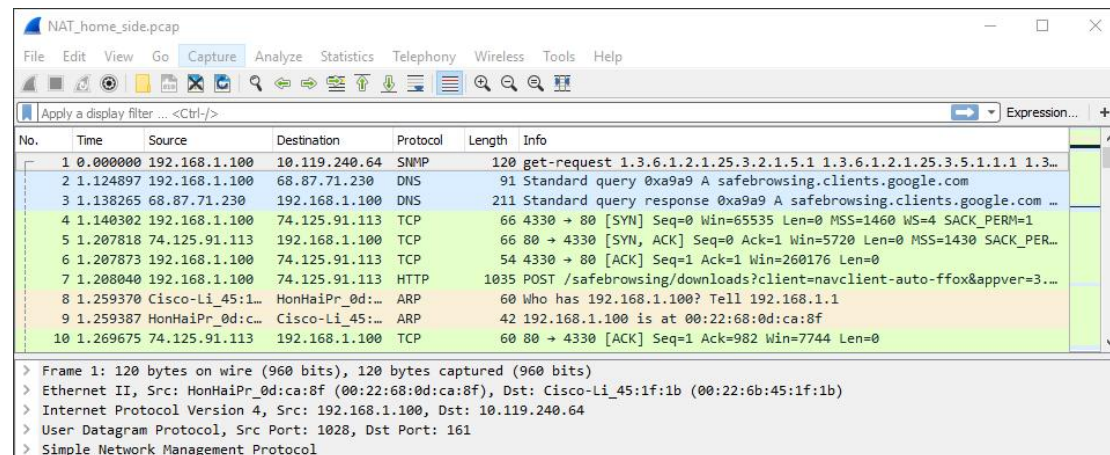


Xueyang (Sean) Wang
XW1154
04/26/2017
CS4793
Homework 07



NAT_home_side.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

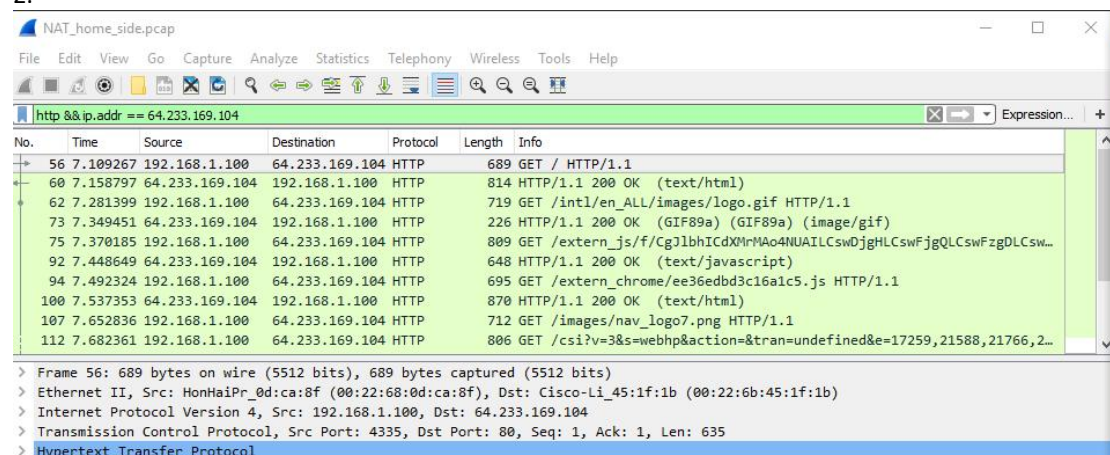
Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	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...
2	1.124897	192.168.1.100	68.87.71.230	DNS	91	Standard query 0xa9a9 A safebrowsing.clients.google.com
3	1.138265	68.87.71.230	192.168.1.100	DNS	211	Standard query response 0xa9a9 A safebrowsing.clients.google.com ...
4	1.140302	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	1.207818	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_PER...
6	1.207873	192.168.1.100	74.125.91.113	TCP	54	4330 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
7	1.208040	192.168.1.100	74.125.91.113	HTTP	1035	POST /safebrowsing/downloads?client=navclient-auto-ffox&appver=3...
8	1.259370	Cisco-Li_45:1...	HonHaiPr_0d:...	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
9	1.259387	HonHaiPr_0d:c...	Cisco-Li_45:...	ARP	42	192.168.1.100 is at 00:22:68:0d:ca:8f
10	1.269675	74.125.91.113	192.168.1.100	TCP	60	80 → 4330 [ACK] Seq=1 Ack=982 Win=7744 Len=0

> Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 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: 10.119.240.64
> User Datagram Protocol, Src Port: 1028, Dst Port: 161
> Simple Network Management Protocol

Figure 1. NAT_Home

1. The IP address of the client is 192.168.1.100
- 2.



NAT_home_side.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http &&ip.addr == 64.233.169.104 Expression...

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) (GIF89a) (image/gif)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/Cg1lbhICdXMmMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCsw...
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/ee36edbd3c16a1c5.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...

> 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
> Hypertext Transfer Protocol

Figure 2. Filtered NAT

3. The source IP address is 192.168.1.100, port: 4335 and the destination IP address is 64.233.169.104, port: 80
4. At 7.158798 is the corresponding 200 OK HTTP message received from the Google server. The source IP address is 64.233.169.104, port: 80 and the destination IP address is 192.168.1.100, port: 4335.

Figure 3 shows a Wireshark capture of a network packet. The packet list shows a TCP segment (No. 54) with source IP 192.168.1.100, destination IP 64.233.169.104, and port 4335. The packet details show the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes show the raw data of the TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
51	7.060269	192.168.1.100	68.87.71.230	DNS	74	Standard query 0xed6a A www.google.com
52	7.073897	68.87.71.230	192.168.1.100	DNS	158	Standard query response 0xed6a A www.google.com CNAME www.1.googl...
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_PER...
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	[TCP segment of a reassembled PDU]
59	7.158761	64.233.169.104	192.168.1.100	TCP	1484	[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)

Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 0, Ack: 1, Len: 0

Figure 3. TCP SYN/ACK segment

5. At 7.075657, the client-to-server TCP SYN segment was sent. The source IP address is 192.168.1.100, port: 4335. The destination IP address is 64.233.169.104, port: 80. For the ACK sent to response to the SYN: the source IP address is 64.233.169.104, port: 80, and the destination IP address is 192.168.1.100, port: 4335. At 7.108986, the ACK is received at the client.

Figure 4 shows a Wireshark capture of a network packet. The packet list shows a GET message (No. 85) with source IP 71.192.34.104, destination IP 64.233.169.104, and port 80. The packet details show the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes show the raw data of the GET message.

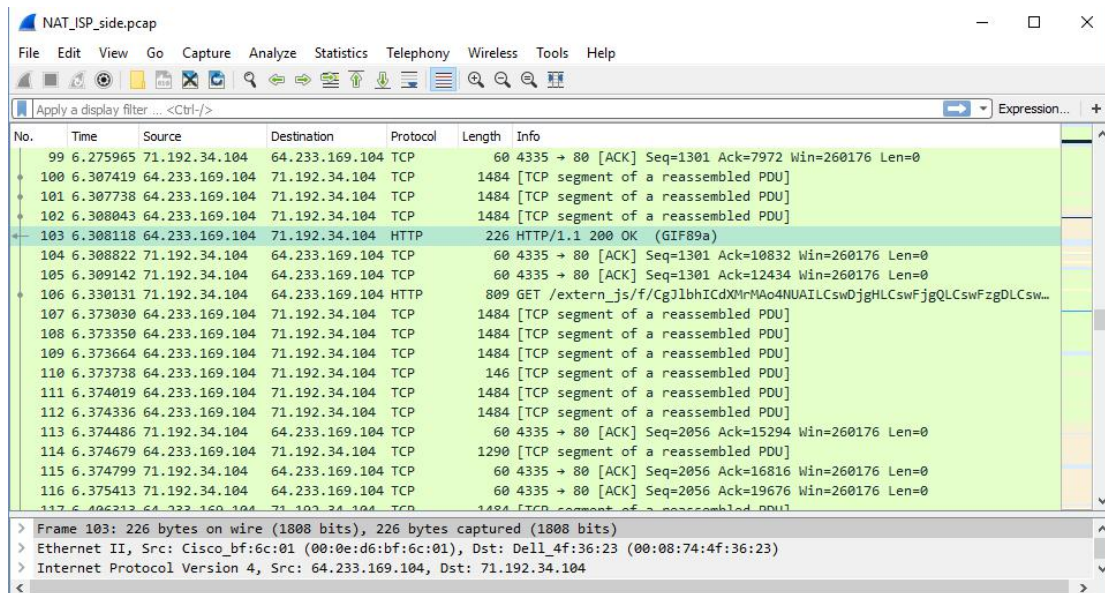
No.	Time	Source	Destination	Protocol	Length	Info
81	6.032738	68.87.71.230	71.192.34.104	DNS	158	Standard query response 0xed6a A www.google.com CNAME www.1.googl...
82	6.035475	71.192.34.104	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
83	6.067775	64.233.169.104	71.192.34.104	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PER...
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
86	6.092755	Cisco_bf:6c:01	Broadcast	ARP	60	Who has 71.192.35.144? Tell 71.192.32.1
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	[TCP segment of a reassembled PDU]
89	6.117407	64.233.169.104	71.192.34.104	TCP	1484	[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
92	6.162091	169.254.247.145	169.254.255...	NBNS	92	Name query NB HPAB9D4C<00>
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	[TCP segment of a reassembled PDU]
95	6.274230	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
96	6.274571	64.233.169.104	71.192.34.104	TCP	1484	[TCP segment of a reassembled PDU]
97	6.274853	64.233.169.104	71.192.34.104	TCP	1290	[TCP segment of a reassembled PDU]
98	6.275315	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0
99	6.275655	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0

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

Figure 4. NAT_ISP

6. At 6.069168, the message appears in the file. The source IP address is 71.192.34.104, port: 4335, and the destination IP address is 64.233.169.104, port: 80. Only the source IP address has changed, everything else is the same.

7. No change in GET message: NO change in Version, Header Length, Flags. Checksum is changed. Since the IP source address has change, and the checksum includes the value of the source IP address, the checksum has changed.



8. At 6.308118, the first 200 OK HTTP message is received. The source IP address 64.233.169.104, port: 80, and the destination IP address is 71.192.34.104, port: 4335. Only the destination IP address has changed.

9. At time 6.035475 and at time 6.067775, respectively. For SYN: the source IP address is 71.192.34.104, port: 4335, and the destination IP address is 64.233.169.104, port: 80. For ACK: the source IP address 64.233.169.104, port: 80, and the destination IP address is 71.192.34.104, port: 4335. For SYN, the source IP address has changed. For ACK, the destination IP address has changed. The port numbers are unchanged.

10.

NAT translate table	
WAN side	LAN side
71.192.34.104, 4335	192.168.1.100, 4335

Extra Credit: No time for research. EMPTY