

- School of Computer Science and Technology, Shandong University
- Lab Report on Computer Networking

Student Number	Name	Class	Lab Title	Period	Date
201900170249	李阳	智能19	NAT v8.0	2h	May 18, 2021

Hardware Environment

- Lenovo Legion Y7000P 2020H(Intel Core i7-10750H, 16GB DDR4)
- Windows 10 Home, Chinese Version

Software Environment

- Wireshark-win64-3.44

Purpose

- Investigate the behavior of the NAT protocol using Wireshark trace files that the lab had captured.

Experimental Records

- Download the zip file and extract the files need for this lab.
- Open the NAT_home_side file, and use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file.
- Focus on the two HTTP messages (GET and 200 OK) and the TCP SYN and ACK segments identified above, and locate these two HTTP messages and two TCP segments in the trace file (NAT_ISP_side) captured on the link between the router and the ISP.
- Open the NAT_ISP_side and answer the questions.

Answer to Questions

1. IP address of the client: 192.168.1.100

No.	Time	Source	Destination	Protocol	Length	Info
7	04:43:01.477175	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/downloads?client=navclient-auto-ffox&

2. Source IP address: 192.168.1.100, Destination IP addresses: 64.233.169.104

TCP source port: 4335, Destination port: 80

Source Address: 192.168.1.100
Destination Address: 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

3. The corresponding 200 OK HTTP message received from the Google server at time 7.158797, the source IP addresses is 64.233.169.104, the destination IP addresses is 192.168.1.100, TCP source port is 80, destination port is 4335.

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.gi
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/CgJlbhICdXMrMA
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascri
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16
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/

Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
Source Port: 80
Destination Port: 4335

4. The client-to-server TCP SYN segment sent at time 7.075657, the source IP address is 192.168.1.100, destination IP address is 64.233.169.104, source port is 4335, destination port is 80.

No.	Time	Source	Destination	Protocol	Length	Info
44	2.038247	74.125.106.31	192.168.1.100	HTTP	526	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
45	2.044751	192.168.1.100	74.125.106.31	HTTP	776	GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-6772
46	2.064877	74.125.106.31	192.168.1.100	HTTP	1089	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
47	2.178596	192.168.1.100	74.125.106.31	TCP	54	4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
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_P
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

Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
Source Port: 4335
Destination Port: 80

The ACK sent in response to the SYN at time 7.108986, the source IP address is 64.233.169.104, destination IP address is 192.168.1.100, source port is 80, destination port is 4335.

No.	Time	Source	Destination	Protocol	Length	Info
44	2.038247	74.125.106.31	192.168.1.100	HTTP	526	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
45	2.044751	192.168.1.100	74.125.106.31	HTTP	776	GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-6772
46	2.064877	74.125.106.31	192.168.1.100	HTTP	1089	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
47	2.178596	192.168.1.100	74.125.106.31	TCP	54	4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
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_P
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

Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 4335

5. Message appear in the NAT_ISP_side trace file at time 6.069168, the source IP address is 71.192.34.104, destination IP address is 64.233.169.104, TCP source port is 4335, destination port is 80.

Source and destination ports, destination IP address are the same, source IP address is different.

85	6.069168	71.192.34.104	64.233.169.104	HTTP	689 GET / HTTP/1.1
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814 HTTP/1.1 200 OK (text/html)
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
103	6.308118	64.233.169.104	71.192.34.104	HTTP	226 HTTP/1.1 200 OK (GIF89a)

Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635					
	Source Port:	4335			
	Destination Port:	80			
	[Stream index:	2]			

6. Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed.

Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635 Source Port: 4335 Destination Port: 80 [Stream index: 2] [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 0101 = Header Length: 20 bytes (5) > Flags: 0x018 (PSH, ACK) Window: 65044 [Calculated window size: 260176] [Window size scaling factor: 4] Checksum: 0xae3 [unverified] [Checksum Status: Unverified]	Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635 Source Port: 4335 Destination Port: 80 [Stream index: 2] [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 0101 = Header Length: 20 bytes (5) > Flags: 0x018 (PSH, ACK) Window: 65044 [Calculated window size: 260176] [Window size scaling factor: 4] Checksum: 0x386d [unverified] [Checksum Status: Unverified]
---	--

7. The first 200 OK HTTP message received from the Google server at time 6.117570, the source IP address is 64.233.169.104, destination IP address is 71.192.34.104, TCP source port is 80, destination port is 4335.

Source and destination ports, source IP address are the same, destination IP address is different.

90	6.117570	64.233.169.104	71.192.34.104	HTTP	814 HTTP/1.1 200 OK (text/html)
93	6.241357	71.192.34.104	64.233.169.104	HTTP	719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
103	6.308118	64.233.169.104	71.192.34.104	HTTP	226 HTTP/1.1 200 OK (GIF89a)

> Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)					
> Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c: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, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760					
	Source Port:	80			
	Destination Port:	4335			

8. The client-to-server TCP SYN segment captured at time 6.035475, the source IP address is 71.192.34.104, destination IP address is 64.233.169.104, source port is 4335, destination port is 80.

Source and destination ports, destination IP address are the same, source IP address is different.

No.	Time	Source	Destination	Protocol	Length	Info
44	0.996890	74.125.106.31	71.192.34.104	HTTP	526	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
45	1.004530	71.192.34.104	74.125.106.31	HTTP	776	GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-67721
46	1.023414	74.125.106.31	71.192.34.104	HTTP	1089	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
48	1.138164	71.192.34.104	74.125.106.31	TCP	60	4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
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
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

Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0					
	Source Port:	4335			
	Destination Port:	80			

The server-to-client TCP ACK segment captured at time 6.067775, the source IP address is 64.233.169.104, destination IP address is 71.192.34.104, source port is 80, destination port is 4335.

Source and destination ports, source IP address are the same, destination IP address is different.

No.	Time	Source	Destination	Protocol	Length	Info
44	0.996890	74.125.106.31	71.192.34.104	HTTP	526	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
45	1.004530	71.192.34.104	74.125.106.31	HTTP	776	GET /safebrowsing/rd/goog-phish-shavar_a_67721-67760.67721-67721
46	1.023414	74.125.106.31	71.192.34.104	HTTP	1089	HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
48	1.138164	71.192.34.104	74.125.106.31	TCP	60	4331 → 80 [ACK] Seq=2876 Ack=20452 Win=260176 Len=0
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_P
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

Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 4335

9.

WAN side	LAN side
71.192.34.104, 4335	192.168.1.100, 4335