gateway padrão, que é o nosso roteador.