Network Systems (201600146/201600197), Test 3

April 9, 2020, 13:45–16:45

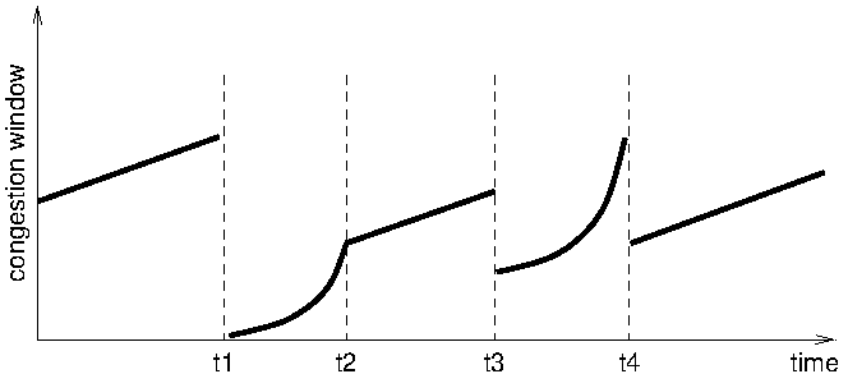
(Taken together with test 2, online at home because of the corona pandemic)

The correct answers are marked with an arrow →; text on grey background gives further explanation.

---

5. Congestion control and QoS

TCP Congestion Control



The above figure shows schematically how TCP's congestion window evolves over time. The connection had already been active for a while before the beginning of the figure. The following three questions are about this figure.

1 pt **Q 5.1** What happened at time t1 ?

→A. Timeout
B. Triple duplicate ack
C. Receive window was full
D. Congestion window was full
E. ECN "congestion experienced" notification was received

1 pt **Q 5.2** In which phase is TCP in the interval between times t2 and t3?

A. Slow start
→B. Additive increase
C. CUBIC
D. This is incorrect behaviour for standard TCP congestion control

1 pt **Q 5.3** In which phase is TCP in the interval between times t3 and t4?

A. Slow start
B. Additive increase
C. CUBIC
→D. This is incorrect behaviour for standard TCP congestion control

This behaviour is incorrect. Between t3 and t4, we see an exponential (looking) growth, but starting far above 0. Standard TCP only does an exponential growth as part of the slow-start phase, but that phase starts with a congestion window of 1 packet, like we see betwen t1 and t2.

1 pt **Q 5.4** In standard TCP congestion control, what role does the receiver play?

A. It calculates the correct window and puts this in the 'receiver window' TCP header field.
B. It retransmits acknowledgements if they are lost.
C. When a packet is lost due to congestion, it asks for a retransmission.
D. It quickly sends three identical acknowledgements when it detects congestion.

→E. It sends an acknowledgement for incoming packets, with the ACK field telling which packet it expects next.

The receiving side in TCP is rather passive, it just sends acknowledgements where appropriate. All the hard work, such as calculating the congestion window, is done by the sending side.

1 pt **Q 5.5** Which statement about ECN is true?

A. ECN is purely a network-layer issue.
B. ECN is purely a transport-layer issue.
C. ECN can only work with TCP flows.
D. If a router supports ECN, it never drops a packet.
→E. None of the above.

ECN concerns both the network layer (routers have to mark packets when they are congested) and the transport layer (where the receiver, upon receiving a congestion notification, has to tell the sender to reduce its sending rate). It is not limited to TCP; other transport-layer protocols could also be made ECN-compliant. And even an ECN-capable router may still drop packets, either when the congestion becomes too bad, or when dealing with end hosts that do not support ECN.

1 pt **Q 5.6** Why is the "slow start" phase called slow start?

A. It is slower than using no congestion control at all.
B. It is too slow on long fat pipes.
C. It is slower than additive increase.
D. It is slower than multiplicative decrease.
E. It is the main cause of slowly loading web pages.

Before TCP congestion control was implemented, TCP would just transmit as much as it wanted (or rather, as much as the receiver window would allow).

Quality of Service

Consider a flow described by a token bucket with $r = 100\,000$ tokens/second and $B = 60\,000$ tokens (assuming one token per byte, as usual). Suppose this flow transmits every 0.4 s a burst of 50 000 bytes. Is this allowed?

Q 5.7

A. Yes, this is allowed.
→B. No, for this to be allowed r should be higher.
C. No, for this to be allowed r should be lower.
D. No, for this to be allowed B should be higher.
E. No, for this to be allowed B should be lower.

Q 5.8 If you answered that r or B should be different, what should its value be?

→ $r \geq 125\,000$ tokens/second.

2 pt *The above two questions together are worth 2 points.*

The flow transmits 50 000 bytes per 0.4 seconds, that is on average 125 000 bytes per second. That is more than r allows, so it should be increased to 125 000 or more.

1 pt **Q 5.9** Suppose this flow transmits every 0.2 s a burst of 10 000 bytes. Is this allowed?

→A. Yes, this is allowed.
B. No, for this to be allowed r should be higher.
C. No, for this to be allowed r should be lower.
D. No, for this to be allowed B should be higher.
E. No, for this to be allowed B should be lower.

Q 5.10 If you answered that r or B should be different, what should its value be?

Both the burst size and the average rate of the flow fit the given token bucket model, so there is no need to change anything.
As a consequence, no answer needs to be given to Q 5.10, and that question is worth 0 points.

Q 5.11 Suppose we have 3 flows, each obeying the above token bucket model, sharing a single link of 400 000 bytes/second. If FIFO scheduling is used, what is the maximum delay a packet from one of the flows can experience?

Value (in seconds):

→ 0.45

Q 5.12 Explanation:

→ Worst case each source transmits nothing for a while, allowing all buckets to fill up completely, and all three drop a maximum number of packets into the network all at once. Then look at the rearmost of all these packets. It's at the rear end of a queue containing $3B = 180\,000$ bytes, which are transmitted at 400 000 bytes per second: that takes $180/450 = 0.45$ seconds.

2 pt *Together, the above two questions (the value and the explanation) are worth 2 points.*

1 pt **Q 5.13** Using Fair Queueing, is it possible that a flow "starves", i.e., doesn't get a chance to transmit its packets due to other flows sending very much data?

→A. No, this is not possible.
B. Yes; to avoid this, Weighted Fair Queueing should be used.
C. This is only possible if at least one of the other flows exceeds the r value of its token bucket specification.
D. This is only possible if at least one of the other flows exceeds the B value of its token bucket specification.
E. This is only possible if all other flows exceed the r value of their token bucket specifications.
F. This is only possible if all other flows exceed the B value of their token bucket specifications.

Fair queueing effectively sets aside an equal fraction of the available bandwidth for each of the flows. So a flow always gets to use that amount of bandwidth, no matter how much data the other flows try to offer.

1 pt **Q 5.14** Is DNS an elasic or a non-elastic application?

A. Non-elastic, as the internet can't reasonably work without it.
B. Non-elastic, as the size of DNS responses cannot be adapted to network conditions.
→C. Elastic, since it can work well regardless of the network bandwidth or delay.
D. Elastic, because it runs on UDP like most multimedia applications.
E. Neither, this classification does not apply to DNS.

1 pt **Q 5.15** Which statement about Integrated Services (IntServ) and Differentiated Services (DiffServ) is correct?

A. IntServ is more scalable than DiffServ.
→B. DiffServ looks up the service class of the packet in the IP header.
C. IntServ looks up the service class of the packet in the UDP header.
D. IntServ is for applications which have both audio and video, while DiffServ is for ones having only audio.
E. DiffServ requires QoS applications to make a reservation, while IntServ doesn't.

1 pt **Q 5.16** DiffServ uses a 6-bit field in the IP header. What consequence does this have?

→A. At most 64 different service classes are possible.
B. At most 64 simultaneous QoS-enabled flows are possible.
C. At most 64 routers can be accomodated in a DiffServ domain.
D. At most 64 hosts can use DiffServ simultaneously.

E. At most 64 hosts can participate in a multicast DiffServ session.

1 pt **Q 5.17** What does it mean if we say that a real-time application behaves in a 'TCP-Friendly' way?

→A. It does not use more bandwidth than TCP would do in the same circumstances.
B. It uses exactly as much bandwidth as TCP would do in the same circumstances.
C. When it shares a bottleneck link with a TCP flow, it will stop sending so as to not disturb the TCP flow.
D. It avoids congestion by using TCP rather than UDP.
E. It avoids congestion by using UDP rather than TCP.

---

6. Security

1 pt **Q 6.1** In WPA2/3 Personal to whom do you authenticate? And to whom in WPA2/3 Enterprise?

AP: Access Point; AS: Authentication Server; PSK: Pre-Shared-Key.

A. Personal: to the AS with credentials. Enterprise: to the AP with a PSK.
B. Personal: to the AS with a PSK. Enterprise to the AP with credentials.
C. Personal: to the AP with credentials. Enterprise: to the AS with a PSK
→D. Personal: to the AP with a PSK. Enterprise to the AS with credentials.

1 pt **Q 6.2** You have a need to send a highly confidential document to a friend. It is of the utmost importance that your communication cannot be read by a third party, now or in the future. What do you use?

A. A communication channel over WEP, IPsec in AH / Transport mode, and SSHv1.
B. A communication channel over WPA2, IPsec in ESP / Transport mode, TLSv1.2, and PGP encryption.
C. A communication channel over WPA4, IPsec in ESP / Tunnel mode, SSHv1, and TLSv1.5.
→D. A communication channel over WPA3, IPsec in ESP / Transport mode, TLSv1.3 and PGP encryption.

A doesn't encrypt or use technologies with flaws. B is almost correct but doesn't guarantee it can't be read in the future. C doesn't exist yet (for the most part).

1 pt **Q 6.3** In which layer and how often is the SSH server's public key presented?

A. In the SSH-CONNECT layer, only for unknown (first) connections.
B. In the SSH-CONNECT layer, on every connection.
C. In the SSH-AUTH layer, only for unknown (first) connections.
D. In the SSH-AUTH layer, on every connection.
E. In the SSH-TRANS layer, only for unknown (first) connections.
→F. In the SSH-TRANS layer, on every connection.

As the book says in section 8.5.2, it's in the SSH-TRANS layer that the client authenticates the server, which involves its public key. This is repeated on every connection, as the client will again want to know to which server it is talking; the client will warn the user if the server presents a different public key than the previous time.

1 pt **Q 6.4** Imagine this scenario, host with address IP_1 is behind router with address IP_A, and host with address IP_2 is behind router with IP_B. Originally there was an IPsec tunnel in transport mode between the two hosts. However, the network operators upgraded the routers and the tunnel was replaced with an IPsec tunnel in tunnel mode between the two routers. You were capturing traffic between the two routers during the upgrade. Did the source and destination addresses in the IP header change? (note: the answers consider one way communication to keep them brief)

A. No, everything stayed the same in the IP headers.
→B. Yes, the source address IP_1 is replaced with IP_A and the destination address IP_2 is replaced with IP_B.
C. Yes, the source address IP_1 is replaced with IP_A and the destination address IP_B is replaced with IP_2.

D. Yes, the source address IP_A is replaced with IP_1 and the destination address IP_2 is replaced with IP_B.
E. Yes, the source address IP_A is replaced with IP_1 and the destination address IP_B is replaced with IP_2.
F. Yes: after the change, all addresses are encrypted and thus unreadable.
G. No: both before and after the change, all addresses were encrypted and thus unreadable.

When transport mode is used, the packets carry the IP addresses of the end hosts involved in the connection, unencrypted because otherwise the network couldn't deliver the packets.
After changing to tunnel mode, the packets between the endhosts are completely (including their IP addresses) encrypted, and transported inside IP packets between the two routers; those packets will have the IP addresses of the routers in their unencrypted IP header.

1 pt **Q 6.5**

For performing a spoofing attack, the attacker counterfeits:

→A. The source IP address.
B. The destination IP address
C. The source UDP/TCP port
D. The destination UDP/TCP port
E. The header checksum
F. The fragment offset

1 pt **Q 6.6** A network has a network firewall configured with the following policies:

1. All traffic inbound is forbidden, unless it belongs to an established connection.
2. All traffic outbound is allowed

The computers on the network behind the firewall can still navigate on the web. Which kind of firewall is deployed:

A. Stateless Firewall
→B. Stateful Firewall
C. Circuit Level Gateway
D. Application Firewall

A stateless firewall can't suffice, as such a firewall doesn't know whether a packet belongs to an established connection.

1 pt **Q 6.7** Suppose you run a web server. You want to do things securely, so you enable HTTPS and you add a firewall in front of the web server. You use a stateless firewall with two rules:

1. All traffic destined to tcp:443 is allowed.

2. All other traffic is dropped.

Are users able to visit your (secure) website?

A. Yes, connections are able to pass through the firewall without problem.
B. No, the TCP SYN is dropped by the firewall.
C. Yes, but you can only do HTTP GET requests, not POST.
→D. No, the TCP SYN+ACK is dropped by the firewall.
E. No, that can only be achieved using a stateful firewall.

The SYN+ACK is dropped because it has source port 443, not destination port 443.

1 pt **Q 6.8**

With the current Covid-19 social-distancing measures in place, staying home is a virtue and a necessity. You decide to make the best of the situation by engaging in a gaming tournament. However, despite you have a very good Internet connection, you find yourself regularly losing connection to the gaming

site. You decide to investigate. Traffic analysis on your home router shows large amount of incoming DNS replies, of type ANY. What is likely to be happening to your connection?

A. your computer is infected and making large number of DNS requests
B. your home connection is being flooded by unwanted traffic gaming traffic
→C. you are the victim of a DNS reflection and amplification attack
D. you are the victim of a DNS flooding attack
E. the gaming software needs DNS to update its status but it is too aggressive for your connection

You didn't send that many DNS requests yourself (otherwise you would have seen them in the traffic analysis), so the large number of replies must be replies to DNS requests sent by someone else. That's a reflection attack: someone else sends DNS requests with your IP address as the source address, so that the responses go to you.

1 pt **Q 6.9**

Every day at 14:00, the RIVM (the Dutch National Institute for Public Health and the Environment) publishes the daily updates on the Covid-19 situation. Today you also try to connect to the website at precisely 14:00. You connection fails with a TCP Reset. This is because the RIVM is experiencing what we call a "flash-crowd", i.e. a number of visitors larger than what a host can handle in a very short amount of time. In a way, you can consider a flash-crowd as a form of benign, legitimate and uncoordinated Denial of Service attack. What is likely to be happening to the RIVM website during a flash crowd?

A. the webserver keeps periodically rebooting
B. your request is put in a queue and will be served eventually, you just need to wait
→C. the TCP/IP stack is full and unable to accept additional requests
D. your request is malformed and has been droppen by the firewall
E. the page you are trying to access is broken, hence the error

Answer B is not correct because the text says that you do receive a TCP RST packet; thus, the server tells you it can't process your packets and doesn't accept (or prematurely terminates) your TCP connection.

Grade calculation

The grade was calculated using the following formula:

$$\text{grade} = \frac{\text{points} - 4.3}{24 - 4.3} \times 9 + 1$$

24 is the maximum number of points for this test.
4.3 is the "guessing factor": it's the number of points one would get on average from giving totally random answers to the multiple-choice questions.