

## Lab 4a - TCP

Wednesday, October 23, 2024 11:28 PM

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to `gaia.cs.umass.edu`? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows).

368	9.528953	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	607	443	→	52935	Len=545		
369	9.528953	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	85	443	→	52935	Len=23		
370	9.528953	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	594	443	→	52935	Len=532		
371	9.528953	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	85	443	→	52935	Len=23		
372	9.529884	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	594	443	→	52935	Len=532		
373	9.529884	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	85	443	→	52935	Len=23		
374	9.530676	192.168.1.244	128.119.245.12	TCP	66	49289	→	80	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM		
375	9.554419	2405:4802:903f:4f0::...	2001:4860:4860::8844	UDP	104	52935	→	443	Len=42		
376	9.613521	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	87	443	→	52935	Len=25		
377	9.750535	128.119.245.12	192.168.1.244	TCP	66	80	→	49288	[SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128		
378	9.750709	192.168.1.244	128.119.245.12	TCP	54	49288	→	80	[ACK] Seq=1 Ack=1 Win=131328 Len=0		
379	9.751416	192.168.1.244	128.119.245.12	TCP	782	49288	→	80	[PSH, ACK] Seq=1 Ack=1 Win=131328 Len=728		
380	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=729 Ack=1 Win=131328 Len=1460		
381	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=2189 Ack=1 Win=131328 Len=1460		
382	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=3649 Ack=1 Win=131328 Len=1460		
383	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=5109 Ack=1 Win=131328 Len=1460		
384	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=6569 Ack=1 Win=131328 Len=1460		
385	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=8029 Ack=1 Win=131328 Len=1460		
386	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=9489 Ack=1 Win=131328 Len=1460		
387	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=10949 Ack=1 Win=131328 Len=1460		
388	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=12409 Ack=1 Win=131328 Len=1460		
389	9.893432	128.119.245.12	192.168.1.244	TCP	66	80	→	49288	[ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128		
Frame 374: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{40F9FDDA-9151-47D2-8000-000000000000} (0:0:0:0:0:0)										0000 34 b5 a3 b7 f1 8e 2c 6d c1 0f cd e1 08 00 45 00 4	.....m.....E
Ethernet II, Src: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1), Dst: CigShanghai_b7:f1:8e (34:b5:a3:b7:f1:8e)										0010 00 34 97 69 40 00 80 06 00 00 c0 a8 01 f4 80 77	4 i@.....w
Internet Protocol Version 4, Src: 192.168.1.244, Dst: 128.119.245.12										0020 f5 0c c0 89 00 50 71 d9 d0 3b 00 00 00 00 80 02	...Pq.....
Transmission Control Protocol, Src Port: 49289, Dst Port: 80, Seq: 0, Len: 0										0030 fa f0 38 47 00 00 02 04 05 b4 01 03 03 08 01 01	..8G.....
										0040 04 02	..

- IP of client: 192.168.1.244
- TCP Port of client: 49288

2. What is the IP address of `gaia.cs.umass.edu`? On what port number is it sending and receiving TCP segments for this connection?

371	9.528953	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	85	443	→	52935	Len=23	
372	9.529884	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	594	443	→	52935	Len=532	
373	9.529884	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	85	443	→	52935	Len=23	
374	9.530676	192.168.1.244	128.119.245.12	TCP	66	49289	→	80	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
375	9.554419	2405:4802:903f:4f0::...	2001:4860:4860::8844	UDP	104	52935	→	443	Len=42	
376	9.613521	2001:4860:4860::8844	2405:4802:903f:4f0::...	UDP	87	443	→	52935	Len=25	
377	9.750535	128.119.245.12	192.168.1.244	TCP	66	80	→	49288	[SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128	
378	9.750709	192.168.1.244	128.119.245.12	TCP	54	49288	→	80	[ACK] Seq=1 Ack=1 Win=131328 Len=0	
379	9.751416	192.168.1.244	128.119.245.12	TCP	782	49288	→	80	[PSH, ACK] Seq=1 Ack=1 Win=131328 Len=728	
380	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=729 Ack=1 Win=131328 Len=1460	
381	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=2189 Ack=1 Win=131328 Len=1460	
382	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=3649 Ack=1 Win=131328 Len=1460	
383	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=5109 Ack=1 Win=131328 Len=1460	
384	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=6569 Ack=1 Win=131328 Len=1460	
385	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=8029 Ack=1 Win=131328 Len=1460	
386	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=9489 Ack=1 Win=131328 Len=1460	
387	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=10949 Ack=1 Win=131328 Len=1460	
388	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288	→	80	[ACK] Seq=12409 Ack=1 Win=131328 Len=1460	
Frame 374: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{40F9FDDA-9151-47D2-8000-000000000000} (0:0:0:0:0:0)										
Ethernet II, Src: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1), Dst: CigShanghai_b7:f1:8e (34:b5:a3:b7:f1:8e)										
Internet Protocol Version 4, Src: 192.168.1.244, Dst: 128.119.245.12										
Transmission Control Protocol, Src Port: 49289, Dst Port: 80, Seq: 0, Len: 0										

- IP of `gaia.cs.umass.edu`: 128.119.245.12
- TCP port for send and receive: 80

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and `gaia.cs.umass.edu`? What is it in the segment that identifies the segment as a SYN segment?

```

368 9.528953 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 60/ 443 → 52935 Len=545
369 9.528953 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 85 443 → 52935 Len=23
370 9.528953 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 594 443 → 52935 Len=532
371 9.528953 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 85 443 → 52935 Len=23
372 9.528984 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 594 443 → 52935 Len=532
373 9.528984 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 85 443 → 52935 Len=23
374 9.530676 192.168.1.244 128.119.245.12 TCP 66 49289 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
375 9.554419 2405:4802:903f:4f0:: 2001:4860:4860::8844 UDP 104 52935 → 443 Len=42
376 9.613521 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 87 443 → 52935 Len=25
377 9.750535 128.119.245.12 192.168.1.244 TCP 66 80 → 49288 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_P
378 9.750709 192.168.1.244 128.119.245.12 TCP 54 49288 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
379 9.751416 192.168.1.244 128.119.245.12 TCP 782 49288 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=728
380 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=729 Ack=1 Win=131328 Len=1460
381 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=2189 Ack=1 Win=131328 Len=1460

Frame 374: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{40F9FDDA-9151-47D2-0000-34 b5 a3 b7 f1 8e 2c}
Ethernet II, Src: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1), Dst: CigShanghai_b7:f1:8e (34:b5:a3:b7:f1:8e)
Internet Protocol Version 4, Src: 192.168.1.244, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49289, Dst Port: 80, Seq: 0, Len: 0
Source Port: 49289
Destination Port: 80
[Stream index: 7]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete, ESTABLISHED (7)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1910100027
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0x3847 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation
[Timestamps]

```

- Sequence number: 0
- SYN segment: Flag: 0x002 (SYN)

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

```

372 9.529884 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 594 443 → 52935 Len=532
373 9.529884 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 85 443 → 52935 Len=23
374 9.530676 192.168.1.244 128.119.245.12 TCP 66 49289 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
375 9.554419 2405:4802:903f:4f0:: 2001:4860:4860::8844 UDP 104 52935 → 443 Len=42
376 9.613521 2001:4860:4860::8844 2405:4802:903f:4f0:: UDP 87 443 → 52935 Len=25
377 9.750535 128.119.245.12 192.168.1.244 TCP 66 80 → 49288 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
378 9.750709 192.168.1.244 128.119.245.12 TCP 54 49288 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
379 9.751416 192.168.1.244 128.119.245.12 TCP 782 49288 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=728
380 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=729 Ack=1 Win=131328 Len=1460
381 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=2189 Ack=1 Win=131328 Len=1460

Frame 377: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{40F9FDDA-9151-47D2-0000-2c 6d c1 0f cd e1 34 b5 a3 b7 f1 8e 08 00 45 1}
Ethernet II, Src: CigShanghai_b7:f1:8e (34:b5:a3:b7:f1:8e), Dst: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.244
Transmission Control Protocol, Src Port: 80, Dst Port: 49288, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 49288
[Stream index: 6]
[Stream Packet Number: 2]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1560979901
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3876590212
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
Window: 29200
[Calculated window size: 29200]
Checksum: 0x039b [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation
[Timestamps]
[SEQ/ACK analysis]

```

- Sequence number of ACK SYN: 0
- Acknowledgement field: 1, is determined by gaia.cs.umass.edu by adding 1 to the initial sequence number of SYN segment from the client computer
- Identifies the segment as a SYNACK segment: Flags 0x012 (SYN,ACK)

6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.



372	9.529884	2001:4860:4860::8844	2405:4802:903f:4f0::	UDP	594 443 → 52935	Len=532	
373	9.529884	2001:4860:4860::8844	2405:4802:903f:4f0::	UDP	85 443 → 52935	Len=23	
374	9.530676	192.168.1.244	128.119.245.12	TCP	66 49289 → 80 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
375	9.554419	2405:4802:903f:4f0::	2001:4860:4860::8844	UDP	104 52935 → 443	Len=42	
376	9.613521	2001:4860:4860::8844	2405:4802:903f:4f0::	UDP	87 443 → 52935	Len=25	
377	9.750535	128.119.245.12	192.168.1.244	TCP	66 80 → 49288 [SYN, ACK]	Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128	
378	9.750709	192.168.1.244	128.119.245.12	TCP	54 49288 → 80 [ACK]	Seq=1 Ack=1 Win=131328 Len=0	
379	9.751416	192.168.1.244	128.119.245.12	TCP	782 49288 → 80 [PSH, ACK]	Seq=1 Ack=1 Win=131328 Len=728 [TCP PDU reassembled in 519]	
380	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=729 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
381	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=2189 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
382	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=3649 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
383	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=5109 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
384	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=6569 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
385	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=8029 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
386	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=9489 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
387	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=10949 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
388	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=12409 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]	
389	9.803602	128.119.245.12	192.168.1.244	TCP	54 49288 → 80 [ACK]	Seq=1 Ack=1 Win=131328 Len=0 MSS=1460 WS=256 SACK_PERM	

- Sequence number: 1
- 7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value (see Section 3.5.3, page 242 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments

- Sequence numbers of the first six segments:

374	9.530676	192.168.1.244	128.119.245.12	TCP	66 49289 → 80 [SYN]	Seq=0 Win=64240 Len=0	
378	9.750709	192.168.1.244	128.119.245.12	TCP	54 49288 → 80 [ACK]	Seq=1 Ack=1 Win=131328 Len=0	
379	9.751416	192.168.1.244	128.119.245.12	TCP	782 49288 → 80 [PSH, ACK]	Seq=1 Ack=1 Win=131328 Len=728	
380	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=729 Ack=1 Win=131328 Len=1460	
381	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=2189 Ack=1 Win=131328 Len=1460	
382	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=3649 Ack=1 Win=131328 Len=1460	
383	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=5109 Ack=1 Win=131328 Len=1460	
384	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=6569 Ack=1 Win=131328 Len=1460	
385	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=8029 Ack=1 Win=131328 Len=1460	
386	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=9489 Ack=1 Win=131328 Len=1460	
387	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=10949 Ack=1 Win=131328 Len=1460	
388	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=12409 Ack=1 Win=131328 Len=1460	
389	9.803602	128.119.245.12	192.168.1.244	TCP	54 49288 → 80 [ACK]	Seq=1 Ack=1 Win=131328 Len=0 MSS=1460 WS=256 SACK_PERM	

- Sequence number: 1, time: 9.750709s, ACK time: 10.023530s, RTT=0.2728s

391	10.023530	128.119.245.12	192.168.1.244	TCP	60 80 → 49288 [ACK]	Seq=1 Ack=729 Win=30720 Len=0	
-----	-----------	----------------	---------------	-----	---------------------	-------------------------------	--

374	9.530676	192.168.1.244	128.119.245.12	TCP	66 49289 → 80 [SYN]	Seq=0 Win=64240 Len=0	
378	9.750709	192.168.1.244	128.119.245.12	TCP	54 49288 → 80 [ACK]	Seq=1 Ack=1 Win=131328 Len=0	
379	9.751416	192.168.1.244	128.119.245.12	TCP	782 49288 → 80 [PSH, ACK]	Seq=1 Ack=1 Win=131328 Len=728	
380	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=729 Ack=1 Win=131328 Len=1460	
381	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=2189 Ack=1 Win=131328 Len=1460	
382	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=3649 Ack=1 Win=131328 Len=1460	
383	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=5109 Ack=1 Win=131328 Len=1460	
384	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=6569 Ack=1 Win=131328 Len=1460	
385	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=8029 Ack=1 Win=131328 Len=1460	
386	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=9489 Ack=1 Win=131328 Len=1460	
387	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=10949 Ack=1 Win=131328 Len=1460	
388	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK]	Seq=12409 Ack=1 Win=131328 Len=1460	
389	9.803602	128.119.245.12	192.168.1.244	TCP	54 49288 → 80 [ACK]	Seq=1 Ack=1 Win=131328 Len=0 MSS=1460 WS=256 SACK_PERM	

- Sequence number: 729, time: 9.751730s, ACK time: 10.023530s, RRT= 0.2718s

```
391 10.023530 128.119.245.12 192.168.1.244 TCP 60 80 → 49288 [ACK] Seq=1 Ack=729 Win=30720 Len=0
```

```
374 9.530676 192.168.1.244 128.119.245.12 TCP 66 49288 → 80 [SYN] Seq=0 Win=64240 Len=0
378 9.750709 192.168.1.244 128.119.245.12 TCP 54 49288 → 80 [ACK] Seq=1 Ack=1 Win=13132
379 9.751416 192.168.1.244 128.119.245.12 TCP 782 49288 → 80 [PSH, ACK] Seq=1 Ack=1 Win=1
380 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=729 Ack=1 Win=131
381 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=2189 Ack=1 Win=13
382 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=3649 Ack=1 Win=13
383 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=5109 Ack=1 Win=13
384 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=6569 Ack=1 Win=13
385 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=8029 Ack=1 Win=13
386 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=9489 Ack=1 Win=13
387 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=10949 Ack=1 Win=13
388 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=12409 Ack=1 Win=13
389 9.803693 192.168.1.244 128.119.245.12 TCP 66 49288 → 80 [SYN] Seq=0 Win=64240 Len=0

[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1460]
Sequence Number: 2189 (relative sequence number)
Sequence Number (raw): 3876592400
[Next Sequence Number: 3649 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1560979902
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x3def [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
```

- Sequence number: 2189, time: 9.751730s, ACK time: 10.028101s, RRT = 0.2763s

```
393 10.028101 128.119.245.12 192.168.1.244 TCP 60 80 → 49288 [ACK] Seq=1 Ack=2189 Win=33664 Len=0
```

```
355 9.476975 192.168.1.244 128.119.245.12 TCP 66 49288 → 80 [SYN] Seq=0 Win=64240 Len=0
374 9.530676 192.168.1.244 128.119.245.12 TCP 66 49288 → 80 [SYN] Seq=0 Win=64240 Len=0
378 9.750709 192.168.1.244 128.119.245.12 TCP 54 49288 → 80 [ACK] Seq=1 Ack=1 Win=13132
379 9.751416 192.168.1.244 128.119.245.12 TCP 782 49288 → 80 [PSH, ACK] Seq=1 Ack=1 Win=1
380 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=729 Ack=1 Win=13
381 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=2189 Ack=1 Win=13
382 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=3649 Ack=1 Win=13
383 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=5109 Ack=1 Win=13
384 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=6569 Ack=1 Win=13
385 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=8029 Ack=1 Win=13
386 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=9489 Ack=1 Win=13
387 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=10949 Ack=1 Win=13
388 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=12409 Ack=1 Win=13
389 9.803693 192.168.1.244 128.119.245.12 TCP 66 49288 → 80 [SYN] Seq=0 Win=64240 Len=0

[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1460]
Sequence Number: 3649 (relative sequence number)
Sequence Number (raw): 3876593860
[Next Sequence Number: 5109 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1560979902
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x3def [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
```

- Sequence number: 3649, time: 9.751730s, ACK time: 10.028101s, RRT = 0.2763s

```
394 10.028101 128.119.245.12 192.168.1.244 TCP 60 80 → 49288 [ACK] Seq=1 Ack=9489 Win=48256 Len=0
```

```
355 9.476975 192.168.1.244 128.119.245.12 TCP 66 49288 → 80 [SYN] Seq=0
374 9.530676 192.168.1.244 128.119.245.12 TCP 66 49288 → 80 [SYN] Seq=0
378 9.750709 192.168.1.244 128.119.245.12 TCP 54 49288 → 80 [ACK] Seq=1
379 9.751416 192.168.1.244 128.119.245.12 TCP 782 49288 → 80 [PSH, ACK]
380 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=7
381 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=2
382 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=3
383 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=5
384 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=6
385 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=8
386 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=9
387 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=1
388 9.751730 192.168.1.244 128.119.245.12 TCP 1514 49288 → 80 [ACK] Seq=1
389 9.803693 192.168.1.244 128.119.245.12 TCP 66 49288 → 80 [SYN] Seq=0

[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1460]
Sequence Number: 5109 (relative sequence number)
Sequence Number (raw): 3876595320
[Next Sequence Number: 6569 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1560979902
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x3def [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
```

- Sequence number: 5109, time: 9.751730s, ACK time: 10.028101s, RRT = 0.2763s

```
394 10.028101 128.119.245.12 192.168.1.244 TCP 60 80 → 49288 [ACK] Seq=1 Ack=9489 Win=48256 Len=0
```



334	9.001300	192.168.1.244	192.168.1.255	NBWS	92	Name query	NB THAINGUYENGITAB&Ic>
352	9.366505	192.168.1.244	128.119.245.12	TCP	66	49288 → 80	[SYN] Seq=0 Win=64240
355	9.476975	192.168.1.244	128.119.245.12	TCP	66	49289 → 80	[SYN] Seq=0 Win=64240
374	9.530676	192.168.1.244	128.119.245.12	TCP	54	49288 → 80	[ACK] Seq=1 Ack=1 Win=
378	9.750709	192.168.1.244	128.119.245.12	TCP	782	49288 → 80	[PSH, ACK] Seq=1 Ack=1
379	9.751416	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=729 Ack=1 Wi
380	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=2189 Ack=1 W
381	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=3649 Ack=1 W
382	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=5109 Ack=1 W
383	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=6569 Ack=1 W
384	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=8029 Ack=1 W
385	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=9489 Ack=1 W
386	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=10949 Ack=1 W
387	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=12409 Ack=1 W
388	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=12409 Ack=1 W

```

[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 1460]
Sequence Number: 6569 (relative sequence number)
Sequence Number (raw): 3876596780
[Next Sequence Number: 8029 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1560979902
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0x3def [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
[RTT: 0.273734000 seconds]

```

- Sequence number: 6569, time: 9.751730s, ACK time: 10.028101s, RTT = 0.2763s

394	10.028101	128.119.245.12	192.168.1.244	TCP	60	80 → 49288	[ACK] Seq=1 Ack=9489 Win=48256 Len=0
-----	-----------	----------------	---------------	-----	----	------------	--------------------------------------

8. What is the length of each of the first six TCP segments?

517	10.578000	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=149645 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
518	10.578000	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=151105 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
519	10.578000	192.168.1.244	128.119.245.12	HTTP	539	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)	
520	10.583514	128.119.245.12	192.168.1.244	TCP	66	80 → 49288	[ACK] Seq=1 Ack=72997 Win=178432 Len=0 SLE=74457 SRE=80297
521	10.583514	128.119.245.12	192.168.1.244	TCP	66	[TCP Dup ACK 520#1] 80 → 49288	[ACK] Seq=1 Ack=72997 Win=179584 Len=0 SLE=74457 SRE=81757
522	10.583514	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=81757 Win=178560 Len=0
523	10.583514	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=83217 Win=177664 Len=0
524	10.583514	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=87597 Win=174592 Len=0
525	10.583514	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=94897 Win=169728 Len=0
526	10.583514	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=99273 Win=181632 Len=0
527	10.702591	2603:1046:1400::15	2405:4802:903f:4f0::...	TCP	74	443 → 49178	[ACK] Seq=36 Ack=69 Win=16382 Len=0
528	10.830085	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=100733 Win=183296 Len=0
529	10.831519	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=103653 Win=189056 Len=0
530	10.831519	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=105113 Win=192000 Len=0
531	10.840007	128.119.245.12	192.168.1.244	TCP	54	80 → 49288	[ACK] Seq=1 Ack=108033 Win=192768 Len=0

```

[RTT: 0.273734000 seconds]
[Bytes in flight: 77133]
[Bytes sent since last PSH flag: 4865]
TCP payload (485 bytes)
TCP segment data (485 bytes)
[108 Reassembled TCP Segments (153849 bytes): #379(728), #380(1460), #381(1460), #382(1460), #383(1460), #384(1460)]
[Frame: 379, payload: 0-727 (728 bytes)]
[Frame: 380, payload: 728-2187 (1460 bytes)]
[Frame: 381, payload: 2188-3647 (1460 bytes)]
[Frame: 382, payload: 3648-5107 (1460 bytes)]
[Frame: 383, payload: 5108-6567 (1460 bytes)]
[Frame: 384, payload: 6568-8027 (1460 bytes)]
[Frame: 385, payload: 8028-9487 (1460 bytes)]
[Frame: 386, payload: 9488-10947 (1460 bytes)]
[Frame: 387, payload: 10948-12407 (1460 bytes)]
[Frame: 388, payload: 12408-13867 (1460 bytes)]
[Frame: 389, payload: 13868-15327 (1460 bytes)]
[Frame: 390, payload: 15328-16787 (1460 bytes)]
[Frame: 391, payload: 16788-18247 (1460 bytes)]
[Frame: 392, payload: 18248-19707 (1460 bytes)]

```

- First segment: 728 bytes
- Other five segment: 1460 bytes

9. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

386	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=9489 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
387	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=10949 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
388	9.751730	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=12409 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
389	9.802433	128.119.245.12	192.168.1.244	TCP	66	80 → 49289	[SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
390	9.802602	192.168.1.244	128.119.245.12	TCP	54	49289 → 80	[ACK] Seq=1 Ack=1 Win=131328 Len=0
391	10.023530	128.119.245.12	192.168.1.244	TCP	60	80 → 49288	[ACK] Seq=1 Ack=729 Win=30720 Len=0
392	10.023659	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=13869 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
393	10.028101	128.119.245.12	192.168.1.244	TCP	60	80 → 49288	[ACK] Seq=1 Ack=2189 Win=33664 Len=0
394	10.028101	128.119.245.12	192.168.1.244	TCP	60	80 → 49288	[ACK] Seq=1 Ack=9489 Win=48256 Len=0
395	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=15329 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
396	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[PSH, ACK] Seq=16789 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
397	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=18249 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
398	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=19709 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
399	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=21169 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
400	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=22629 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
401	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=24089 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
402	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=25549 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
403	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=27009 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
404	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=28469 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
405	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=29929 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
406	10.028261	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=31389 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
407	10.028261	192.168.1.244	128.119.245.12	TCP	782	49288 → 80	[PSH, ACK] Seq=32849 Ack=1 Win=131328 Len=728 [TCP PDU reassembled in 519]
408	10.028957	128.119.245.12	192.168.1.244	TCP	60	80 → 49288	[ACK] Seq=1 Ack=13869 Win=56960 Len=0
409	10.029071	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=33577 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
410	10.029071	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=35037 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
411	10.029071	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=36497 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
412	10.029071	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=37957 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
413	10.029071	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=39417 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
414	10.029071	192.168.1.244	128.119.245.12	TCP	1514	49288 → 80	[ACK] Seq=40877 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]
415	10.294412	128.119.245.12	192.168.1.244	TCP	60	80 → 49288	[ACK] Seq=1 Ack=15329 Win=59904 Len=0

- Minimum amount of buffer space at packet 389: 29200 bytes
- The sender is never throttled due to lacking of receiver buffer space by

10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).

```

# 510 10.578000 192.168.1.244 128.119.245.12 HTTP 539 POST /wireshark-labs/lab3-1-reply
# 520 10.583514 128.119.245.12 192.168.1.244 TCP 66 80 → 49288 [ACK] Seq=1 Acks=72997
# 521 10.583514 128.119.245.12 192.168.1.244 TCP 66 [TCP Dup ACK 520w1] 80 → 49288 [A
# 522 10.583514 128.119.245.12 192.168.1.244 TCP 54 80 → 49288 [ACK] Seq=1 Acks=81757
# 523 10.583514 128.119.245.12 192.168.1.244 TCP 54 80 → 49288 [ACK] Seq=1 Acks=8321
# 524 10.583514 128.119.245.12 192.168.1.244 TCP 54 80 → 49288 [ACK] Seq=1 Acks=87597
# 525 10.583514 128.119.245.12 192.168.1.244 TCP 54 80 → 49288 [ACK] Seq=1 Acks=94897
# 526 10.583514 128.119.245.12 192.168.1.244 TCP 54 80 → 49288 [ACK] Seq=1 Acks=99273
# 537 10.703501 3592.1035.1400.035 3495.1593.0026.160 TCP 72 443 → 49178 [ACK] Seq=26 Ack=50
[Bytes sent since last PSH flag: 4865]
TCP payload (485 bytes)
TCP segment data (485 bytes)
# 108 Reassembled TCP Segments (153049 bytes): #379(728), #380(1460), #381(1460), #382(1460), #383(1460), #384
[frame 379, payload: 8-727 (728 bytes)]
[frame 380, payload: 728-2187 (1460 bytes)]
[frame 381, payload: 2188-3647 (1460 bytes)]
[frame 382, payload: 3648-5107 (1460 bytes)]
[frame 383, payload: 5108-6567 (1460 bytes)]
[frame 384, payload: 6568-8027 (1460 bytes)]
[frame 385, payload: 8028-9487 (1460 bytes)]
[frame 386, payload: 9488-10947 (1460 bytes)]
[frame 387, payload: 10948-12407 (1460 bytes)]
[frame 388, payload: 12408-13867 (1460 bytes)]
[frame 389, payload: 13868-15327 (1460 bytes)]
[frame 390, payload: 15328-16787 (1460 bytes)]
[frame 391, payload: 16788-18247 (1460 bytes)]

```

- Data the receiver ACK is the payload
  - o 727 bytes
  - o 2187-728 bytes
  - o ...

12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

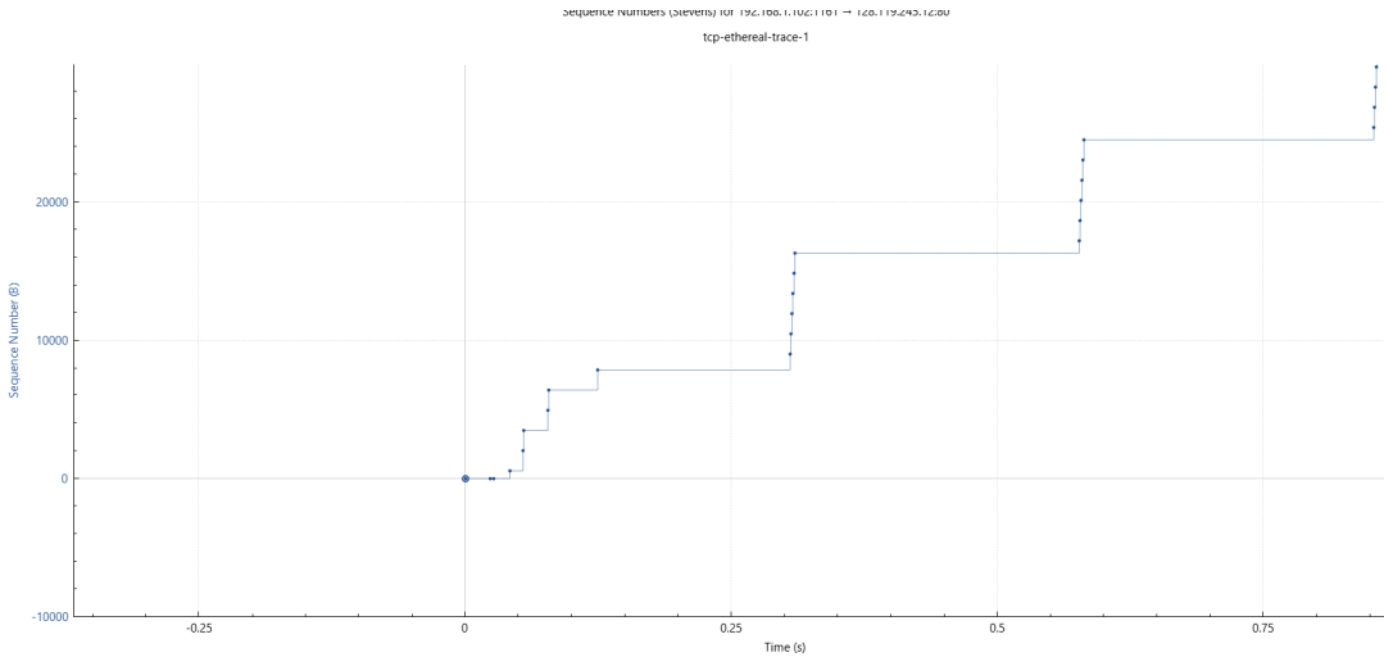
```
[Frame: 507, payload: 139188-139639 (1468 bytes)]
[Frame: 508, payload: 137648-139999 (1468 bytes)]
[Frame: 509, payload: 139108-140559 (1468 bytes)]
[Frame: 510, payload: 140568-142019 (1468 bytes)]
[Frame: 511, payload: 142028-143479 (1468 bytes)]
[Frame: 512, payload: 143488-144939 (1468 bytes)]
[Frame: 513, payload: 144948-146399 (1468 bytes)]
[Frame: 514, payload: 146408-147859 (1468 bytes)]
[Frame: 515, payload: 147868-148319 (324 bytes)]
[Frame: 516, payload: 148184-149634 (1468 bytes)]
[Frame: 517, payload: 149644-151103 (1468 bytes)]
[Frame: 518, payload: 151104-152563 (1468 bytes)]
[Frame: 519, payload: 152564-153048 (485 bytes)]
[Segment count: 108]
[Reassembled TCP length: 153049]
```

- Total bytes of file: 153048 bytes

540	9.855338	128.119.245.12	192.168.1.244	TCP	54 80 → 49288 [ACK] Seq=1 Acl=142021 Win=265856 Len=0
541	9.855338	128.119.245.12	192.168.1.244	TCP	54 80 → 49288 [ACK] Seq=1 Acl=148185 Win=278144 Len=0
542	9.855338	128.119.245.12	192.168.1.244	TCP	54 80 → 49288 [ACK] Seq=1 Acl=153050 Win=287872 Len=0
543	9.855338	128.119.245.12	192.168.1.244	HTTP	831 HTTP/1.1 200 OK (text/html)
378	9.750709	192.168.1.244	128.119.245.12	TCP	54 49288 → 80 [ACK] Seq=1 Acl=1 Win=131328 Len=0
379	9.751416	192.168.1.244	128.119.245.12	TCP	782 49288 → 80 [PSH, ACK] Seq=1 Acl=1 Win=131328 Len=728 [TCP PDU reassembled in 519]
380	9.751730	192.168.1.244	128.119.245.12	TCP	1514 49288 → 80 [ACK] Seq=729 Acl=1 Win=131328 Len=1460 [TCP PDU reassembled in 519]

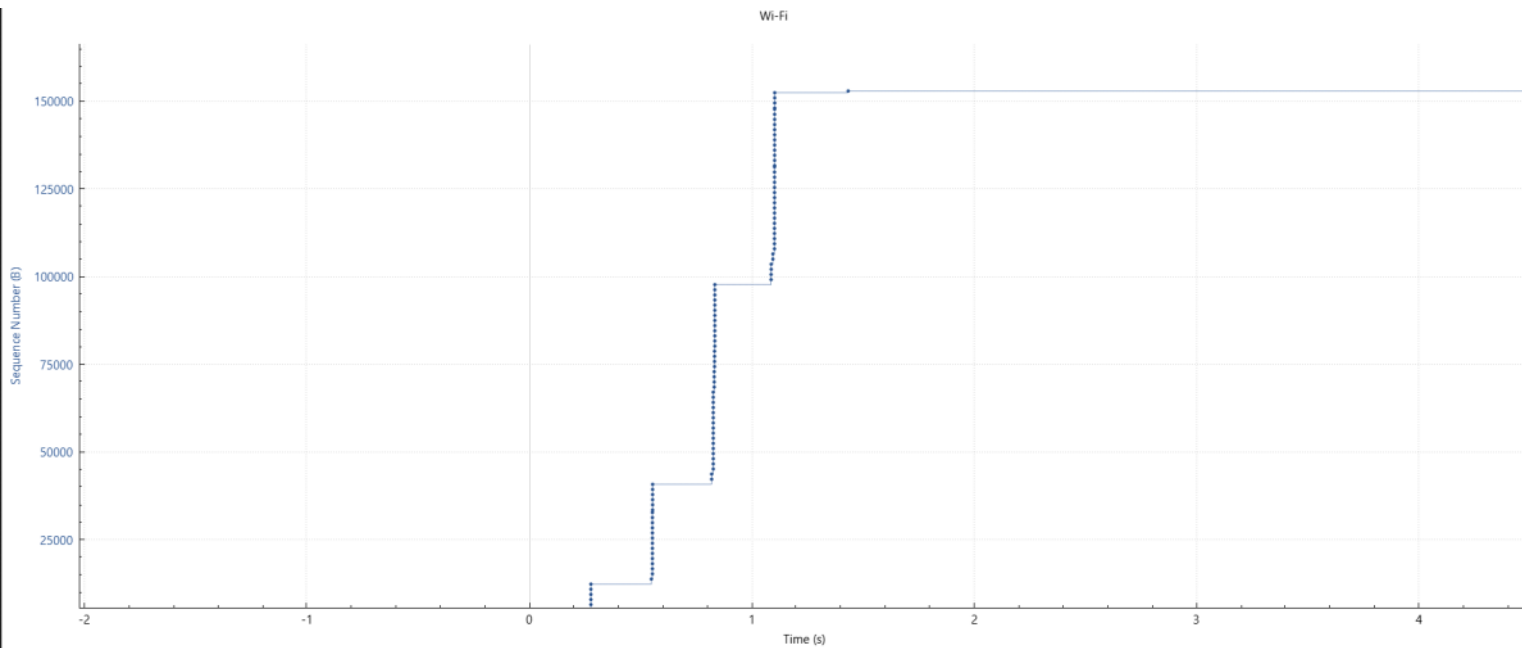
- Time to transmit:  $10.8553 - 9.7514 = 1.1039s$   
 $\Rightarrow$  Throughput:  $153048 / 1.1039 = 138642.993 \text{ Byte/s} = 135.3926 \text{ KB/s}$

ComputerNetwork Page 6



- slowstart phase (0 - 0.3s): the sequence number rises quickly over a short period
- congestion avoidance (0.3 - inf) the slope of the sequence number increase becomes less steep

14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu



- slow start phase: 0 - 1.1s the sequence number rises quickly over a short period (steep upward steps).
- congestion avoidance: 1.1s - 4.4s the slope of the sequence number increase becomes less steep



# Lab 5b - DHCP lab

Thursday, October 24, 2024 3:13 PM

## 1. Are DHCP messages sent over UDP or TCP?

No.	Time	Source	Destination	Protocol	Length	Info
28	1.827229	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xafa2140c
34	2.343502	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xafa2140c
212	10.673606	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x899ba273
271	12.787544	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x899ba273
302	14.301297	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release - Transaction ID 0x8e4f28a9
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover - Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer - Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360	DHCP Request - Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0xa1849ec8
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release - Transaction ID 0x45d1c3a3
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover - Transaction ID 0x1efc5691
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer - Transaction ID 0x1efc5691
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0x1efc5691
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0x1efc5691

Frame 28: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{40F9FDDA-9151-4... 0000 ff ff  
Ethernet II, Src: Intel\_5f:09:33 (88:d8:2e:5f:09:33), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 0010 01 4  
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255 0020 ff f  
User Datagram Protocol, Src Port: 68, Dst Port: 67 0030 14 0  
Source Port: 68 0040 00 0  
Destination Port: 67 0050 00 0  
Length: 308 0060 00 0  
Checksum: 0xd50d [unverified] 0070 00 0  
[Checksum Status: Unverified] 0080 00 0  
[Stream index: 6] 0090 00 0  
[Stream Packet Number: 1] 00a0 00 0  
[Timestamps] 00b0 00 0  
UDP payload (308 bytes) 00c0 00 0  
Dynamic Host Configuration Protocol (Discover) 00d0 00 0  
00e0 00 0  
00f0 00 0  
0100 00 0  
0110 00 0  
0120 88 d

- Send over UDP

2. Draw a timing diagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

- Timing diagram:

344	20.077021	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover - Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer - Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0xdeed530d

- Discover:

- Source port: 68
- Dest port: 67

212	10.673606	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x899ba273
271	12.787544	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x899ba273
302	14.301297	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release - Transaction ID 0x8e4f28a9
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover - Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer - Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360	DHCP Request - Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0xa1849ec8
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release - Transaction ID 0x45d1c3a3
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover - Transaction ID 0x1efc5691
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer - Transaction ID 0x1efc5691
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0x1efc5691
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0x1efc5691

Frame 344: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface \Device\NPF\_{40F9FDDA-9151-4... 0000 ff ff ff ff ff ff 2c 6  
Ethernet II, Src: Intel\_0f:cd:ce1 (2c:6d:c1:0f:cd:ce1), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 0010 01 4b 61 a1 00 00 80 11  
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255 0020 ff ff 00 44 00 43 01 3  
User Datagram Protocol, Src Port: 68, Dst Port: 67 0030 53 0d 00 00 00 00 00 00  
Source Port: 68 0040 00 00 00 00 00 2c 6  
Destination Port: 67 0050 00 00 00 00 00 00 00 00  
Length: 311 0060 00 00 00 00 00 00 00 00  
Checksum: 0x2210 [unverified] 0070 00 00 00 00 00 00 00  
[Checksum Status: Unverified] 0080 00 00 00 00 00 00 00  
[Stream index: 6] 0090 00 00 00 00 00 00 00  
[Stream Packet Number: 5] 00a0 00 00 00 00 00 00 00  
[Timestamps] 00b0 00 00 00 00 00 00 00  
UDP payload (303 bytes) 00c0 00 00 00 00 00 00 00  
Dynamic Host Configuration Protocol (Discover) 00d0 00 00 00 00 00 00 00  
00e0 00 00 00 00 00 00 00  
00f0 00 00 00 00 00 00 00  
0100 00 00 00 00 00 00 00  
0110 00 00 00 00 00 63 8

- Offer:



- Source port: 67
- Dest port: 68

271	12.787544	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request	- Transaction ID 0x899ba
302	14.301297	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release	- Transaction ID 0x8e4f2
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover	- Transaction ID 0xdeed5
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer	- Transaction ID 0xdeed5
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request	- Transaction ID 0xdeed5
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0xdeed5
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0x82578
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request	- Transaction ID 0x34d70
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0x82578
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360	DHCP Request	- Transaction ID 0xa1849
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0xa1849
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release	- Transaction ID 0x45d1c
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover	- Transaction ID 0x1efc5
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer	- Transaction ID 0x1efc5
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request	- Transaction ID 0x1efc5
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0x1efc5

```

Frame 379: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{40F9FDDA-9151-
Ethernet II, Src: DrayTek 12:5a:18 (00:1d:aa:12:5a:18), Dst: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)
Internet Protocol Version 4, Src: 191.16.1.2, Dst: 191.16.11.129
User Datagram Protocol, Src Port: 67, Dst Port: 68
  Source Port: 67
  Destination Port: 68
  Length: 308
  Checksum: 0xa65d [unverified]
  [Checksum Status: Unverified]
  [Stream index: 28]
  [Stream Packet Number: 2]
  [Timestamps]
  UDP payload (300 bytes)
Dynamic Host Configuration Protocol (Offer)

```

- Request:

- Source port: 68
- Dest port: 67

271	12.787544	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request	- Transaction ID 0x899ba273
302	14.301297	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release	- Transaction ID 0x8e4f28a9
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover	- Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer	- Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request	- Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request	- Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360	DHCP Request	- Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0xa1849ec8
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release	- Transaction ID 0x45d1c3a3
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover	- Transaction ID 0x1efc5691
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer	- Transaction ID 0x1efc5691
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request	- Transaction ID 0x1efc5691
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0x1efc5691

```

Frame 381: 372 bytes on wire (2976 bits), 372 bytes captured (2976 bits) on interface \Device\NPF_{40F9FDDA-9151-
Ethernet II, Src: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
  Source Port: 68
  Destination Port: 67
  Length: 338
  Checksum: 0xb8aa [unverified]
  [Checksum Status: Unverified]
  [Stream index: 6]
  [Stream Packet Number: 6]
  [Timestamps]
  UDP payload (330 bytes)
Dynamic Host Configuration Protocol (Request)

```

- ACK:

- Source port: 67
- Dest port: 68

381	21.083443	0.0.0.0	255.255.255.255	DHCP	372 DHCP Request	- Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360 DHCP Request	- Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xa1849ec8
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342 DHCP Release	- Transaction ID 0x45d1c3a3
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0x1efc5691
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342 DHCP Offer	- Transaction ID 0x1efc5691
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372 DHCP Request	- Transaction ID 0x1efc5691
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0x1efc5691

```

Frame 382: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{40F9FDDA-9151-0000-0000-000000000000}
Ethernet II, Src: DrayTek 12:5a:18 (00:1d:aa:12:5a:18), Dst: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)
Internet Protocol Version 4, Src: 191.16.1.2, Dst: 191.16.11.129
User Datagram Protocol, Src Port: 67, Dst Port: 68
  Source Port: 67
  Destination Port: 68
  Length: 308
  Checksum: 0xa35d [unverified]
  [Checksum Status: Unverified]
  [Stream index: 28]
  [Stream Packet Number: 3]
  [Timestamps]
  UDP payload (300 bytes)
  Dynamic Host Configuration Protocol (ACK)

```

3. What is the link-layer (e.g., Ethernet) address of your host?

No.	Time	Source	Destination	Protocol	Length	Info
28	1.827229	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xafa2140c
34	2.343502	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xafa2140c
212	10.673606	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x899ba273
271	12.787544	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x899ba273
302	14.301297	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release - Transaction ID 0x8e4f28a9
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover - Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer - Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360	DHCP Request - Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0xa1849ec8
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release - Transaction ID 0x45d1c3a3
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover - Transaction ID 0x1efc5691
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer - Transaction ID 0x1efc5691
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0x1efc5691
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK - Transaction ID 0x1efc5691

```

UDP payload (303 bytes)
Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xdeed530d
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Discover)
  Option: (61) Client identifier
  Option: (50) Requested IP Address (191.16.11.129)

```

- Mac address: 2c:6d:c1:0f:cd:e1

4. What values in the DHCP discover message differentiate this message from the DHCP request message?

- Option 53:
  - o DHCP: request (3)



34	2.343502	0.0.0.0	255.255.255.255	DHCP	352 DHCP Request	- Transaction ID 0xafa2140c
212	10.673606	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x899ba273
271	12.787544	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x899ba273
302	14.301297	191.16.11.129	191.16.1.2	DHCP	342 DHCP Release	- Transaction ID 0x8e4f28a9
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342 DHCP Offer	- Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372 DHCP Request	- Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360 DHCP Request	- Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xa1849ec8
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342 DHCP Release	- Transaction ID 0x45d1c3a3
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0x1efc5691
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342 DHCP Offer	- Transaction ID 0x1efc5691
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372 DHCP Request	- Transaction ID 0x1efc5691
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0x1efc5691

Seconds elapsed: 0	
Bootp flags: 0x0000 (Unicast)	
Client IP address: 0.0.0.0	
Your (client) IP address: 0.0.0.0	
Next server IP address: 0.0.0.0	
Relay agent IP address: 0.0.0.0	
Client MAC address: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)	
Client hardware address padding: 00000000000000000000	
Server host name not given	
Boot file name not given	
Magic cookie: DHCP	
Option: (53) DHCP Message Type (Request)	
Length: 1	
DHCP: Request (3)	
Option: (61) Client Identifier	
Length: 7	
Hardware type: Ethernet (0x01)	
Client MAC address: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)	
Option: (50) Requested IP Address (191.16.11.129)	
Length: 4	
Requested IP Address: 191.16.11.129	

o DHCP: discover (1)

34	2.343502	0.0.0.0	255.255.255.255	DHCP	352 DHCP Request	- Transaction ID 0xafa2140c
212	10.673606	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x899ba273
271	12.787544	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x899ba273
302	14.301297	191.16.11.129	191.16.1.2	DHCP	342 DHCP Release	- Transaction ID 0x8e4f28a9
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342 DHCP Offer	- Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372 DHCP Request	- Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360 DHCP Request	- Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xa1849ec8
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342 DHCP Release	- Transaction ID 0x45d1c3a3
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0x1efc5691
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342 DHCP Offer	- Transaction ID 0x1efc5691
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372 DHCP Request	- Transaction ID 0x1efc5691
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0x1efc5691

Seconds elapsed: 0	
Bootp flags: 0x0000 (Unicast)	
Client IP address: 0.0.0.0	
Your (client) IP address: 0.0.0.0	
Next server IP address: 0.0.0.0	
Relay agent IP address: 0.0.0.0	
Client MAC address: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)	
Client hardware address padding: 00000000000000000000	
Server host name not given	
Boot file name not given	
Magic cookie: DHCP	
Option: (53) DHCP Message Type (Discover)	
Length: 1	
DHCP: Discover (1)	
Option: (61) Client identifier	
Length: 7	
Hardware type: Ethernet (0x01)	
Client MAC address: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)	
Option: (50) Requested IP Address (191.16.11.129)	
Length: 4	
Requested IP Address: 191.16.11.129	

5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

34	2.343502	0.0.0.0	255.255.255.255	DHCP	352 DHCP Request	- Transaction ID 0xafa2140c
212	10.673606	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x899ba273
271	12.787544	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x899ba273
302	14.301297	191.16.11.129	191.16.1.2	DHCP	342 DHCP Release	- Transaction ID 0x8e4f28a9
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342 DHCP Offer	- Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372 DHCP Request	- Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360 DHCP Request	- Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xa1849ec8
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342 DHCP Release	- Transaction ID 0x45d1c3a3
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0x1efc5691
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342 DHCP Offer	- Transaction ID 0x1efc5691
2408	46.385933	0.0.0.0	255.255.255.255	DHCP	372 DHCP Request	- Transaction ID 0x1efc5691
2409	46.402067	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0x1efc5691

- First four Transaction-ID: 0xdeed530d
- Second four Transaction-ID: 0x1efc5691 (I get the third one as a second one)
- Purpose: enabling the client to identify the related dhcp answer to each request

6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP



address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

344	20.077021	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover	- Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer	- Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request	- Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0xdeed530d

	Src IP	Dest IP
Discover	0.0.0.0	255.255.255.255
- Offer	191.16.1.2	191.16.11.129
Request	0.0.0.0	255.255.255.255
ACK	191.16.1.2	191.16.11.129

7. What is the IP address of your DHCP server?

- IP address of DHCP server: 191.16.1.2

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

- IP address offer: 191.16.11.129

UDP payload (300 bytes)

Dynamic Host Configuration Protocol (Offer)

Message type: Boot Reply (2)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xdeed530d

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 191.16.11.129

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: Intel\_0f:cd:e1 (2c:6d:c1:0f:cd:e1)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Offer)

Length: 1

DHCP: Offer (2)

Option: (54) DHCP Server Identifier (191.16.1.2)

Length: 4

DHCP Server Identifier: 191.16.1.2

Option: (51) IP Address Lease Time

Length: 4

IP Address Lease Time: 5 minutes (300)

Option: (58) Renewal Time Value

Length: 4

Renewal Time Value: 2 minutes, 30 seconds (150)

Option: (59) Rebinding Time Value

Length: 4

9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?

- A value of 0.0.0.0 indicates that there is no relay agent.

10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Offer)

Length: 1

DHCP: Offer (2)

Option: (54) DHCP Server Identifier (191.16.1.2)

Length: 4

DHCP Server Identifier: 191.16.1.2

Option: (51) IP Address Lease Time

Length: 4

IP Address Lease Time: 5 minutes (300)

Option: (58) Renewal Time Value

Length: 4

Renewal Time Value: 2 minutes, 30 seconds (150)

Option: (59) Rebinding Time Value

Length: 4

```

IP Address Lease Time: 5 minutes (300)
  Option: (58) Renewal Time Value
    Length: 4
    Renewal Time Value: 2 minutes, 30 seconds (150)
  Option: (59) Rebinding Time Value
    Length: 4
    Rebinding Time Value: 4 minutes, 22 seconds (262)
  Option: (1) Subnet Mask (255.255.0.0)
    Length: 4
    Subnet Mask: 255.255.0.0
  Option: (3) Router
    Length: 4
    Router: 191.16.1.2
  Option: (6) Domain Name Server
    Length: 4
    Domain Name Server: 191.16.1.2
  Option: (255) End
    Option End: 255
    Padding: 00000000000000000000000000000000

```

- The router line indicates where the client should send messages by default.
- The subnet mask line tells the client which subnet mask to use.

11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

- The client accept this IP address because the request IP address is the same with the offer one in **request field**

302	14.301297	191.16.11.129	191.16.1.2	DHCP	342	DHCP Release	- Transaction ID 0x8e4f28a9
344	20.077021	0.0.0.0	255.255.255.255	DHCP	345	DHCP Discover	- Transaction ID 0xdeed530d
379	21.080930	191.16.1.2	191.16.11.129	DHCP	342	DHCP Offer	- Transaction ID 0xdeed530d
381	21.083443	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request	- Transaction ID 0xdeed530d
382	21.091061	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0xdeed530d
415	21.392952	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0x825781d7
443	21.816303	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request	- Transaction ID 0x34d708ab
857	23.126717	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0x825781d7
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360	DHCP Request	- Transaction ID 0xa1849ec8
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342	DHCP ACK	- Transaction ID 0xa1849ec8

```

Transaction ID: 0xdeed530d
Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
  Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)
  Option: (50) Requested IP Address (191.16.11.129)
    Length: 4
    Requested IP Address: 191.16.11.129
  Option: (54) DHCP Server Identifier (191.16.1.2)
    Length: 4
    DHCP Server Identifier: 191.16.1.2
  Option: (12) Host Name

```

12. Explain the purpose of the lease time. How long is the lease time in your experiment?

- A lease time is supplied along with the configuration information that DHCP transmits to a client. The client is permitted to use the allocated IP address for this amount of time
- The lease time in my experiment: 5 minutes

857	23.126717	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request	- Transaction ID 0x8257
1593	26.485541	191.16.11.129	191.16.1.2	DHCP	360 DHCP Request	- Transaction ID 0xa184
1606	26.490328	191.16.1.2	191.16.11.129	DHCP	342 DHCP ACK	- Transaction ID 0xa184
2345	38.069962	191.16.11.129	191.16.1.2	DHCP	342 DHCP Release	- Transaction ID 0x45d1
2406	46.242941	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0x1efc
2407	46.383644	191.16.1.2	191.16.11.129	DHCP	342 DHCP Offer	- Transaction ID 0x1efc

```

Client MAC address: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
  Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
  Option: (54) DHCP Server Identifier (191.16.1.2)
    Length: 4
    DHCP Server Identifier: 191.16.1.2
  Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: 5 minutes (300)
  Option: (58) Renewal Time Value
    Length: 4
    Renewal Time Value: 2 minutes, 30 seconds (150)
  Option: (59) Rebinding Time Value
    Length: 4
    Rebinding Time Value: 4 minutes, 22 seconds (262)
  Option: (1) Subnet Mask (255.255.0.0)
    Length: 4
    Subnet Mask: 255.255.0.0

```

13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

- DHCP Release Message is the request to release the IP back to the DHCP Server.
- There is no ACK for this.
- Nothing happens if the release message is lost. The client will continue operation until its IP lease expires.

14. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

- Yes, there are many ARP packets
- An ARP request is sent when a device needs a MAC address associated with an IP address, and it does not have an entry for the IP address in its ARP table. This is used to map MACs to IPs in the local network.

No.	Time	Source	Destination	Protocol	Length	Info
1020	23.540977	DrayTek_12:5a:18	Broadcast	ARP	60	Who has 191.16.12.78? Tell 191.16.1.2
1300	24.041173	76:77:0b:65:51:5c	Broadcast	ARP	42	ARP Announcement for 191.16.10.24
1310	24.152818	Intel_5f:09:33	Broadcast	ARP	42	Who has 191.16.11.189? (ARP Probe)
1381	24.350941	Intel_0f:cd:e1	Broadcast	ARP	42	ARP Announcement for 191.16.11.129
1396	24.452760	76:77:0b:65:51:5c	Broadcast	ARP	42	ARP Announcement for 191.16.10.24
1417	24.599655	DrayTek_12:5a:18	Broadcast	ARP	60	Who has 191.16.12.78? Tell 191.16.1.2
1445	24.763782	76:77:0b:65:51:5c	Broadcast	ARP	42	ARP Announcement for 191.16.10.24
1446	24.763782	76:77:0b:65:51:5c	Broadcast	ARP	42	Who has 191.16.1.2? Tell 191.16.10.24
1460	25.069786	Intel_5f:09:33	Broadcast	ARP	42	ARP Announcement for 191.16.11.189
1484	25.220575	76:77:0b:65:51:5c	Broadcast	ARP	42	Who has 191.16.1.2? Tell 191.16.10.24
1493	25.595528	DrayTek_12:5a:18	Broadcast	ARP	60	Who has 191.16.12.78? Tell 191.16.1.2
1533	26.356698	Intel_0f:cd:e1	Broadcast	ARP	42	ARP Announcement for 191.16.11.129
1894	27.114611	Intel_5f:09:33	Broadcast	ARP	42	ARP Announcement for 191.16.11.189
2016	28.241686	DrayTek_12:5a:18	Broadcast	ARP	60	Who has 191.16.11.177? Tell 191.16.1.2
2084	28.889856	TPLink_89:17:c2	Broadcast	ARP	60	Who has 191.16.10.61? (ARP Probe)
2096	29.265863	DrayTek_12:5a:18	Broadcast	ARP	60	Who has 191.16.10.179? Tell 191.16.1.2
2113	29.673810	CloudNetwork_1e:0c:...	Broadcast	ARP	60	Who has 169.254.169.254? Tell 191.16.10.172
2125	30.189456	DrayTek_12:5a:18	Broadcast	ARP	60	Who has 191.16.11.177? Tell 191.16.1.2
2132	30.405805	DrayTek_12:5a:18	Broadcast	ARP	60	Who has 191.16.10.156? Tell 191.16.1.2
2139	31.007309	CloudNetwork_1e:0c:...	Broadcast	ARP	60	Who has 169.254.169.254? Tell 191.16.10.172
2145	31.007309	DrayTek_12:5a:18	Broadcast	ARP	60	Who has 191.16.12.117? Tell 191.16.1.2
2146	31.007309	TPLink_89:17:c2	Broadcast	ARP	60	ARP Announcement for 191.16.10.61
2169	31.390797	DrayTek_12:5a:18	Intel_0f:cd:e1	ARP	60	Who has 191.16.11.129? Tell 191.16.1.2



# Lab 5a - IP

Thursday, October 24, 2024 5:00 PM

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.

The screenshot shows a Wireshark packet capture. The packet list pane displays several ICMP Echo (ping) requests and replies. The first packet (No. 154) is selected, and the packet details pane shows the expanded Internet Protocol section. The packet is an ICMP Echo (ping) request from 191.16.11.129 to 128.119.245.12. The packet details pane shows the following information:

- Frame 154: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF\_{40F9FDDA-9151-...}
- Ethernet II, Src: Intel\_0f:cd:e1 (2c:6d:c1:0f:cd:e1), Dst: DrayTek\_12:5a:18 (00:1d:aa:12:5a:18)
- Internet Protocol Version 4, Src: 191.16.11.129, Dst: 128.119.245.12
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 520
  - Identification: 0xa3fe (41982)
  - 000. .... = Flags: 0x0
  - ...0 0000 1011 1001 = Fragment Offset: 1480
  - Time to Live: 255
  - Protocol: ICMP (1)
  - Header Checksum: 0xd527 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 191.16.11.129
  - Destination Address: 128.119.245.12
  - [2 IPv4 Fragments (1980 bytes): #153(1480), #154(500)]
  - [Stream index: 17]
- Internet Control Message Protocol

- IP address: 191.16.11.129
2. Within the IP packet header, what is the value in the upper layer protocol field?
    - The value of the upper layer protocol field is ICMP (0X01)

The screenshot shows the packet details pane for the selected packet. The Internet Protocol section is expanded, showing the following information:

- Ethernet II, Src: Intel\_0f:cd:e1 (2c:6d:c1:0f:cd:e1), Dst: DrayTek\_12:5a:18 (00:1d:aa:12:5a:18)
- Internet Protocol Version 4, Src: 191.16.11.129, Dst: 128.119.245.12
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 520
  - Identification: 0xa3fe (41982)
  - 000. .... = Flags: 0x0
  - ...0 0000 1011 1001 = Fragment Offset: 1480
  - Time to Live: 255
  - Protocol: ICMP (1)
  - Header Checksum: 0xd527 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 191.16.11.129
  - Destination Address: 128.119.245.12
  - [2 IPv4 Fragments (1980 bytes): #153(1480), #154(500)]
  - [Stream index: 17]
- Internet Control Message Protocol

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
  - There are 20 bytes in the IP header which leaves 36 bytes for the payload of the IP datagram because we were sending a packet of length 56 bytes.

```

▶ Ethernet II, Src: Intel_0f:cd:e1 (2c:6d:c1:0f:cd:e1), Dst: DrayTek_12:5a:18 (00:1d:aa:12:5a:18)
▼ Internet Protocol Version 4, Src: 191.16.11.129, Dst: 128.119.245.12
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0xa3fe (41982)
  ▶ 000. .... = Flags: 0x0
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0xd527 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 191.16.11.129
  Destination Address: 128.119.245.12
  ▶ [2 IPv4 Fragments (1980 bytes): #153(1480), #154(500)]
    [Stream index: 17]
▶ Internet Control Message Protocol

```

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

- The fragment offset is set to 0, therefore, the packet has not been fragmented.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer? It is the header checksum and identification

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

Constant:

- Version (IPv4)
- Header length
- IP source (because of sending from same place)
- IP destination (because of contacting the same site\_
- Upper layer protocol (always using ICMP)

Must stay constant:

- Same as above

Must change:

- Header checksum (header changes)
- Identification (to verify packets)

7. Describe the pattern you see in the values in the Identification field of the IP datagram

The identification field's value increases by 1 in each request

8. What is the value in the Identification field and the TTL field?

```

  Identification: 0xa400 (41984)
  ▶ 000. .... = Flags: 0x0
  ...0 0000 1011 1001 = Fragment Offset: 1480
  ▶ Time to Live: 2

```

- Identification: 41984
- TTL: 2

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

- The Identification field varies across all replies since it needs to have a unique value. If two or more replies share the same value, it indicates that they are fragments of a larger packet.
- The TTL field remains unchanged because the time to live for the first hop router is consistent.

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

```

▼ Internet Protocol Version 4, Src: 191.16.11.129, Dst: 128.119.245.12
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 1500
  Identification: 0xa3fe (41982)
  ▶ 001. .... = Flags: 0x1, More fragments
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0xb20c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 191.16.11.129
  Destination Address: 128.119.245.12
  [Reassembled IPv4 in frame: 154]
  [Stream index: 17]

```







Thursday, October 24, 2024 5:50 PM

What is the IP address of the client?

IP address of client: 192.168.1.100

```

46 03:43:02.334012 74.125.106.31 192.168.1.100 HTTP 1009 HTTP/1.1 200 OK (application/vnd.google.safebrowsing-chunk)
47 03:43:02.467731 74.125.106.31 192.168.1.100 TCP 54 4331 + 80 [ACK] Seq=2876 Ack=20452 Win=20176 Len=0
48 03:43:02.548423 192.168.1.100 69.183.241.120 UDP 153 15525 + 41490 Len=111
49 03:43:02.598576 69.183.241.120 ICMP 126 Destination unreachable (Port unreachable)
50 03:43:06.269041 192.168.1.100 10.119.240.64 SNMP 120 get-request 1.3.6.1.2.1.25.3.2.1.5.1.3.6.1.2.1.25.3.5.1.1.3.6.1.2.1.25.3.5.1.2.1
51 03:43:07.329044 192.168.1.100 DNS 68 87.71.230 74 Standard query 0x0da A www.google.com
52 03:43:07.344932 48.87.71.230 192.168.1.100 DNS 158 Standard query response 0x0da A www.google.com CHAIN www.1.google.com A 64.233.169.104
53 03:43:07.344792 192.168.1.100 64.233.169.104 TCP 66 4335 + 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WScale=0 SACK_PERM=0
54 03:43:07.378121 64.233.169.104 192.168.1.100 TCP 66 80 + 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1030 SACK_PERM=0
55 03:43:07.378180 192.168.1.100 64.233.169.104 TCP 54 4335 + 80 [ACK] Seq=1 Ack=1 Win=20176 Len=0
56 03:43:07.378482 192.168.1.100 64.233.169.104 HTTP 689 GET / HTTP/1.1
57 03:43:07.409063 64.233.169.104 192.168.1.100 TCP 60 80 + 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
58 03:43:07.427567 64.233.169.104 192.168.1.100 TCP 1484 80 + 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP PDU reassembled in 60]
59 03:43:07.427896 64.233.169.104 192.168.1.100 TCP 1484 80 + 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP PDU reassembled in 60]
60 03:43:07.427932 64.233.169.104 192.168.1.100 HTTP 814 HTTP/1.1 200 OK (text/html)
61 03:43:07.427979 192.168.1.100 64.233.169.104 TCP 54 4335 + 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
62 03:43:07.550534 192.168.1.100 HTTP 715 GET /intl/en_ALL/images/logo.gif HTTP/1.1
63 03:43:07.561554 192.168.1.100 TCP 399 80 + 4335 [PSH, ACK] Seq=3621 Ack=1381 Win=8320 Len=255 [TCP PDU reassembled in 73]
64 03:43:07.564711 64.233.169.104 192.168.1.100 TCP 1484 80 + 4335 [ACK] Seq=3875 Ack=1381 Win=8320 Len=1430 [TCP PDU reassembled in 73]
65 03:43:07.584776 192.168.1.100 TCP 54 4335 + 80 [ACK] Seq=1301 Ack=5306 Win=201716 Len=0
66 03:43:07.585055 64.233.169.104 192.168.1.100 TCP 1484 80 + 4335 [ACK] Seq=5306 Ack=1381 Win=8320 Len=1430 [TCP PDU reassembled in 73]

```

The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes) into the Filter: field in Wireshark .

No.	Time	Source	Destination	Protocol	Length	Info
56	03:43:07.378402	192.168.1.100	64.233.169.104	HTTP	689	GET / HTTP/1.1
60	03:43:07.427932	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	03:43:07.550534	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_all/images/logo.gif HTTP/1.1
73	03:43:07.618586	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	03:43:07.639320	192.168.1.100	64.233.169.104	HTTP	889	GET /extern_js/f/cgllbhICd0Mv8oBwUAtLcSuDjglHCsuFjqQcswZgDGLcSwGtgTJLcswHTgTLcsw HTTP/1.1 200 OK (text/javascript)
94	03:43:07.717784	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
96	03:43:07.761459	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/se0eddb3clka2c.js HTTP/1.1
100	03:43:07.800644	64.233.169.104	192.168.1.100	HTTP	370	HTTP/1.1 200 OK (text/html)
107	03:43:07.921971	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	03:43:07.951406	192.168.1.100	64.233.169.104	HTTP	896	GET /csi?v=3&webAction=&tram=undefined&e=37259,21588,21766,21920&ei=25025xsb164_Ce3w HTTP/1.1 200 OK (PNG)
119	03:43:07.954921	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	03:43:07.978625	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1
124	03:43:08.000618	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content
127	03:43:08.032636	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)	0000	00 22 6b 45 1f 1b 00 22 68 0d ca bf 00 00 45 00	"kE..." h.... E-
Ethernet II, Src: HnMtlalPrcis_Bdica:bf (00:22:6b:0d:ca:bf), Dst: Ciscollinksys_451f:1b (00:22:6b:45:1f:1b)		0010	02 a3 ad ac 40 00 00 00 36 a5 ea c0 a0 01 64 40 e9	...@... J...dp
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104		0020	a9 67 6f 6c 6e 50 f8 32 06 4e 00 48 3f 95 50 18	...P-2 .6 .0B P
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq.: 1, Ack: 1, Len: 635		0030	f6 14 aa f3 00 0a 48 45 54 20 2f 20 48 54 54 50	.....GE T / HTTP
Hypertext Transfer Protocol		0040	2f 31 2e 31 9d 0a 48 6f 73 74 3a 20 77 77 77 2e	/I..H st: sss
		0050	67 6f 6f 6c 6e 2a 2e 63 6f 6d 0a 55 73 65 72	gongle-...s...g
		0060	2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 63 2f	-Agent: Mozilla/
		0070	35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b	5.0 (Win down; U;
		0080	20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b	Windows NT 5.1;
		0090	20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 39 2e 3b	en-US; rv:1.9.0
		00a0	2e 31 34 29 28 47 65 63 60 6f 2f 32 30 39 30	.14) Sec ko/20090
		00b0	38 32 37 30 37 20 46 69 72 65 66 6f 78 2f 33 2e	8270? fi ref=33.2
		00c0	30 2e 31 34 20 28 4e 45 54 20 43 4c 52 30 33	0.14 [N ET CLR 3.
		00d0	2e 35 2e 33 30 37 32 39 29 0d 0a 41 63 63 65 70	.5.30729 ) Accp
		00e0	74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70	t: text/html,app
		00f0	6c 69 63 61 74 69 6f 6e 2f 78 68 74 6c 6c 2b 78	lication/xhtml+xml
		0100	6d 6c 2e 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	ml,application/x
		0110	6d 6c 3b 71 3d 30 2e 39 2a 2f 2f 2a 3b 71 3d 30	mjpeg,qvga,z
		0120	2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75	& Accpt=langua
		0130	61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e 3b 71 3d	age: en-us,en;q

Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and

TCP source and destination ports on the IP datagram carrying this HTTP GET?

Source IP address: 192.168.1.100, destination IP address: 64.233.169.104

```
Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits) on interface 0  
Ethernet II, Src: HonHaiPrecis_0d:ca:8f (00:22:68:0d:ca:8f), Dst: CiscoLinksys_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
```

TCP source port: 4335 , TCP destination port: 80

```
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635  
Source Port: 4335  
Destination Port: 80
```

At what time is the corresponding 200 OK HTTP message received from the Google server?  
What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

56	03:43:07.378402	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1
60	03:43:07.427932	64.233.169.104	192.168.1.100	HTTP	814 HTTP/1.1 200 OK (text/html)
62	03:43:07.550534	192.168.1.100	64.233.169.104	HTTP	719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	03:43:07.618586	64.233.169.104	192.168.1.100	HTTP	226 HTTP/1.1 200 OK (GIF89a)

```
Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits) on interface 0  
Ethernet II, Src: CiscoLinksys_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPrecis_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  
[3 Reassembled TCP Segments (3620 bytes): #58(1430), #59(1430), #60(760)]  
Hypertext Transfer Protocol  
Line-based text data: text/html (12 lines)
```

Time: 03:43:07.427932

Source IP: 64.233.169.104, Destination IP: 192.168.1.100

Source port: 80, Destination port: 4335

Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter “tcp”, only TCP segments will be displayed by Wireshark).

53	03:43:07.344792	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
54	03:43:07.378121	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 WS=64
55	03:43:07.378188	192.168.1.100	64.233.169.104	TCP	54 4335 → 80 [ACK] Seq=1 Ack=1 Win=268176 Len=0

SYN segment:

Source IP address: 192.168.1.100

Destination IP address: 64.233.169.104



Source port: 4335

Destination port: 80

Time: 03:43:07.244792

ACK response:

Source IP address: 64.233.169.104

Destination IP address: 192.168.1.100

Source port: 80

Destination port: 4335

Time: 03:43:07.378121

ACK received at the client at time: 03:43:07.378188

In the NAT\_ISP\_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where  $t=7.109267$  is time at which this was sent as recorded in the NAT\_home\_side trace file). At what time does this message appear in the NAT\_ISP\_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT\_ISP\_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

85	03:43:07.800232	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
90	03:43:07.848634	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK
93	03:43:07.972421	71.192.34.104	64.233.169.104	HTTP	719	GET /intl/en_ALL/
103	03:43:08.039182	64.233.169.104	71.192.34.104	HTTP	226	HTTP/1.1 200 OK
106	03:43:08.061195	71.192.34.104	64.233.169.104	HTTP	809	GET /extern_js/f/
121	03:43:08.138430	64.233.169.104	71.192.34.104	HTTP	648	HTTP/1.1 200 OK
125	03:43:08.183334	71.192.34.104	64.233.169.104	HTTP	695	GET /extern_chrom
131	03:43:08.227298	64.233.169.104	71.192.34.104	HTTP	870	HTTP/1.1 200 OK
135	03:43:08.264283	71.192.34.104	74.125.91.113	HTTP	709	GET /generate_204
137	03:43:08.321770	74.125.91.113	71.192.34.104	HTTP	179	HTTP/1.1 204 No C
139	03:43:08.343865	71.192.34.104	64.233.169.104	HTTP	712	GET /images/nav_l
141	03:43:08.373770	71.192.34.104	64.233.169.104	HTTP	800	GET /images/nav_l

> Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)	000
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)	001
> Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104	002
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635	003
> Hypertext Transfer Protocol	004
	005
	006

Time sent: 03:43:07.800232

Source IP: 71.192.34.104, Destination IP: 64.233.169.104

Source port: 4335, Destination port: 80

The IP address of source has changed compared to question 3.

Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

No fields in the HTTP GET message has changed

The checksum field in the IP datagram carrying the HTTP GET is changed

The checksum change because the IP source address has changed

In the NAT\_ISP\_side trace file, at what time is the first 200 OK HTTP message received from

the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

Time: 03:43:07.848634

Source IP address: 64.233.169.104, Destination IP address: 71.192.34.104

Source port: 80, Destination port: 4335

The destination IP address has changed

85	03:43:07.800232	71.192.34.104	64.233.169.104	HTTP	689 GET / HTTP/1.1
90	03:43:07.848634	64.233.169.104	71.192.34.104	HTTP	814 HTTP/1.1 200 OK (text/html)
93	03:43:07.972421	71.192.34.104	64.233.169.104	HTTP	719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
103	03:43:08.039182	64.233.169.104	71.192.34.104	HTTP	226 HTTP/1.1 200 OK (GIF89a)
106	03:43:08.061195	71.192.34.104	64.233.169.104	HTTP	809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswOjg
121	03:43:08.138430	64.233.169.104	71.192.34.104	HTTP	648 HTTP/1.1 200 OK (text/javascript)
125	03:43:08.183334	71.192.34.104	64.233.169.104	HTTP	695 GET /extern_chrone/ee36edbd3c16alc5.js HTTP/
131	03:43:08.227298	64.233.169.104	71.192.34.104	HTTP	870 HTTP/1.1 200 OK (text/html)
135	03:43:08.264283	71.192.34.104	74.125.91.113	HTTP	709 GET /generate_204 HTTP/1.1
137	03:43:08.321770	74.125.91.113	71.192.34.104	HTTP	179 HTTP/1.1 204 No Content
139	03:43:08.343865	71.192.34.104	64.233.169.104	HTTP	732 GET /images/nav_logo7.png HTTP/1.1

> Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)	0000 00 08 74 4f 36 23 00 0e
> Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)	0010 03 20 f6 1e 00 00 33 06
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104	0020 22 68 00 50 10 ef e9 4f
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760	0030 00 6e aa 39 00 00 b6 ca
> [3 Reassembled TCP Segments (3620 bytes): #88(1430), #89(1430), #90(760)]	0040 e3 f0 a2 aa e3 94 1b 70
> Hypertext Transfer Protocol	0050 94 b4 16 21 25 59 3c 02
> Line-based text data: text/html (12 lines)	0060 1c 57 44 ed 14 89 e5 f8
	0070 4b 37 2c 3b 8a a1 32 42
	0080 c4 79 49 5f 6c b5 a5 c5

In the NAT\_ISP\_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

82	03:43:07.766539	71.192.34.104	64.233.169.104	TCP	66 4335 → 80 [SYN] Seq=0 Min=65535 Len=0 MSS=1460 WS=4 SACK_PERM
83	03:43:07.798839	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 WS=64

SYN segment

Time: 03:43:07.766539

Source IP: 71.192.34.104, Destination IP: 64.233.169.104

Source port: 4335, Destination port: 80

ACK segment

Time: 03:43:07.798839

Source IP: 64.233.169.104, Destination IP: 71.192.34.104

Source port: 80, Destination port: 4335

For the SYN, the source IP address has changed, while for the ACK, the destination IP address has changed

Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

NAT translation table

WAN: 71.192.34.104, 4335

LAN: 192.168.1.100, 4335