ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TIK Institut für Technische Informatik und Kommunikationsnetze

Department ITET
Lecture SS 2016

Prof. Dr. Laurent Vanbever
Thomas Holterbach, Tobias Bühler

Exam: Communication Networks

30 August 2016, 09:00–12:00, Room HIL F 61

General Remarks:

- ▷ Write your **name** and your **ETH student number** below on this front page.
- ▷ Put your **legitimation card** on your desk.
- ▷ Check if you have received **all task sheets** (Pages **1 - 22**).
- ▷ Do **not separate** the **task sheets**.
- ▷ Write your answers directly on the task sheets. If you need more space, please use your own extra sheets.
- ▷ If you use extra sheets, use a **new sheet of paper** for **each task** and write your name and the exam task number in the **upper right corner**.
- ▷ **Read each task completely before you start solving it**.
- ▷ **For the best mark, it is not required to score all points.**
- ▷ Please answer either in **English or German**.
- ▷ **Write clearly** in blue or black ink (not red) using a **pen**, not a pencil.
- ▷ **Cancel** invalid parts of your solutions **clearly**.
- ▷ At the end of the exam, hand your **solutions in together with all extra sheets**.

Special aids:

- ▷ All written materials (vocabulary books, lecture and lab scripts, exercises, etc.) are allowed.
- ▷ Using a calculator is allowed, but the use of electronic communication tools (mobile phone, computer, etc.) is strictly forbidden.

Family name: Student legi nr.:

First name: Signature: .....

Do not write in the table below (used by correctors only):

Task	Points	Sig.
Ethernet & Switching	/20	
Intra-domain routing	/17	
Inter-domain routing	/47	
Reliable transport	/39	
Applications	/30	
Security	/20	
Software-Defined Networking	/7	
Total	/180	

Task 1: Ethernet & Switching **20 Points**

a) Warm-up **(6 Points)**

For the following true/false questions, check either *true*, *false* or nothing. For each question answered correctly, one point is added. For each question answered falsely, one point is removed. There is always one correct answer. This subtask gives at least 0 points.

true ☐ false ☐ Assume two hosts A and B in the same IP subnet are connected via an Ethernet switch X. The destination MAC in the IP packets sent by A to B is the MAC address of X.

true ☐ false ☐ When an Ethernet switch has a packet to send on a full-duplex port, it first listens to the medium and waits until it is idle.

true ☐ false ☐ Ethernet switches only rely on the lower 24 bits of the MAC address (*i.e.*, the part assigned by the vendor) for forwarding.

true ☐ false ☐ Consider a host with a statically configured IP address (82.130.102.59/24) and an empty state which runs the command "ping 8.8.8.8". The first packet the host will generate is an ARP request for the MAC address corresponding to 8.8.8.8.

true ☐ false ☐ Consider a set of Ethernet switches which have just finished building a spanning tree. If a host connected to one of them sends a broadcast packet, each and every switch would see *exactly* one copy of the broadcasted packet.

true ☐ false ☐ In a shared medium with few frame collisions, CSMA/CD leads to faster throughput than CSMA/CA.

b) Ethernet, everywhere **(2 Points)**

Suppose that Ethernet is the only LAN technology out there, so every host in the Internet is part of a local Ethernet segment and has one globally-unique MAC address.

One of your friends has a bold idea, she wants to get rid of IP addresses and instead turn the entire Internet into one gigantic Ethernet switch.

Give and justify two *distinct* reasons why using existing Ethernet protocols for this is a bad idea. Do *not* consider security or privacy.

Reason 1: _____

Reason 2: _____

c) Summer pruning **(12 Points)**

Consider the layer-2 network composed of 5 Ethernet switches depicted in Figure 1. Each link is annotated with its propagation delay (*e.g.*, it takes 10 ms for a message originated by switch 2 to arrive at switch 9). The switches are running the Spanning Tree Protocol (STP) as described in the course. All links have a cost of 1. When equal-cost paths to the root are encountered, switches break the tie based on the sender ID (lower is better). You can consider that the STP computation time is negligible. Two hosts (H1 and H2) are connected to switch 9 and switch 1, respectively.

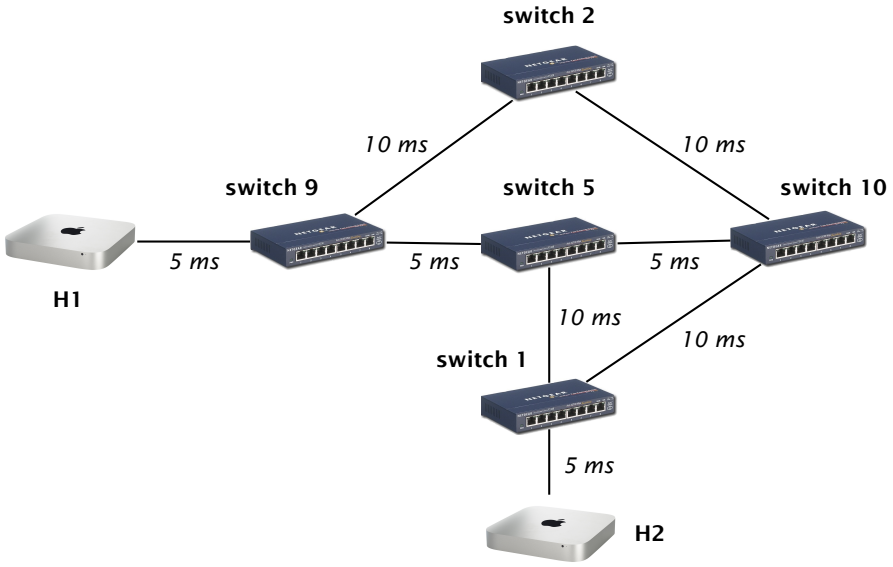

Figure 1: A simple, yet loopy layer-2 network.

(i) Assume first that an unfortunate network operator disabled the STP on all switches. Explain, by completing Figure 2, what happens in this network if H1 sends (at $t = 0$) an Ethernet frame to H2. In particular, for each time step, show what information on H1 the switches store in their forwarding tables, that is, indicate the next hop they would use to send a frame to H1. The information for $t = 0$ ms to $t = 10$ ms (grey box) are already provided. The right part of the table is only for your notes and is not graded.

(5 Points)

	Next hop (switch) to H1					For your own notes (not graded)
Time (ms)	Switch 1	Switch 2	Switch 5	Switch 9	Switch 10	
0	?	?	?	?	?	
5	?	?	?	direct	?	
10	?	?	9	direct	?	
15						
20						
25						

Note: "?" stands for "no next hop known".

Figure 2: Forwarding table changes by sending an Ethernet frame from H1 to H2.

(ii) After having observed a complete network meltdown, our poor network operator realizes her mistake. She activates STP on all switches and restarts the network. Consider switch 9, just after the network has started. Initially, it considers itself as the root and sends $(9, 0, 9)$ as Bridge Protocol Data Unit (BPDU) messages to its neighbors. Indicate the sequence of BPDU messages that switch 9 will send to its neighbors as it learns about other switches in the network. Write your answer as a list of BPDUs of the form $(root\_id, distance, sending\_switch)$ starting with $(9, 0, 9)$.

(3 Points)

(iii) Cross all the links (in Figure 3) that end up **deactivated** in the steady state, once all the switches have converged on the final spanning tree. (2 Points)

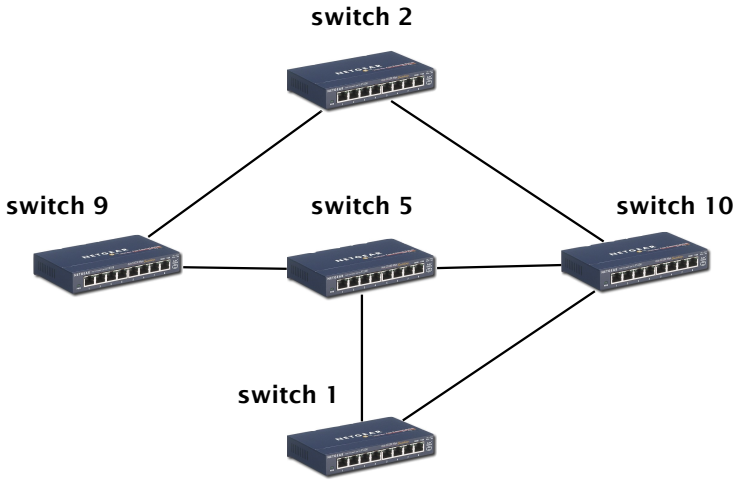

Figure 3: Cross the deactivated links.

(iv) Assume now that switch 1 fails which triggers a new recomputation of the spanning tree. Cross all links (in Figure 4) that end up **deactivated** in the steady state, once all the switches have converged on the final spanning tree. (2 Points)

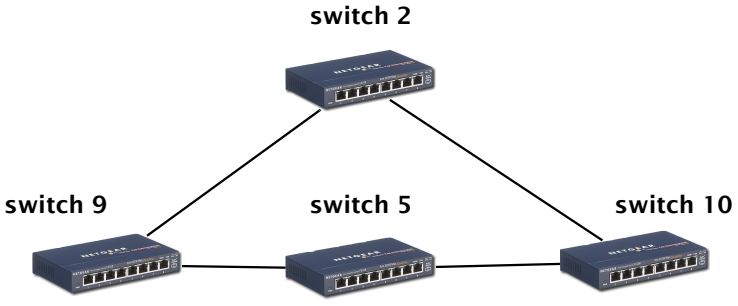

Figure 4: Cross the deactivated links.

Task 2: Intra-domain routing **17 Points**

a) Warm-up **(6 Points)**

For the following true/false questions, check either *true*, *false* or nothing. For each question answered correctly, one point is added. For each question answered falsely, one point is removed. There is always one correct answer. This subtask gives at least 0 points.

true ☐ false ☐ Consider a positively weighted graph G. Applying the Bellman-Ford (used by distance-vector protocols) or Dijkstra (used by link-state protocols) algorithm on G would lead to the same forwarding state.

true ☐ false ☐ Link-state protocols (such as OSPF) are guaranteed to compute loop-free forwarding state as long as the link-state databases are consistent on all routers.

true ☐ false ☐ Link-state protocols (such as OSPF) require routers to maintain less state than distance-vector protocols (such as RIP).

true ☐ false ☐ Poisoned reverse solves the problem of count-to-infinity.

true ☐ false ☐ Consider a positively weighted graph G. Multiplying all link weights by 2 would change the all-pairs shortest paths computed by the Dijkstra algorithm on G.

true ☐ false ☐ Consider a positively weighted graph G. Adding 1 to all link weights would change the all-pairs shortest paths computed by the Dijkstra algorithm on G.

b) Keeping network weights under control **(11 Points)**

As a fresh network engineer, you are called to help some network operators struggling with their link weight settings in their brand new OSPF network.

(i) The operators tell you that they want to minimize the number of hops taken by the traffic in their network. How should they set their link weights to realize this objective? (1 Point)

(ii) After some more thinking the network operators realize that it might be better for their customers to actually maximize their throughput by systematically routing traffic along paths with higher capacity instead of minimizing hop count. How should they set their link weights now? (2 Points)

(iii) Happy with your advices, the network operators now ask you to help them setting their weights for their secondary OSPF-based network which has been running in production for a while. Their secondary network is composed of 9 routers (A to I) and is depicted in Figure 5 along with the current weight setting.

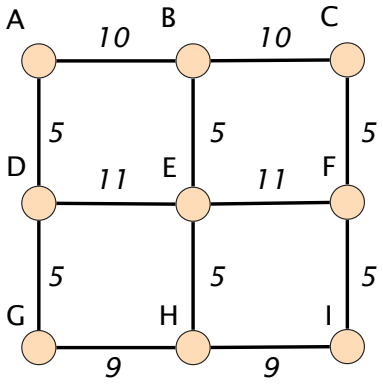

Figure 5: An OSPF-based network.

Draw the shortest path computed by every node to reach router D. Answer directly on Figure 6 using an arrow pointing to the next-hop each router uses to reach D.

(2 Points)

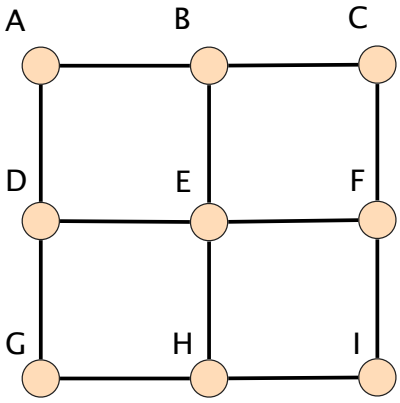

Figure 6: Draw the shortest-path tree to D.

(iv) The network operators then explain you that the link (E, F) is almost continuously overloaded with traffic. They ask you to identify *two distinct ways* to reweight a single link such that traffic from source F to destination D ends up diverted away from the (E, F) link without affecting the path between *any* other source-destination pairs. For instance, traffic from F to E should *still* flow along the (E, F) edge, but not the traffic from F to D. Do not rely on how routers choose between multiple paths with the same (smallest) cost. Your answer should uniquely identify the link (use the adjacent router IDs) along with the new weight.

(6 Points)

1/ Link and new weight: _____

2/ Link and new weight: _____

Task 3: Inter-domain routing **47 Points**

a) Warm-up **(5 Points)**

For the following true/false questions, check either *true*, *false* or nothing. For each question answered correctly, one point is added. For each question answered falsely, one point is removed. There is always one correct answer. This subtask gives at least 0 points.

true ☐ false ☐ BGP necessarily computes shortest-paths (when considering the numbers of AS hops traversed).

true ☐ false ☐ A simplified BGP protocol without policies and in which routes would be selected based on the AS-PATH length would be guaranteed to converge.

true ☐ false ☐ When following the selection and exportation policies based on customers, peers and providers, ISPs can advertise different routes for the same prefix p to their neighbors.

true ☐ false ☐ BGP policies often lead to asymmetric routing. Yet, the forward and reverse paths will always have the same length in terms of number of AS hops.

true ☐ false ☐ By sending the same prefix p to multiple providers, multi-homed BGP networks increase the size of the forwarding table of all routers in the Internet.

b) Routing wedding **(2 Points)**

Explain how a BGP router uses the information from the IGP to build its forwarding table.

c) Got a good exit strategy? (10 Points)

Consider the ISP network composed of 5 routers (A, B, C, D, E) depicted in Figure 7. Three of these routers, A, E and D, are connected to routers located in neighboring ASes via eBGP. These neighboring routers are indicated by X, Y and Z. Each of them advertises the same three distinct IP prefixes $p1$, $p2$ and $p3$.

The three tables in Figure 7 indicate the Local-Preference (LP) associated to each external prefix by A, E and D along with their corresponding AS-PATH length. For instance, A learns a route to $p1$ from X with an AS-PATH length of 10 to which it associates a LP of 200. Internally, the ISP uses an iBGP full-mesh to distribute the BGP routes and OSPF as intra-domain routing protocol. The weight of each internal link is indicated next to it.

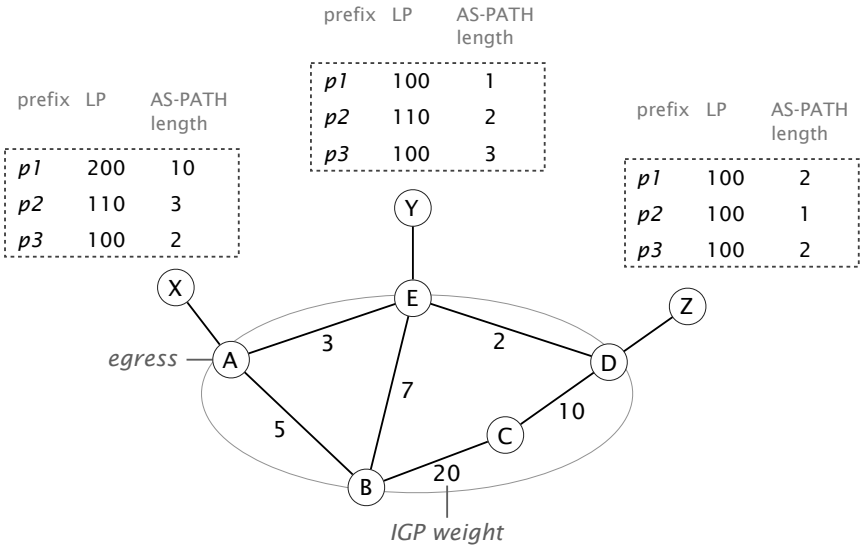

Figure 7: A simple ISP network which receives BGP routes for 3 different external prefixes ($p1$, $p2$, $p3$) from 3 routers (X, Y, Z) located in neighboring ASes.

For each router in the ISP, indicate the router ID of the selected egress (A, E, D) along with the router ID of the internal next-hop (A, B, C, D, E or *direct*) used to reach it. *Only* use the tables in Figure 8 for your answer.

A

prefix	egress	internal NH
p1		
p2		
p3		

B

prefix	egress	internal NH
p1		
p2		
p3		

C

prefix	egress	internal NH
p1		
p2		
p3		

D

prefix	egress	internal NH
p1		
p2		
p3		

E

prefix	egress	internal NH
p1		
p2		
p3		

Figure 8: Fill in the following tables with the selected egress and internal next-hop.

d) Primary *vs* backup **(15 Points)**

Consider the BGP network depicted in Figure 9. Single-headed plain arrows point from providers to their customers (Sunrise is the provider of ETH), while double-headed dashed arrows connect peers (Swisscom and Deutsche Telekom are peers). ETH is the only AS to originate a prefix (82.130.68.0/22) which it advertises to its two providers: Sunrise and Deutsche Telekom.

The link between ETH and Sunrise has a high delay, so high that when ETH advertises a BGP announcement, Sunrise systematically receives it first via Swisscom before receiving it on the direct link.

Given its poor performance, ETH wishes to use the link with Sunrise as a backup link only: ETH *never* wants to receive traffic on it *unless* the primary link with Deutsche Telekom is down. ETH has a special contract with Sunrise for this. In particular, Sunrise decides to enforce the ETH policy by setting the Local-Preference (LP) associated to ETH prefix to the minimum value (1) when learned on the direct link and to a higher value (150) when learned via its provider. In contrast, Swisscom and Deutsche Telekom apply the default selection and exportation BGP policies based on their customers, peers and providers.

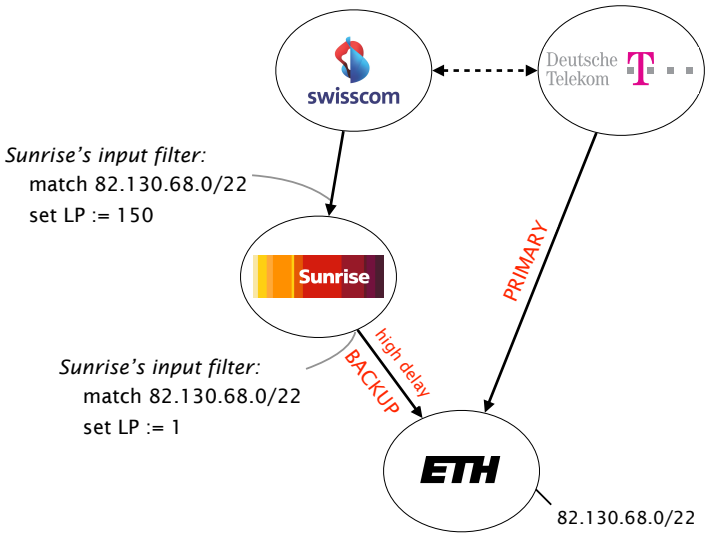

Figure 9: A simple BGP network

(i) Could ETH realize this backup policy alone, without the help (*i.e.*, the dedicated policy) from Sunrise? Why or why not? (2 Points)

(ii) In the steady state, what are the paths used by all networks to reach ETH? (3 Points)

From Sunrise: _____

From Swisscom: _____

From Deutsche Telekom: _____

(iii) Assume now that the link between Deutsche Telekom and ETH fails. What BGP messages are exchanged and what are now the paths used by all networks to reach ETH? (4 Points)

(iv) After some hard maintenance work, the link between ETH and Deutsche Telekom is finally put back online. Again, what BGP messages are exchanged and what are the paths used by all networks to reach ETH? Are the paths compliant with the ETH backup policy? Explain. (6 Points)

e) Visibility **(15 Points)**

Consider now the network depicted in Figure 10. Single-headed plain arrows point from providers to their customers (AS A is the provider of AS D), while double-headed dashed arrows connect peers (AS D and AS E are peers). Each AS in the network originates a unique prefix that it advertises to all its BGP neighbors. Each AS also applies the default selection and exportation BGP policies based on their customers, peers and providers.

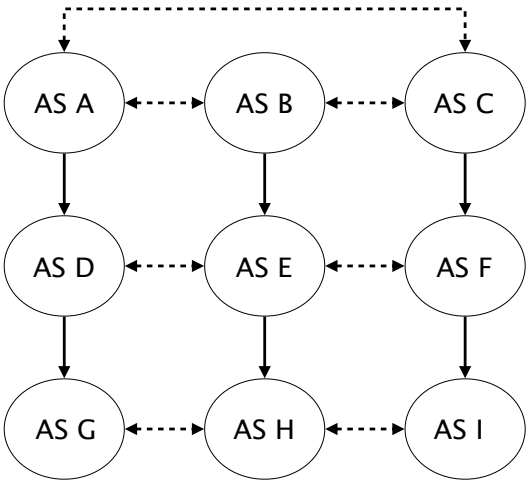

Figure 10: A simple BGP network

(i) What path (sequence of ASes) is followed when AS G sends packets destined to the prefix originated by AS E? (2 Points)

(ii) What path (sequence of ASes) is followed when AS F sends packets destined to the prefix originated by AS G? (2 Points)

(iii) Suppose AS A and AS C give you a "dump" of all the BGP routes they *learn* for every destination. You then extract all links from the AS paths seen in those "dumps" and use them to construct a view of the AS-level topology. Draw the resulting AS-level topology in Figure 11. (5 Points)

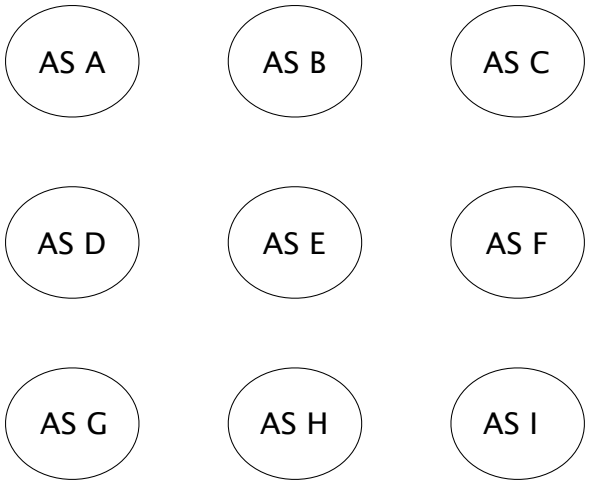

Figure 11: Draw the inferred AS-level topology.

(iv) Give the minimum set of ASes that must provide a "dump" of each route they learn for all the edges (the ones in Figure 10) to be visible? Justify your answer. (6 Points)

Task 4: Reliable Transport **39 Points**

a) Warm-up **(4 Points)**

Consider that Alice and Bob communicate with each other using a transport protocol based on Go-Back-N (GBN). More particularly, they use the most basic version of GBN. For every received data segment, the receiver answers with an ACK. The ACK number refers to the next expected in-order sequence number and cumulatively acknowledges all the previous data segments. Out-of-order packets are *not* saved in a buffer. There are no mechanisms in place to signal dropped or out-of-order packets. To recover from heavy packet losses a timeout value is used and data segments are retransmitted once the timeout is reached.

Answer the following true/false questions considering the above protocol. Check either *true*, *false* or nothing. For each question answered correctly, one point is added. For each question answered falsely, one point is removed. There is always one correct answer. This subtask gives at least 0 points.

true	false	
☐	☐	The protocol used by Alice and Bob is a sliding window protocol.
☐	☐	Only the length of the timeout value influences the transmission duration of a message.
☐	☐	A file can be successfully transmitted even if the number of ACKs received by the sender is smaller than the number of transmitted data segments.
☐	☐	A dropped packet is the only possibility for duplicate ACKs at the sender.

b) Selective Repeat **(9 Points)**

To speed-up the communication, Alice and Bob decide to add support for Selective Repeat to the GBN protocol. Figure 12 (on the next page) shows the successful transmission of 8 data segments ($D1$ to $D8$). Here is a *non-exhaustive* list of the choices Alice and Bob made to implement Selective Repeat:

- The sender saves all the transmitted but so far not acknowledged data segments in a sender buffer which can contain up to 4 segments;
- The receiver answers with an ACK for every received data segment. The ACK number always points to the next expected in-order data segment and cumulatively acknowledges all the previous data segments. Out-of-order segments are saved in a buffer and delivered (removed from the buffer) as soon as the missing packets arrive;
- Lost packets are detected based on duplicate ACKs received by the sender. If the sender receives 3 duplicate ACKs, the missing segment is immediately retransmitted.

(i) Fill in the missing parts for the sender and receiver in Figure 12. For the ACK segments, use the following syntax: AN acknowledges the correct reception of all the data segments up to and including $N-1$. If there are no segments in the sender buffer or the out-of-order buffer, indicate it clearly by crossing the corresponding buffer. (7 Points)

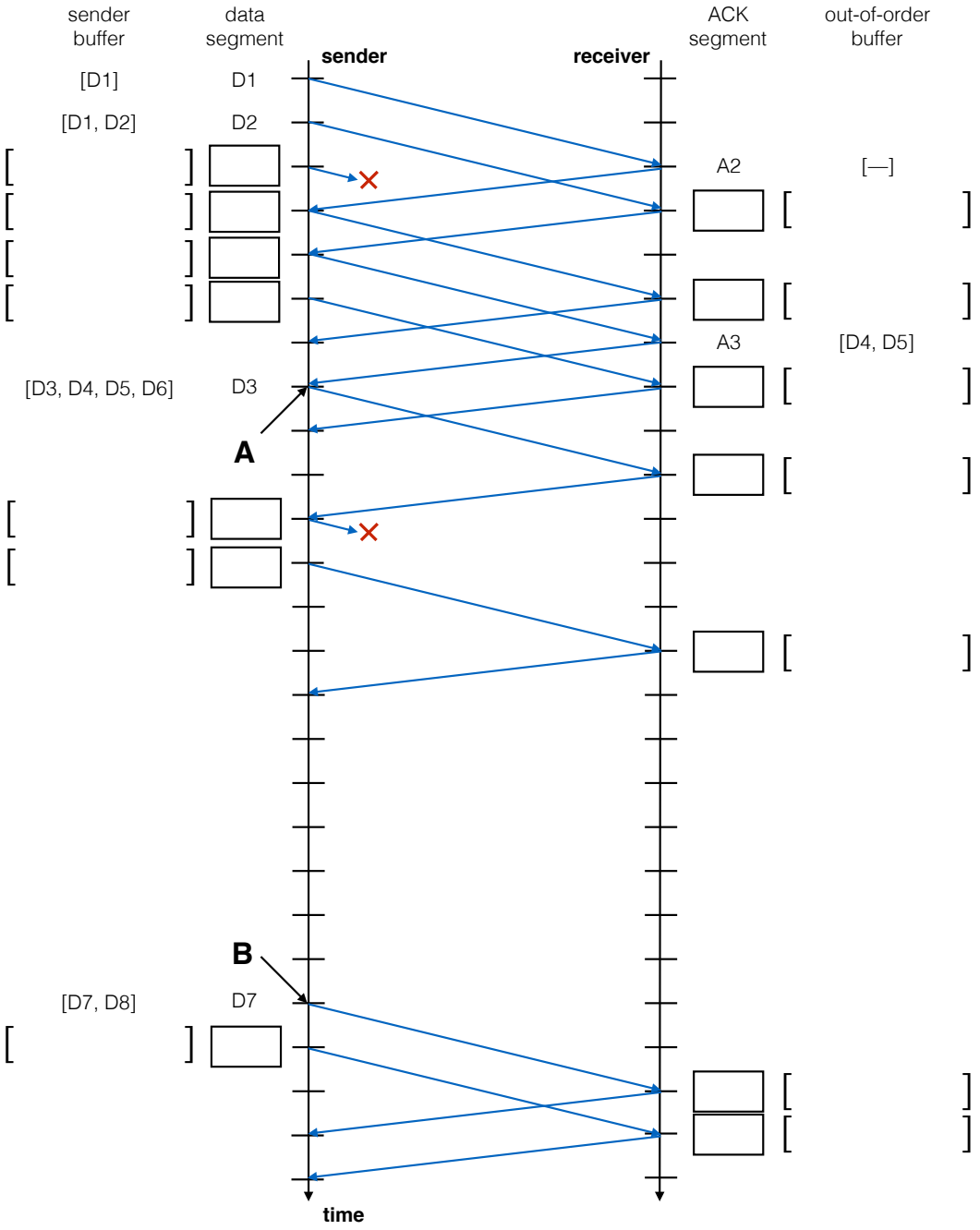

Figure 12: Nearly complete time-sequence diagram of a GBN protocol with Selective Repeat.

(ii) What is happening at point **A** and point **B** (see Figure 12 on the left side)? (2 Points)

Event at point **A**: _____

Event at point **B**: _____

c) Selective Acknowledgement (SACK) (9 Points)

Alice wants to improve the protocol even more. She therefore tries to implement Selective Acknowledgements (SACK). Her first implementation attempt is as follows:

- The sender keeps all the transmitted but non-acknowledged data segments in a sender buffer;
- **Every time** the receiver gets a data segment, it answers with an ACK (as before) containing a SACK header acknowledging **all** the already received out-of-order segments;
- If the sender receives an ACK with a SACK header, it compares its sender buffer to the SACK header and **immediately** retransmits all the packets which are in the sender buffer but not in the SACK header.

(i) Alice and Bob are using this SACK version to communicate over an unreliable connection in which packets are often lost or arrive out-of-order.

Unfortunately, they do not observe the expected performance improvements. Explain why the used SACK implementation does **not** provide one of the expected feature: the ability to reduce the number of retransmitted data segments. (3 Points)

(ii) Describe **two** distinct improvements to Alice's SACK implementation which would reduce the number of retransmitted packets but still improve the communication speed compared to a GBN implementation without SACK. (6 Points)

Improvement 1:

Improvement 2:

d) Congestion control **(17 Points)**

Figure 13 depicts the evolution of the size of the TCP congestion window of the sender. Beware, it is *not* drawn to scale.

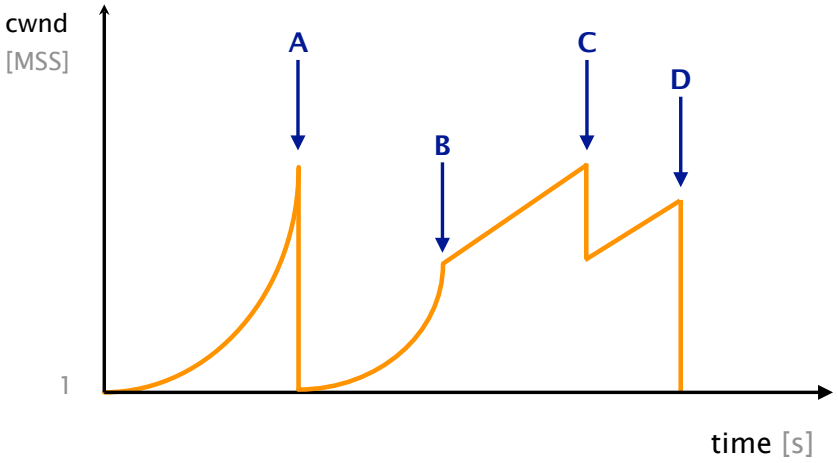

Figure 13: Evolution of the size of the congestion window, *not* drawn to scale.

(i) Describe **two** distinct reasons for the sender to decrease its congestion window all the way down to 1 Maximum Segment Size (MSS) at point A. (2 Points)

Reason 1:

Reason 2:

(ii) Consider that the MSS of the connection is 1 000 bytes which is also the initial size of the congestion window. **Point A** occurs after a total of 7 000 bytes of payload data have been written by the sender in the network while **Point B** happens 600 ms after the beginning of the connection. What is the round-trip-time (RTT) of the network? Do not forget that at time $t = 0$, the sender needs to open the connection before being able to transmit. The transmission delay in this network is negligible, so your answer should only consider the propagation delay. **Describe all the steps in your answer**, an answer without any explanation will give no points. (5 Points)

(iii) What is the window size (in bytes) of the sender at point B? (2 Points)

(iv) If point C happens 2 seconds after point B, what is the window size of the sender (in bytes) at point C? You can assume that the RTT is constant. If you have not answered to (ii) and (iii), you can use the variables *rtt* and *wnd_size_B* as placeholders in your answer. (4 Points)

(v) Assume that the window size at point D is 16 000 bytes and that it drops to 1 000 (1 MSS) after the packet loss. How much time will it take for the window of the sender to reach at least 16 000 bytes assuming no further loss? You can express your answer as a number of RTTs if you have not answered to (ii). (4 Points)

Task 5: Applications **30 Points**

a) Warm-up **(6 Points)**

For the following true/false questions, check either *true*, *false* or nothing. For each question answered correctly, one point is added. For each question answered falsely, one point is removed. There is always one correct answer. This subtask gives at least 0 points.

true ☐ false ☐ A DNS query for an A record (IPv4 address) may return multiple IP addresses in the answer.

true ☐ false ☐ A short TTL on an A record response increases traffic either at the root name server or at the name server responsible for the corresponding top-level domain.

true ☐ false ☐ Consider a local DNS resolver (such as the one maintained by ETH) which has just cached an A record for facebook.com with a TTL of 60 seconds. 5 seconds later, an ETH host generates a DNS query for the A record of facebook.com. This query causes the resolver to reset the TTL of the record to 60 seconds.

true ☐ false ☐ An HTTP/1.1 server can only host as many different websites as it has IP addresses.

true ☐ false ☐ An HTTP/1.1 server will proactively notify a client when a ressource expires.

true ☐ false ☐ Network Address Translation (NAT) boxes *only* rewrite the source port and destination IP address on outgoing packets.

b) In naming we trust **(9 Points)**

(i) Explain **two** distinct reasons why many DNS server operators disable recursive queries and only allow iterative queries instead. (2 Points)

Reason 1: _____

Reason 2: _____

(ii) As we saw in the course, DNS operators often rely on BGP Anycast to distribute the load on multiple servers spread across the Internet. With BGP Anycast, it is possible for different packets (and therefore, requests), sent by the same client (e.g., your laptop at ETH), to reach servers located in different locations. Explain: *(i)* why it is possible; and *(ii)* whether it is a problem or not. (4 Points)

(iii) Consider now a CDN which considers replicating static Web content using BGP Anycast. Explain whether having packets from the same client going to distinct replicas would be acceptable or not. (3 Points)

c) Going big **(15 Points)**

After a dozen of successful projects as a network engineer, your company decides to name you responsible for managing the new ch.ch (Swiss Authorities) infrastructure. The current website is indeed hosted on a single server and is often down, suffering from too many (legitimate or not) concurrent requests.

For hosting the new website, the Swiss government was particularly ambitious and built two datacenters in Zürich and Geneva containing 1000 servers each. It also obtained a public /23 IPv4 prefix. You can assume that the new website contains *only* static information.

Your objective is threefold:

1. You want to make sure that you spread the load *across* the two datacenters;
2. You want to make sure that you spread the load on the 1000 servers *within* each datacenter;
3. You also want to make sure that the service remains up even if one of the datacenters is disconnected from the Internet due to a natural disaster or a simple power cut.

Describe how you would solve each objective, including the technique(s) but most importantly how you would use it (them). Make sure to explain why your solution solves the problem. **Be specific in your answer**, simply mentioning the name of a technology will give no points.

(i) Explain how you can distribute the load across the two datacenters. (5 Points)

(ii) Explain how you can distribute the load on the 1000 servers within each datacenter. (5 Points)

(iii) Explain how you can ensure that the service remains up, even if one datacenter fails. (5 Points)

Task 6: Security **20 Points**

a) Warm-up **(6 Points)**

For the following true/false questions, check either *true*, *false* or nothing. For each question answered correctly, one point is added. For each question answered falsely, one point is removed. There is always one correct answer. This subtask gives at least 0 points.

true ☐ false ☐ Anybody can create a certificate attesting the ownership of a public key.

true ☐ false ☐ When implemented properly, public key cryptography runs much faster than symmetric key cryptography.

true ☐ false ☐ A passive Man-in-the-Middle (MITM) attacker observing all packets during the TLS handshake could infer from them the private key used for the communication and decrypt it.

true ☐ false ☐ Enabling DNSsec for non top-level domain names (e.g., for ethz.ch) requires to use the private key of the root DNS zone (i.e., the one created during the DNSsec root signing ceremony).

true ☐ false ☐ DNSsec does not prevent amplification attacks.

true ☐ false ☐ By validating the origin of a BGP announcement and the content of the AS-PATH, BGPsec guarantees that IP packets are forwarded along the advertised path.

b) BGP, with a security twist **(14 Points)**

Consider the Internet topology composed of 7 ASes depicted in Figure 14. Single-headed plain arrows point from providers to their customers (AS A is the provider of AS D), while double-headed dashed arrows connect peers (AS D and AS E are peers). AS E advertises a single prefix: 82.130.68.0/22 to all its neighbors. All ASes apply the default selection and exportation BGP policies based on their customers, peers and providers.

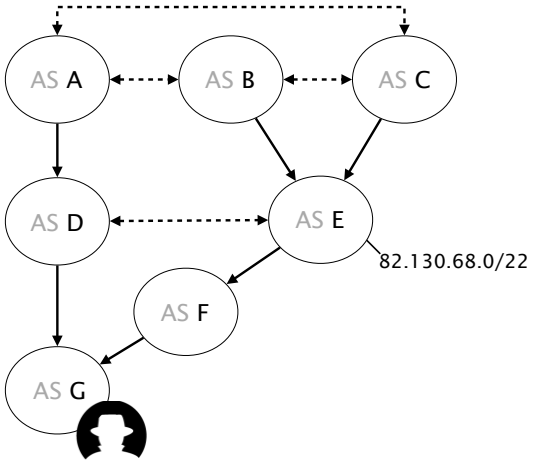

Figure 14: A simple Internet, with a malicious AS.

(i) Assume that AS G is malicious and wants to attract traffic destined to 82.130.68.0/22. Knowing that BGP is purely based on trust, it decides to see how much traffic it can attract by advertising the exact same prefix (82.130.68.0/22) to all its neighbors. List all the ASes for which it manages to divert traffic from. (3 Points)

(ii) AS G realizes it could attract more traffic by advertising more-specific prefixes. As such, it decides to advertise 82.130.68.0/23 and 82.130.70.0/23 instead of the /22. List all the ASes for which it manages to divert traffic from. (3 Points)

(iii) AS G is still not satisfied as it realizes that it essentially blackholes all the traffic it diverts. As such, TCP connections immediately die preventing AS G from extracting useful information from unencrypted flows. Specify how AS G could modify its announcements to AS D and AS F to keep at least one valid path towards the legitimate destination. Your answer must include the actual content of the announcements. (4 Points)

(iv) Explain how: *(i)* AS E could locally realize that another AS advertises its prefixes; and *(ii)* what it can locally do to retrieve at least partial connectivity. By locally, we mean that AS E should not rely on any other services (such as a monitoring service) or on the help of another AS. (4 Points)

Task 7: Software-Defined Networking **7 Points**

a) Warm-up **(4 Points)**

For the following true/false questions, check either *true*, *false* or nothing. For each question answered correctly, one point is added. For each question answered falsely, one point is removed. There is always one correct answer. This subtask gives at least 0 points.

true ☐ false ☐ SDN mandates all data-plane traffic to go to the SDN controller.

true ☐ false ☐ SDN aims at simplifying network management at the price of having a single point-of-failure: the SDN controller.

true ☐ false ☐ One of the objective of SDN is to improve the way network operators provision forwarding state in a network.

true ☐ false ☐ The OpenFlow protocol provides the SDN controller with a network-wide view of the network topology.

b) Shapeshifter **(3 Points)**

As we have seen during the course, an OpenFlow switch can serve as an IP router. Consider a routing application (running in the SDN controller) which has computed 3 forwarding rules:

1. 13.1.2.0/24 forwards out link 2;
2. 13.0.0.0/8 forwards out link 1;
3. 13.1.0.0/16 forwards out link 3.

What priority should these rules have in the OpenFlow switch?