



Atividade Prática: Análise 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 0xffffffff00 broadcast 192.168.0.255
```

Ping no wireshark:

The image shows a Wireshark capture of ICMP ping traffic. The packet list pane displays several ping requests and replies. The packet details pane shows the structure of an ICMP Echo (ping) request, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol header.

No.	Time	Source	Destination	Protocol	Length	Info
201	18.160453	192.168.0.221	192.168.0.100	ICMP	74	Echo (ping) request id=0x0001, seq=9802/18982, ttl=128 (reply in 202)
202	18.175155	192.168.0.100	192.168.0.221	ICMP	74	Echo (ping) reply id=0x0001, seq=9802/18982, ttl=64 (request in 201)
205	19.106759	192.168.0.221	192.168.0.100	ICMP	74	Echo (ping) request id=0x0001, seq=9803/19238, ttl=128 (reply in 206)
206	19.114055	192.168.0.100	192.168.0.221	ICMP	74	Echo (ping) reply id=0x0001, seq=9803/19238, ttl=64 (request in 205)
249	20.114997	192.168.0.221	192.168.0.100	ICMP	74	Echo (ping) request id=0x0001, seq=9804/19494, ttl=128 (reply in 251)
251	20.124878	192.168.0.100	192.168.0.221	ICMP	74	Echo (ping) reply id=0x0001, seq=9804/19494, ttl=64 (request in 249)
256	21.117585	192.168.0.221	192.168.0.100	ICMP	74	Echo (ping) request id=0x0001, seq=9805/19750, ttl=128 (reply in 258)
258	21.127475	192.168.0.100	192.168.0.221	ICMP	74	Echo (ping) reply id=0x0001, seq=9805/19750, ttl=64 (request in 256)

Frame 201: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C955A48E-10CB-4CDA-BCCE-F3A288C1FCC0}, Ethernet II, Src: ASRockIncorp_10:e8:47 (9c:6b:00:10:e8:47), Dst: Apple_1d:03:e4 (f0:79:60:1d:03:e4)
Destination: Apple_1d:03:e4 (f0:79:60:1d:03:e4)
Source: ASRockIncorp_10:e8:47 (9c:6b:00:10:e8:47)
Type: IPv4 (0x0800)
[Stream index: 8]
Internet Protocol Version 4, Src: 192.168.0.221, Dst: 192.168.0.100
Internet Control Message Protocol

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

Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
62	12.813164	192.168.0.221	224.0.0.251	MDNS	93 Standard query 0x0000 ANY DESKTOP-G55DHS5D._dosvc._tcp.local, "QM" question
63	12.813263	fe80::37db:7233:48f...	ff02::fb	MDNS	113 Standard query 0x0000 ANY DESKTOP-G55DHS5D._dosvc._tcp.local, "QM" question
64	12.892013	192.168.0.221	52.2.0.237	TLSv1.2	92 Application Data
65	13.040994	52.2.0.237	192.168.0.221	TCP	60 9000 → 53271 [ACK] Seq=1 Ack=39 Win=180 Len=0
66	13.068514	192.168.0.221	224.0.0.251	MDNS	381 Standard query response 0x0000 PTR, cache flush DESKTOP-G55DHS5D._dosvc._tcp.local
67	13.068638	fe80::37db:7233:48f...	ff02::fb	MDNS	401 Standard query response 0x0000 PTR, cache flush DESKTOP-G55DHS5D._dosvc._tcp.local
68	13.068717	192.168.0.221	224.0.0.251	MDNS	317 Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-G55DHS5D.local
69	13.068795	fe80::37db:7233:48f...	ff02::fb	MDNS	337 Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-G55DHS5D.local
70	15.020088	2804:14c:6584:4d58::	2600:1901:1:a8::	TLSv1.2	117 Application Data
71	15.048439	2600:1901:1:a8::	2804:14c:6584:4d58::	TCP	74 443 → 51070 [ACK] Seq=1 Ack=44 Win=1047 Len=0
72	15.066376	2600:1901:1:a8::	2804:14c:6584:4d58::	TLSv1.2	114 Application Data
73	16.007262	2804:14c:6584:4d58::	2600:1901:1:a8::	TCP	74 51070 → 443 [ACK] Seq=44 Ack=41 Win=255 Len=0
74	19.672148	2804:14c:6584:4d58::	2804:14d:1:0:181:21::	DNS	94 Standard query 0x4a37 A www.google.com
75	19.672214	2804:14c:6584:4d58::	2804:14d:1:0:181:21::	DNS	94 Standard query 0x04eb AAAA www.google.com
76	19.682435	2804:14d:1:0:181:21::	2804:14c:6584:4d58::	DNS	110 Standard query response 0x4a37 A www.google.com A 142.251.132.36
77	19.688360	2804:14d:1:0:181:21::	2804:14c:6584:4d58::	DNS	122 Standard query response 0x04eb AAAA www.google.com AAAA 2800:3f0:4004:812::2004
78	19.691978	2804:14c:6584:4d58::	2800:3f0:4004:812::	ICMPv6	94 Echo (ping) request id=0x0001, seq=4512, hop limit=128 (reply in 79)
79	19.725370	2800:3f0:4004:812::	2804:14c:6584:4d58::	ICMPv6	94 Echo (ping) reply id=0x0001, seq=4512, hop limit=113 (request in 78)
80	20.698568	fe80::ca5d:38ff:fe8...	ff02::16	ICMPv6	110 Multicast Listener Report Message v2
81	20.703134	2804:14c:6584:4d58::	2800:3f0:4004:812::	ICMPv6	94 Echo (ping) request id=0x0001, seq=4513, hop limit=128 (reply in 83)
82	20.731561	fe80::ca5d:38ff:fe8...	ff02::16	ICMPv6	110 Multicast Listener Report Message v2
83	20.737736	2800:3f0:4004:812::	2804:14c:6584:4d58::	ICMPv6	94 Echo (ping) reply id=0x0001, seq=4513, hop limit=113 (request in 81)
84	21.701072	fe80::ca5d:38ff:fe8...	ff02::1	ICMPv6	190 Router Advertisement from c8:5d:38:8f:15:b5
85	21.719376	2804:14c:6584:4d58::	2800:3f0:4004:812::	ICMPv6	94 Echo (ping) request id=0x0001, seq=4514, hop limit=128 (reply in 86)
86	21.751497	2800:3f0:4004:812::	2804:14c:6584:4d58::	ICMPv6	94 Echo (ping) reply id=0x0001, seq=4514, hop limit=113 (request in 85)
87	22.503085	192.168.0.221	162.247.243.29	TLSv1.2	874 Application Data
88	22.541236	162.247.243.29	192.168.0.221	TCP	60 443 → 64805 [ACK] Seq=911 Ack=2461 Win=329 Len=0
89	22.679748	162.247.243.29	192.168.0.221	TLSv1.2	509 Application Data, Application Data
▶ Frame 76: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{C955A48E-10CB-4CDA-BCCE-F...}					
▶ Ethernet II, Src: HUMAN_8f:15:b5 (c8:5d:38:8f:15:b5), Dst: ASRockIncorp_10:e8:47 (9c:6b:00:10:e8:47)					
▶ Destination: ASRockIncorp_10:e8:47 (9c:6b:00:10:e8:47)					
▶ Source: HUMAN_8f:15:b5 (c8:5d:38:8f:15:b5)					
Type: IPv6 (0x86dd)					
[Stream index: 0]					

Yahoo:

No.	Time	Source	Destination	Protocol	Length Info
164	45.000812	192.168.0.221	54.145.217.104	TCP	55 [TCP Spurious Retransmission] 57549 → 443 [ACK] Seq=0 Ack=1 Win=254 Len=0
165	45.155757	54.145.217.104	192.168.0.221	TCP	66 [TCP Dup ACK 181] 443 → 57549 [ACK] Seq=1 Ack=1 Win=254 Len=0 SILENCE
166	45.819959	2804:14c:6584:4d58::	2600:1901:1:a8::	TLSv1.2	117 Application Data
167	45.840391	2600:1901:1:a8::	2804:14c:6584:4d58::	TCP	74 443 → 51070 [ACK] Seq=41 Ack=87 Win=1047 Len=0
168	45.966525	2600:1901:1:a8::	2804:14c:6584:4d58::	TLSv1.2	114 Application Data
169	46.000328	2804:14c:6584:4d58::	2600:1901:1:a8::	TCP	74 51070 → 443 [ACK] Seq=87 Ack=87 Win=254 Len=0
170	46.000328	192.168.0.221	52.2.0.237	TCP	89 [TCP Retransmission] 64767 → 443 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=35
171	49.430509	192.168.0.221	162.159.136.234	TLSv1.2	172 Application Data
172	49.455017	162.159.136.234	192.168.0.221	TCP	60 443 → 63922 [ACK] Seq=35 Ack=258 Win=16 Len=0
173	49.578861	162.159.136.234	192.168.0.221	TLSv1.2	88 Application Data
174	49.629477	192.168.0.221	162.159.136.234	TCP	54 63922 → 443 [ACK] Seq=258 Ack=69 Win=250 Len=0
175	52.057012	fe80::ca5d:38ff:fe8...	ff02::16	ICMPv6	110 Multicast Listener Report Message v2
176	52.399083	2804:14c:6584:4d58::	2804:14d:1:0:181:21::	DNS	93 Standard query 0x4693 A www.yahoo.com
177	52.399056	2804:14c:6584:4d58::	2804:14d:1:0:181:21::	DNS	93 Standard query 0x369f AAAA www.yahoo.com
178	52.400085	2804:14d:1:0:181:21::	2804:14c:6584:4d58::	DNS	202 Standard query response 0x4693 A www.yahoo.com CNAME me-yepi-cf-www.g06.yahooads.net A 200.152.162.189 A 200.152.162.136 A 200.152.162.137 A 200.152.162.143
179	52.400950	2804:14d:1:0:181:21::	2804:14c:6584:4d58::	DNS	250 Standard query response 0x369f AAAA www.yahoo.com CNAME me-yepi-cf-www.g06.yahooads.net AAAA 2804:1bc:114:2002 AAAA 2804:1bc:114:2000 AAAA 2804:1bc:114:2001
180	52.413947	2804:14c:6584:4d58::	2804:1bc:114:2002	ICMPv6	94 Echo (ping) request id=0x0001, seq=4516, hop limit=128 (reply in 181)
181	52.446718	2804:1bc:114:2002	2804:14c:6584:4d58::	ICMPv6	94 Echo (ping) reply id=0x0001, seq=4516, hop limit=53 (request in 180)
182	52.502853	fe80::ca5d:38ff:fe8...	ff02::16	ICMPv6	110 Multicast Listener Report Message v2
183	52.552099	192.168.0.221	162.247.243.29	TLSv1.2	674 Application Data
184	52.565763	162.247.243.29	192.168.0.221	TLSv1.2	509 Application Data, Application Data
185	52.566522	192.168.0.221	162.247.243.29	TLSv1.2	1248 Application Data
186	52.580107	162.247.243.29	192.168.0.221	TCP	60 443 → 64922 [ACK] Seq=2806 Ack=7165 Win=237 Len=0
187	52.611121	192.168.0.221	162.247.243.29	TCP	54 64885 → 443 [ACK] Seq=4921 Ack=2731 Win=254 Len=0
188	52.707146	192.168.0.221	162.247.243.29	TCP	35 [TCP Keep-Alive] 64744 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=0
189	52.739057	162.247.243.29	192.168.0.221	TCP	66 [TCP Keep-Alive ACK] 443 → 64744 [ACK] Seq=1 Ack=2 Win=418 Len=0 SILENCE
190	52.742225	162.247.243.29	192.168.0.221	TLSv1.2	455 Application Data, Application Data
191	52.762516	192.168.0.221	162.247.243.29	TCP	65 64922 → 443 [ACK] Seq=2165 Ack=2617 Win=255 Len=0
▶ Frame 76: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{C955A48E-10CB-4CDA-BCCE-F...}					
▶ Ethernet II, Src: HUMAN_8f:15:b5 (c8:5d:38:8f:15:b5), Dst: ASRockIncorp_10:e8:47 (9c:6b:00:10:e8:47)					
▶ Destination: ASRockIncorp_10:e8:47 (9c:6b:00:10:e8:47)					
▶ Source: HUMAN_8f:15:b5 (c8:5d:38:8f:15:b5)					
Type: IPv6 (0x86dd)					
[Stream index: 0]					
▶ Internet Protocol Version 6, Src: 2804:14d:1:0:181:21::132:2, Dst: 2804:14c:6584:4d58::fb:c9:9339:fa26:d1d4					

Cisco:

No.	Time	Source	Destination	Protocol	Length	Info
236	62.761955	192.168.0.221	192.247.243.29	TCP	54	64922 → 443 [FIN, ACK] Seq=8359 Ack=2803 Win=255 Len=0
237	62.762077	192.247.243.29	192.168.0.221	TLSv1.2	70	Application Data
238	62.762106	192.247.243.29	192.247.243.29	TCP	54	64922 → 443 [ACK] Seq=8360 Ack=2827 Win=0 Len=0
239	62.801052	192.247.243.29	192.168.0.221	TCP	60	443 → 64922 [ACK] Seq=2828 Ack=8360 Win=342 Len=0
240	62.805043	192.168.0.221	52.2.0.237	TLSv1.2	92	Application Data
241	63.856480	52.2.0.237	192.168.0.221	TCP	60	9000 → 53271 [ACK] Seq=77 Ack=115 Win=180 Len=0
242	63.100304	2004:14c:6584:4d58::	2004:14d:110:181:21::	DNS	93	Standard query 0x276 A www.cisco.com
243	63.100369	2004:14c:6584:4d58::	2004:14d:110:181:21::	DNS	93	Standard query 0x276 AAAA www.cisco.com
244	63.111557	2004:14d:110:181:21::	2004:14c:6584:4d58::	DNS	315	Standard query response 0x453b AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwwds.cisco.com.edgekey.net CNAME wwwwds.cisco.com.edgekey.net.globalredir.akadns.net
245	63.111557	2004:14d:110:181:21::	2004:14c:6584:4d58::	DNS	275	Standard query response 0x276 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwwds.cisco.com.edgekey.net CNAME wwwwds.cisco.com.edgekey.net.globalredir.akadns.net
246	63.115441	2004:14c:6584:4d58::	2004:1419:3080:104::	ICMPv6	94	Echo (ping) request id=0x0001, seq=4520, hop limit=128 (reply in 247)
247	63.146900	2004:1419:3080:104::	2004:14c:6584:4d58::	ICMPv6	94	Echo (ping) reply id=0x0001, seq=4520, hop limit=55 (request in 246)
248	64.132454	2004:14c:6584:4d58::	2004:1419:3080:104::	ICMPv6	94	Echo (ping) request id=0x0001, seq=4521, hop limit=128 (reply in 249)
249	64.175651	2004:1419:3080:104::	2004:14c:6584:4d58::	ICMPv6	94	Echo (ping) reply id=0x0001, seq=4521, hop limit=55 (request in 248)
250	65.136657	2004:14c:6584:4d58::	2004:1419:3080:104::	ICMPv6	94	Echo (ping) request id=0x0001, seq=4522, hop limit=128 (reply in 251)
251	65.147833	2004:1419:3080:104::	2004:14c:6584:4d58::	ICMPv6	94	Echo (ping) reply id=0x0001, seq=4522, hop limit=55 (request in 250)
252	66.143158	2004:14c:6584:4d58::	2004:1419:3080:104::	ICMPv6	94	Echo (ping) request id=0x0001, seq=4523, hop limit=128 (reply in 253)
253	66.154585	2004:1419:3080:104::	2004:14c:6584:4d58::	ICMPv6	94	Echo (ping) reply id=0x0001, seq=4523, hop limit=55 (request in 252)
254	66.316793	192.168.0.221	52.20.144.41	TLSv1.2	89	Application Data
255	66.816900	192.168.0.221	52.20.144.41	TCP	89	[TCP Retransmission] 64788 → 443 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=35
256	67.138993	192.168.0.221	52.20.144.41	TCP	89	[TCP Retransmission] 64788 → 443 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=35
257	67.793186	192.168.0.221	52.20.144.41	TCP	89	[TCP Retransmission] 64788 → 443 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=35
258	67.838663	MPMAX_8f151b5	ASRockIncorp_10:e8::	ARP	60	Who has 192.168.0.221? Tell 192.168.0.1
259	67.838688	ASRockIncorp_10:e8::	MPMAX_8f151b5	ARP	42	192.168.0.221 is at 8c:00:00:10:e8:47
260	67.838688	192.168.0.221	52.20.144.41	TCP	58	[TCP Retransmission] 64788 → 443 [PSH, ACK] Seq=1 Ack=1 Win=254 Len=35
261	68.993580	192.168.0.221	52.86.188.173	TLSv1.2	93	Application Data
262	69.142189	52.86.188.173	192.168.0.221	TLSv1.2	93	Application Data
263	69.185265	192.168.0.221	52.86.188.173	TCP	54	51531 → 443 [ACK] Seq=118 Ack=118 Win=255 Len=0
Frame 76: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF{C955448E-10CB-ACDA-BCEE-P} eth0						
Ethernet II, Src: MPMAX_8f151b5 (d:5d:30:8f:15:b5), Dest: ASRockIncorp_10:e8:47 (9c:00:00:10:e8:47)						
Destination: ASRockIncorp_10:e8:47 (9c:00:00:10:e8:47)						
Source: MPMAX_8f151b5 (d:5d:30:8f:15:b5)						
Type: IPv4 (0x0800)						
[Stream index 0]						

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 local, 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 aos 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 é usado para a entrega local, ou seja, para encontrar o próximo dispositivo no caminho dentro da sua própria rede. No caso, para sair para a internet, o roteador é usado 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.