

CO 323 Computer Communication Networks

Labotary Session 2

E/13/377

1.

1.1 TCP traffic (Client – 10.40.18.73, Server – 10.40.18.74):

Frame 58: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

Interface id: 0 (any)

Encapsulation type: Linux cooked-mode capture (25)

Arrival Time: Apr 1, 2017 14:18:31.141209000 Sri Lanka Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1491036511.141209000 seconds

[Time delta from previous captured frame: 0.000037000 seconds]

[Time delta from previous displayed frame: 0.000037000 seconds]

[Time since reference or first frame: 19.405650000 seconds]

Frame Number: 58

Frame Length: 92 bytes (736 bits)

Capture Length: 92 bytes (736 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: sll:ethertype:ip:tcp:data]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

> Linux cooked capture

> Internet Protocol Version 4, Src: 10.40.18.74, Dst: 10.40.18.73

> Transmission Control Protocol, Src Port: 36095 (36095), Dst Port: 5001 (5001),

Source Port: 36095

Destination Port: 5001

[Stream index: 2]

[TCP Segment Len: 24]

Sequence number: 1 (relative sequence number)

[Next sequence number: 25 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

1.2 TCP traffic (Client – 10.40.18.74, Server – 10.40.18.73):

Frame 58: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

Interface id: 0 (any)

Encapsulation type: Linux cooked-mode capture (25)

Arrival Time: Apr 1, 2017 14:18:31.141209000 Sri Lanka Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1491036511.141209000 seconds

[Time delta from previous captured frame: 0.000037000 seconds]

[Time delta from previous displayed frame: 0.000037000 seconds]

[Time since reference or first frame: 19.405650000 seconds]

Frame Number: 58

Frame Length: 92 bytes (736 bits)

Capture Length: 92 bytes (736 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: sll:ethertype:ip:tcp:data]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

> Linux cooked capture

> Internet Protocol Version 4, Src: 10.40.18.74, Dst: 10.40.18.73

> Transmission Control Protocol, Src Port: 36095 (36095), Dst Port: 5001 (5001),

Source Port: 36095

Destination Port: 5001

[Stream index: 2]

[TCP Segment Len: 24]

Sequence number: 1 (relative sequence number)

[Next sequence number: 25 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

1.1 TCP traffic (Client – 10.40.18.73, Server – 10.40.18.74):

Frame 40: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.40.18.73, Dst: 10.40.18.74
0100 = Version: 4
... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1498
Identification: 0x789c (30876)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x8394 [validation disabled]
Source: 10.40.18.73
Destination: 10.40.18.74
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 59343 (59343), Dst Port: 5001 (5001)
Source Port: 59343
Destination Port: 5001
Length: 1478

1.2 TCP traffic (Client – 10.40.18.74, Server – 10.40.18.73):

Frame 47: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.40.18.74, Dst: 10.40.18.73
0100 = Version: 4
... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1498
Identification: 0x8cd1 (36049)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0x6f5f [validation disabled]
Source: 10.40.18.74
Destination: 10.40.18.73
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 50569 (50569), Dst Port: 5001 (5001)
Source Port: 50569
Destination Port: 5001
Length: 1478

2. TCP three way handshaking:

- Client = 10.40.18.73 & Server = 10.40.18.73
- [SYN] Packet
- Sequence number = 0 & Acknowledgement number = 0

Frame 27: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.40.18.73, Dst: 10.40.18.74
0100 = Version: 4
... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0xfcd0 (64960)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x9419 [validation disabled]
Source: 10.40.18.73
Destination: 10.40.18.74
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 36625 (36625), Dst Port: 5001 (5001), Seq=0
Source Port: 36625
Destination Port: 5001
[Stream Index: 1]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
Header Length: 40 bytes
Flags: 0x002 (SYN)

- [SYN ACK] Packet
- Sequence number = 0 & Acknowledgement number = 1

Frame 28: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface...

Linux cooked capture

Internet Protocol Version 4, Src: 10.40.18.74, Dst: 10.40.18.73

0100 = Version: 4
 0101 = Header Length: 20 bytes
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0x0000 (0)
 > Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 64
 Protocol: TCP (6)
 > Header checksum: 0x01da [validation disabled]
 Source: 10.40.18.74
 Destination: 10.40.18.73
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 5001 (5001), Dst Port: 36625 (36625), S...

Source Port: 5001
 Destination Port: 36625
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 0 (relative sequence number)
 Acknowledgment number: 1 (relative ack number)
 Header Length: 40 bytes
 > Flags: 0x012 (SYN, ACK)

- [ACK] Packet
- Sequence number = 1 & Acknowledgement number = 1

Frame 29: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface...

Linux cooked capture

Internet Protocol Version 4, Src: 10.40.18.73, Dst: 10.40.18.74

0100 = Version: 4
 0101 = Header Length: 20 bytes
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0xfdc1 (64961)
 > Flags: 0x02 (Don't Fragment)
 Fragment offset: 0
 Time to live: 64
 Protocol: TCP (6)
 > Header checksum: 0x0420 [validation disabled]
 Source: 10.40.18.73
 Destination: 10.40.18.74
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 36625 (36625), Dst Port: 5001 (5001), S...

Source Port: 36625
 Destination Port: 5001
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Acknowledgment number: 1 (relative ack number)
 Header Length: 32 bytes
 > Flags: 0x010 (ACK)

3. TCP connection establishment delay:

- Time of first [SYN] packet = 1.375352
- Time of first [SYN ACK] packet = 1.375629
- Time of first [ACK] packet = 1.375663

Therefore TCP connection establishment delay = 1.375663 - 1.375352 = 0.000311

4. Initial sequence numbers are shown as zero in each direction. Because normally initial sequence number is a random number. But a software like Wireshark, set the first sequence number to 0. This is called relative sequence number.

5.

```
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  Maximum segment size: 1460 bytes
    Kind: Maximum Segment Size (2)
    Length: 4
    MSS Value: 1460
  TCP SACK Permitted Option: True
    Kind: SACK Permitted (4)
    Length: 2
  Timestamps: TSval 135059, TSecr 0
    Kind: Time Stamp Option (8)
    Length: 10
    Timestamp value: 135059
    Timestamp echo reply: 0
  No-Operation (NOP)
    Type: 1
    0... .... = Copy on fragmentation: No
    .00. .... = Class: Control (0)
    ...0 0001 = Number: No-Operation (NOP) (1)
  Window scale: 7 (multiply by 128)
    Kind: Window Scale (3)
    Length: 3
    Shift count: 7
    Multiplier: 128
```

1. Maximum segment size
2. TCP SACK permitted option
3. Timestamps
4. Window scale

6. TCP connection teardown message sequence

Server – 10.40.18.73

Client – 10.40.18.74

1. [FIN, PSH, ACK] Packet

Packet 54: 11.400782, 10.40.18.73 → 10.40.18.74, TCP, 412 bytes, Seq=1170865857, Ack=1170866201, Flags=[FIN, PSH, ACK].

Packet details:

- Internet Protocol Version 4, Src: 10.40.18.73, Dst: 10.40.18.74
- Transmission Control Protocol, Src Port: 36625, Dst Port: 5001, Seq: 1170865857, Ack: 1170866201, Window: 0, Len: 32, Flags: FIN, PSH, ACK

2.

Packet 54: 11.400782, 10.40.18.73 → 10.40.18.74, TCP, 412 bytes, Seq=1170865857, Ack=1170866201, Flags=[FIN, PSH, ACK].

Packet details:

- Internet Protocol Version 4, Src: 10.40.18.73, Dst: 10.40.18.74
- Transmission Control Protocol, Src Port: 36625, Dst Port: 5001, Seq: 1170865857, Ack: 1170866201, Window: 0, Len: 32, Flags: FIN, PSH, ACK

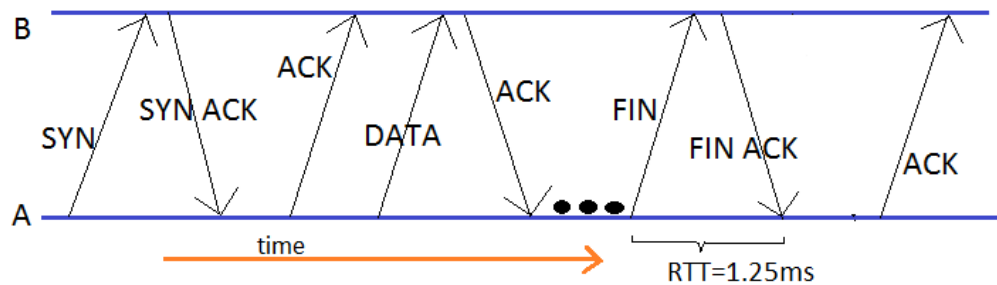
3.

Frame 54195: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.40.18.73, Dst: 10.40.18.74

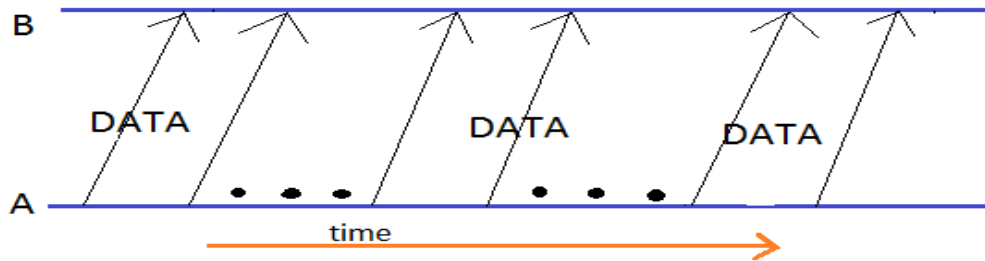
0100 = Version: 4
.... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport ...
Total Length: 52
Identification: 0x783c (30780)
Flags: 0x02 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x89a5 [validation disabled]
[Good: False]
[Bad: False]
Source: 10.40.18.73
Destination: 10.40.18.74
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 36625 (36625), Dst Port: 5001 (5001),--
Source Port: 36625
Destination Port: 5001
[Stream Index: 1]
[TCP Segment Len: 0]
Sequence number: 1170866202 (relative sequence number)
Acknowledgment number: 2 (relative ack number)
Header Length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 229
[Calculated window size: 29312]
[Window size scaling factor: 128]
Checksum: 0xe8a1 [validation disabled]

Between two FIN and FIN ACK packets, sent ACK another packets. Because those packets were lost previously.

7. Traffic pattern for TCP



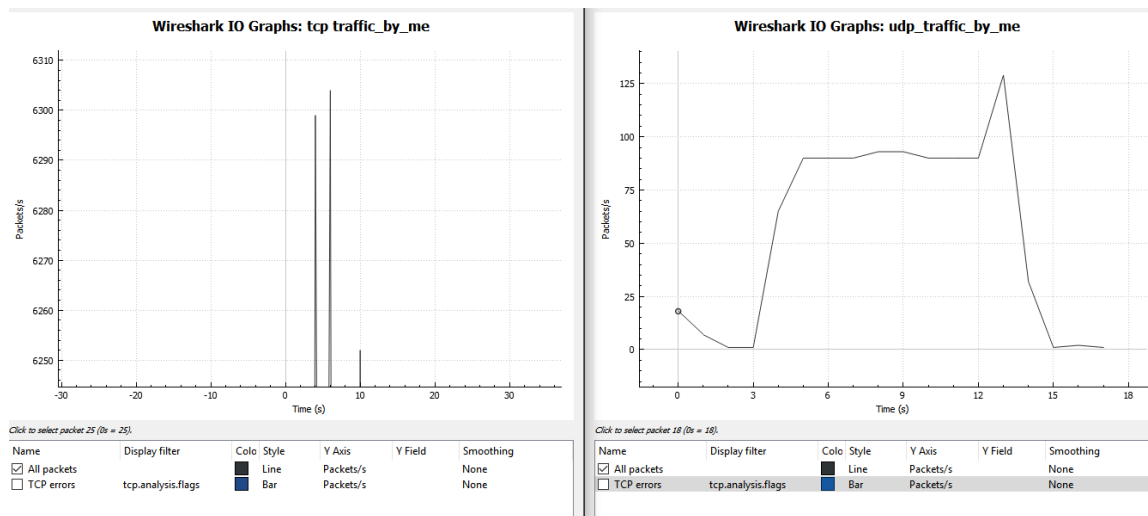
Traffic pattern for UDP



8. Throughput is number of frames send per second.

Server = 10.40.18.73

Client – 10.40.18.74

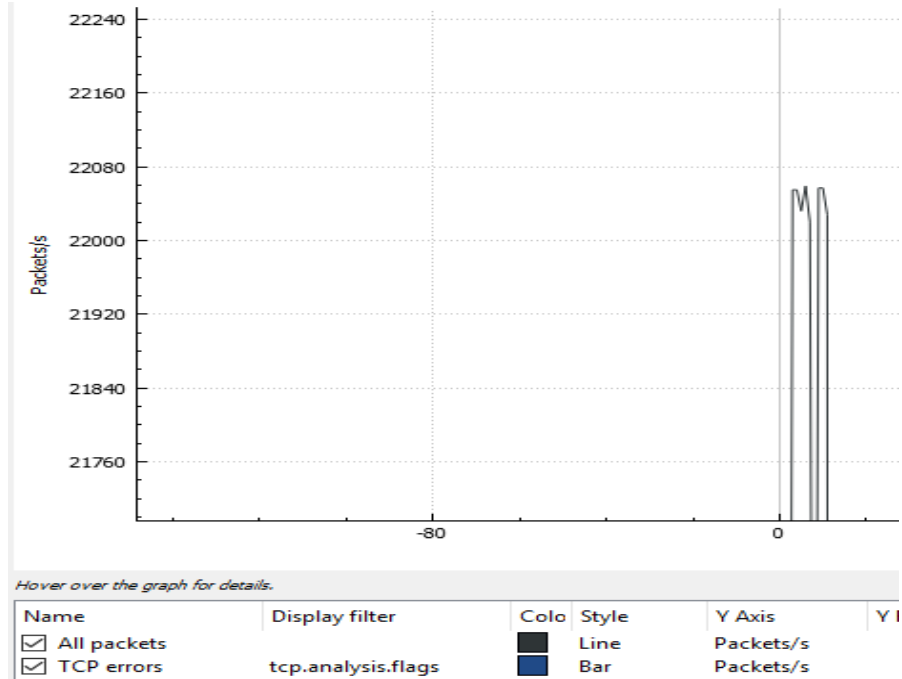


According to these two graphs and the data of iperf, throughput of the TCP connection gets a max value, but for small time. But UDP connection gets a low, but steady value for the throughput. But theoretically UDP is faster than TCP and the reason is ACK packet that permits a continuous packet stream, instead of TCP that acknowledges a set of packets.

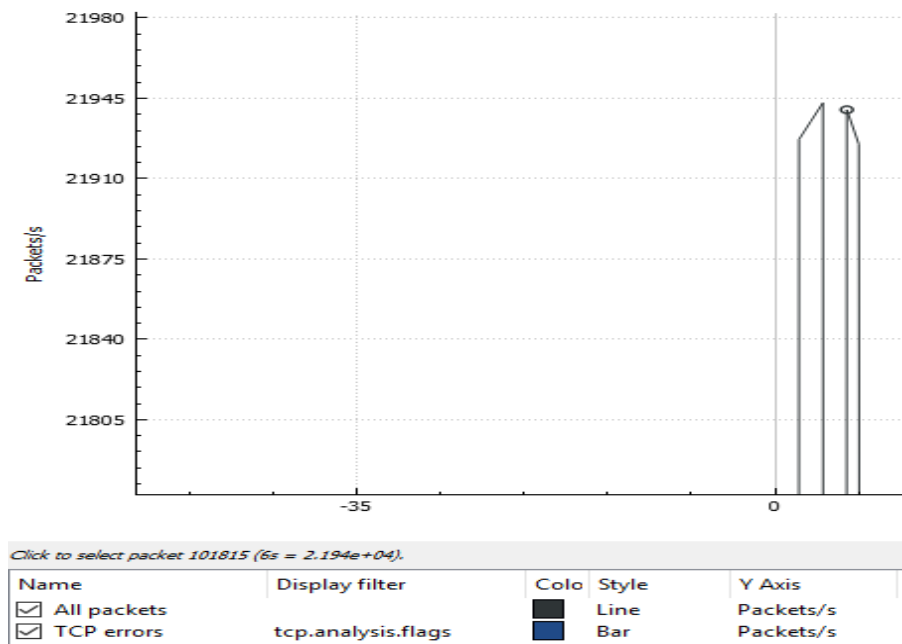
9. When changing the MTU, number of packets per second are changing.

Below graphs are showing the maximum packets per second when MTU is changing.

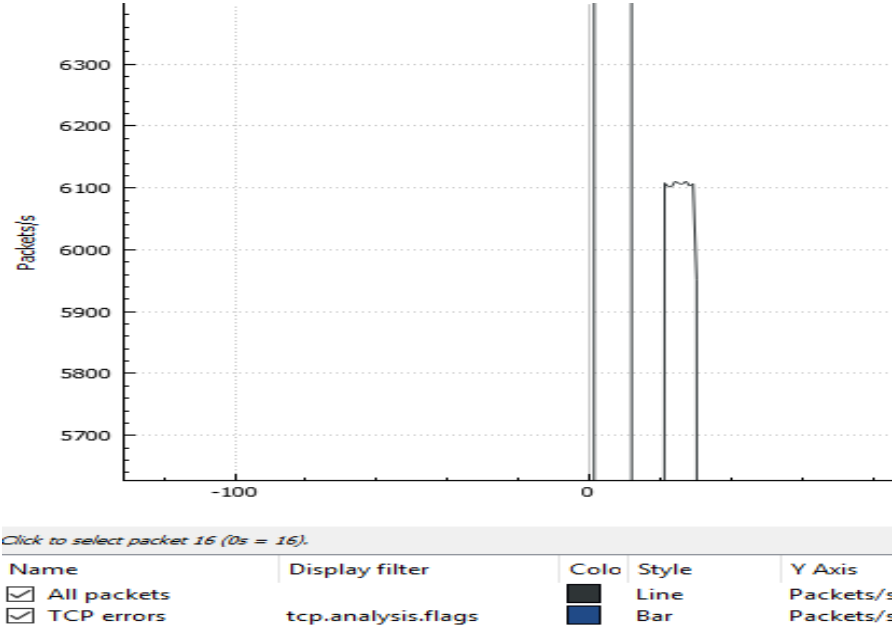
1. MTU = 500:



2. MTU = 1000:



3. MTU = 1500:



10. When MTU size is getting bigger, packets/s is gets lower. When inspecting the traffic patterns in above graphs, the peaks of three graphs are different. For higher MTUs, gets more stable peak and lower MTUs gets unstable peaks. Therefore we can assume that when MTU is getting higher, it comes to a saturation.