TIME LIMIT: 90 minutes

START: 21:40

END: 23:10

(Q1)

(a)

(i)

https://192.168.1.1 ½ mark

Use http instead of https – not all routers support https

(ii)

??? 0/1 - Go to the port forwarding or port triggering submenu (may change depending on router model)

(iii)

Port 60000 - It is a dynamic port designed for temporary use (such as for this #NetOpsAthon event. (I could choose any port from 49152 to 65535)

(iv)

The device you want to access the event from, in order to allow port forwarding from the router to your device

Firewall for router, not local device

(b)

Throughput=2Mbps = 2\*10^6 bps

L (number of bits) = 1GB = 8 \* 10^9 bits

Transmission Delay = (8\*10^9) / (2\*10^6) = 4000s

transfer time = propagation delay + transmission delay

69mins \* 60 + 42 secs = propagation delay + 4000s

propagation delay = 4182 - 4000 seconds

= 182 seconds

Assume speed of light, c, = 3 \* 10 ^ 8 m/s

s = d/t => d = s \* t

d = c\*t

= 3\*10^8 \* 182

= 5.46\*10^10 metres

= 5.46\*10^7 km

--------------------------

Final Answer: 5.46\*10^7 km

4/4

(c)

Assumption: All lines beginning with "#MKAY" are from the server at example.edu to the client and all other lines are from the client to the server.

OHAI is a plane-text protocol/application being used e.g. telnet. Connection-oriented (not necessarily TCP since we are “connecting to port 12345” – 2/4

The client is connecting to the example.edu server via the OHAI command. The second line "#MKAY" represents the server's acknowledgement of the client attempting to connect with it, and signals that the server is ready to receive any commands. "PORT 12345" is the client telling the server to connect to the client on the client's port 12345 (when connecting, but not yet), which is acknowledged by the server saying "#MKAY PORT SET.TO 12345). Then the client asks for a file given by "/path/to/file.txt" using the "GIEF" command. To send the file, the server has to finally establish the actual connection, so it does so with "#MKAY CONNECTING TO 12345" before sending the file itself to the client on port 12345. This corresponds to the line "#MKAY CONNECTING TO 12345". The server then signals that it is prepared for any other requests and that the task is complete with "#MKAY". The client's message "KTHXBAI" is to tell the server it is disconnecting and "#MKAY DISCONNECTING" indicates the server has acknowledged this and is ending the connection.

The "OHAI" command could be translated to "HELLO", "#MKAY" to "OKAY" or "READY" (for more input), "GIEF" to "GIVE" and "KTHXBAI" to "GOODBYE".

(d)

The use of SSTHRESH terminology indicates the use of the Slow Start congestion control algorithm, so I will use Slow Start for this question. Also assume that the receiver window (for B) is always greater than the congestion window. As there is no data loss, for every packet it receives, B sends a good acknowledgement back to A. (So no packets are ever dropped/retransmitted)

Batch 1:

Initialise the congestion window, W\_0 = MSS. So the window is initially one byte.

So in the first round trip, one byte is transferred, so the character "A" is transferred to B.

Batch 2:

Since W\_0 <= SSTHRESH, increase W\_1 by one MSS for each acknowledgement. As we only have one acknowledgement, W\_1 = 2B.

So in the second round trip, send two packets of 1B each (and therefore characters "B" and "C".

Batch 3:

W\_1 <= SSTHRESH. So W\_2 = W\_1 + (1 \* MSS) \* 2 good acknowledgements = 4B. So in this transfer, transfer bytes "D", "E", "F", "G".

So the data transfer is complete in 3 trips. At this stage, W\_2 > SSTHRESH so future transfers would use congestion avoidance until a packet loss or timeout occurs.

(e)

(i) Allow

(ii) 49152-65535

(iii) Allow

(iv) 20, 21

(v) TCP

(vi) 25, 110, ephemeral (assuming there are multiple different mail servers within the subnet)

(vii) TCP

(viii) Enable POP3 Mail Server access (+SMTP(S) to send email)

(ix) Allow

(x) \*

(xi) 53

(xii) Deny

(2)

(a)

(A, D, 5) => (A, D, 11) as (A, C, 4) and (C, D, 7)

(B, D, 8) => (B, D, 12) as B to C is 5 and C to D is 7 B does not change as it is not broadcasting D and there is no direct route from B to D (known route, although one existed)

(C, D, 7) => (C, D, 15) as C to A is now 4 and A to D is 11

(E, D, 9) => (E, D, 15) as E to B is 7 and B to D is now 8. (E, D, as B does not have a direct route to D

(b) Port 25 is reserved for SMTP. The local address localhost:25, corresponding to the SMTP port is mapped to foreign address 0.0.0.0:0, which represents an unknown network address, while ports 54322, 54321, 54320 are local addresses mapped to localhost:25. So these ephemeral ports appear as the SMTP port of the device, so the virus allows a hacker connected to port 54322 to forward emails via the SMTP protocol to appear as if they were the true owner of the email. 54322 has established a connection, while 54321 and 54320 have not. This means that a hacker is currently using the SMTP connection on port 54322.

(c) The MAC Address for IP 10.0.1.2 is 55:66:77:88:99:00, not 12:34:56:78:90:AB. This is a ARP poisoning/MAC spoofing attack. It hopes to replicate a different MAC address to the correct MAC address, so traffic is redirected to the spoofed MAC address instead of the real one. (So requests and frames are sent to the spoofing party instead of the real server).

(ii)Add a new router in between Server0 and Switch0.

(iii) Replace the hub with a switch.

(d) (i) They should purchase ethernet cables, UTP for low costs, coaxial or optical fiber if cost is not as important. This is required to connect the desktops to the internet, as well as supply switches/routers with access to other networks

(ii) purchase wireless access points/repeaters to enable wireless communication between devices within the same network, e.g. mobiles. And purchase a router to create their own subnet for all their devices. Within the subnet purchase switches to create a star topology for quick communication.

(e)

(i)

- BGP is for inter-AS routing not intra-AS

- SHA is no longer a secure encryption method SHA is for hashing not encryption

- QUIC has not existed for that long

- ACLs are stateless firewalls ACLs can be stateful. But statelike should be stateless.

(ii) Maintaining and updating networking security measures, to ensure secure communication (given by encryption and firewalls). Optimising sub net speed given, by strong focus on Intra-AS routing and need for experience in optimisation of transport/network layer.