TDTS21 – Advanced Networking [vt 2025 version of the course]
Final Examination: 14:00 on Thursday, June 5, 2025
Total Marks: 40
Grade Requirements: Three (24/40); four (30/40); and five (38/40).
Assistance: None (closed book, closed notes, and no electronics)
Instructor/examiner: Niklas Carlsson

General instructions

- Read all instructions carefully, including these!
- Some questions have multiple tasks/parts; please remember to address *all*.
- The total possible marks granted for each question are given in parentheses. The entire test will be graded out of 40. This gives you 10 marks per hour, or six minutes per mark, **plan your time accordingly**.
- The exam consists of (6+1) = 7 questions. Please check that this exam is complete.
- When applicable, please explain and clearly show how you derived your answers.
- Your final answers should be clearly stated.
- Where a discourse or discussion is called for, be concise and precise.
- If necessary, state any assumptions you made in answering a question.
- Answer questions as precisely and clearly as possible. Solving the *wrong* question may result in deductions! It is better to solve the *right* question incorrectly, than the *wrong* question correctly.
- Please answer in English. Use Swedish only if needed (e.g., for unknown words).
- Many questions are designed to be answered using concrete example **figures/tables**. Please try to use figures/tables/bullets and be as precise and clear as possible.

2025 exam (in-person)

- Please **number pages**, answer **at most one question per page**, report **answers in the same order** as the corresponding questions appear in the exam, and clearly state your **assigned AID at the top/header of each page**.

Good luck with the exam!

Question 1: Intro and address basics (10 points)

Consider a scenario in which you view a video on the YouTube website. Assume that the video is served from a datacenter located in eastern USA and you are located on the LiU campus. Furthermore, consider the IPv4 packets associated with the video transfer, including both requests and video content.

a) Please draw an image of the end-to-end data path as well as all entities mentioned as part of this question.

b) For each of the addresses listed next, please draw an image, and briefly (and clearly!) explain how your machine obtains the following addresses (i) your own IP address, (ii) your MAC address, and (iii) the YouTube server's IP address.

c) Draw an image and explain how the following addresses are used to determine a good end-to-end path in the above scenario: (iv) Google's AS number and (v) LiU's AS number.

d) Explain which of these addresses are used in the control plane and which are used in the data plane.

e) Please show the address-related header information associated with a "packet" sent from your computer to the above YouTube server (using HTTPS) when it passes your network interface card. The image should clearly indicate how encapsulation is done and should include MAC addresses, IP addresses, port numbers, and web-related addresses.

f) Please indicate what addresses from part (e) that would be visible (and not visible) to Wireshark or another packet analyzer (when using HTTPS).

g) Using the above example, please explain how (or why not) your computer can learn about the server's (i) host name, (ii) IP addresses, and (iii) MAC address.

Question 2: TCP basics (4 points)

Use figures and examples to illustrate why TCP's additive increase and multiplicative decrease (AIMD) mechanism provides some stability and fairness.

Question 3: BGP basics and trends (6 points)

Consider now BGP routing.

a) Please draw a figure that clearly shows an example where BGP may result in a sub-optimal routing path and use the figure to explain why BGP would result in a sub-optimal route in this case.

b) Please show and explain how some content providers' use of peering agreements has changed over time and the impact that this has had on the "distances" observed on the Internet.

c) Please show and explain (using an example scenario) how an AS can perform an interception attack of a prefix.

Question 4: TCP and QUIC (6 points)

First, use figures and example numbers to illustrate how Cubic TCP differs from TCP Reno under some example scenario. Your example scenario should illustrate all phases of a typical TCP connection and should cover both the initial handshake phase as well as loss events detected using both duplicate ACKs and timeouts.

Second, list and briefly explain the key ideas behind (i) BBR, (ii) compounded TCP, and (iii) QUIC. Please be concise and use a sentence or two per bullet.

Question 5: Tail statistics (6 points)

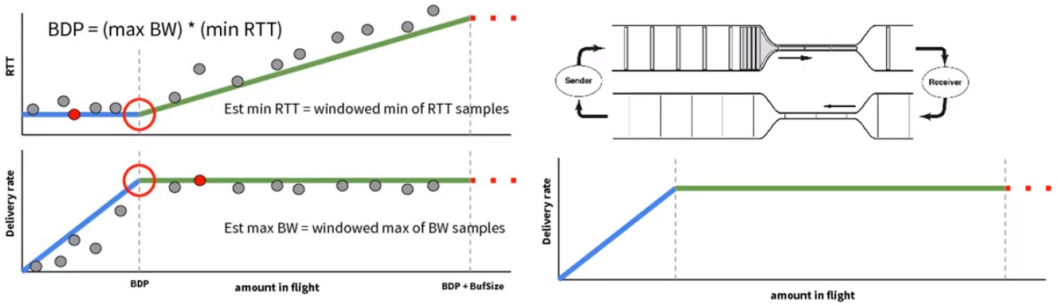
Consider tail statistics

a) Please explain how a heavy-tailed distribution relates to an exponential distribution and support your answer with figures that compare well-selected example distributions that illustrate your answer.
b) Please draw example plots that include examples of both a power-law distribution and an exponential distribution when plotted on (i) lin-lin scale, (ii) lin-log scale, and (iii) log-log scale. Your plots should clearly show which curve is which and their main characteristics.
c) Please list and explain at least two papers from the class that considered heavy-tailed distributions, and for each paper, describe one example distribution.

Question 6: Favorite papers (8 points)

First, identify your two favorite papers from the course and write down their titles, the venue they were published, and the author names. Second, using a single sentence per paper, briefly and clearly describe the main contribution(s) of these two papers. Third, pick one paper (possibly one of the above papers) that you liked and that either in the paper or some presentation of the paper (but not the lecture notes) used a figure that you found particularly insightful. Write down the title of the paper. Fourth, please re-draw the figure (or some variation thereof) and explain the key insights that you learned (or that somebody else can learn) from the figure.

Example hint: As two example figures, for the BBR papers, I personally like the following two figure pairs:



Here, I am looking to see what figures you may have seen in the course and what you found particularly insightful in them, as well as what you learned from those figures (and/or others can learn from them).

Bonus (only on original exam)

Question 7: HTTPS, Certificates, and MITM attacks (6 points)

Please use a clear step-by-step figure explaining how you can execute a HTTPS interception, or man-in-the-middle (MITM) attack, on a client that accidentally has agreed to trust your root certificate. In this question, please clearly show the certificates being communicated (using public-key crypto) **and** the basic Diffie-Hellman key exchanges. Your figure should clearly show the use of public keys, certificate chains, and the creation of shared secrets. Ideally, to make things more concrete, please also include a concrete example based on an example website from which you extract the certificate, domain name, identify the public key used, the root that the "bad" entity may have managed you to trust. For examples of "bad" websites that you could use for this example, please feel free to leverage a suitable example certificate from badssl.com.

Good luck!!