

Universidade Federal de Uberlândia – UFU

Bacharelado em Sistemas de Informação - Campus Monte Carmelo

GS1524 - Redes de computadores - 2021/1

RENAN JUSTINO REZENDE SILVA - 11921BSI223

Atividade 10 NAT

• O objetivo desta atividade é entender melhor o NAT. Leia o texto e execute os passos que estão no arquivo (Wireshark_NAT.pdf). Durante os passos no arquivo, serão indicados itens para serem respondidos. As perguntas a seguir referem-se à atividade no arquivo (Wireshark_NAT.pdf). Os arquivos necessários para a execução dessa atividade estão dentro de arqs10.zip.

1. Qual é o endereço IP do cliente?

Time	Source	Destination	Protocol	Length	Info
0.000000	192.168.1.100	10.119.240.64	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
1.124897	192.168.1.100	68.87.71.230	DNS	91	Standard query 0xa9a9 A safebrowsing.clients.google.com
1.138265	68.87.71.230	192.168.1.100	DNS	211	Standard query response 0xa9a9 A safebrowsing.clients.google.com CNAME clients.1.google.c
4.140302	192.168.1.100	74.125.91.113	TCP	66	4330 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
5.1207818	74.125.91.113	192.168.1.100	TCP	66	80 → 4330 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
6.1207873	192.168.1.100	74.125.91.113	TCP	54	4330 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
7.1208040	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/downloads?client=navclient-auto-ffox&appver=3.0.14&pver=2.2&wkey=AKEg
8.1259370	Cisco-Li_45:1f:1b	HonHaiPr_0d:ca:8f	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
9.1259387	HonHaiPr_0d:ca:8f	Cisco-Li_45:1f:1b	ARP	42	192.168.1.100 is at 00:22:68:0d:ca:8f
10.1269675	74.125.91.113	192.168.1.100	TCP	60	80 → 4330 [ACK] Seq=1 Ack=982 Win=7744 Len=0
11.1274062	74.125.91.113	192.168.1.100	HTTP	853	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-update)
12.1474508	192.168.1.100	74.125.91.113	TCP	54	4330 → 80 [ACK] Seq=982 Ack=800 Win=259376 Len=0
13.1528648	74.125.91.113	192.168.1.100	TCP	853	[TCP Spurious Retransmission] 80 → 4330 [PSH, ACK] Seq=1 Ack=982 Win=7744 Len=799
14.1528673	192.168.1.100	74.125.91.113	TCP	54	[TCP Dup ACK 12#1] 4330 → 80 [ACK] Seq=982 Ack=800 Win=259376 Len=0
15.1529354	192.168.1.100	68.87.71.230	DNS	89	Standard query 0x1773 A safebrowsing-cache.google.com
16.1549501	68.87.71.230	192.168.1.100	DNS	140	Standard query response 0x1773 A safebrowsing-cache.google.com CNAME safebrowsing.cache.l
17.1550220	192.168.1.100	74.125.106.31	TCP	66	4331 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
18.1572197	74.125.106.31	192.168.1.100	TCP	66	80 → 4331 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=64

1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
eth II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:68:45:1f:1b)
eth Protocol Version 4, Src: 192.168.1.100, Dst: 10.119.240.64
IP ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 106
Identification: 0xa262 (41570)
Flags: 0x00
0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0xdb5c [validation disabled]
Header checksum status: Unverified
... Address: 192.168.1.100

Figura 1: IP cliente

R = O endereço IP do cliente é 192.168.1.100

2. O cliente realmente se comunica com vários servidores diferentes do Google para implementar a "navegação segura". O servidor principal do Google que servirá a página principal do Google tem o endereço IP 64.233.169.104. Para exibir apenas os frames contendo mensagens HTTP enviadas de/para este servidor Google, digite a expressão "http && ip.addr == 64.233.169.104" (sem aspas) no campo Filtro: no Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
56	7.189267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhIcdXhW4o4MUAiLCswDjgHLCswfjgQLCswfzgDLCSwGdELCswGTgJLCswHTgZLCswJTj3iA
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16alc5.js HTTP/1.1
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=25025sb164_CeJvxxa0M0&r
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)

Figura 2: Expressão pedida

R = Digitada a expressão pedida na questão 2 para filtrar http && ip.addr == 64.233.169.104

3. Considere agora o HTTP GET enviado do cliente para o servidor do Google (cujo endereço IP é o endereço IP 64.233.169.104) no momento 7.109267. Quais são os endereços IP de origem e destino e as portas TCP de origem e destino no datagrama IP que carrega este HTTP GET?

No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMnMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCsw
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edb3c16a1c5.js HTTP/1.1
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,2
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)

> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
Source Port: 4335
Destination Port: 80
[Stream index: 2]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 635]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 4164040421
[Next Sequence Number: 636 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3914283157

Figura 3: HTTP GET no momento 7.10

R = O IP de origem é o 192.168.1.100 e o IP de destino é o 64.233.169.104. A porta TCP de origem é a 4335 e a porta TCP de destino é a 80.

4. A que horas¹ a mensagem HTTP 200 OK correspondente é recebida do servidor do Google? Quais são os endereços IP de origem e destino e as portas TCP de origem e destino no datagrama IP que carrega esta mensagem HTTP 200 OK?

No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMnMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGdG
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edb3c16a1c5.js HTTP/1.1
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)

> Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
Source Port: 80
Destination Port: 4335
[Stream index: 2]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 760]
Sequence Number: 2861 (relative sequence number)
Sequence Number (raw): 3914286017
[Next Sequence Number: 3621 (relative sequence number)]
Acknowledgment Number: 636 (relative ack number)
Acknowledgment number (raw): 4164041056

Figura 4: HTTP GET OK

R = No tempo 7.158797. O IP de origem é o 64.233.169.104 e o IP de destino é o 192.168.1.100. A porta TCP de origem é a 80 e a porta de destino é a 4335.

5. Lembre-se de que antes que um comando GET possa ser enviado a um servidor HTTP, o TCP deve primeiro configurar uma conexão usando o handshake SYN/ACK de três vias. A que horas é enviado o segmento TCP SYN de cliente para servidor que configura a conexão usada pelo GET enviado no tempo 7.109267? Quais são os endereços IP de origem e destino e as portas de origem e destino para o segmento TCP SYN? Quais são os endereços IP de origem e destino e as portas de origem e destino do ACK enviado em resposta ao SYN. A que horas este ACK é recebido no cliente? (Observação: para encontrar esses segmentos, você precisará limpar a expressão de filtro inserida acima no item 2. Se você inserir o filtro "tcp", apenas os segmentos TCP serão exibidos pelo Wireshark).

53	7.075657	192.168.1.100	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
55	7.109053	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
57	7.140728	64.233.169.104	192.168.1.100	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
58	7.158432	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled
59	7.158761	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)

53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
 Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
 Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
 Source Port: 4335
 Destination Port: 80
 Stream index: 2
 Conversation completeness: Incomplete, DATA (15)
 TCP Segment Len: 0
 Sequence Number: 0 (relative sequence number)
 Sequence Number (raw): 4164040420
 Next Sequence Number: 1 (relative sequence number)
 Acknowledgment Number: 0
 Acknowledgment number (raw): 0
 Window Length: 65535 (0)

Figura 5: TCP SYN

54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
55	7.109053	192.168.1.100	64.233.169.104	TCP	54	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
57	7.140728	64.233.169.104	192.168.1.100	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
58	7.158432	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
59	7.158761	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)

54: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
 Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
 100 ... = Version: 4
 ... 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 Total Length: 52
 Identification: 0xf61a (63002)
 Flags: 0x00
 ... 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 50
 Protocol: TCP (6)
 Header Checksum: 0xe62b [validation disabled]
 Header checksum status: Unverified
 Source Address: 64.233.169.104

Figura 6: TCP SYN ACK

R = É enviado no tempo 7.075657. O endereço IP de origem é o 192.168.1.100 e o de destino é o 64.233.169.104. A porta TCP de origem é a 4335 e a de destino 80. O IP de origem do ACK é 64.233.169.104, IP destino do ACK é 192.168.1.100. A porta de origem do ACK é 80 e a porta de destino do ACK é 4335. Este ACK é recebido pelo cliente no tempo 7.108986.

6. No arquivo NAT_ISP_side, encontre a mensagem HTTP GET enviada do cliente para o servidor do Google no horário 7.109267 (onde t=7.109267 é o horário em que foi enviado conforme registrado no arquivo NAT_home_side). A que horas esta mensagem aparece ao arquivo de rastreamento NAT_ISP_side? Quais são os endereços IP de origem e de destino e as portas de origem e destino TCP no

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and zooming. The main display area is divided into three panes: the packet list, packet details, and packet bytes.

The packet list pane shows a list of captured packets. The selected packet is Frame 85, which is an HTTP GET request. The details pane for this packet shows the following information:

- Frame 85:** 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
- Ethernet II, Src:** Dell_4f:36:23 (00:08:74:4f:36:23), **Dst:** Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
- Internet Protocol Version 4, Src:** 71.192.34.104, **Dst:** 64.233.169.104
- Transmission Control Protocol, Src Port:** 4335, **Dst Port:** 80, **Seq:** 1, **Ack:** 1, **Len:** 635
- Hypertext Transfer Protocol**

The packet details pane shows the structure of the HTTP request, including the GET method, the URL, and the User-Agent header.

R = A mensagem apareceu no tempo 6.069168. O IP de origem é o 71.192.34.104 e o IP de destino que transporta a mensagem é o 64.233.169.104. A porta TCP de origem é a 4335 e a de destino 80. O único campo que mudou foi o IP de origem, os outros campos permaneceram iguais.

R = Nenhum campo do HTTP GET foi alterado. Os campos de comprimento do cabeçalho, versão e flags não mudaram, já o campo checksum mudou. O valor de checksum muda pelo fato de que o IP de origem também foi alterado o que altera este valor por estar incluso.

```

103 6.308118 64.233.169.104 64.233.169.104 HTTP 226 HTTP/1.1 200 OK (GIF89a)
106 6.330131 71.192.34.104 64.233.169.104 HTTP 809 GET /extern_js/f/CgJlbhIcdX0rMac4lNUAlCswDjgHLCswFjwqLCSwfZgDLCSwGDgELCSwGtGJLCSwHT
121 6.407366 64.233.169.104 71.192.34.104 HTTP 648 HTTP/1.1 200 OK (text/javascript)
125 6.452270 71.192.34.104 64.233.169.104 HTTP 695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
131 6.496234 64.233.169.104 71.192.34.104 HTTP 870 HTTP/1.1 200 OK (text/html)
135 6.532319 71.192.34.104 71.192.34.104 HTTP 709 GET /generate_204 HTTP/1.1
137 6.590706 74.125.91.113 71.192.34.104 HTTP 179 HTTP/1.1 204 No Content
139 6.612801 71.192.34.104 64.233.169.104 HTTP 712 GET /images/nav_logo0.png HTTP/1.1
144 6.642308 71.192.34.104 64.233.169.104 HTTP 806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=25025sb1G4
149 6.644609 64.233.169.104 71.192.34.104 HTTP 1359 HTTP/1.1 200 OK (PNG)
154 6.669397 71.192.34.104 64.233.169.104 HTTP 670 GET /favicon.ico HTTP/1.1
157 6.696669 64.233.169.104 71.192.34.104 HTTP 269 HTTP/1.1 204 No Content
160 6.722293 64.233.169.104 71.192.34.104 HTTP 1204 HTTP/1.1 200 OK (image/x-icon)

=====
name 103: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
network II, Src: CiscoBf6c:01 (00:0e:d6:b16c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
Transmission Control Protocol, Seq: 4335, Port: 4335, Seq: 12262, Ack: 1301, Len: 172
Reassembled TCP Segments (8813 bytes): #94(255), #95(1430), #96(1430), #97(1236), #100(1430), #101(1430), #102(1430), #103(172)]
Hypertext Transfer Protocol
museview.GIF, Version: GIF89a

```

Figura 8: HTTP OK 200 do NAT ISP SIDE

R = A mensagem HTTP 200 ok foi recebida no tempo 6.308118. O IP de origem desta mensagem é o 64.233.169.104 e o de destino 71.192.34.104. A porta TCP de origem da mensagem é a 80 e a de destino 4335. O campo que é diferente é o IP de destino, os demais campos permaneceram iguais.

9. No arquivo NAT_ISP_side, em que momento o segmento TCP SYN cliente-para-servidor e o segmento TCP ACK servidor-para-cliente correspondente aos segmentos na questão 5 foram capturados? Quais são os endereços IP de origem e destino e as portas de origem e destino para esses dois segmentos? Quais desses campos são iguais e quais são diferentes da sua resposta á pergunta 5?

82	6.035475	71.192.34.104	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
83	6.067775	64.233.169.104	71.192.34.104	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM=1 WS=64
84	6.068754	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
87	6.099637	64.233.169.104	71.192.34.104	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
88	6.117078	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
89	6.117407	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment of a reassembled PDU]
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)
91	6.118515	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
94	6.273849	64.233.169.104	71.192.34.104	TCP	309	80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP segment of a reassembled PDU]

e 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 rnet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
 rnet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
 mission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

Figura 9: TCP SYN E TCP ACK do NAT ISP SIDE

R = Momento em que o TCP SYN foi capturado = 6.035475.

Momento em que o TCP ACK foi capturado = 6.067775.

IP de origem TCP SYN = 71.192.34.104

IP de destino TCP SYN = 64.233.169.104

IP de origem TCP ACK = 64.233.169.104

IP de destino TCP ACK = 71.192.34.104

Porta TCP de origem TCP SYN = 4335

Porta TCP de destino TCP SYN = 80

Porta TCP de origem TCP ACK = 80

Porta TCP de destino TCP ACK = 4335

Para o segmento TCP SYN, o campo de IP de origem mudou e os outros campos são iguais, portas. Para o segmento TCP ACK, o campo de IP de destino mudou e os outros campos são iguais, portas.

10. Baseando-se nas respostas das questões 1 a 8, preencha as entradas da tabela de tradução NAT para conexão HTTP considerada nas questões 1 a 8.

NAT TRANSLATE TABLE

WAN side: IP 71.192.34.104, porta TCP 4335.

LAN side: IP 192.168.1.100, porta TCP 4335.