Assignment No. 1

Meet Patel

(B00899516)

CSCI 6704: Advance Topics in Networks

Dr. Srini Sampalli

Dalhousie University

Fall 2022

Question 1: Exploratory question

Evolution of TCP/IP from its predecessor ARPAnet

The forerunner of today's TCP/IP was the Advanced Research Projects Agency (ARPA), which created and launched the super network ARPAnet in 1969. In the early generations of this technology, there was just one essential protocol named TCP. This precursor of modern TCP was invented in 1973, and it was subsequently revised and correctly specified in RFC 675, Specification of Internet Transmission Control Program, published in December 1974. Cerf and Kahn utilised the principles of CYCLADES, a French packet switching network built and supervised by Louis Pouzin in 1973, during the creation of TCP. It was created to investigate alternatives to the ARPANET design and to aid network development in general. TCP/IP evolved into the standard Internet communications protocol, allowing digital computers to connect across large distances. TCP oversees collecting and reassembling data packets, whereas IP ensures that packets are sent to the correct destination. TCP/IP was created in the 1970s and was approved as the protocol standard for ARPANET (the Internet's forerunner) in 1983 [1].

Features of TCP/IP

1. logical Addressing
   An address that has been set up using network software is known as a logical address. An IP address is the TCP/IP term for a computer's logical address. Each physical address for a network device is different. An identification number provided to the card at the manufacturing serves as the actual address. On a local area network, low-lying hardware-conscious protocols use the physical address of the adapter to transport data over the physical network. A network, a subnet on a network, and a machine on a subnet are each uniquely identified by a network ID number, a subnet ID number, and a host ID number. There are several network kinds, and each one has a unique method of data delivery [2].

2. Routing
   In order to send information over the network to its destination location, a router is a specialised device that can read logical addressing information is used and it also A router separates a local subnet from the broader network. Wider and big networks, like the Internet, include several routers and offer a variety of routes from the source to the destination. TCP/IP is remarkably effective in transmitting packets from one network segment to the next. Data addressed to a different computer or device on the local subnet doesn't pass via the router [2].

3. Support
   Due to the possibility of several network applications running simultaneously on the same machine, the protocol software must offer a way to identify which incoming packet corresponds with each programme. Through some set of logical channels known as ports,

TCP/IP achieves this interface between the network and the applications. This port has a special id for the purpose of distinguish it [2].

4. Controlling errors and directing flow
   Features that guarantee dependable data transport throughout the network are offered by the TCP/IP protocol suite. One of these characteristics is recognising the successful reception of a network communication. Another is verifying data for transmission mistakes and m any of these error-checking, flow-control, and acknowledgement capabilities are defined by TCP's Transport layer [2].

Differences between TCP/IP and the OSI (Open-Source Interconnect) layered model.

The fundamental distinction between the TCP/IP Model and the OSI Model is that the former is a conceptual framework that can be used to describe how a network works, whilst the latter is a collection of communication protocols that can be used to link network devices to the Internet. Considering the layers, then The TCP/IP Model is made up of the Network Interface, Internet, Transport, and Application layers, whereas the first seven levels of the OSI Model are Physical, Data Link, Network, Transport, Session, Presentation, and Application [3].

What is RFC (Request for Comments)?

An RFC is a document that defines a new technology or improves an existing technology. Online policies and procedures, concepts, techniques, and programmes are evaluated, described, and defined in a Request for Comments (RFC) which is a numbered document. RFCs contain a substantial portion of the standards that are implemented online. A few core RFCs have been formally approved as standards. However, even if a significant number of RFCs are not given "Standard" status, they are still applied globally. The reason for this is that the people or organisations working on an RFC spend most of their time on protocols rather than on the validation process [4].

What is the role of IETF (Internet Engineering Task Force)?

The Internet Engineering Task Force (IETF) is the foremost Internet standards organisation, developing open standards using open techniques. It is a vast open worldwide community of network designers, operators, vendors, and researchers interested with the advancement of Internet architecture and its smooth operation. The technical work of the IETF is done in Working Groups, which are divided into several Areas based on subject. The IAB oversees the RFC editor and provides technical instructions to guarantee the smooth running of the internet as part of its oversight of the IETF's activity [5][6].

Reference

[1] "History of TCP/IP," *Scos Training*, 02-Jul-2019. [Online]. Available: https://scos.training/history-of-tcp-ip/ [Accessed: Oct 1st , 2022].

[2] "TCP/IP Tutorial," *Yaldex.com*. [Online]. Available: http://www.yaldex.com/tcp_ip/0672325659_ch01lev1sec3.html [Accessed: Oct 1st , 2022].

[3] "Difference between TCP/IP and OSI Model," *BYJUS*, 19-Oct-2020. [Online]. Available: https://byjus.com/free-ias-prep/difference-between-tcp-ip-and-osi-model/ [Accessed: Oct 1st , 2022].

[4] "Request for Comments (RFC)," *Nfon.com*. [Online]. Available: https://www.nfon.com/en/get-started/cloud-telephony/lexicon/knowledge-base-detail/request-for-comments-rfc [Accessed: Oct 1st , 2022].

[5] K. T. Hanna, "Internet Engineering Task Force (IETF)," *Whatis.com*, 26-Oct-2021. [Online]. Available: https://www.techtarget.com/whatis/definition/IETF-Internet-Engineering-Task-Force [Accessed: Oct 1st , 2022].

[6] "About," *IETF*. [Online]. Available: https://www.ietf.org/about/ [Accessed: Oct 1st , 2022].

Question 2: Virtual Circuit Packet Switching

Consider the following network that uses virtual circuit packet switching.

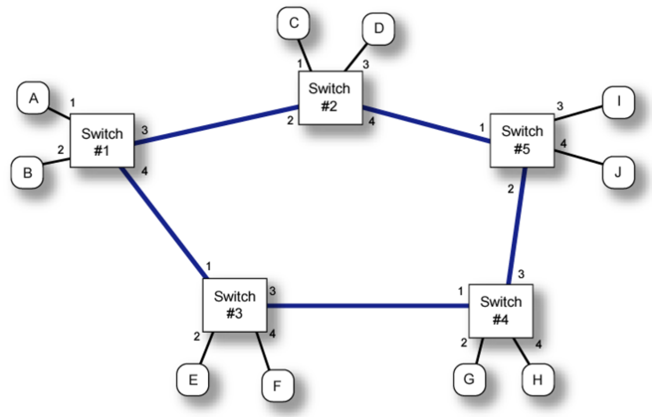


Figure 1: Virtual Circuit Packet Switching

The following virtual circuit paths need to be set up:

Host A to Host J via Switch #2
Host B to Host H via Switch #2 and #5
Host C to Host E via Switch #1
Host D to Host H via Switch #5
Host F to Host I via Switch #4
Host E to Host B via Switch #4, #5 and #2 Host G to Host D via Switch #5
Host H to Host C via Switch #3 and #1 Host I to Host F via Switch #4
Host J to Host A via Switch #2

Switch #1			
Incoming		**Outgoing**	
VCin	**In Port**	**VCout**	**Out Port**
10	1	20	3
10	2	30	3
20	3	30	4
60	3	70	2
40	4	50	3
30	3	40	1

Switch #2			
Incoming		**Outgoing**	
VCin	**In Port**	**VCout**	**Out Port**
20	2	30	4
30	2	40	4
10	1	20	2
10	3	20	4
50	4	60	2
30	4	40	3
50	2	60	1
20	4	30	2

Switch #3			
Incoming		Outgoing	
VCin	In Port	VCout	Out Port
30	1	40	2
10	4	20	3
10	2	30	3
30	3	40	1
40	3	50	4

Switch #4			
Incoming		Outgoing	
VCin	In Port	VCout	Out Port
50	3	60	4
30	3	40	4
20	1	30	3
30	1	40	3
10	2	20	3
10	4	30	1
20	3	40	1

Switch #5			
Incoming		Outgoing	
VCin	In Port	VCout	Out Port
30	1	40	4
40	1	50	2
20	1	30	2
30	2	40	3
40	2	50	1
20	2	30	1
10	3	20	2
10	4	20	1

Question 3: Bandwidth delay problems

(A) Consider the following scenario:
N = number of hops between two end systems
L = length of the message in bits
B = bandwidth in bits per second, on all links
P = packet size in bits (for datagram and virtual circuit packet switching)
The size is the same for all packets, and it includes the message portion plus any overhead
H = overhead for each packet in bits (for datagram packet switching only; ignore the overhead for virtual circuit packet switching)
S = call set up time in seconds (for circuit switching and virtual circuit packet switching)
R = call release time in seconds (for circuit switching and virtual circuit packet switching)
D = propagation delay per hop in seconds
Ignore queuing and processing delays.

If N = 8, L= 4096, B = 1024, P = 128, H = 32, S = 0.2, R = 0.1, D = 0.001, compute the end-to-end delay for the following three cases:

1. **Message is sent using circuit switching**

   Transmission Delay = L / R
   = 4096 / 1024
   = 4 sec

   Total Propagation Delay = 0.001 * 8
   = 0.008 sec

   End to End Delay = S + R + Transmission Delay + Total Propagation Delay
   = 0.2 + 0.1 + 4 + 0.008
   = **4.308 sec**

   The end-to-end delay for the message sent using circuit switching is **4.308 seconds.**

2. **Message is sent using datagram packet switching**

   Size of Data in each packet = Packet Size – Overhead Size
   = 128 – 32
   = 96 bits

   Number of packets = L / 96
   = 4096 / 96

= 43 Packets

Transmission Delay = (P/B) * Number of Packets * N
= (128 / 1024) * 43 * 8
= 43 sec

For the first hop,

D1 = Time required to transmit and deliver all packets in the first hop

Hence, D1 = Number of packets * (P/B + D)
= 43 * (128/1024 + 0.001)
= 43 * (0.125 + 0.001) = 43 * 0.126
= 5.418 seconds

The time needed to transport the last packet over the remaining hops is now given by D2 = D3 =... = D8.

Therefore, D2 = D3 = ... = D8 = P/B+D
= (128/1024 + 0.001)
= 0.125 + 0.001
= 0.126

Hence, we can say that

Total delay (T) = D1 + D2 + D3 + D4 + D5 + D6 + D7 + D8
= 5.418 + 0.126 + 0.126 + 0.126 + 0.126+ 0.126 + 0.126 + 0.126
= **6.3 seconds**

The end-to-end delay for the message sent using datagram packet switching is **6.3 seconds.**

3. **Message is sent using virtual circuit packet switching**

Number of Packets = L / P
= 4096 / 128
= 32 Packets

Now for the first hop, D1 = Time required to transmit and deliver all packets in the first hop

Therefore, D1 = Number of packets * (P/B + D)
= 32 * (128/1024 + 0.001)
= 32 * (0.125 + 0.001) = 32 * 0.126
= 4.032 seconds

The time needed to transport the last packet over the remaining hops is now given by D2 = D3 =... = D8

Therefore, D2 = D3 = ... = D8 = P/B+D
= (128/1024 + 0.001) = 0.125 + 0.001
= 0.126

Hence, we can say that,

Total delay (T) = S + (D1 + D2 + D3 + D4 + D5 + D6 + D7 + D8) + R
= 0.2 + 4.032 + 0.126 + 0.126 + 0.126 + 0.126+ 0.126 + 0.126 + 0.126 + 0.1
= 0.2 + 4.914 + 0.1
= **5.214 seconds**

The end-to-end delay for the message sent using virtual circuit packet switching is **5.2 seconds.**

(B) Consider two hosts, A and B, connected by a single link of bandwidth R bits per sec. Suppose that the two hosts are separated by m meters, and suppose the propagation speed along the link is s meters/sec. Host A is to send a packet of size L bits to Host B. Ignore the processing and queuing delays. Suppose s = 2.5 X 10^8, L = 100 bits, and R = 28 kbps. Find the distance m so that the propagation delay equals transmission delay.

Propagation speed = s = 2.5 * 10^8 meter/sec

Packet size = L = 100 bits

Bandwidth = R = 28 kbps = 2.8 *10^4 bits/sec

Propagation Delay = Transmission Delay

Distance = M meter = ?

Propagation Delay = Transmission Delay

M / s =L / R

M = (L / R) * s

M = (L * s) / R

M = (100 * 2.5 * 10^8) / (2.8 * 10^4)

M = $(100 * 2.5 * 10^4) / 2.8$

M = **892,857.15 meter**

(C) Suppose two hosts, A and B, are separated by 20,000 kilometers, and are connected by a direct link of R = 2 Mbps. Suppose the propagation speed over the link is $2.5*10^8$ meters/sec. Consider sending a file of 800,000 bits from Host A to Host B. Suppose the file is sent continuously as one big message. How long does it take to send the file?

Suppose now the file is broken up into 20 packets each with each packet containing 40,000 bits. Suppose the receiver acknowledges each packet and the transmission time of an acknowledgement packet is 100 ms. Finally, assume that the sender cannot send a packet until the preceding one is acknowledged. How long does it take to send the file?

Distance = M = 20,000 km = $2 * 10^7$ meters

Bandwidth = R = 2 Mbps = $2 * 10^6$ bps

Propagation Speed = S = $2.5 * 10^8$ meters/sec

Length of Message = L = 800,000 bits = $8 * 10^5$ bits

1. **Message is sent continuously**

End to End Delay = Transmission Delay + Propagation Delay
= (L/ R) + (M / S)
= $(8 * 10^5 / 2 * 10^6) + (2 * 10^7 / 2.5 * 10^8)$
= (0.4) + (0.08)
= 0.48 sec

So, it will take **0.48 sec** to send a file.

2. **Message is broken and sent**

Number of Packets = 20
Size of Packet = P = 40,000 bits = $4 * 10^4$ bits
Transmission time of acknowledgement packet = 100 ms = 0.1 sec

Delay per packet = Transmission delay + Propagation delay for each data packet + propagation delay for each ack data packet + ack delay
= (P / R) + (M / S) + (M / S) + 0.1

$= (4 * 10^4 / 2 * 10^6) + (2 * 10^7 / 2.5 * 10^8) + (2 * 10^7 / 2.5 * 10^8) + 0.1$
$= 0.02 + 0.08 + 0.08 + 0.1$
$= 0.28$ sec

Delay for all packets = Delay per packet * number of packets
= 0.28 * 20
= 5.6 sec

So, it will take **5.6 sec** to send a file.

Question 4: TCP/IP Encapsulation Discovery using Wireshark

1. **Figure 2** is responsible for representing request made and response received from the following website: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
First Line in the figure represent the **request made** and Second Line represent the **response received**.

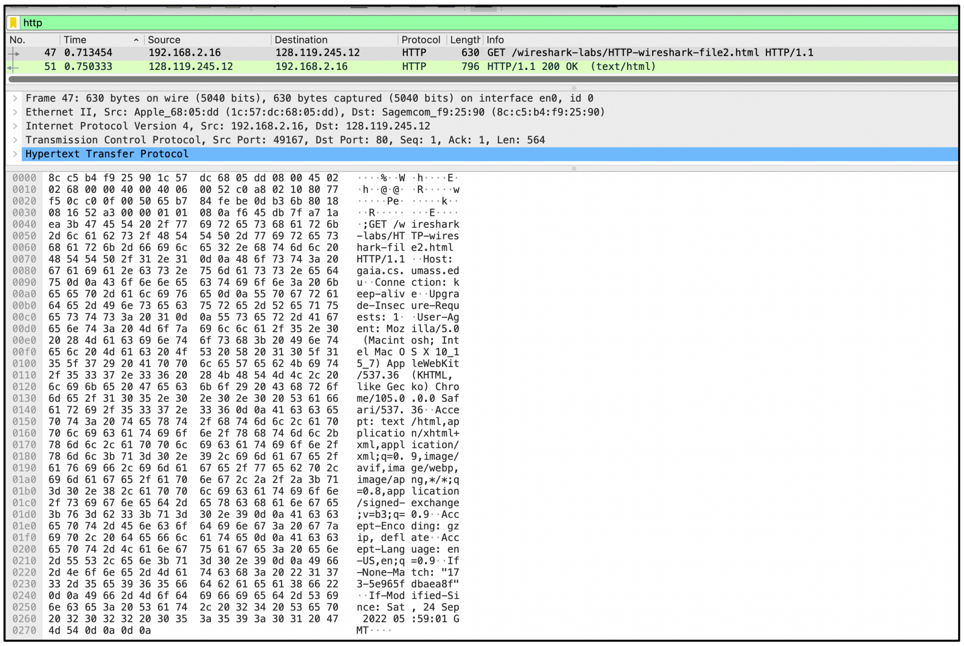


Figure 2: Represent request made and response received from website: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

2. **Figure 3** is responsible for representing Application Layer Component for the **request message**

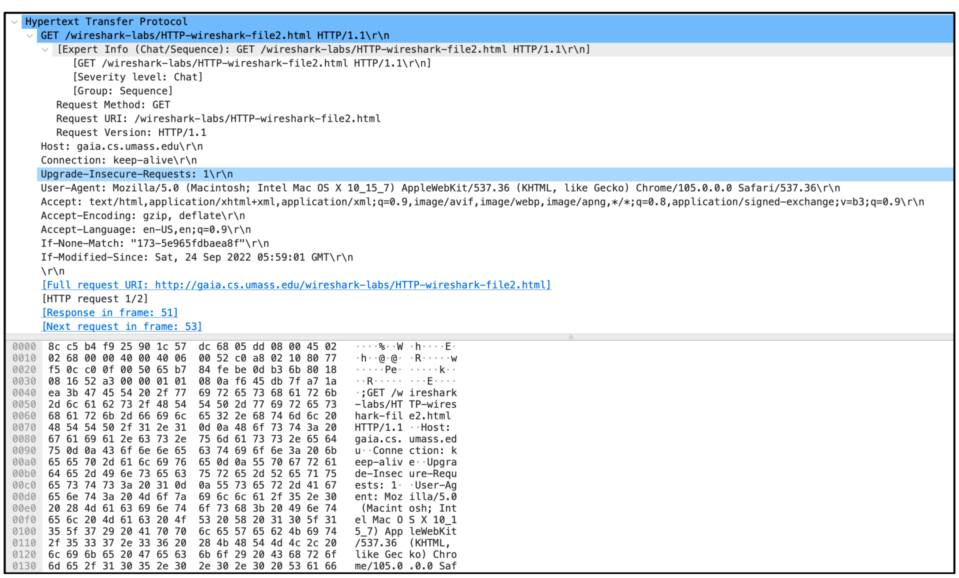
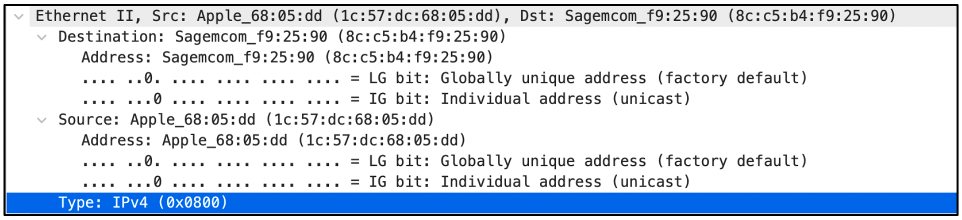


Figure 3: Application Layer Componenet

3. **Figure 4** is responsible for representing the **Ethernet Header Component** for the request message.



```
Ethernet II, Src: Apple_68:05:dd (1c:57:dc:68:05:dd), Dst: Sagemcom_f9:25:90 (8c:c5:b4:f9:25:90)
  Destination: Sagemcom_f9:25:90 (8c:c5:b4:f9:25:90)
    Address: Sagemcom_f9:25:90 (8c:c5:b4:f9:25:90)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Apple_68:05:dd (1c:57:dc:68:05:dd)
    Address: Apple_68:05:dd (1c:57:dc:68:05:dd)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

Figure 4: Ethernet Header Component for Request Message captured using Wireshark Tool

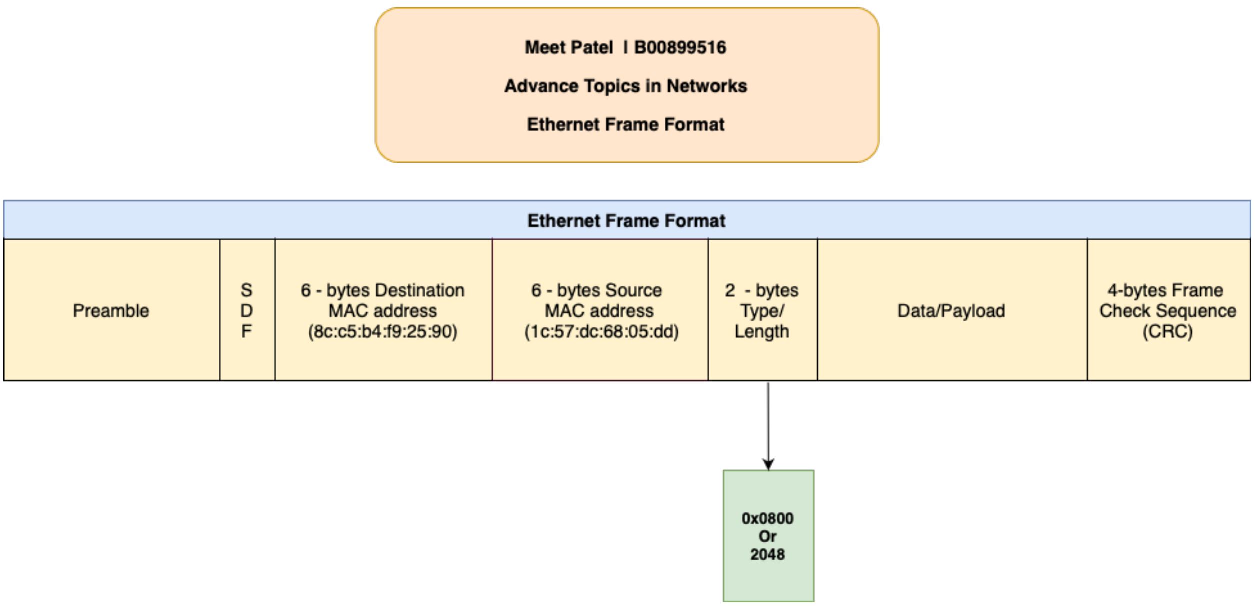


Figure 5: Ethernet Header Component for request message build using https://app.diagrams.net/ (& bytes Prw)

4. **Figure 5** is responsible for representing the **IP Header Component** for the request message.

```
Internet Protocol Version 4, Src: 192.168.2.16, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..10 = Explicit Congestion Notification: ECN-Capable Transport codepoint '10' (2)
    Total Length: 616
    Identification: 0x0000 (0)
    Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x0052 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.2.16
    Destination Address: 128.119.245.12
```

Figure 6: IP Header Component for the Request Message captured using Wireshark Tool

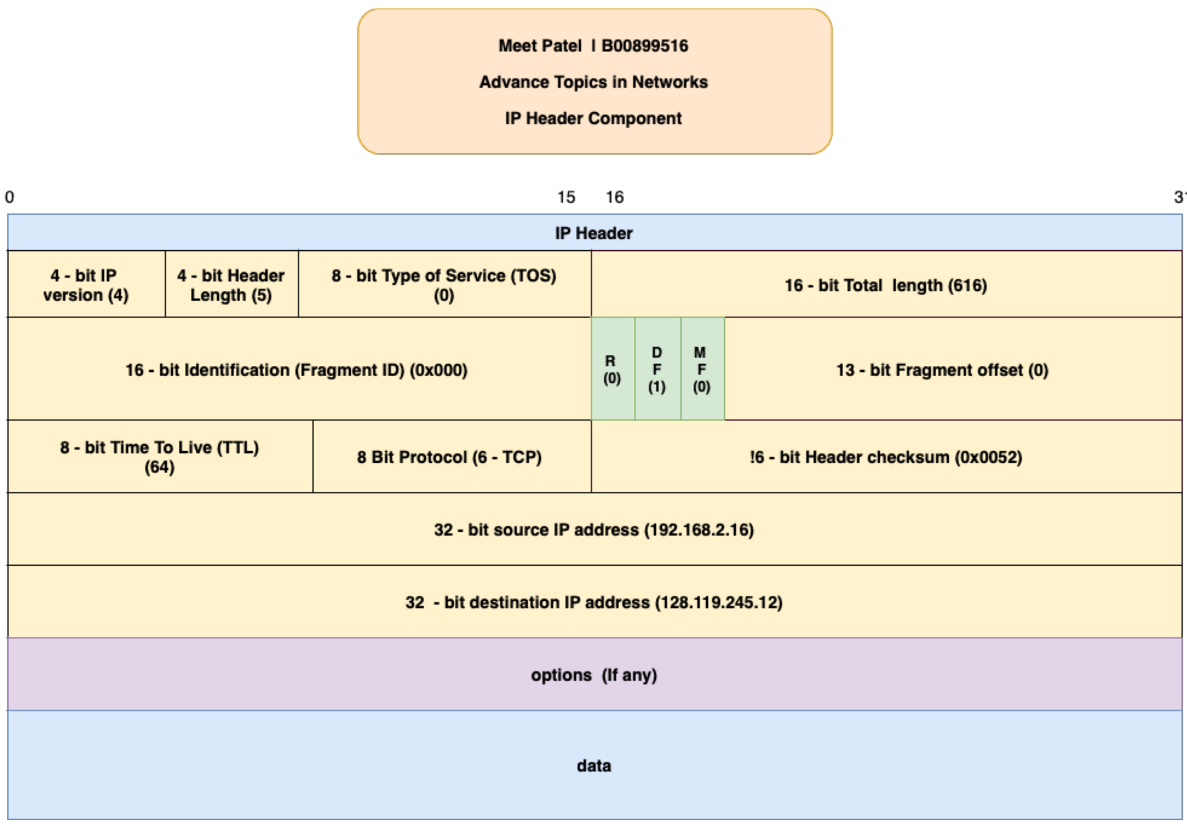


Figure 7: IP Header Component for request message build using https://app.diagrams.net/

5. Figure 6 is responsible for representing the **TCP Header Component** for the request message.

```
Transmission Control Protocol, Src Port: 49167, Dst Port: 80, Seq: 1, Ack: 1, Len: 564
    Source Port: 49167
    Destination Port: 80
    [Stream index: 2]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 564]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1706525950
    [Next Sequence Number: 565    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3188568939
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window: 2070
    [Calculated window size: 132480]
    [Window size scaling factor: 64]
    Checksum: 0x52a3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (564 bytes)
```

Figure 8: the TCP Header Component for the Request Message captured using Wireshark Tool

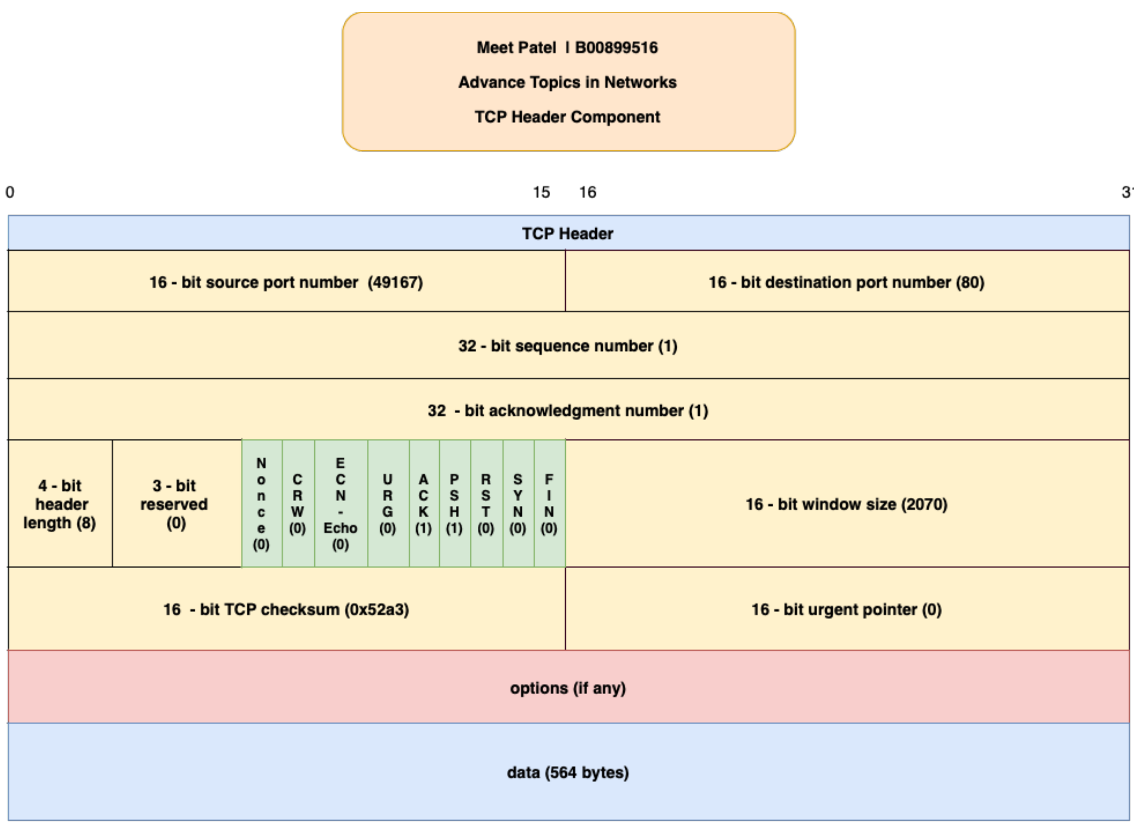


Figure 9: TCP Header Component for request message build using https://app.diagrams.net/

Question: Are you able to find the Data Link Trailer in the Ethernet frame capture in Wireshark? Why or why not? (Write a brief answer by looking up web resources).

Answer: Because the data cannot be intercepted or altered, data link trailers can boost security. Wireshark is only capable of capturing data that the packet capture library, the network interface device, or the OS's native raw packet capture mechanism let it to collect. The sender computer's NIC (Network Interface Card) determines the Data Link Trailer's value. This traffic is forwarded to the NIC after passing through the Wireshark's capture engine because it is being sent from the sender's machine.

Reference

[1] "Wireshark Q&A", *Osqa-ask.wireshark.org*, 2022. [Online]. Available: https://osqa-ask.wireshark.org [Accessed: 02- Oct- 2022].