



A U B U R N
U N I V E R S I T Y

COMP 4320

Introduction to Computer Networks

Project #: Lab 2

Logan Bolton

10/17/2025

Executive Summary

This report analyzes the behavior of TCP, UDP, and IPv4/IPv6 protocols using Wireshark packet captures and traceroute tests.

Table of Contents

Table of Contents

Executive Summary	2
Table of Contents	3
1 Part 1 – TCP	4
1.1 Beginning Questions.....	4
1.2 TCP Basics.....	5
1.3 TCP congestion control in action	9
2 Part 2 – UDP	9
2.1 UDP Packet Information.....	9
1. There are four fields: 4 fields: Source Port, Destination Port, Length and Checksum.	9
3 Part 3 - Traceroute	12
3.1 IPv4 vs IPv6	12
4 AI Use Reflation Statement.....	16

1 Part 1 – TCP

1.1 Beginning Questions

1. My IP address is 192.191.190.193 and my port number is 56100.

327	6.928213	192.191.190.193	35.186.224.45	TLSv1.2	109	Application Data	
328	6.931969	40.126.28.12	192.191.190.193	TCP	60	443 → 57904 [RST]	
329	6.940799	0.307312000	217.21.95.185	TCP	66	80 → 56100 [ACK]	
330	6.940801	0.307076000	217.21.95.185	TCP	66	80 → 56100 [ACK]	
331	6.940802	0.307053000	217.21.95.185	TCP	66	80 → 56100 [ACK]	
332	6.940974	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
333	6.941044	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
334	6.941046	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
335	6.941064	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
336	6.941065	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
337	6.941077	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
338	6.941080	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
339	6.941083	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
340	6.941085	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
341	6.941088	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
342	6.941091	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
343	6.941093	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
344	6.941096	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
345	6.941099	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
346	6.941100	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
347	6.941102	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	
348	6.941103	192.191.190.193	217.21.95.185	TCP	1514	56100 → 80 [ACK]	

> Frame 332: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
> Ethernet II, Src: Apple_33:36:98 (00:a9:97:33:36:98), Dst: 02:ff:5b:79:4b:00 (02:ff:5b:79:4b:00)
> Internet Protocol Version 4, Src: 192.191.190.193, Dst: 217.21.95.185
▼ Transmission Control Protocol, Src Port: 56100, Dst Port: 80, Seq: 13695, Ack: 1, Len: 1448
 Source Port: 56100
 Destination Port: 80
 [Stream index: 20]
 [Stream Packet Number: 17]
 > [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 1448]
 Sequence Number: 13695 (relative sequence number)
 Sequence Number (raw): 2125700341
 [Next Sequence Number: 15143 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 1844185029
 1000 = Header Length: 32 bytes (8)
 > Flags: 0x010 (ACK)
 Window: 2058
 [Calculated window size: 131712]

Transmission Control Protocol

2. The server IP address is 217.21.95.185. The port number is 80.

331	6.940802	0.307053000	217.21.95.185	192.191.190.193	TCP	66	8
332	6.940974		192.191.190.193	217.21.95.185	TCP	1514	5
333	6.941044		192.191.190.193	217.21.95.185	TCP	1514	5
334	6.941046		192.191.190.193	217.21.95.185	TCP	1514	5
335	6.941064		192.191.190.193	217.21.95.185	TCP	1514	5
336	6.941065		192.191.190.193	217.21.95.185	TCP	1514	5
337	6.941077		192.191.190.193	217.21.95.185	TCP	1514	5
338	6.941080		192.191.190.193	217.21.95.185	TCP	1514	5
339	6.941083		192.191.190.193	217.21.95.185	TCP	1514	5
340	6.941085		192.191.190.193	217.21.95.185	TCP	1514	5
341	6.941088		192.191.190.193	217.21.95.185	TCP	1514	5
342	6.941091		192.191.190.193	217.21.95.185	TCP	1514	5
343	6.941093		192.191.190.193	217.21.95.185	TCP	1514	5
344	6.941096		192.191.190.193	217.21.95.185	TCP	1514	5
345	6.941099		192.191.190.193	217.21.95.185	TCP	1514	5
346	6.941100		192.191.190.193	217.21.95.185	TCP	1514	5
347	6.941102		192.191.190.193	217.21.95.185	TCP	1514	5
348	6.941103		192.191.190.193	217.21.95.185	TCP	1514	5

> Frame 332: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, i
> Ethernet II, Src: Apple_33:36:98 (80:a9:97:33:36:98), Dst: 02:ff:5b:79:4b:00 (02:ff:5b:79:4b:00)
> Internet Protocol Version 4, Src: 192.191.190.193, Dst: 217.21.95.185
▼ Transmission Control Protocol, Src Port: 56100, Dst Port: 80, Seq: 13695, Ack: 1, Len: 1448
 Source Port: 56100
 Destination Port: 80
 [Stream index: 20]
 [Stream Packet Number: 17]
 [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 1448]

1.2 TCP Basics

1. The segment that initiates the connection has a relative sequence number of 0. It can be identified by how it says [SYN] and Seq=0 in the info.

```
> Frame 258: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0  
> Ethernet II, Src: Apple_33:36:98 (80:a9:97:33:36:98), Dst: 02:ff:5b:79:4b:00 (02:ff:5b:79:4b:00)  
> Internet Protocol Version 4, Src: 192.191.190.193, Dst: 217.21.95.185  
▼ Transmission Control Protocol, Src Port: 56099, Dst Port: 80, Seq: 0, Len: 0  
    Source Port: 56099  
    Destination Port: 80  
    [Stream index: 19]  
    [Stream Packet Number: 1]  
    [Conversation completeness: Incomplete_ESTABLISHED (7)]  
    [TCP Segment Len: 0]  
    Sequence Number: 0 (relative sequence number)  
    Sequence Number (raw): 4107981164  
    Next Sequence Number: 1 (relative sequence number)  
    Acknowledgment Number: 0  
    Acknowledgment number (raw): 0  
    1011 .... = Header Length: 44 bytes (11)  
    > Flags: 0x002 (SYN)  
    Window: 65535  
    [Calculated window size: 65535]  
    Flags (tcp.flags), 12 bits
```

2. The sequence number of the reply is 0. The value of the acknowledgement field is 1. Since the seq value was 0, the ack value was +1, resulting in the value 1. [SYN, ACK] in the info identifies it as a SYNACK segment.

```

> Frame 303: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0
> Ethernet II, Src: 02:ff:5b:79:4b:00 (02:ff:5b:79:4b:00), Dst: Apple_33:36:98 (80:a9:97:33:36:98)
> Internet Protocol Version 4, Src: 217.21.95.185, Dst: 192.191.190.193
> Transmission Control Protocol, Src Port: 80, Dst Port: 56100, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 56100
    [Stream index: 20]
    [Stream Packet Number: 2]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0      (relative sequence number)
    Sequence Number (raw): 1844185028
    [Next Sequence Number: 1      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 2125686647
    1010 .... = Header Length: 40 bytes (10)
    Flags: 0x012 (SYN, ACK)
    Window: 31856
    [Calculated window size: 31856]
    Checksum: 0xb904 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
    > [Timestamps]
    > [SEQ/ACK analysis]

```

3. The sequence number of the segment containing the POST command was 148359.

No.	Time	Rtt	Source	Destination	Protocol	Length	Info
471	7.617598		192.191.190.193	217.21.95.185	HTTP	1101	POST /upload.php HTTP/1.1

```

> Frame 471: 1101 bytes on wire (8808 bits), 1101 bytes captured (8808 bits) on interface en0, id 0
> Ethernet II, Src: Apple_33:36:98 (80:a9:97:33:36:98), Dst: 02:ff:5b:79:4b:00 (02:ff:5b:79:4b:00)
> Internet Protocol Version 4, Src: 192.191.190.193, Dst: 217.21.95.185
> Transmission Control Protocol, Src Port: 56100, Dst Port: 80, Seq: 148359, Ack: 1, Len: 1035
    Source Port: 56100
    Destination Port: 80
    [Stream index: 20]
    [Stream Packet Number: 132]
    > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1035]
    Sequence Number: 148359      (relative sequence number)
    Sequence Number (raw): 2125835005
    [Next Sequence Number: 149394      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 1844185029
    1000 .... = Header Length: 32 bytes (8)
    > Flags: 0x018 (PSH, ACK)
    Window: 2058
    [Calculated window size: 131712]
    [Window size scaling factor: 64]
    Checksum: 0xf3a5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    > [Timestamps]
    > [SEQ/ACK analysis]
    TCP payload (1035 bytes)
    TCP segment data (1035 bytes)
    > [104 Reassembled TCP Segments (149393 bytes): #305(662), #306(1448), #307(1448), #308(1448), #309(1448), #310(1448), #311(1448), #312(1448), #313(1448), #314(1448), #315(1448), #316(1448), #317(1448), #318(1448), #319(1448), #320(1448), #321(1448), #322(1448), #323(1448), #324(1448), #325(1448), #326(1448), #327(1448), #328(1448), #329(1448), #330(1448), #331(1448), #332(1448), #333(1448), #334(1448), #335(1448), #336(1448), #337(1448), #338(1448), #339(1448), #340(1448), #341(1448), #342(1448), #343(1448), #344(1448), #345(1448), #346(1448), #347(1448), #348(1448), #349(1448), #350(1448), #351(1448), #352(1448), #353(1448), #354(1448), #355(1448), #356(1448), #357(1448), #358(1448), #359(1448), #360(1448), #361(1448), #362(1448), #363(1448), #364(1448), #365(1448), #366(1448), #367(1448), #368(1448), #369(1448), #370(1448), #371(1448), #372(1448), #373(1448), #374(1448), #375(1448), #376(1448), #377(1448), #378(1448), #379(1448), #380(1448), #381(1448), #382(1448), #383(1448), #384(1448), #385(1448), #386(1448), #387(1448), #388(1448), #389(1448), #390(1448), #391(1448), #392(1448), #393(1448), #394(1448), #395(1448), #396(1448), #397(1448), #398(1448), #399(1448), #400(1448), #401(1448), #402(1448), #403(1448), #404(1448), #405(1448), #406(1448), #407(1448), #408(1448), #409(1448), #410(1448), #411(1448), #412(1448), #413(1448), #414(1448), #415(1448), #416(1448), #417(1448), #418(1448), #419(1448), #420(1448), #421(1448), #422(1448), #423(1448), #424(1448), #425(1448), #426(1448), #427(1448), #428(1448), #429(1448), #430(1448), #431(1448), #432(1448), #433(1448), #434(1448), #435(1448), #436(1448), #437(1448), #438(1448), #439(1448), #440(1448), #441(1448), #442(1448), #443(1448), #444(1448), #445(1448), #446(1448), #447(1448), #448(1448), #449(1448), #450(1448), #451(1448), #452(1448), #453(1448), #454(1448), #455(1448), #456(1448), #457(1448), #458(1448), #459(1448), #460(1448), #461(1448), #462(1448), #463(1448), #464(1448), #465(1448), #466(1448), #467(1448), #468(1448), #469(1448), #470(1448), #471(1448), #472(1448), #473(1448), #474(1448), #475(1448), #476(1448), #477(1448), #478(1448), #479(1448), #480(1448), #481(1448), #482(1448), #483(1448), #484(1448), #485(1448), #486(1448), #487(1448), #488(1448), #489(1448), #490(1448), #491(1448), #492(1448), #493(1448), #494(1448), #495(1448), #496(1448), #497(1448), #498(1448), #499(1448), #500(1448), #501(1448), #502(1448), #503(1448), #504(1448), #505(1448), #506(1448), #507(1448), #508(1448), #509(1448), #510(1448), #511(1448), #512(1448), #513(1448), #514(1448), #515(1448), #516(1448), #517(1448), #518(1448), #519(1448), #520(1448), #521(1448), #522(1448), #523(1448), #524(1448), #525(1448), #526(1448), #527(1448), #528(1448), #529(1448), #530(1448), #531(1448), #532(1448), #533(1448), #534(1448), #535(1448), #536(1448), #537(1448), #538(1448), #539(1448), #540(1448), #541(1448), #542(1448), #543(1448), #544(1448), #545(1448), #546(1448), #547(1448), #548(1448), #549(1448), #550(1448), #551(1448), #552(1448), #553(1448), #554(1448), #555(1448), #556(1448), #557(1448), #558(1448), #559(1448), #560(1448), #561(1448), #562(1448), #563(1448), #564(1448), #565(1448), #566(1448), #567(1448), #568(1448), #569(1448), #570(1448), #571(1448), #572(1448), #573(1448), #574(1448), #575(1448), #576(1448), #577(1448), #578(1448), #579(1448), #580(1448), #581(1448), #582(1448), #583(1448), #584(1448), #585(1448), #586(1448), #587(1448), #588(1448), #589(1448), #590(1448), #591(1448), #592(1448), #593(1448), #594(1448), #595(1448), #596(1448), #597(1448), #598(1448), #599(1448), #600(1448), #601(1448), #602(1448), #603(1448), #604(1448), #605(1448), #606(1448), #607(1448), #608(1448), #609(1448), #610(1448), #611(1448), #612(1448), #613(1448), #614(1448), #615(1448), #616(1448), #617(1448), #618(1448), #619(1448), #620(1448), #621(1448), #622(1448), #623(1448), #624(1448), #625(1448), #626(1448), #627(1448), #628(1448), #629(1448), #630(1448), #631(1448), #632(1448), #633(1448), #634(1448), #635(1448), #636(1448), #637(1448), #638(1448), #639(1448), #640(1448), #641(1448), #642(1448), #643(1448), #644(1448), #645(1448), #646(1448), #647(1448), #648(1448), #649(1448), #650(1448), #651(1448), #652(1448), #653(1448), #654(1448), #655(1448), #656(1448), #657(1448), #658(1448), #659(1448), #660(1448), #661(1448), #662(1448), #663(1448), #664(1448), #665(1448), #666(1448), #667(1448), #668(1448), #669(1448), #670(1448), #671(1448), #672(1448), #673(1448), #674(1448), #675(1448), #676(1448), #677(1448), #678(1448), #679(1448), #680(1448), #681(1448), #682(1448), #683(1448), #684(1448), #685(1448), #686(1448), #687(1448), #688(1448), #689(1448), #690(1448), #691(1448), #692(1448), #693(1448), #694(1448), #695(1448), #696(1448), #697(1448), #698(1448), #699(1448), #700(1448), #701(1448), #702(1448), #703(1448), #704(1448), #705(1448), #706(1448), #707(1448), #708(1448), #709(1448), #710(1448), #711(1448), #712(1448), #713(1448), #714(1448), #715(1448), #716(1448), #717(1448), #718(1448), #719(1448), #720(1448), #721(1448), #722(1448), #723(1448), #724(1448), #725(1448), #726(1448), #727(1448), #728(1448), #729(1448), #730(1448), #731(1448), #732(1448), #733(1448), #734(1448), #735(1448), #736(1448), #737(1448), #738(1448), #739(1448), #740(1448), #741(1448), #742(1448), #743(1448), #744(1448), #745(1448), #746(1448), #747(1448), #748(1448), #749(1448), #750(1448), #751(1448), #752(1448), #753(1448), #754(1448), #755(1448), #756(1448), #757(1448), #758(1448), #759(1448), #760(1448), #761(1448), #762(1448), #763(1448), #764(1448), #765(1448), #766(1448), #767(1448), #768(1448), #769(1448), #770(1448), #771(1448), #772(1448), #773(1448), #774(1448), #775(1448), #776(1448), #777(1448), #778(1448), #779(1448), #780(1448), #781(1448), #782(1448), #783(1448), #784(1448), #785(1448), #786(1448), #787(1448), #788(1448), #789(1448), #790(1448), #791(1448), #792(1448), #793(1448), #794(1448), #795(1448), #796(1448), #797(1448), #798(1448), #799(1448), #800(1448), #801(1448), #802(1448), #803(1448), #804(1448), #805(1448), #806(1448), #807(1448), #808(1448), #809(1448), #810(1448), #811(1448), #812(1448), #813(1448), #814(1448), #815(1448), #816(1448), #817(1448), #818(1448), #819(1448), #820(1448), #821(1448), #822(1448), #823(1448), #824(1448), #825(1448), #826(1448), #827(1448), #828(1448), #829(1448), #830(1448), #831(1448), #832(1448), #833(1448), #834(1448), #835(1448), #836(1448), #837(1448), #838(1448), #839(1448), #840(1448), #841(1448), #842(1448), #843(1448), #844(1448), #845(1448), #846(1448), #847(1448), #848(1448), #849(1448), #850(1448), #851(1448), #852(1448), #853(1448), #854(1448), #855(1448), #856(1448), #857(1448), #858(1448), #859(1448), #860(1448), #861(1448), #862(1448), #863(1448), #864(1448), #865(1448), #866(1448), #867(1448), #868(1448), #869(1448), #870(1448), #871(1448), #872(1448), #873(1448), #874(1448), #875(1448), #876(1448), #877(1448), #878(1448), #879(1448), #880(1448), #881(1448), #882(1448), #883(1448), #884(1448), #885(1448), #886(1448), #887(1448), #888(1448), #889(1448), #890(1448), #891(1448), #892(1448), #893(1448), #894(1448), #895(1448), #896(1448), #897(1448), #898(1448), #899(1448), #900(1448), #901(1448), #902(1448), #903(1448), #904(1448), #905(1448), #906(1448), #907(1448), #908(1448), #909(1448), #910(1448), #911(1448), #912(1448), #913(1448), #914(1448), #915(1448), #916(1448), #917(1448), #918(1448), #919(1448), #920(1448), #921(1448), #922(1448), #923(1448), #924(1448), #925(1448), #926(1448), #927(1448), #928(1448), #929(1448), #930(1448), #931(1448), #932(1448), #933(1448), #934(1448), #935(1448), #936(1448), #937(1448), #938(1448), #939(1448), #940(1448), #941(1448), #942(1448), #943(1448), #944(1448), #945(1448), #946(1448), #947(1448), #948(1448), #949(1448), #950(1448), #951(1448), #952(1448), #953(1448), #954(1448), #955(1448), #956(1448), #957(1448), #958(1448), #959(1448), #960(1448), #961(1448), #962(1448), #963(1448), #964(1448), #965(1448), #966(1448), #967(1448), #968(1448), #969(1448), #970(1448), #971(1448), #972(1448), #973(1448), #974(1448), #975(1448), #976(1448), #977(1448), #978(1448), #979(1448), #980(1448), #981(1448), #982(1448), #983(1448), #984(1448), #985(1448), #986(1448), #987(1448), #988(1448), #989(1448), #990(1448), #991(1448), #992(1448), #993(1448), #994(1448), #995(1448), #996(1448), #997(1448), #998(1448), #999(1448), #1000(1448)
```

4.

```
[TCP Segment Len: 0]
Sequence Number: 1      (relative sequence number)
Sequence Number (raw): 1844185029
[Next Sequence Number: 1      (relative sequence number)]
Acknowledgment Number: 149394      (relative ack number)
Acknowledgment number (raw): 2125836040
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x010 (ACK)

[Stream Packet Number: 132]
> [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 1035]
Sequence Number: 148359      (relative sequence number)
Sequence Number (raw): 2125835035
[Next Sequence Number: 149394      (relative sequence number)]
Acknowledgment Number: 1      (relative ack number)
Acknowledgment number (raw): 1844185029
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x018 (PSH, ACK)
Window Size: 30208
```

The POST segment has relative sequence number 148359, was sent at 7.617598 s, its first ACK arrived at 7.929438 s, so the RTT = 7.929438 – 7.617598 = 0.311840 s. The initial EstimatedRTT = 311.84 ms

5. The length is 1035.

```
> Frame 471: 1101 bytes on wire (8808 bits), 1101 bytes captured (8808 bits) on interface en0, id 0
> Ethernet II, Src: Apple_33:36:98 (80:a9:97:33:36:98), Dst: 02:ff:5b:79:4b:00 (02:ff:5b:79:4b:00)
> Internet Protocol Version 4, Src: 192.191.190.193, Dst: 217.21.95.185
▼ Transmission Control Protocol, Src Port: 56100, Dst Port: 80, Seq: 148359, Ack: 1, Len: 1035
  Source Port: 56100
  Destination Port: 80
  [Stream index: 20]
  [Stream Packet Number: 132]
> [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 1035]
Sequence Number: 148359      (relative sequence number)
Sequence Number (raw): 2125835035
```

6. The minimum calculated window size was 30208. There was never any throttling through window size 0.

```

Acknowledgegment Number (raw): 2125700571
1000 .... = Header Length: 32 bytes (8)
> Flags: 0x010 (ACK)
Window: 236
[Calculated window size: 30208]
[Window size scaling factor: 128]
Checksum: 0x2b76 [unverified]
[Checksum Status: Unverified]

```

7. There were no retransmissions.

8. The first covering ACK has acknowledgment number 149,394 and it acknowledges 149,394 bytes in total.

```

[Bytes in flight: 70057]
[Bytes sent since last PSH flag: 148731]
TCP payload (339 bytes)
TCP segment data (339 bytes)
[111 Reassembled TCP Segments (149393 bytes):
[Frame: 138, payload: 0-661 (662 bytes)]
[Frame: 139, payload: 662-2035 (1374 bytes)]
[Frame: 140, payload: 2036-3400 (1374 bytes)]

```

9. 149,393 bytes over 0.311840 s gives throughput $\approx 479,069 \text{ B/s} \approx 468 \text{ KB/s} \approx 3.83 \text{ Mb/s}$.

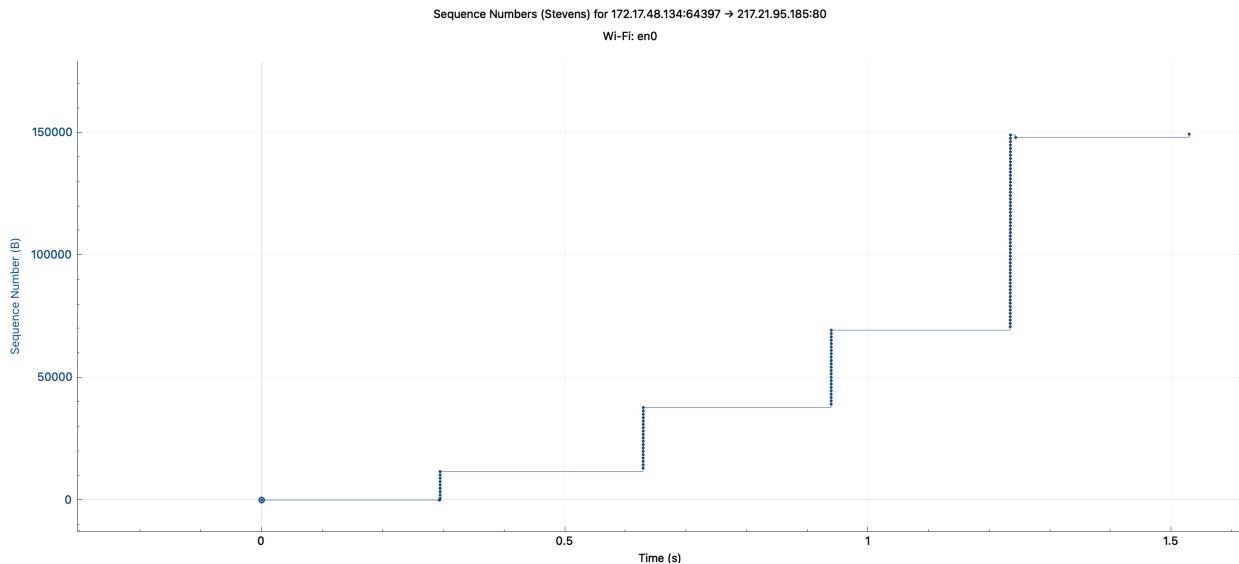
```

> Ethernet II, Src: 02:11:50:79:40:00 (02:11:50:79:40:00), Dst: Apple_35:50:96 (00:a9:97:35:50:96)
> Internet Protocol Version 4, Src: 217.21.95.185, Dst: 192.191.190.193
> Transmission Control Protocol, Src Port: 80, Dst Port: 56100, Seq: 1, Ack: 149394, Len: 0
    Source Port: 80
    Destination Port: 56100
    [Stream index: 20]
    [Stream Packet Number: 158]
    > [Conversation completeness: Incomplete, DATA (15)]
        [TCP Segment Len: 0]
        Sequence Number: 1 (relative sequence number)
        Sequence Number (raw): 1844185029
        [Next Sequence Number: 1 (relative sequence number)]
        Acknowledgment Number: 149394 (relative ack number)
        Acknowledgment number (raw): 2125836040
        1000 .... = Header Length: 32 bytes (8)
    > Flags: 0x010 (ACK)
    Window: 1302
    [Calculated window size: 166656]
    [Window size scaling factor: 128]
    Checksum: 0xd82 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    > [Timestamps]
    > [SEQ/ACK analysis]

```

1.3 TCP congestion control in action

1. The low start is visible from about 0.28 s through 1.34 s. The upload completes before any transition to congestion avoidance. Unlike the ideal model, it starts with a larger initial window and shows irregular growth.



2 Part 2 – UDP

2.1 UDP Packet Information

1. There are four fields: Source Port, Destination Port, Length and Checksum.

```
▼ User Datagram Protocol, Src Port: 3722, Ds
  Source Port: 3722
  Destination Port: 3722
  Length: 12
  Checksum: 0x1b21 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 6]
  [Stream Packet Number: 3]
```

2. Each UDP header field is 2 bytes. The total header size is 8 bytes

▼ User Datagram Protocol, Src Port: 3722, Dst Port:
 Source Port: 3722
 Destination Port: 3722
 Length: 12
 Checksum: 0x1b21 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 6]
 [Stream Packet Number: 3]
 > [Timestamps]
 UDP payload (4 bytes)
 ▼ Data (4 bytes)
 Data: 6c2a0000
 [Length: 4]

● ⚙ Source Port (udp.srcport), 2 bytes

3. It is the size of the headers (8 bytes) and the size of the data (4 bytes). The $8 + 4 = \text{Length } 12$.

Stream index: 20
▼ User Datagram Protocol, Src Port: 3722, Dst Port: 3722
 Source Port: 3722
 Destination Port: 3722
 Length: 12
 Checksum: 0x1b21 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 6]
 [Stream Packet Number: 3]
 > [Timestamps]
 UDP payload (4 bytes)
 ▼ Data (4 bytes)
 Data: 6c2a0000
 [Length: 4]

● ⚙ User Datagram Protocol (udp), 8 bytes

4. The max IPv4 size is 65,535 bytes. The IPv4 header is 20 bytes. The UDP header is 8 bytes. $65,535 - 20 - 8 = 65,507$ total bytes

```
✓ Ethernet II, Src: Apple [apple_33:30:98] (00:03:30:33:30:98), Dst: Cisco [cisco_01:17:81] (00:0c:29:01:17:81)
  Internet Protocol Version 4, Src: 172.17.48.134, Dst: 192.191.190.31
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 32
      Identification: 0x4ba5 (19365)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: UDP (17)
      Header Checksum: 0xd3b1 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 172.17.48.134
      Destination Address: 192.191.190.31
      [Stream index: 20]
    < User Datagram Protocol, Src Port: 3722, Dst Port: 3722
      Source Port: 3722
      Destination Port: 3722
      Length: 12
      Checksum: 0x1b21 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 6]
      [Stream Packet Number: 3]
    > [Timestamps]
      UDP payload (4 bytes)
    < Data (4 bytes)
      Data: 6c2a0000
      [Length: 4]
```

Internet Protocol Version 4 (ip), 20 bytes

5. The largest possible value is 65,535.

6. UDP's IP protocol number is 17 (decimal) = 0x11 (hex)

```
> Differentiated Services Field: 0x00 (DSCP: CS0,
  Total Length: 32
  Identification: 0x4ba5 (19365)
> 000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xd3b1 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.17.48.134
```

7. The source and destination ports flip values between the packets

11168	18.714297	74.125.136.95	172.17.48.134	QUIC
11169	18.839608	172.17.48.134	172.217.215.113	UDP
11170	18.873864	172.217.215.113	172.17.48.134	UDP
11186	19.118427	172.17.48.134	74.125.136.95	QUIC
11187	19.152789	74.125.136.95	172.17.48.134	QUIC

```
> Frame 11170: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_5c:a5:cf (74:8f:c2:5c:a5:cf), Dst: Apple_33:36:98 (80:a9:97:33:36:98)
> Internet Protocol Version 4, Src: 172.217.215.113, Dst: 172.17.48.134
< User Datagram Protocol, Src Port: 443, Dst Port: 53793
  Source Port: 443
  Destination Port: 53793
  Length: 33
  Checksum: 0x1120 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 5]
  [Stream Packet Number: 20]
  > [Timestamps]
  UDP payload (25 bytes)
```

3 Part 3 - Traceroute

3.1 IPv4 vs IPv6

1. I used the commands “sudo traceroute -P icmp google.com” for IPv4 and “sudo traceroute6 -l www.google.com” for IPv6. The commands listed in the lab manual did not work for me, but I found equivalent commands for my MacBook. They both output ICMP echo probes.

(udp.dstport >= 33434 && udp.dstport <= 33600) icmp.type == 11						
Time frame.time_relative	Sequence	Rtt	Source	Destination	Protocol	Length
339	9.063233		172.20.10.1	172.20.10.10	ICMP	
341	9.069333		172.20.10.1	172.20.10.10	ICMP	
343	9.073054		172.20.10.1	172.20.10.10	ICMP	
1840	69.183560		69.83.37.170	172.20.10.10	ICMP	
1842	69.222764		69.83.37.170	172.20.10.10	ICMP	
1844	69.252780		69.83.37.170	172.20.10.10	ICMP	
1979	74.307859		69.83.37.161	172.20.10.10	ICMP	
1981	74.343067		69.83.37.161	172.20.10.10	ICMP	
1983	74.378266		69.83.34.132	172.20.10.10	ICMP	
1985	74.413122		69.83.34.132	172.20.10.10	ICMP	
1987	74.447788		69.83.34.132	172.20.10.10	ICMP	
1989	74.483248		69.83.33.75	172.20.10.10	ICMP	
1991	74.528297		69.83.33.75	172.20.10.10	ICMP	
1993	74.565336		69.83.33.75	172.20.10.10	ICMP	

```
(base) log@LogTrapbook ~ % sudo traceroute -P icmp google.com

Password:
traceroute: Warning: google.com has multiple addresses; using 192.178.162.138
traceroute to google.com (192.178.162.138), 64 hops max, 72 byte packets
 1  172.20.10.1 (172.20.10.1)  8.855 ms  5.293 ms  3.690 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  170.sub-69-83-37.myvzw.com (69.83.37.170)  56.504 ms  38.047 ms  29.978 ms
 7  * 161.sub-69-83-37.myvzw.com (69.83.37.161)  49.967 ms  34.296 ms
 8  132.sub-69-83-34.myvzw.com (69.83.34.132)  35.171 ms  34.026 ms  34.707 ms
 9  75.sub-69-83-33.myvzw.com (69.83.33.75)  35.389 ms  44.079 ms  36.839 ms
10  * * *
11  customer.alter.net (152.179.11.214)  47.374 ms  43.720 ms  60.490 ms
12  74.125.243.61 (74.125.243.61)  39.599 ms  46.576 ms  34.919 ms
13  74.125.243.48 (74.125.243.48)  39.648 ms  45.279 ms  42.482 ms
14  108.170.229.80 (108.170.229.80)  39.671 ms  43.821 ms  41.106 ms
15  209.85.252.127 (209.85.252.127)  41.036 ms  50.940 ms  44.968 ms
16  209.85.251.133 (209.85.251.133)  63.888 ms  71.114 ms  54.516 ms
17  142.251.233.47 (142.251.233.47)  45.818 ms  46.893 ms  53.201 ms
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  mh-in-f138.1e100.net (192.178.162.138)  81.633 ms  67.802 ms  50.495 ms
```

```
(base) log@LogTrapbook:~ % sudo traceroute6 -I www.google.com
Password:
traceroute6: Warning: www.google.com has multiple addresses; using 2607:f8b0:4024:c09::63
traceroute6 to www.google.com (2607:f8b0:4024:c09::63) from 2600:1005:b1a7:e7a3:41d1:65c6:1615:f4ec, 64 hops max, 20 byte packets
 1  2600:1005:b1a7:e7a3:50ee:9b1a:c7ab:7cb5  3.576 ms  3.347 ms  3.720 ms
 2  * * *
 3  2001:4888:21:2203:245:192::231  38.046 ms  40.302 ms  34.722 ms
 4  * * *
 5  2001:4888:21:2009:245:26::  54.859 ms  36.996 ms  40.812 ms
 6  2001:4888:21:2009:245:25::2  44.149 ms  39.710 ms  44.946 ms
 7  2001:4888:21:2008:245:26::  41.995 ms  41.563 ms  35.622 ms
 8  2001:4888:21:1033:245:1::10  41.821 ms  36.792 ms  54.712 ms
 9  2001:4888:21:1020:245:1::11  44.877 ms  62.317 ms  42.365 ms
10  loopback1.atl0gauy-ppr01-cc.alter.net  33.326 ms  51.101 ms  43.353 ms
11  2600:803:df::33a  37.653 ms  41.323 ms  45.188 ms
12  2001:4860:0:1::407f  56.416 ms  46.417 ms  70.795 ms
13  2001:4860:0:1::2480  49.035 ms  57.021 ms  48.675 ms
14  2001:4860::c:4002:faa3  71.198 ms  48.628 ms  63.380 ms
15  2001:4860::c:4002:ac20  47.863 ms  51.232 ms  56.820 ms
16  2001:4860::cc:4001:99b3  60.423 ms  58.242 ms  47.951 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  mg-in-f99.1e100.net  83.654 ms  53.544 ms  54.437 ms
```

Time frame.time_relative	Rtt	Source	Destination	Protocol	Length	Info
338 9.054712		172.20.10.10	192.178.162.138	ICMP	86	Echo (ping) request id=0xe658, seq=
339 9.063233		172.20.10.1	172.20.10.10	ICMP	70	Time-to-live exceeded (Time to live=
340 9.064148		172.20.10.10	192.178.162.138	ICMP	86	Echo (ping) request id=0xe658, seq=
341 9.069333		172.20.10.1	172.20.10.10	ICMP	70	Time-to-live exceeded (Time to live=
342 9.069440		172.20.10.10	192.178.162.138	ICMP	86	Echo (ping) request id=0xe658, seq=
343 9.073054		172.20.10.1	172.20.10.10	ICMP	70	Time-to-live exceeded (Time to live=
344 9.073130		172.20.10.10	192.178.162.138	ICMP	86	Echo (ping) request id=0xe658, seq=

2. IPv4 took 27 hops and IPv6 took 22 hops. The IPv4 path is 5 hops longer than the IPv6 path.

3. For hop 14, IPv6 ≈ 61.07 ms vs IPv4 ≈ 41.53 ms and for hop 12, IPv6 ≈ 57.88 ms vs IPv4 ≈ 40.36 ms. One possible reason for the difference is due to different routing domains on v6. The v6 path shows AT&T/Google v6 prefixes, while v4 went through Verizon/AlterNet before Google.

4. For IPv4, the TTL is 1 and the other values are 0x00 → DSCP: CS0, ECN: Not-ECT. For IPv6, the Flow Label is 0x70000, the Traffic Class is 0x00 (DSCP CS0, ECN Not-ECT). Both things prevent packets from looping endlessly in the network by limiting how many hops they can take.

```
649 20.9/9498          2600:1005:b1a:/e/a... 2600::1005:c09... ICMPv6      /4 Echo (ping) request
650 21.017230          2001:4888:21::2203... 2600:1005:b1a7:e7a... ICMPv6      122 Time Exceeded (0)
653 21.092057          2600:1005:b1a7:e7a... 2607:f8b0:4024:c09... ICMPv6      74 Echo (ping) request
654 21.132111          2001:4888:21::2203... 2600:1005:b1a7:e7a... ICMPv6      122 Time Exceeded (0)
655 21.132335          2600:1005:b1a7:e7a... 2607:f8b0:4024:c09... ICMPv6      74 Echo (ping) request
656 21.166869          2001:4888:21::2203... 2600:1005:b1a7:e7a... ICMPv6      122 Time Exceeded (0)

> Frame 653: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0
> Ethernet II, Src: Apple_33:36:98 (80:a9:97:33:36:98), Dst: 2a:c7:09:6c:4f:64 (2a:c7:09:6c:4f:64)
> Internet Protocol Version 6, Src: 2600:1005:b1a7:c7a3:41d1:65c6:1615:f4ec, Dst: 2607:f8b0:4024:c09::63
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 00.... .... .... .... = Differentiated Services Codepoint: Default (0)
  .... ...00 .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  .... 0111 0000 0000 0000 0000 = Flow Label: 0x70000
  Payload Length: 20
  Next Header: ICMPv6 (58)
  Hop Limit: 3
  > Source Address: 2600:1005:b1a7:e7a3:41d1:65c6:1615:f4ec
  > Destination Address: 2607:f8b0:4024:c09::63
    [Stream index: 17]
  > Internet Control Message Protocol v6
```

5. The * entries means that one or more routers did not send a response. One reason for this is because of ICMPv6 Time Exceeded errors.

2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=13, hop limit=5 (no r
2001:4888:21:2009:...	2600:1005:b1a7:e7a...	ICMPv6	122 Time Exceeded (Hop limit exceeded in transit)
2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=14, hop limit=5 (no r
2001:4888:21:2009:...	2600:1005:b1a7:e7a...	ICMPv6	122 Time Exceeded (Hop limit exceeded in transit)
2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=15, hop limit=5 (no r
2001:4888:21:2009:...	2600:1005:b1a7:e7a...	ICMPv6	122 Time Exceeded (Hop limit exceeded in transit)
2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=16, hop limit=6 (no r
2001:4888:21:2009:...	2600:1005:b1a7:e7a...	ICMPv6	122 Time Exceeded (Hop limit exceeded in transit)
2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=17, hop limit=6 (no r
2001:4888:21:2009:...	2600:1005:b1a7:e7a...	ICMPv6	122 Time Exceeded (Hop limit exceeded in transit)
2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=18, hop limit=6 (no r
2001:4888:21:2009:...	2600:1005:b1a7:e7a...	ICMPv6	122 Time Exceeded (Hop limit exceeded in transit)
2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=19, hop limit=7 (no r
2001:4888:21:2008:...	2600:1005:b1a7:e7a...	ICMPv6	122 Time Exceeded (Hop limit exceeded in transit)
2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=20, hop limit=7 (no r
2001:4888:21:2008:...	2600:1005:b1a7:e7a...	ICMPv6	122 Time Exceeded (Hop limit exceeded in transit)
2600:1005:b1a7:e7a...	2607:f8b0:4024:c09...	ICMPv6	74 Echo (ping) request id=0xe656, seq=21, hop limit=7 (no r

4 AI Use Reflation Statement

I used ChatGPT to help explain some of the concepts of the lab like UDP, and IPv4 vs IPv6. I also used it to help generate Wireshark commands that could filter down to relevant packets that I wanted to find. I wrote all of the answers in this report. I found that ChatGPT was good at high level explanations, but it did hallucinate some non-existent features in Wireshark.

By writing this reflection, I acknowledge that AI is a support tool, not a substitute for my own effort, and I take full responsibility for the final submission.