Chair of Distributed Systems and Security
School of Computation, Information and Technology
Technical University of Munich

Esolution
Place student sticker here

Note:

- During the attendance check a sticker containing a unique code will be put on this exam.
- This code contains a unique number that associates this exam with your registration number.
- This number is printed both next to the code and to the signature field in the attendance check list.

Computer Networking and IT-Security

Exam:	INHN0012 / Retake	**Date:**	Wednesday 3rd April, 2024
Examiner:	Prof. Dr.-Ing. Stephan Günther	**Time:**	13:00 – 14:30
	Leander Seidlitz, M.Sc.		

Working instructions

- This exam consists of **16 pages** with a total of **6 problems** and a **cheatsheet**.
  Please make sure now that you received a complete copy of the exam.
- The total amount of achievable credits in this exam is 93 credits.
- Detaching pages from the exam is prohibited.
- Allowed resources:
  - one **non-programmable pocket calculator**
  - one **analog dictionary** English ↔ native language
- Subproblems marked by * can be solved without results of previous subproblems.
- **Answers are only accepted if the solution approach is documented.** Give a reason for each answer unless explicitly stated otherwise in the respective subproblem.
- Do not write with red or green colors nor use pencils.
- Physically turn off all electronic devices, put them into your bag and close the bag.

Left room from ________ to ________ / Early submission at ________

Problem 1 Multiple Choice (18 credits)

The following subproblems are multiple choice / multiple answer, i. e. at least one answer per subproblem is correct. Subproblems with a single correct answer are graded with 1 credit if correct. Those with more than one correct answers are graded with 0.5 credit per correct answer and -0.5 credit per wrong answer. Missing crosses have no influence. The minimal amount of credits per subproblem is 0 credits.

Mark correct answers with a cross ☒
To undo a cross, completely fill out the answer option ■
To re-mark an option, use a human-readable marking ×■

a)* Which of the following statements regarding layering according to the ISO / OSI model are true?

- ☐ The application is Layer 7
- ☐ In general, protocols implement functions of only one layer
- ☒ The user is not part of the model
- ☒ The Layer 3 SDU is the Layer 4 PDU

b)* Given a message "`AABB ABBB AABB AABA`" $\in$ {`A`,`B`} (spaces added for readability only) from a uniform message source, which is the information content of character `A`?

- ☐ 0.5 bit
- ☒ 1 bit
- ☐ 0.25 bit
- ☐ 2 bit

c)* Which are interior routing protocols?

- ☒ RIPv2
- ☐ BGP
- ☐ CSR
- ☒ OSPF

d)* Which of the following statements regarding Layer 2 adresses in IEEE-like protocols are true?

- ☐ Can be resolved over the Internet
- ☒ 6 B long
- ☐ Used for routing over the Internet
- ☒ Compatible between different IEEE standard
- ☐ Divided into network and host part
- ☐ Uniquely identify a specific device

e)* Which of the following statements regarding media access control schemes are true (provided that nodes adhere to the standard)?

- ☐ Fairness cannot be ensured in wireless networks
- ☒ CSMA/CD ensures fairness
- ☐ CSMA/CD is used in wireless networks
- ☐ Token Passing is nondeterministic
- ☐ CSMA/CD is deterministic
- ☒ Token Passing ensures fairness

f)* Which of the following are Ethernet broadcast addresses?

- ☐ bb:bb:bb:bb:bb:bb
- ☒ `ff:ff:ff:ff:ff:ff`
- ☐ `00:00:00:00:00:00`
- ☐ `33:33:ff:ff:ff:ff`

g)* Which of the following are valid 802.11 operating modes?

- ☐ MDF (Multi-Frequency-Drift) mode
- ☒ ad-hoc mode
- ☒ infrastructure mode
- ☐ multicast mode

h)* What is correct regarding IPv6?

- ☒ Source and Destination address are 128 bits long
- ☒ The IPv6 header including its extension header must always be a multiple of 8 B
- ☐ The header contains a CRC32 checksum
- ☐ Fragmentation is handled the same way as in IPv4

i)* NAT...

- [ ] is equivalent to a firewall.
- [x] translates private IPv4 addresses to an external address and back.
- [ ] adds 4 B overhead to the Ethernet header.
- [ ] does not work with IPv4 fragmentation.

j)* Which of the following are TCP phases?

- [x] slow start
- [x] congestion avoidance
- [ ] congestion control
- [ ] flow control

k)* Which is the correctly shortened version of the IPv6 address `2001:0db8:0000:0000:0001:0000:0000:0001`?

- [x] `2001:0db8::1:0:0:1`
- [ ] `2001:0db8:0:0:1:0:0:1`
- [ ] `2001:0db8::1::1`

l)* Which of the following are DNS query types?

- [ ] informative query
- [x] recursive query
- [x] iterative query
- [ ] curious query

m)* Which of the following are DNS record types?

- [x] A
- [ ] RPT
- [x] MX
- [ ] SDR
- [ ] AAAAAA
- [ ] NSS

n)* What is true regarding ECC?

- [x] For a comparable security level the key size is smaller compared to RSA
- [ ] ECC algorithms are resistant against quantum computers
- [ ] ECC stands for Extreme Curve Cryptography
- [ ] The private key is equal to the public key

o)* Which of the following hash algorithms are vulnerable to length-extension attacks?

- [x] SHA-512
- [ ] SHA-224
- [ ] SHA-384
- [x] SHA-256

p)* What are properties of password hash functions?

- [x] They reduce an arbitrary amount of data to a fixed-length digest
- [ ] They are built to be extremely fast
- [x] They are intentionally slow
- [ ] They never fulfill the properties of a cryptographic hash function

q)* Which of the following are stream ciphers?

- [ ] AES-CBC
- [x] AES-CTR
- [ ] AES-ECB
- [ ] RSA

Problem 2 Analog University of Munich [Security and General Questions] (18.5 credits)

This task is long and has an above average amount of description. It is best to work top to bottom.

At Analog University of Munich (AUM), most administrative processes are done using forms printed on paper. In order to reduce that paper trail, management has decided to digitize many of the processes.
As usual in public service, you have become part of this transformation without being asked. Your role is to ensure the security and safety of the processes being created.

a)* Name the five remaining security goals (in any order) you know from the lecture. Hint: the first letters form DCAAAC

1. Data Integrity
2. Confidentiality
3. Availability
4. Authenticity
5. Accountability
6. Controlled Access

b) Mention **and** describe any two of the goals (**except Availability**) in the context of this task.
Example: Availability: The system for handling grades shall always be accessible to the employees.

Despite having “Munich” in its name, AUM has multiple locations. One of them is located in Singapore, while another is located in Heilbronn. As most processes will function in a digital manner in the future, you need a secure communication channel to replace regular mail. You decide on using **IPsec**.

Simplified, each of the locations has a private network, which needs to be connected to the other networks. Each network has a **border router**, which interfaces the (insecure) **internet**. There is no dedicated line of communication between the locations other than the internet.

c)* Describe the IPsec setup you would install in this scenario. Discuss which network devices IPsec tunnels terminate on, as well as how the policy installed looks like (use natural language).

An IPsec tunnel per location pair exists. The tunnnels terminate at the corresponding border routers. The policy secures the traffic destined to each of the locations, that is, traffic that is intended for one of the other locations is secured when leaving a location, but traffic for other destinations is not handled and routed into the regular internet.

With the network secured, you analyze a different aspect of the migration: Signatures previously made on paper have to be replaced by digital signatures.

A colleague proposes the following signing scheme:

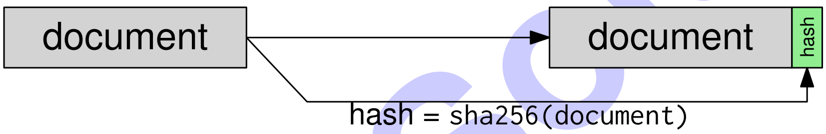


Figure 2.1: The proposed signing scheme as **Block Diagram**.

d)* Explain why this scheme (Figure 2.1) does not provide a digital signature.

The security of this scheme is roughly equivalent to a checksum as there is no secret involved in "signing". It thereby does not provide any data authenticity.

The same colleague proposes a reworked scheme, based on the assumption that each employee possesses a secret `key`.

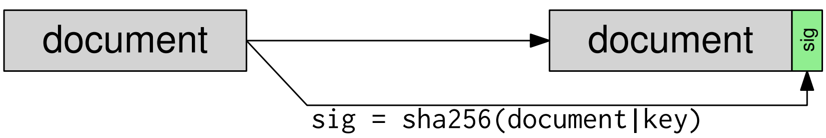


Figure 2.2: The reworked signing scheme. | denotes concatenation.

e) Compare the security of the new scheme (Figure 2.2) to the previous scheme (Figure 2.1). Discuss whether replay attacks are relevant in the context of signed documents, and whether the scheme protects against such attacks.

The scheme introduces a key and thereby provides data authenticity, given the key is secret and individual per entity. Replay attacks are relevant as this is basically the difference between a copy and the original, between which we cannot distinguish in case of digital documents. The scheme does not protect against replay attacks.

The colleague proposes symmetric pair-wise shared secrets as `key` between each of the parties that have to sign and verify documents.

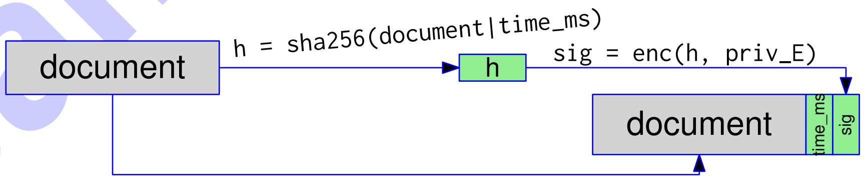
f)* How many shared secrets are necessary given there are n such parties. **Do not justify your answer.**

$\frac{(n-1)\cdot n}{2}$

Clearly, this scheme does not scale for the number of employees of AUM. Therefore, AUM introduces a **Certificate Authority (CA)**, which verifies an employees identity and hands out certificates. Each entity possesses a **`keypair = (priv_E,pub_E)`**. A certificate's data structure is as follows:

```
cert = {
    info = {
        Name,
        valid from,
        valid until,
        pub_E,
        CA public key
    },
    signature = {
        sign(sha256(info), private key CA)
    }
}
```

g)* Draw the **block diagram** for a different signing scheme, using the certificate (Listing directly above). Additionally, provide resistance against replay attacks.
Draw only the signing process, no verification, CA structure, . . . !
You may use the following functions: `enc(data,key)`, `dec(data,key)`, `sign(data,key)`, `verify(data,key)`, `sha256(data)`, `time_ms (current time in milliseconds)`. | denotes concatenation.



- Scheme somewhat resembles a signing scheme
- Scheme provides data authenticity
- Scheme uses the certificate infrastructure (== is asymm)
- Scheme is not replayable

Problem 3 NAT and static routing (14 credits)

Wie consider the network depicted in Figure 3.1. PC1 and PC2 are connected via switch S to each other and their default gateway R1. The subnets 172.29.79.192/27 are being used in the local network. R1 is connected to R2 (located at a service provider) over a transport network (/30 prefix).

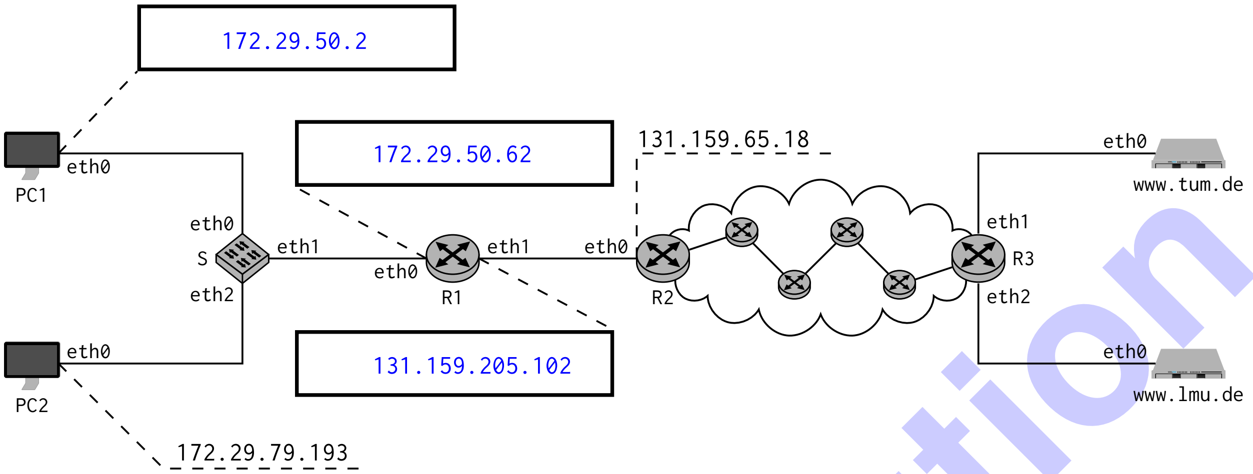


Figure 3.1: Network topology

a)* Assign PC1 the lowest usable IP address of the local subnet. Write it directly into Figure 3.1.

b)* Assign R1.eth0 the highest usable IP address of the local subnet. Write it directly into Figure 3.1.

c)* Assign R1.eth1 a usable address of the transport network. Write it directly into Figure 3.1.

d)* Which transport layer protocol and destination port will be used if PC1 accesses https://www.tum.de/?

TCP 443

We shorten IP and MAC addresses by the scheme <device>.<interface>, e. g. R1.eth0 for the respective MAC or IP address at interface eth0 on Router R1.
R1 supports NAT such that PCs can access the internet. The NAT table of R1 looks as shown in Table 3.1. PC2 has already established a connection with hosts on the internet.

Prot.	Local IP	Local Port	Global IP	Global Port	Remote IP	Remote Port
tcp	172.29.79.193	53050	R1.eth1	53050	tum.eth0	443
tcp	172.29.79.193	55222	R1.eth1	55222	lmu.eth0	80
tcp	172.29.50.2	55222	R1.eth1	55223	tum.eth0	443

Table 3.1: NAT-Tabelle von Router R1

PC1 now also accesses https://www.tum.de. It thereby chooses the random source port 55222.

e) Add the corresponding entries in Table 3.1.

Note for the following subproblems that there are 4 additional routers between R2 and R3.

f) For the request from `PC1` to `https://www.tum.de`, add the header fields at the three indicated positions in the empty tables in Figure 3.2. If a field is not unique, use a sensible value. **Notes:**

- If you were unable to solve Subproblem d), you may use destination port 8080.
- IP and MAC addresses should be abreviated by `<device>.<interface>`, e, g. `PC2.eth0`.
- The hostname of the server hosting `www.tum.de` may be abbreviated by `tum`.

Src MAC	PC1.eth0
Dst MAC	R1.eth0
Src IP	PC1.eth0
Dst IP	tum.eth0
TTL	63
Src Port	55222
Dst Port	443

Src MAC	R1.eth1
Dst MAC	R2.eth0
Src IP	R1.eth1
Dst IP	tum.eth0
TTL	62
Src Port	55223
Dst Port	443

Src MAC	R3.eth1
Dst MAC	tum.eth0
Src IP	R1.eth1
Dst IP	tum.eth0
TTL	56
Src Port	55223
Dst Port	443

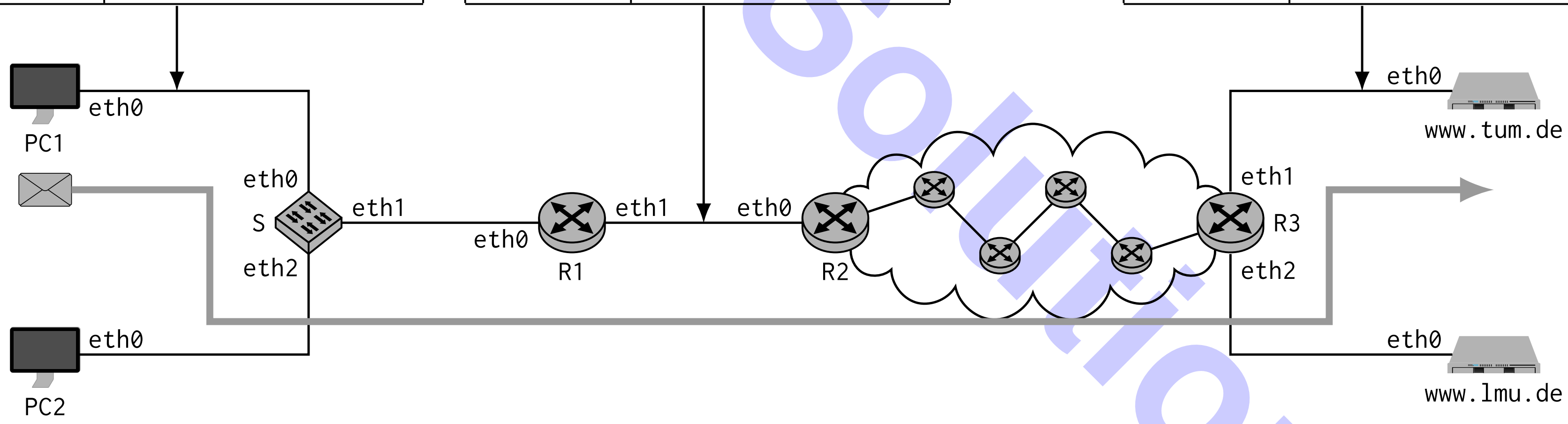


Figure 3.2: Preprint for Subproblem f)

g) For the reply from `tum` to `PC1`, add the header fields at the three indicated positions in the empty tables in Figure 3.2. If a field is not unique, use a sensible value. **Notes:**

- IP and MAC addresses should be abreviated by `<device>.<interface>`, e, g. `PC2.eth0`.
- The hostname of the server hosting `www.tum.de` may be abbreviated by `tum`.

Src MAC	R1.eth0
Dst MAC	PC1.eth0
Src IP	tum.eth0
Dst IP	PC1.eth0
TTL	56
Src Port	443
Dst Port	55222

Src MAC	R2.eth0
Dst MAC	R1.eth1
Src IP	tum.eth0
Dst IP	R1.eth1
TTL	57
Src Port	443
Dst Port	55223

Src MAC	tum.eth0
Dst MAC	R3.eth1
Src IP	tum.eth0
Dst IP	R1.eth1
TTL	63
Src Port	443
Dst Port	55223

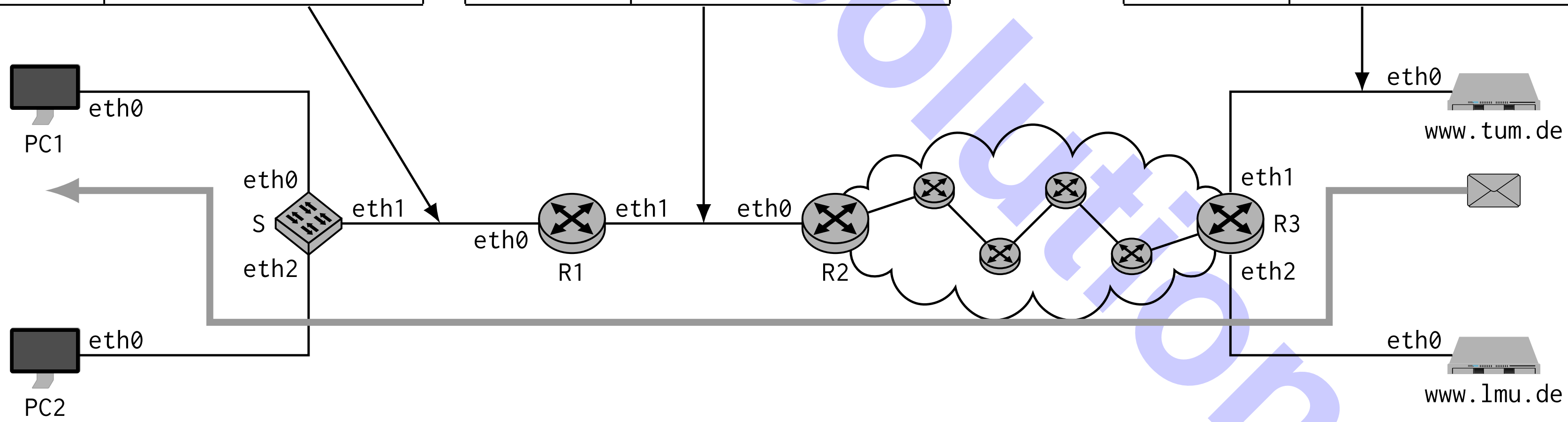


Figure 3.3: Preprint for Subproblem g)

Problem 4 Wireshark (17.5 credits)

Consider the Ethernet frame depicted in Figure 4.1. In the following, we will analyze this frame step by step.

0x0000	00	50	56	00	37	d1	94	f7	ad	4f	08	00	86	dd	60	00
0x0010	00	00	00	26	06	37	20	03	00	0a	08	7f	a4	a7	f0	2b
0x0020	0c	99	bc	65	10	70	2a	01	04	f9	00	4a	45	89	00	00
0x0030	00	00	00	10	00	01	9e	7e	00	19	e2	f3	fc	63	09	19
0x0040	51	40	80	18	00	e0	34	69	00	00	01	01	08	0a	bf	7b
0x0050	27	04	0a	71	cd	de	45	48	4c	4f	0d	0a	86	dd	08	00

Figure 4.1: Ethernet frame including checksums.

For each of the following subproblems, clearly mark the respective header fields in Figure 4.1. **Take care that markings can uniquely be related to individual subproblems**, i. e., note the subproblem above markings. Answers that cannot be followed **will not be graded**.

a)* Mark the transmitter address of layer 2 in Figure 4.1.

b)* Mark the receiver address of layer 2 in Figure 4.1.

c)* Mark the frame check sequence in Figure 4.1.

d)* What protocol is used as L3 PDU? Mark the respective header field in in Figure 4.1.

IPv6

e) State the layer 3 source address in its usual and fully abbreviated form.

`2003:a:87f:a4a7:f02b:c99:bc65:1070`

f) State the layer 3 destination address in its usual and fully abbreviated form.

`2a01:4f9:4a:4589:::10:1`

g) What protocol is used as L4 PDU? Mark the respective header field in in Figure 4.1.

TCP

h) At which offset does the layer 4 PDU start? Give an explicit reason how you determine this offset.

Offset: `0x0036` Reason: Next Header indicates TCP, thus fixed length 40 B IPv6 header

i) What type is the layer 7 protocol probably?

The source port is an ephemeral port.However, the destination port 25 (`0x0019` suggests that it is SMTP.

j) For what purpose is that protocol used?

Mail transfer between MTAs.

k) Determine the offset where the L7 PDU starts. Give an explicit reason how you determine this offset.

Offset: `0x0042` Reason: Offset = `0x8` ⇒ 32 B TCP header

l) Decode the first 5 B of the L7 SDU.

ASCII coded string starting at offset `0x0042`: `0x45 0x48 0x4c 0x4f 0x0d 0x0a` = `EHLO\r\n`

Problem 5 TCP (18 credits)

We consider the impact of faults in the network on the transport layer. To that end, we assume the simplified version of **TCP Reno** introduced in the lecture.

a)* Briefly explain **goal and implementation** of TCP's **congestion control**.

Avoid overload within the network by adapting the sender window.

b)* Briefly explain **goal and implementation** of TCP's **flow control**.

Avoid overload at the receiver by allowing the receiver to artificially limit the sender window.

We now consider a specific chain of events that influence the size of the congestion window. Figure 6.1 shows the size of the congestion window in multiples of the MSS over time in multiples of the RTT. The window size after connection establishment initially starts at a size of 1 MSS.

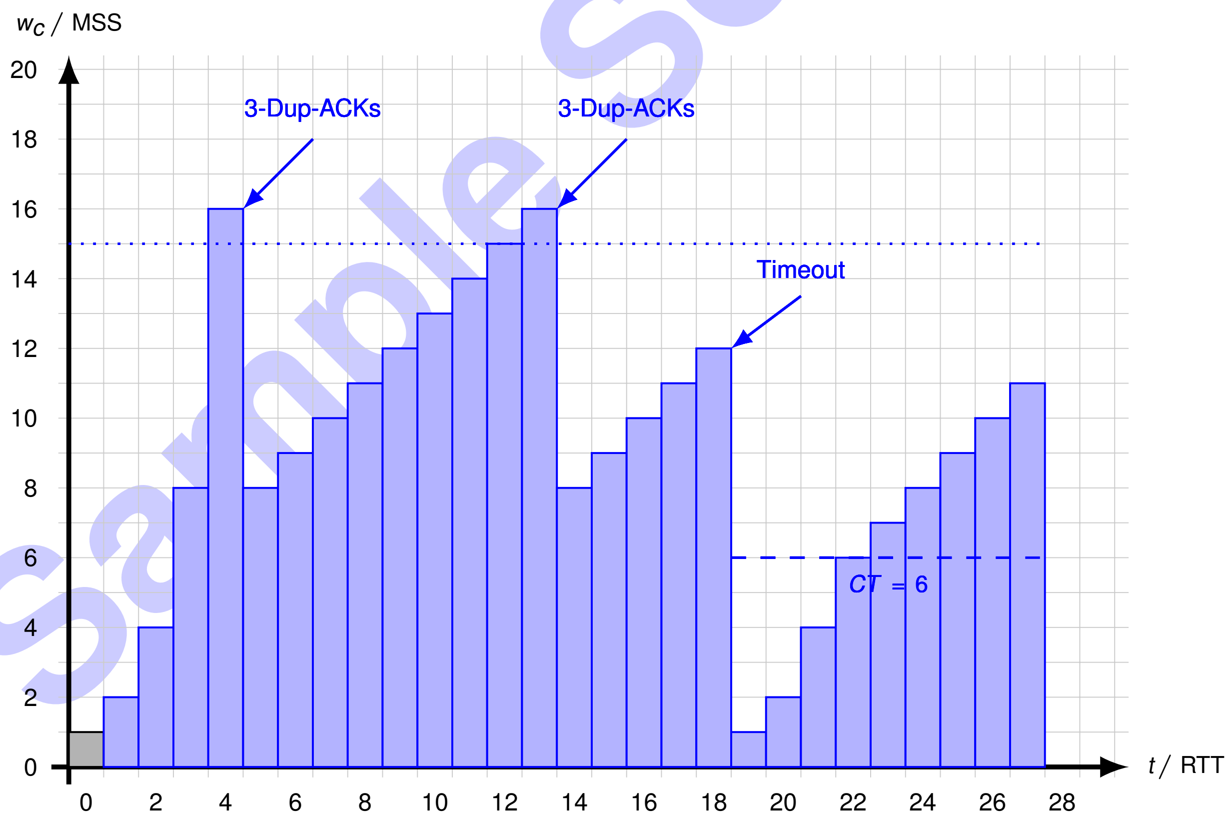


Figure 5.1: Preprint for Subproblems c) and g). An addition preprint can be found at the end of the exam.
Clearly strike out invalid solutions.

The **maximum bandwith** along the path from source to destination is 15 MSS/RTT. Thereby, segment loss occurs as soon as this threshold is crossed. For now, we assume that no timeouts occur.

c)* Draw the evolution of w_c for $t < 18$ RTT in Figure 6.1. **Mark / name the events** leading to a reduction of w_c.

d) Derive the long-term average data rate that can be achieved.

By counting segments of a whole phase: $\frac{(8+9+10+11+12+13+14+15+15)\,\text{MSS}}{9\,\text{RTT}} \approx 11,89\,\frac{\text{MSS}}{\text{RTT}}$

Alternatively, by using the TCP formula (see tutorials): $n = \frac{3}{8}x^2 + \frac{3}{4}x$, for $x = 16$ get $n = 108$ at a loss rate of $\theta = \frac{1}{108}$.
Therefore, the time between segment losses is $T = \left(\frac{x}{2} + 1\right) \cdot \text{RTT} = \left(\frac{16}{2} + 1\right)\,\text{RTT} = 9\,\text{RTT}$.
The achievable data rate is therefore $r_{\text{TCP}} = \frac{108\,\text{MSS}}{9\,\text{RTT}} \cdot (1 - \frac{1}{108}) \approx 11,89\,\frac{\text{MSS}}{\text{RTT}}$.

At $t = 18$ RTT **a timeout occurs.**

e)* What is the most likely cause for such a timeout?

All segments or ACKs are lost, i. e., the sender does not get any feedback whether segments have arrived.

f)* In which way does the timeout differ from receiving duplicate acknowledgements?

Duplicate acknowledgements indicate that some segments still made it to the receiver.

g) Assuming that there are no more losses after that timeout, complete the evolution of w_c in Figure 6.1 for $t \leq 28$ RTT.

h)* Describe the problem for TCP Reno if layers 1 – 3 are too unreliable.

TCP's congestion control mechanism interprets any kind of segment loss as a result of an overload situation.It does not consider the case of randomly lost segments due to transmission errors resulting from, for instance, noisy links, collisions etc.
As a consequence, TCP would decrease w_c and thus never utilize the available bandwidth, which is the wrong decision in such cases.

Problem 6 Short questions (7 credits)

The following subproblems can be solved independently of each other.

a)* We developed a small chat application written in Python in the lecture. A central line of the event loop was:

```
rfd, _, _ = select(rfds, [], [])
```

Explain the function / syscall as well as the named parameter and return value.

- `select()` watches as set / list of file descriptors for activity (in that case for becoming available for reading).
- `rfds` is the list of file descriptors to be watched.
- The return value `rfd` is the list of file descriptors that became available (for reading).

b)* Briefly describe the main difference between a hub and a switch.

Switches forward frames via the port to which the receiver is connected (if there is an entry in the switching table).
Hubs forward frames to all ports except the one via which the frame was received.

c)* Why are three MAC addresses usually used for IEEE 802.11 (WLAN), but only two MAC addresses for IEEE 802.3 (Ethernet)?

Because the AP is not transparent for WLAN clients, i. h. it must be explicitly addressed as an intermediate station between the sender and receiver.
Switches are transparent to other devices.

d)* What is source coding?

Removing redundancy.

e)* Briefly describe the main difference between CSMA/CD and CSMA/CA.

CSMA/CA randomizes media access even when the medium is free (fixed contention window with optional backoff interval), while CSMA/CD only does this after a collision has occurred.
Alternative: Because CSMA/CA cannot reliably detect collisions, confirmation is expected on layer 2. With CSMA/CD, on the other hand, a frame is considered successfully transmitted if no collision was detected during transmission.

Additional space for solutions–clearly mark the (sub)problem your answers are related to and strike out invalid solutions.

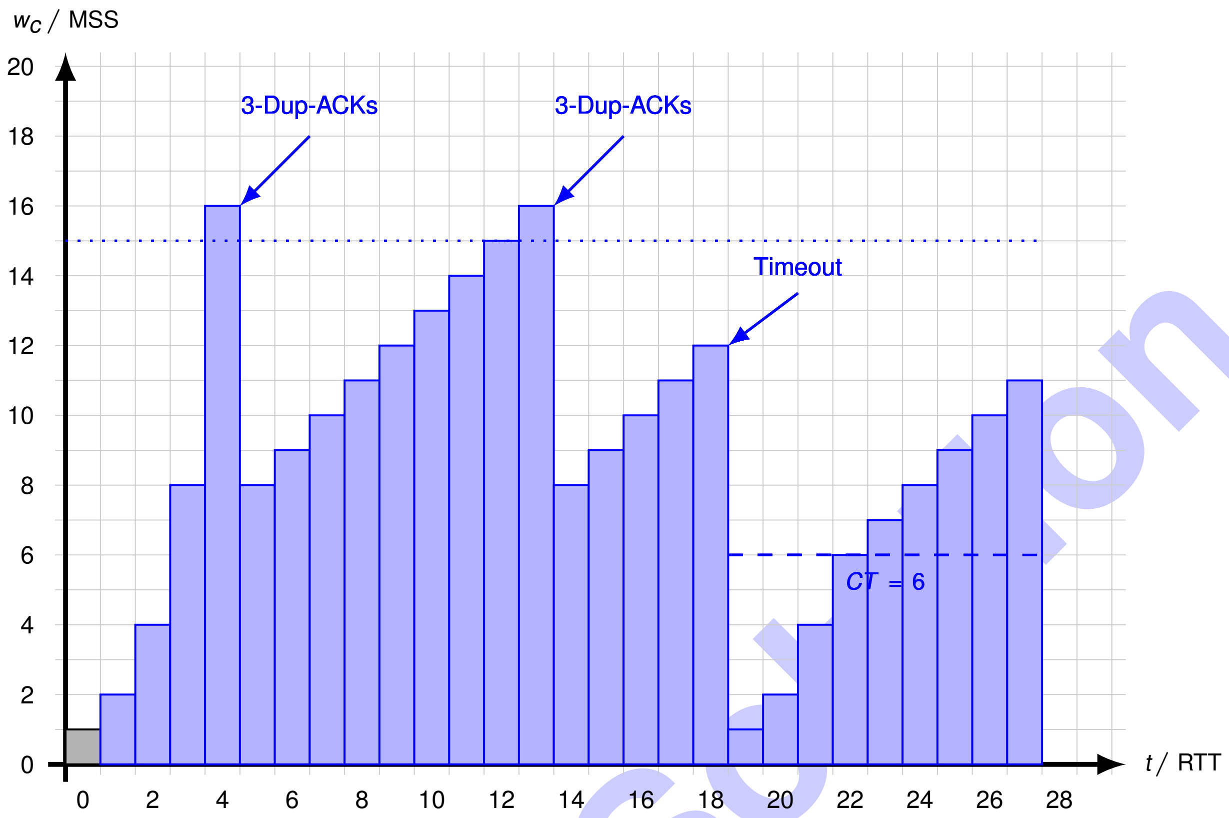


Figure 6.1: Preprint for Subproblems 5 c) and g). **Clearly strike out invalid solutions.**