Network Questions

Why do HTTP, SMTP, and POP3 run on top of TCP rather than on UDP?

> tcp is morereliable than udp,udp may have failures or data loss, so we can't afford to have losses inhttp,smtp,pop3 and so on. Accurate data is very important is all this protocols

What information is used by a process running on one host to identify a process running on another host?

> The IP address of the destination host and the port number of the destination socket.

For a P2P file-sharing application, do you agree with the statement, “There is no notion of client and server sides of a communication session”? Why or why not?

> No. As stated in the text, all communication sessions have a client side and a server side. In a P2P file-sharing application, the peer that is receiving a file is typically the
> client and the peer that is sending the file is typically the server.

Recall that TCP can be enhanced with SSL to provide process-to-process security services, including encryption. Does SSL operate at the transport layer or the application
layer? If the application developer wants TCP to be enhanced with SSL, what does the developer have to do?

> SSL operates at the application layer. The SSL socket takes unencrypted data from the application layer, encrypts it and then passes it to the TCP socket. If the

application developer wants TCP to be enhanced with SSL, he/she has to include the SSL code in the application

Consider a new peer Alice who joins BitTorrent without possessing any chunks. Without any chunks, she cannot become a top-four uploader for any of the other peers, since
she has nothing to upload. How then will Alice get her first chunk?

Alice will get her first chunk as a result of she being selected by one of her neighbors as a result of an “optimistic unchoke,” for sending out chunks to her

What encryption services are provided by HTTP?

HTTP does not provide any encryption services

Suppose within your web browser you click on a link to obtain a web page. Suppose that the IP address for the associated URL is not cached in your local host, so that a DNS look up is
necessary to obtain the IP address. Suppose that n DNS servers are visited before your host receives the IP address from DNS; the successive visits incur a RTT of RTT1 , ...,
RTTN . Further suppose that web page associated with the link contains exactly one object, a small amount of HTML text. Let RTT0 denote the RTT between the local host and the
server containing the object. Assuming zero transmission time of the object, how much time elapses from when the client clicks on the link until the client receives the object

The total amount of time to get the IP address is
- RTT1 +RTT2 +... +RTTN .
- Once the IP address is known, RTT0 elapses to set up
the TCP connection and another
- RTT0 elapses to request and receive the small object.

The total response time is
• 2RTT0 +RTT1 +RTT2 +... +RTTN

Describe how Web caching can reduce the delay in receiving a requested object. Will Web
caching reduce the delay for all objects requested by a user or for only some of the objects?

Web caching is used to reduce the time needed for a client to get a reply for the request that he sent. Web caching is done by a server (Proxy Server) that could be closer to the client. This server stores the object that the client asks for. If this server has the object stored when a client asks for that, it will send the object directly to the client and the delay will be reduced. But this does not happen every time. If the server does not have the object needed by the client it will forward the request to the origin server and wait for its reply. This will cause a greater delay. So we can say that the delay cannot be reduced for all objects requested from the client because it depends if the origin server has the reply or not

Consider an e-commerce site that wants to keep a purchase record for each of its customers.Describe how this can be done with cookies ?

When a user visits the e-commerce site for the first time, the website will return a cookie number,which is stored on the user's host, managed by the browser. The cookie number is present in cookie header and isgenerated by the server of the e-commerce website, and the number is unique for every customer. The clientreceives the response along with the header and the number with a line appended to a special cookie file. The filecontains the server name and the user's associated ID number. In the subsequent request to the same server theclient includes a cookie header which consists of a header line which specifies the id number for that server.During each visit or purchase from the e-commerce website, the browser sends the cookie number back to thewebsite server. This cookie number is used to identify the user (or browser) who is visiting the site.

Suppose Alice, with a Web-based e-mail account (such as Hotmail or Gmail), sends a message to Bob, who accesses his mail from his mail server using POP3. Discuss how the message gets from Alice's host to Bob's host. Be sure to list the series of application-layer protocols that are used to move the message between the two hosts.

Alice sends a message to her mail server using her browser, so over HTTP,then her mail server sends the same message to Bob's mail server using SMTP. After that, then Bob's mail server sends the message to the host using POP3.

From a user's perspective, what is the difference between the download-and-delete mode
and the download-and-keep mode in POP3

POP3 has two modes: the delete mode and the keep mode. In the delete mode, themail is deleted from the mailbox after each retrieval. In the keep mode, the mailremains in the mailbox after retrieval. The delete mode is normally used when the useris working at her permanent computer and can save and organize the received mail afterreading or replying. The keep mode is normally used when the user accesses her mailaway from her primary computer (e.g., a laptop). The mail is read but kept in the systemfor later retrieval and organizing

Is it possible for an organization's Web server and mail server to have exactly the same alias for ahostname (for example, foo.com)? What would be the type for the RR that contains the hostname ofthe mail server?

Yes, it is possible for an organization to have same alias for a host name for Web Server and mail server. This was possible because MX (Mail exchanger) record permits the same. The type for the RR that contains the hostname of the mail server is "MX"i.e. Type=MX. Then if required DNS client would query with Type=CNAME for getting canonical hostname for the alias hostname.

In BitTorrent, suppose Alice provides chunks to Bob throughout a 30-second interval. Will Bob necessarily return the favor and provide chunks to Alice in this same interval? Why or why not?

It is not necessary that Bob will also provide chunks to Alice. Alice has to be in the top 4 neighbors of Bob for Bob to send out chunks to her (or through random selection);this might not occur even if Alice provides chunks to Bob throughout a 30-second interval

What is an overlay network? Does it include routers? What are the edges in the overlay network

The overlay network in a P2P file sharing system consists of the nodes participating in the file sharing system and the logical links between the nodes. There is a logical link (an "edge" in graph theory terms)from node A to node B if there is a semi-permanent TCP connection between A and B. An overlay network does not include routers

CDNs typically adopt one of two different server placement philosophies. Name and briefly describe these two philosophies.

Enter Deep Bring home

1. Enter deep:it is pioneered by Akamai. It deploys server clusters in access ISPs (ISPs direct accessing end users) all over the world. The goal of Enter deep is to get close to end users, thereby improving user-perceived delay and throughput by decreasing the number of links. Routers between the end user and then CDN cluster from which it receives content. Because of this highly distributed design, the task of maintaining and managing the clusters becomechallenging.

2. Bring home: It can be taken by Limelight and other CDN companies; it brings the ISPs home by building large clusters at a smaller number of key locations and connecting these clusters using a private high-speed network. Instead of getting inside the access ISPs, these CDNs typically place each cluster at a location that is simultaneously near the point of presence of many tier-1 ISPs. Compared with the enter-deep design, the bring-home design typically results

in lower maintenance and management overhead, possibly at the expense of higher delay and lower throughout to end users.

Besides network-related considerations such as delay, loss, and bandwidth performance,there are many additional important factors that go into designing a CDN server selection strategy. What are they?

ISP delivery cost

Load on the clusters

The description of the important factors isThe clusters may be chosen based on different cost structures, so that the ISP delivery cost is minimized in .

Load on the clusters, we should be bothered when a client is to be directed to a cluster, so that the client is not directed to an overloaded cluster

In Section 2.7, the UDP server described needed only one socket, whereas the TCP server
needed two sockets. Why? If the TCP server were to support n simultaneous connections, each
from a different client host, how many sockets would the TCP server need?

With the UDP server, there is no welcoming socket, and all data from different clients enters the server through this one socket. With the TCP server, there is a welcoming socket, and each time a client initiates a connection to the server, a new socket is created. Thus, to support n simultaneous connections, the server would need n+1 sockets

For the client-server application over TCP described in Section 2.7, why must the server program be executed before the client program?

For the client- server application over UDP, why may the client program be executed before the server program? TCP requires a connection so the server must be ready in order to communicate. UDP does not require a connection so it does not worry about the server.

A user requests a Web page that consists of some text and three images. For this page, the client will send one request message and receive four response messages.

This statement is false. The client would receive a response for each request so if it sent a request then it would get a response of the same amount. So if it send three requests it would get three responses and so on

Two distinct Web pages (for example,and) can be sent over the same persistent connection.

This is true. The book says “Moreover, multiple web pages residing on the same server can be sent from the sever to the same client over a single persistent TCP connection.” This suggestion that both web pages are from the MIT and are probably on the same server.

With non persistent connections between browser and origin server, it is possible for a single TCP segment to carry two distinct HTTP request messages.

This statement is false. A non-persistent connection would handle each web page in a separate connection. So each separate connection needs a new request

What is the difference between a host and an end system? List several different types of end systems. Is a Web server an end system?

There is no difference between a host and an end system. In the internet, all devices are called hosts and end systems. So, hosts and end systems are used interchangeably. The types of end systems are PCs,Workstations, Web servers, email servers, PDAs, TVs, Cell Phones, Tablets, etc. A web server is an end system.

List six access technologies. Classify each one as home access, enterprise access, or wide-area wireless access.?

Dial-up modem over telephone line: home

DSL over telephone line - Home/ Small office.

Cable to HFC - Home

100 Mbps switched Ethernet - Enterprise

Wifi - Home/Enterprise

3G/4G- Wide area wireless

Is HFC transmission rate dedicated or shared among users? Are collisions possible in a downstream HFC channel? Why or why not?

HFC bandwidth is shared among the users. On the downstream channel, all packets emanate
from a single source, namely, the head end. Thus, there are no collisions in the downstream
channel.

Describe the most popular wireless Internet access technologies today. Compare and contrast them.

10. There are two popular wireless Internet access technologies today:

a) Wifi (802.11) In a wireless LAN, wireless users transmit/receive packets to/from an base
station (i.e., wireless access point) within a radius of few tens of meters. The base station is
typically connected to the wired Internet and thus serves to connect wireless users to the wired
network.

b) 3G and 4G wide-area wireless access networks. In these systems, packets are transmitted over the same wireless infrastructure used for cellular telephony, with the base station thus being managed by a telecommunications provider. This provides wireless access to users within a radius of tens of kilometers of the base station

Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has
three links, of rates
a. Assuming no other traffic in the network, what is the throughput for the file transfer?
b. Suppose the file is 4 million bytes. Dividing the file size by the throughput, roughly how
long will it take to transfer the file to Host B?
c. Repeat (a) and (b), but now with R reduced to 100 kbps.

a) 500 kbps b) 64 seconds c) 100kbps; 320 seconds

The file size= 4 million bytes

Convert million bytes to bits

=32000000 bits.

From (a), Throughput for the file transfer=500 Kbps

=500000 bps

Dividing the file size by the throughput,roughly how long will it take to transfer the file to Host B:

=file size/hroughput for the file transfer

=32000000 bits/500000 bps

=64 seconds

How long does it take a packet of length 1,000 bytes to propagate over a link of distance 2,500 km, propagation speed 2.5 · 108 m/s, and transmission rate 2 Mbps? More generally, how long does it take a packet of length L to propagate over a link of distance d, propagation speed s, and transmission rate R bps? Does
this delay depend on packet length? Does this delay depend on transmission rate?

Transmission delay = L/R

= 8 bits/byte * 1,000 bytes / 2,000,000 bps

= 4 ms

Propagation delay = d/s

= 2,500 / 2.5×105

= 10 ms

Therefore, the total time = 4ms + 10 ms = 14 ms

c) As stated above, the propagation delay does not depend on packet length.

d) As stated above, the propagation delay does not depend on transmission rate.

Suppose end system A wants to send a large file to end system B. At a very high level, describe how end system A creates packets from the file. When one of these packets arrives to a packet switch, what information in the packet does the switch use to determine the link onto which the packet is forwarded? Why is packet switching in the Internet analogous to driving from one city to another and asking directions along the way?

End system A breaks the large file into chunks. To each chunk, it adds header generating multiple packets from the file. The header in each packet includes the address of the destination: end system B. The packet switch uses the destination address to determine the outgoing link. Asking which road to take is analogous to a packet asking which outgoing link it should be forwarded on, given the packet's address.

List five tasks that a layer can perform. Is it possible that one (or more) of these tasks could be performed by two (or more) layers?

The following list five tasks that a layer can perform:

1. Flow control

2. Error control
3. Segmentation and reassembly
4. Multiplexing
5. Connection setup

What is an application-layer message? A transport-layer segment? A network-layer datagram? A link-layer frame?

Application-layer message: data which an application wants to send and passed onto the transport layer;

transport-layer segment: generated by the transport layer and encapsulates application-layer message with transport layer header;

network-layer datagram: encapsulates transport-layer segment with a network-layer header;

link layer frame: encapsulates network layer datagram with a link-layer header.

Which layers in the Internet protocol stack does a router process? Which layers does a link-layer switch process? Which layers does a host process?

Routers process layers 1 through 3.

Link layer switches process layers 1 through 2.

Hosts process all five layers.

Consider sending a packet from a source host to a destination host over a fixed route. List the delay components in the end-to-end delay. Which of these delays are constant and which are variable?

The delay components are processing delays, transmission delays, propagation delays, and queuing delays. All of these delays are fixed, except for the queuing delays, which are variable.

Suppose users share a 2 Mbps link. Also suppose each user transmits continuously at 1 Mbps when transmitting, but each user transmits only 20 percent of the time.

When a circuit switching is used, how many users can be supported?

2 users can be supported because each user requires half of the link bandwidth

For the remainder of this problem suppose packet switching is used. When will there be essentially no queuing delay before the link if two or fewer users transmit at the same time? What will there be a queuing delay if three users transmit at the same time

Since each user requires 1Mbps when transmitting, if two or fewer users transmit simultaneously, a maximum of 2Mbps will be required. Since the available bandwidth of the shared link is 2Mbps, there will be no queuing delay before the link. Whereas, if three users transmit simultaneously, the bandwidth required will be 3Mbps which is more than the available bandwidth of the shared link. In this case, there will be queuing delay before the link.

Find the probability that a given user is transmitting?

Probability that a given user is transmitting = 0.2

Suppose now there are three users. Find the probability that at any given time, all three users are transmitting simultaneously. Find the fraction of time during which the queue grows?

Probability that all three users are transmitting simultaneously = (3/3)p^3(1-p)^(3-3) = (0.2)^3 = 0.008. Since the queue grows when all the users are transmitting, the fraction of time during which the queue grows (which is equal to the probability that all three users are transmitting simultaneously) is 0.008.

Consider a TCP connection between Host A and Host B. Suppose that the TCP segments
traveling from Host A to Host B have source port number x and destination port

number y. What are the source and destination port numbers for the segments traveling from Host B to Host A?

Source port number y and destination port number x.

Describe why an application developer might choose to run an application over UDP rather than TCP?

An application developer may not want its application to use TCP's congestion control, which can throttle the application's sending rate at times of congestion. Often, designers of IP telephony and IP videoconference applications choose to run their applications over UDP because they want to avoid TCP's congestion control. Also, some applications do not need the reliable data transfer provided by TCP.

Why is it that voice and video traffic is often sent over TCP rather than UDP in today's internet? (hint: the answer we are looking for has nothing todo with TCP'S congestion-control mechanism.)

Since most firewalls are configured to block UDP traffic, using TCP for video and voice traffic lets the traffic though the firewalls

Is it possible for an application to enjoy reliable data transfer evenwhen the application runs over UDP? If so how?

Yes. The application developer can put reliable data transfer into theapplication layer protocol. This would require a significant amount of work anddebugging, however

Suppose a process in Host C has a UDP socket with port number 6789. Suppose both Host
A and Host B each send a UDP segment to Host C with destination port number 6789. Will both of these segments be directed to the same socket at Host C? If so, how will the process at Host C know that these two segments originated from two different hosts?

Yes, both segments will be directed to the same socket. the application uses the source IP to distinguish the segments

Suppose that a Web server runs in Host C on port 80. Suppose this Web server uses persistent connections, and is currently receiving requests from two different Hosts, A and B. Are all of the requests being sent through the same socket at Host C? If they are being passed through different sockets, do both of the sockets have port 80?

No, because the socket is identified by src ip ,src port, dst ip, dst port. For each persistent connection, the Web server creates a separate “connection socket”. Each connection socket is identified with a four---tuple: (source IP address, source port number,destination IP address, destination port number). When host C receives and IP datagram, it examines these four fields in the datagram/segment to determine to which socket it should pass the payload of the TCP segment. Thus, the requests from A and B pass through different sockets

For each persistent connection, the Web server creates a separate “connection socket”. Each connection socket is identified with a four-tuple: (source IP address, source port number, destination IP address, destination port number). When host C receives and IP datagram, it examines these four fields in the datagram/segment to determine to which socket it should pass the payload of the TCP segment. Thus, the requests from A and B pass through different sockets. The identifier for both of these sockets has 80 for the destination port; however, the identifiers for these sockets have different values for source IP addresses. Unlike UDP, when the transport layer passes a TCP segment’s payload to the application process, it does not specify the source IP address, as this implicitly specified by the socket identifier.

In our rdt protocols, why did we need to introduce sequence numbers?

Sequence numbers are used to find out whether the receiver is receiving new data or is it are transmission

In our rdt protocols, why did we need to introduce timers?

> Timers are needed to handle losses in the channel. If an ACK for a packet is not received with in a period, then it is assumed that the packet is lost. So, the packet is transmitted again.

Suppose that the roundtrip delay between sender and receiver is constant and known to
the sender. Would a timer still be necessary in protocol rdt 3.0 , assuming that packets can
be lost? Explain

> A timer would still be necessary in the protocol rdt 3.0. If the round trip time is known then the only advantage will be that, the sender knows for sure that either the packet or the ACK (or NACK) for the packet has been lost, as compared to the real scenario, where the ACK (or NACK) might still be on the way to the sender, after the timer expires. However, to detect the loss, for each packet,a timer of constant duration will still be necessary at the sender

Host A is sending to Host B a large file over a TCP connection. Assume that Host B has no data to send to Host A. Host B will not send acknowledgments to Host A because Host B cannot piggyback the acknowledgments on data. F

The size of the TCP rwnd never changes throughout the duration of the connection. F

Suppose Host A is sending to Host B a large file over a TCP connection. The numberof unacknowledged bytes that A sends cannot exceed the size of the receive buffer. T (Unacknowledged data is the difference between the last byte sent and the last byte ACK'ed.)

Suppose Host A is sending a large file to Host B over a TCP connection. If the sequence number for a segment of this connection is m, then the sequence number for the subsequent segment will necessarily be m + 1. F

The TCP segment has a field in its header for rwnd T (Every TCP segment has a current value of rwnd in the receive window. Suppose that the last SampleRTT in a

TCP connection is equal to 1 sec. The current value of Timeout Interval for the connection will necessarily be > 1sec)

Suppose that the last SampleRTT in a TCP connection is equal to 1 sec. The current value of Timeout Interval for the connection will necessarily be > 1sec . F

Suppose Host A sends one segment with sequence number 38 and 4 bytes of data over a TCP connection to Host B. In this same segment the acknowledgment number is necessarily 42. T

(The sequence number for a segment is the byte-stream number of the first byte in the segment, in this case, 38. The acknowledgement number is the sequence number of the next byte expected, or the first byte of the next segment, in this, since bytes 38, 39, 40, and 41 would be sent, the next byte segment expected is 42, which is the value placed as the acknowledgement number.)

Suppose Host A sends two TCP segments back to back to Host B over a TCP connection.
The first segment has sequence number 90; the second has sequence number 110

a. How much data is in the first segment?

110-90=20byte

b. Suppose that the first segment is lost but the second segment arrives at B. In the
acknowledgment that Host B sends to Host A, what will be the acknowledgment number?

90, because seq 90 packet is what B expects next

Consider the Telnet example discussed in Section 3.5 . A few seconds after the user types
the letter ‘C,’ the user types the letter ‘R.’ After typing the letter ‘R,’ how many segments are
sent, and what is put in the sequence number and acknowledgment fields of the segments

Number of segments: first segment where seq= 43, ack =80;

Second segment: seq = 80, ack = 44

Third segment; seq = 44, ack = 81

Suppose two TCP connections are present over some bottleneck link of rate R bps. Both
connections have a huge file to send (in the same direction over the bottleneck link). The
transmissions of the files start at the same time. What transmission rate would TCP like to give
to each of the connections?

Transmission rate would TCP like to give to each of the connections= R/2

True or false? Consider congestion control in TCP. When the timer expires at the sender,
the value of ssthresh is set to one half of its previous value

False. The slow start threshold(ssthresh) is set to one half of its previous value in the congestion window.

We have said that an application may choose UDP for a transport protocol because UDP
offers finer application control (than TCP) of what data is sent in a segment and

when.

a. Why does an application have more control of what data is sent in a segment?

Comparing with the TCP. When the application ready to send some data to the destination. The first step is to send the message to the socket. After that, the data would to the TCP buffer pass the Socket. Finally, the TCP would grip the data from the TCP buffer. So, the TCP would have more control than the application about what data would send. However,the UDP. Whatever the data gave from the application, the UDP put these messages to the segment directly. So the application can get more control what data would be send

b. Why does an application have more control on when the segment is sent?

Comparing to the TCP. TCP due to the congestion control and flow control. There would be much more delay putting the segment from the buffer to the network layer. However, the UDP does not have these controls, so it means it does not concern about these delays. So an application has more control when the segment is sent over the UDP.

Consider transferring an enormous file of L bytes from Host A to Host B. Assume an MSS
of 536 bytes.

a. What is the maximum value of L such that TCP sequence numbers are not exhausted?

Recall that the TCP sequence number field has 4 bytes.

L = 2^(4*8) = 4,294,967,296 bits = 232 bits

b. For the L you obtain in (a), find how long it takes to transmit the file. Assume that a total
of 66 bytes of transport, network, and data-link header are added to each segment
before the resulting packet is sent out over a 155 Mbps link. Ignore flow control and

congestion control so A can pump out the segments back to back and continuously

Maximum segment size (MSS) = 536 bytes
Segments data=2^{32}/536
=8012999

Total header fields = 66 bytes.

Total number of bytes through the 155Mbps link = 8012999×66 bytes
= 528857934 bytes

Transmitted data = $(2^{32} + 528857934)$
= 4.824×10^9 bytes

$$\text{Transmit time} = \frac{4.824 \times 10^9 \times 8 \text{bits}}{155 \times 10^6 \text{ bps}} \approx \boxed{249} \text{ seconds}$$

Host A and B are communicating over a TCP connection, and Host B has already received
from A all bytes up through byte 126. Suppose Host A then sends two segments to Host B back to- back. The first and second segments contain 80 and 40 bytes of data, respectively. In the first
segment, the sequence number is 127, the source port number is 302, and the destination port
number is 80. Host B sends an acknowledgment whenever it receives a segment from Host A.

a. In the second segment sent from Host A to B, what are the sequence number, source
port number, and destination port number?

Sequence number = first segment of sequence number+ destination port number

=127+80

=207

So, sequence number=207

Source port number = 302

Destination port number= 80

b. If the first segment arrives before the second segment, in the acknowledgment of the first
arriving segment, what is the acknowledgment number, the source port number, and the
destination port number?

Acknowledgement number= 207

Source port number = 80

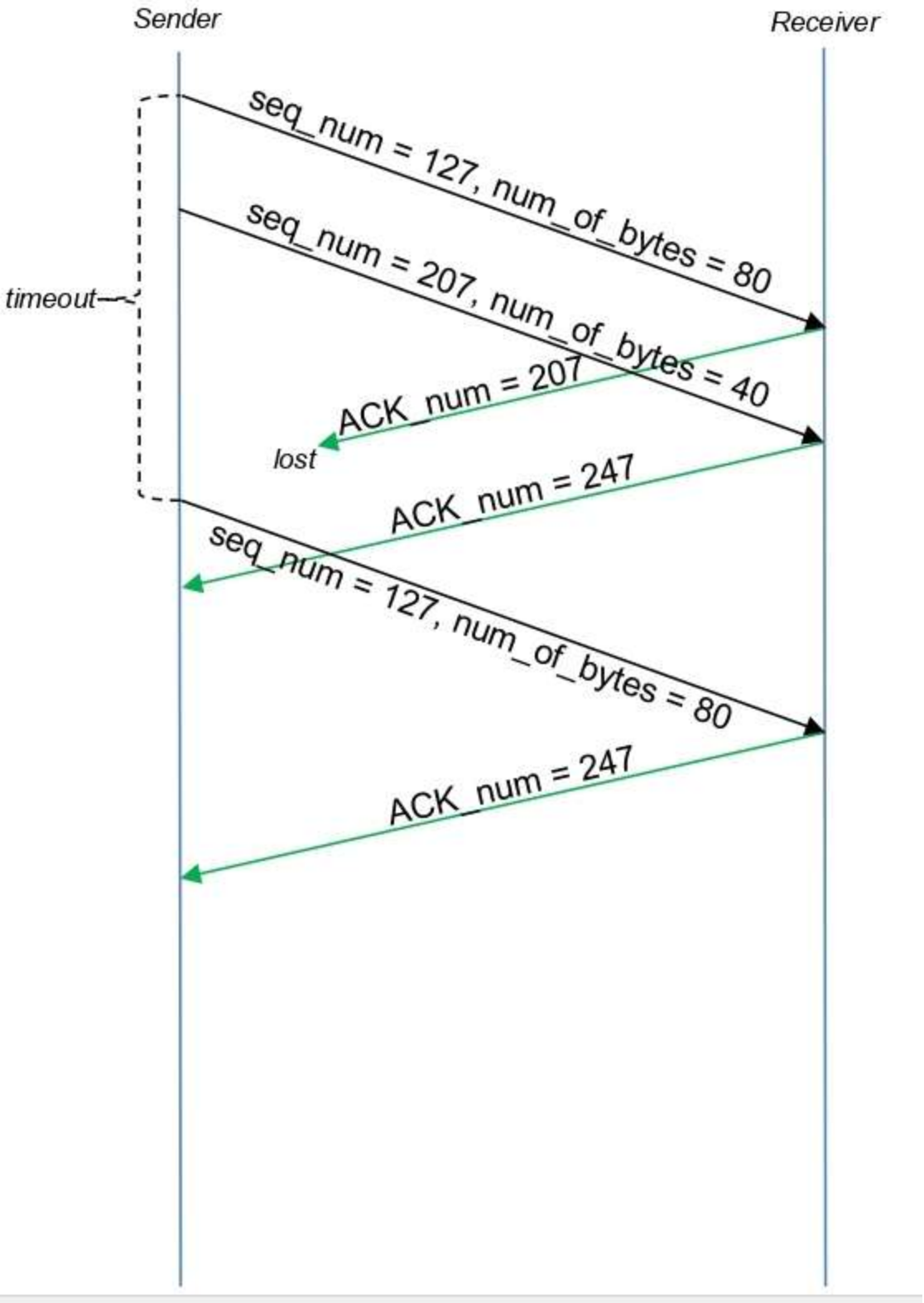
Destination port number= 302

c. If the second segment arrives before the first segment, in the acknowledgment of the first
arriving segment, what is the acknowledgment number?

Acknowledgement number=127

d. Suppose the two segments sent by A arrive in order at B. The first acknowledgment is
lost and the second acknowledgment arrives after the first timeout interval. Draw a timing
diagram, showing these segments and all other segments and acknowledgments sent.
(Assume there is no additional packet loss.) For each segment in your figure, provide the
sequence number and the number of bytes of data; for each acknowledgment

that you
add, provide the acknowledgment number.


Sender
Receiver
seq_num = 127, num_of_bytes = 80
seq_num = 207, num_of_bytes = 40
timeout
ACK_num = 207
lost
ACK_num = 247
seq_num = 127, num_of_bytes = 80
ACK_num = 247

In Section 3.5.3 , we discussed TCP’s estimation of RTT. Why do you think TCP avoids
measuring the SampleRTT for retransmitted segments?

The retransmitted segments contain the same data and the same sequence numbers
as the previously sent packets. Therefore, for the retransmitted segments, we would expect the same ACK numbers as the previously sent TCP segments. When we receive these paticular ACKs from the receiver, we don't really know or care whether they were sent as responses to the retransmitted segments or to the previously sent TCP segment.

It is possible that after a very short time, we receive the ACK for the retransmitted data segment. But that could actually be a delayed ACK for the original TCP segment. Either the data transmission or the ACK reply was probably delayed. Both of them could result in a late ACK. If we count this time in to compute the RTT estimation, we would mistakenly drop the RTT average by a big percentage. This RTT would trigger a faster retransmission, which would worsen the already jammed network traffic.

P34. Assuming TCP Reno is the protocol experiencing the behavior shown above, answer the following questions. In all cases, you should provide a short discussion justifying your answer.

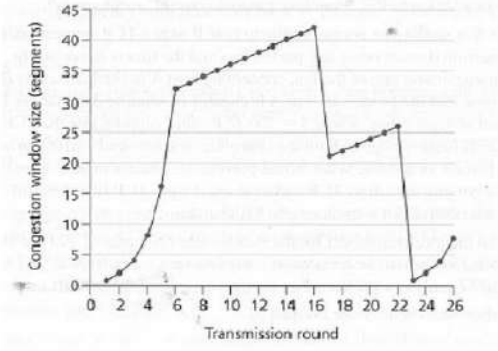
a. Identify the intervals of time when TCP slow start is operating.

b. Identify the intervals of time when TCP slow start is operating.

c. After the 16th transmission round, is segment loss detected by a triple duplicate ACK or by a timeout

d. After the 22nd transmission round, is segment loss detected by a triple duplicate ACK or by a timeout

e. What is the initial value of threshold at the first transmission round?



f. what is the value of threshold at the 18th transmission round

g. what is the value of threshold at the 24th transmission round

h. During what transmission round is the 70th segment sent?

i. Assuming a pkt loss is detected after the 26th round by the receipt of a triple duplicate ACK, what will be the values of the congestion window size and of threshold?

a) TCP slow start is operating in the intervals [1,6] and
[23,26]
b) TCP congestion avoidance is operating in the intervals [6,16] and [17,22]
c) After the 16th transmission round, packet loss is
recognized by a triple duplicate ACK. If there was a timeout, the congestion window size would have dropped to 1.
d) After the 22nd transmission round, segment loss is detected due to timeout,

and hence the congestion window size is set to 1.
e) The threshold is initially 32, since it is at this window size that slow start stops and congestion
avoidance begins.

f) The threshold is set to half the value of the congestion window when packet loss is detected. When loss is detected during transmission round 16, the congestion windows size is 42. Hence the threshold is 21 during the 18th transmission round.

g) The threshold is set to half the value of the congestion window when packet loss is detected. When loss is detected during transmission round 22, the congestion windows size is 26. Hence the threshold is 13 during the 24th transmission round.

h) During the 1st transmission round, packet 1 is sent; packet 2 - 3 are sent in the 2nd transmission round; packets 4 - 7 are sent in the 3rd transmission round; packets 8 -15 are sent in the 4th transmission round;
packets16 -31 are sent in the 5th transmission round; packets 32
-63 are sent in the 6th transmission round; packets 64 – 97 are sent in the 7th transmission round. Thus packet 70 is sent in the 7th transmission round.
i) The congestion window and threshold will be set to half the current value of the congestion window when the loss occurred. Thus the new values of the threshold and window will be 4.

What is meant by destination-based forwarding? How does this differ from generalized forwarding (assuming you've read Section 4.4 , which of the two approaches are adopted by Software-Defined Networking)?

> destination-based: router forwards datagram based on destination IP address
> -generalized: router forwards based on other factors too, like header field values (TCP/UDP source/destination port numbers, etc.)

Suppose that an arriving packet matches two or more entries in a router's forwarding table. With traditional destination-based forwarding, what rule does a

router apply to determine which of these rules should be applied to determine the output port to which the arriving packet should be switched?

A router uses longest prefix matching to determine which link interface a packet will be forwarded to if the packet's destination address matches two or more entries in the forwarding table. In this case, the packet that has the longest prefix match with the packet's destination will be the one forwarded to the link interface.

Describe how packet loss can occur at input ports. Describe how packet loss at input ports can be eliminated (without using infinite buffers).

Packet loss occurs if queue size at the input port grows large because of slow switching fabric speed and thus exhausting router’s buffer space. It can be eliminated if the switching fabric speed is at least n times as fast as the input line speed, where n is the number of input ports

Describe how packet loss can occur at output ports. Can this loss be prevented by increasing the switch fabric speed?

Packet loss can occur if the queue size at the output port grows large because of slow outgoing line-speed. Cant be prevented

What is HOL blocking? Does it occur in input ports or output ports?

HOL blocking – a queued packet in an input queue must wait for transfer through the fabric because it is blocked by another packet at the head of the line. It occurs at the input port.

Do routers have IP addresses? If so, how many?

Yes. They have one address for each interface.

Suppose there are three routers between a source host and a destination host. Ignoring fragmentation, an IP datagram sent from the source host to the

destination host will travel over how many interfaces? How many forwarding tables will be indexed to move the datagram from the source to the destination

8 interfaces; 3 forwarding tables

Suppose an application generates chunks of 40 bytes of data every 20 msec, and each
chunk gets encapsulated in a TCP segment and then an IP datagram. What percentage of each
datagram will be overhead, and what percentage will be application data

50% overhead. IP→40bytes, TCP →40bytes.

Suppose you purchase a wireless router and connect it to your cable modem. Also suppose that your ISP dynamically assigns your connected device (that is, your wireless router)
one IP address. Also suppose that you have five PCs at home that use 802.11 to wirelessly
connect to your wireless router. How are IP addresses assigned to the five PCs? Does the
wireless router use NAT? Why or why not?

Typically the wireless router includes a DHCP server. DHCP is used to assign IP addresses to the 5 PCs and to the router interface. Yes, the wireless router also uses NAT as it obtains only one IP address from the ISP.

what is meant by a "plug-and play" or "zeroconf" protocol?

plug and play is a configuration of a host to a network. automatic configuration is zeroconf

What is meant by the “match plus action” operation of a router or switch? In the case of
destination-based forwarding packet switch, what is matched and what is the

action taken? In
the case of an SDN, name three fields that can be matched, and three actions that can be taken

> Match plus action" means that a router or a switch tries to find a match between some of the header values of a packet with some entry in a flow table, and then based on that match, the router decides to which interface(s) the packet will be forwarded and even some more operations on the packet. In the case of destination-based forwarding packet switch, a router only tries to find a match between a flow table entry with the destination IP address of an arriving packet, and the action is to decide to which interface(s) the packet will be forwarded. In the case of an SDN, there are many fields can be matched, for example, IP source address, TCP source port, and source MAC address; there are also many actions can be taken, for example, forwarding, dropping, and modifying a field value.

Name three header fields in an IP datagram that can be "matched" in OpenFlow 1.0 generalized forwarding. What are three IP datagram header fields that cannot be "matched" in OpenFlow?

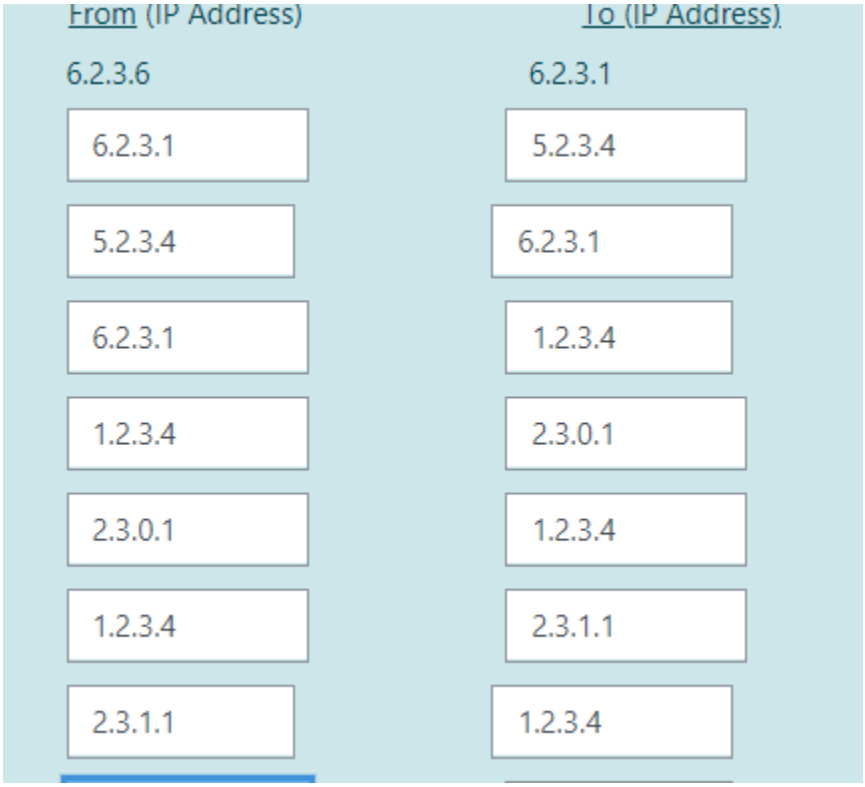
> Three example header fields in an IP datagram that can be matched in OpenFlow 1.0 generalized forwarding are IP source address, TCP source port, and source MAC address. Three fields that cannot be matched are: TTL field, datagram length field, header checksum (which depends on TTL field).

forwarding: move packets from router's input to appropriate router output

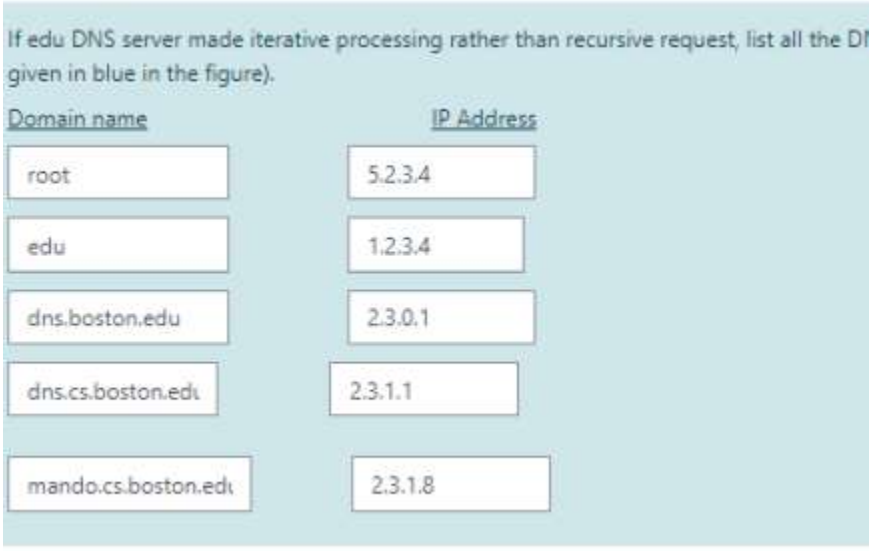
routing: determine route taken by packets from source to destination

Usually routing runs continuously to establish the routing tables before the packets are forwarded and in anticipation of packets.

Some clues not to memorize



From (IP Address)	To (IP Address)
6.2.3.6	6.2.3.1
6.2.3.1	5.2.3.4
5.2.3.4	6.2.3.1
6.2.3.1	1.2.3.4
1.2.3.4	2.3.0.1
2.3.0.1	1.2.3.4
1.2.3.4	2.3.1.1
2.3.1.1	1.2.3.4



If edu DNS server made iterative processing rather than recursive request, list all the DI given in blue in the figure).

Domain name	IP Address
root	5.2.3.4
edu	1.2.3.4
dns.boston.edu	2.3.0.1
dns.cs.boston.edu	2.3.1.1
mando.cs.boston.edu	2.3.1.8

List all the DNS mappings (domain name – IP address) in the local DNS server's cache after all the queries have been processed given in blue in the figure).

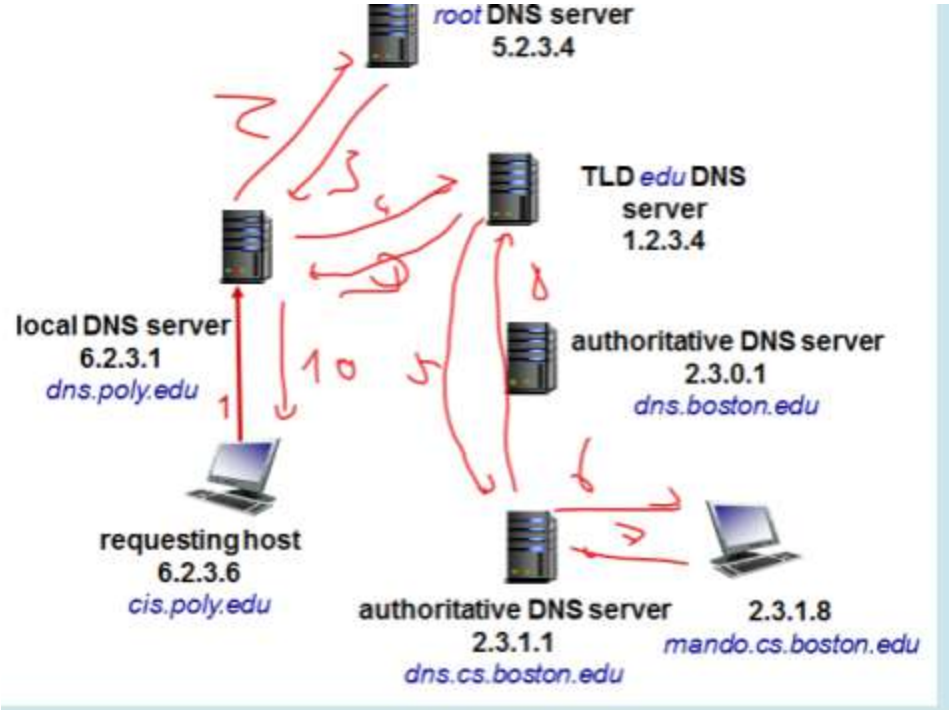
Domain name	IP Address
root	5.2.3.4
edu	1.2.3.4
dns.cs.boston.edu	2.3.1.1
mando.cs.boston.edu	2.3.1.8
cis.poly.edu	6.2.3.6

If edu DNS server made iterative processing rather than recursive request, list all the DNS mappings (domain name – IP addres server's cache after all the queries have been processed. (Domain names are given in blue in the figure).

Domain name	IP Address
root	5.2.3.4
edu	1.2.3.4
dns.cs.boston.edu	2.3.1.1
mando.cs.boston.edu	2.3.1.8
cis.poly.edu	6.2.3.6

bunu yaptım

Number	From (IP Address)	To (IP Address)
1	6.2.3.6	6.2.3.1
2	6.2.3.1	5.2.3.4
3	5.2.3.4	6.2.3.1
4	6.2.3.1	1.2.3.4
5	1.2.3.4	2.3.1.1
6	2.3.1.1	2.3.1.8
7	2.3.1.8	2.3.1.1
8	2.3.1.1	1.2.3.4
9	1.2.3.4	6.2.3.1
10	6.2.3.1	6.2.3.6



Organization 1 → 200.23.64.1 - 200.23.79.254
Organization 2 → 200.23.80.1 - 200.23.175.254
Organization 3 → 200.23.96.1 - 200.23.111.254
Organization 4 → 200.23.112.1 - 200.23.127.254