

This image shows a full page of blank graph paper. The grid consists of small, uniform squares formed by thin, light gray lines. There are no margins, text, or other markings on the page.

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 answer are graded with 1 credit per correct answer and -1 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)* What is the type of the following identifier or address? 70:2e:10:af:7f:ex:81:f0

☐ MAC address

☐ IPv4 address

☐ IPv6 address

☐ None of the listed options

☐ IP identifier

☐ Port number

b)* What is the approximate SNR when sending a signal with a power of 220 mW and a noise power of 5 mW is measured?

☐ ~2.6 dB

☐ 44

☐ ~0.2

☐ ~16.4 dB

☐ 68

☐ ~70.4 dB

c)* Given is an encoder, that converts code words of length 8 bit to channel words of length 10 bit. How much added redundancy is contained in 22 channel words?

☐ 2 bit

☐ 220 bit

☐ 22 bit

☐ 176 bit

☐ 18 bit

☐ 44 bit

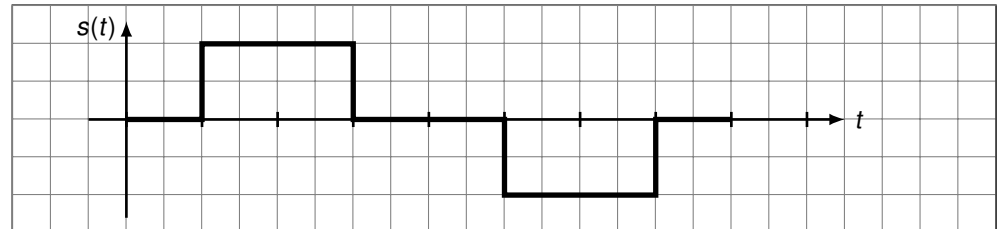
d)* Given is the baseband signal shown below, which encodes the bit sequence 0101 0101. Which line code was used to encode the signal?

☐ NRZ

☐ Manchester

☐ RZ

☐ Rect

☐ MLT-3


e)* Which modulation scheme(s) does the adjacent signal constellation diagram represent?

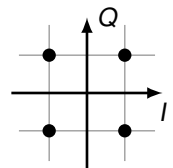
☐ 2+2-AM

☐ 2+2-AK

☐ 4-QAM

☐ 2+2-PSK

☐ BPSK

☐ 4-ASK


f)* The header(s) of which protocol(s) can occur immediately after an Ethernet header?

☐ DNS

☐ UDP

☐ ICMPv6

☐ ARP

☐ ICMPv4

☐ NDP

g)* Which IP header fields are **guaranteed** to change when a packet is routed from one endpoint to another over multiple hops?

☐ Version

☐ Flow label

☐ TTL

☐ Fragment Offset

☐ Traffic Class

☐ Header Checksum

☐ Destination IP Address

☐ Protocol

☐ IHL

h)* Consider the IPv4 address range **10.8.0.0/24** that is divided into **eight** subnets with 32 addresses each. Which statements about these subnets are true?

- ☐ 10.8.0.255 is the broadcast address of the fourth subnet.
- ☐ 10.8.0.224 is the network address of the last subnet.
- ☐ The prefix length of the subnets is /21.
- ☐ Each subnet has 30 host-assignable addresses.
- ☐ 255.255.255.224 is the subnet mask of each subnet.
- ☐ 10.8.0.32 is the first host-assignable IP address in the second subnet.

i)* What is the *Maximum Segment Size (MSS)* between two directly connected hosts if the MTU is 1 280 B? Assume that IPv6 and TCP are used without extension headers or options.

- ☐ 1 280 B
- ☐ 1 260 B
- ☐ 1 220 B
- ☐ 980 B
- ☐ 1 460 B
- ☐ 1 440 B

j)* Which of the following properties apply to link-state routing protocols?

- ☐ Routers have no information about the network topology.
- ☐ The operating principle is similar to the Bellman-Ford algorithm.
- ☐ The operating principle is similar to Dijkstra's algorithm.
- ☐ Routers regularly exchange status messages.
- ☐ Routers determine a minimum spanning tree from the exchanged information.
- ☐ Routers only exchange cumulative costs with each other.

k)* Which are **not** standard HTTP methods?

- ☐ FETCH
- ☐ PUT
- ☐ GET
- ☐ POST
- ☐ DELETE
- ☐ HEAD

l)* What is correct regarding DNS?

- ☐ The TTL specifies how long a resource record may be cached.
- ☐ A resolver contacts at most one nameserver during iterative querying.
- ☐ Every resolver is an authoritative nameserver.
- ☐ PTR records must be in the same zone as the corresponding A records.
- ☐ A nameserver sends iterative queries.
- ☐ Multiple nameservers can be authoritative for the same zone.

Problem 2 Switching WiFi (16 credits)

Given is the network shown in Figure 2.1. Assume that the notebooks are associated with the access point AP and that the switching table of SW is empty.

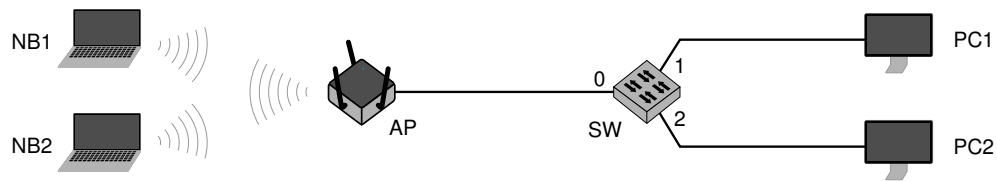


Figure 2.1: Topology

0 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ a)* Mark all collision domains in Figure 2.1. Make sure that interfaces are clearly associated with the respective collision domain.

1 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ b)* Briefly argue how many broadcast domains there are in this topology.

0 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

1 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

0 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ c)* Argue for both the switch SW and the access point AP whether they have a MAC address or not.

Hint: Consider whether the device is transparent to the communication or not.

1 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

2 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

3 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

NB1 wants to send a message **to PC2**. Assume that NB1 knows the MAC address of PC2.

0 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ d) Name all MAC addresses that are present in the frame on the link **from NB1 and AP** by specifying the respective device name. Additionally specify the meaning(s) of the addresses:

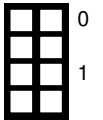
- SA: Source Address
- DA: Destination Address
- TA: Transmitter Address
- RA: Receiver Address

Hint: There are more rows than needed.

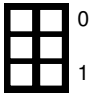
Address/Device	Meaning(s)

The frame now reaches the switch SW.

e)* Argue to which ports (0,1,2) the switch will forward the frame to.



f)* Update the switching table in Table 2.1 so that it reflects the state after the frame passed the switch.

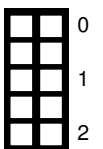


Subtask	Address/Device	Port
f)		
i)		

Table 2.1: Switching table of switch SW

g) Name all MAC addresses that are present in the frame on the link **from SW and PC2** by specifying the respective device name. Additionally specify the meaning(s) of the addresses.

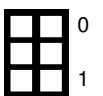
Hint: There are more rows than needed.



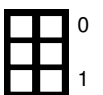
Address/Device	Meaning(s)

PC2 responds to the request with another frame.

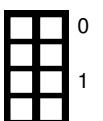
h) Argue to which ports (0,1,2) the switch will forward the frame **of the response** to.



i) Update the switching table in Table 2.1 so that it reflects the state after the frame **of the response** passed the switch.



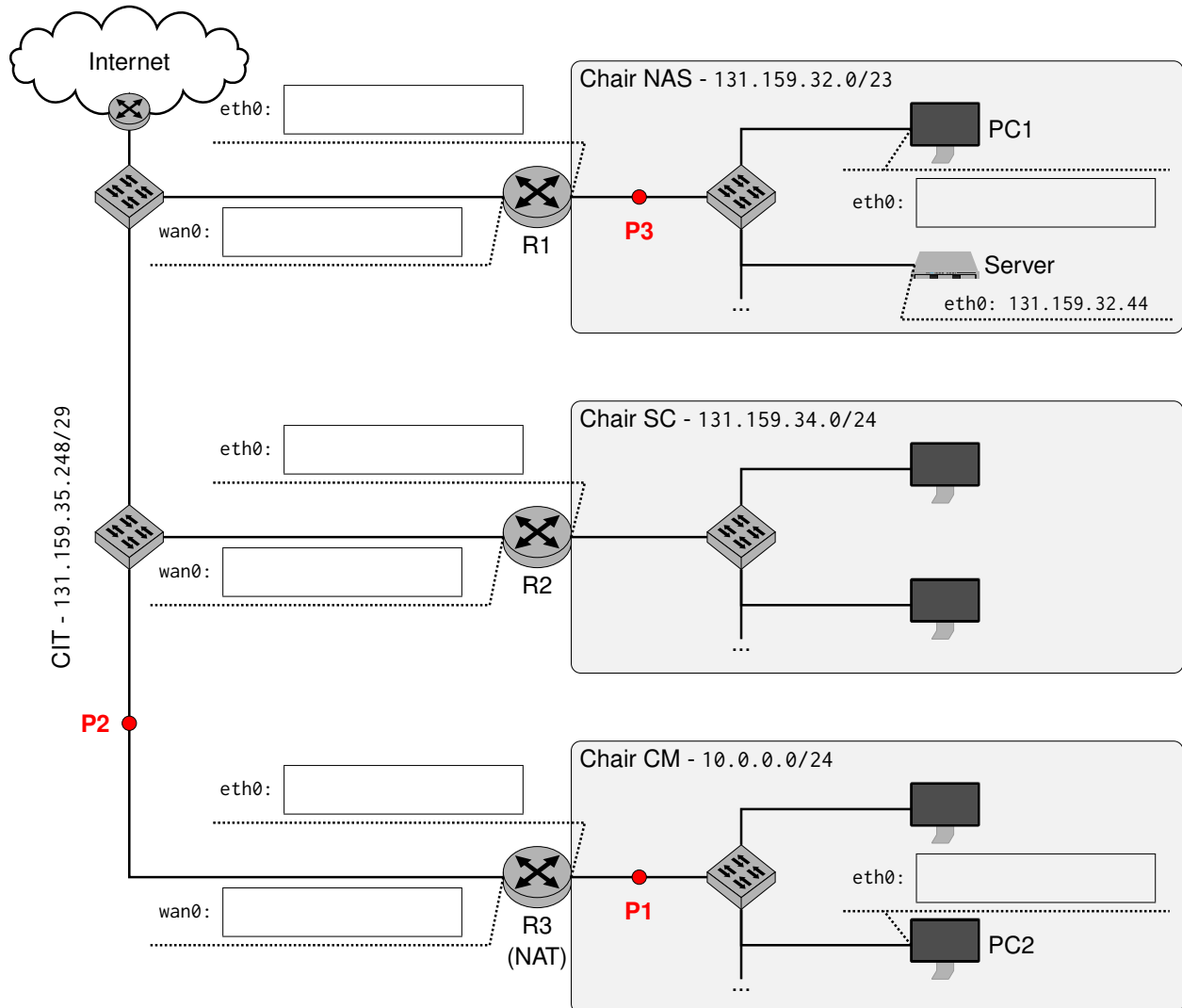
j)* Name and explain a possible Denial of Service attack that can be performed on the wireless part of the network.



Problem 3 CIT Chairlink (15 credits)

In this task, you configure internal networks of and between chairs of the *School of Computation, Information and Technology*. All networks use public IPv4 addresses, except for the one of the CM chair. Unfortunately there were not enough addresses left, so they use a private address range and R3 implements NAT. Assume that all caches of all devices are empty.

a)* Assign valid IP addresses to the named interfaces in the topology. Mind the respective address ranges! Routers should have the last address of a network. When there are multiple routers, addresses should be in ascending order of the router index (i.e. R3 should have the highest address).



b)* Calculate the number of usable host addresses in the NAS network.

After the network setup, **PC1** wants to send an HTTP request to **Server** in the same network and already knows the IP address of the server. At this point however, PC1 is not able to contact the server.

c)* Explain why PC1 cannot contact the server, what information is missing and how that information can be obtained.

	0
	1
	2
	3
	4
	5

0
1
2
3
4

Problem 4 Wired shark (15 credits)

You are a network administrator at a media company and maintain a part of their network infrastructure shown in Figure 4.1:

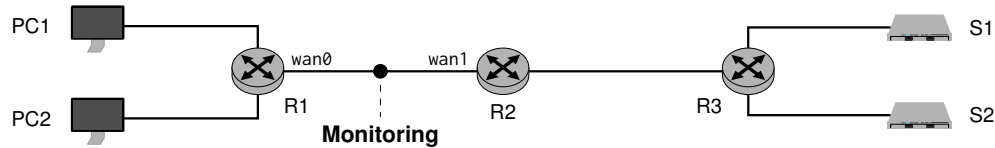


Figure 4.1: Network topology

Today, you are tasked with debugging a problem in a legacy video stream. You use Wireshark to monitor frames on the link between routers R1 and R2 and see multiple frames **from PC1 that should reach server S2**, but do not. Figure 4.2 shows such a frame.

```

0x0000  30  ee  a4  4b  43  d5  e0  63      da  89  f1  ee  86  dd  60  07
0x0010  45  3d  00  84  06  3f  20  01      0d  b8  11  ab  00  01  32  44
0x0020  d7  ff  fe  65  dc  73  20  01      0d  b8  11  ab  00  0d  00  00
0x0030  00  00  00  00  00  02  c2  65      01  bb  a2  77  24  07  00  00
0x0040  00  00  80  02  fa  f0  ee  b8      00  00  01  01  08  0a  b8  ba
0x0050  4a  00  2b  cf  d4  80  a8  52      a7  c9  99  1d  82  10  37  ..

```

Figure 4.2: Ethernet frame (truncated)

First, you decide to gather some information about the involved devices and protocols.

Please note: Depending on the subproblem you must or should mark relevant parts of the hexdump—ensure that the markings are clearly associated with the subtask. Answers where the solution approach is not documented sufficiently **will not be graded**. Note down MAC and IP addresses in their respective formats and, in case of IPv6, their shortened form.

- 0

1

a)* What is the MAC address of R1.wan0? Only name and mark the respective header field.

Address:
Field:
- 0

1

b)* What is the MAC address of R2.wan1? Only name and mark the respective header field.

Address:
Field:
- 0

1

c)* Which network layer protocol is used?

Protocol:
Reasoning:
- 0

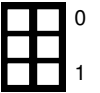
1

2

d) What is the IP address of PC1? Only name and mark the respective header field.

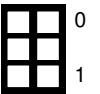
Address:
Field:

e) Through which mechanism was the IP address of PC1 most likely obtained? Explain shortly.



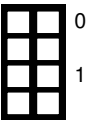
f) Which transport layer protocol is used?

Protocol:	Reasoning:
-----------	------------



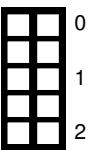
g) Which application layer protocol is most likely used?

Protocol:	Reasoning:
-----------	------------



h) At what index (e.g. 0x0065) in the frame does the PDU of layer 5 start?

Index:	Reasoning:
--------	------------



Then, you see another packet on the monitored link with an ICMPv6 message that provides additional information about the underlying problem. Figure 4.3 shows only the header and payload of the ICMP message.

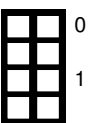
```

0x0000  01 00 ff ff 00 00 00 00    60 07 45 3d 00 84 06 3f
0x0010  20 01 0d b8 11 ab 00 01    32 44 d7 ff fe 65 dc 73
0x0020  20 01 0d b8 11 ab 00 0d    00 00 00 00 00 00 00 02
0x0030  c2 65 01 bb a2 77 24 07    00 00 00 00 80 02 fa ..
  
```

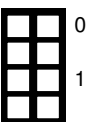
Figure 4.3: ICMPv6 message (truncated)

i)* What is the underlying cause of the ICMP message? Remember to name and mark respective fields.

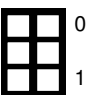
Message cause:
Reasoning:



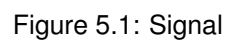
j) Argue which device in the topology created this ICMP message.



k) Explain what you might need to change in your network such that the packets are successfully received.



Given is the analog signal of a sensor, shown in Figure 5, that represents the current draw of a motor. In order to process the signal in a controller, it must be converted to a digital signal through sampling and quantization.



0  a)* Enter the numerical values of the quantization steps in the first row of Table 5.1. Choose the quantization steps linearly with minimal quantization error in l_q .
 1  **Hint:** there are more columns than necessary.
 2  b)* Enter the binary code words corresponding to the quantization steps in the second row of Table 5.1.

Table 5.1: Quantization steps and their code words[illegible]

Table 5.2: Sample points, quantized values, and code words

f) Map the quantized values back to the respective code words and enter the code words in the third row of Table 5.2.

g)* Calculate the maximum quantization error inside I_q .

[illegible]

A diagram showing a 2x4 grid of squares. The first column is labeled '0' and the second column is labeled '1'.

The current resolution is too coarse for the intended application. Instead, a much lower quantization error of $q'_{\max} = 0.1$ should be achieved.

h)* Determine the number of quantization steps M' required to achieve the maximum error $q'_{\max}$.

[illegible]

A diagram showing a 2x4 grid of squares. The first two columns are labeled '0' and '1' respectively, indicating the parity of the column index.

i) Determine the code word length if M' code words are used.

[illegible]

A diagram showing a 2x2 grid of squares. The top row is labeled '0' and the bottom row is labeled '1'.

Problem 6 HTTP Security (13 credits)

A friend of yours, Bob, wants to get into self-hosting a server with a webservice, but is unfortunately quite inexperienced. Luckily you have advanced knowledge about networking and IT security to help Bob out. Initially he asks you some questions about how he can set up user accounts on his web server.

a) Differentiate the terms Authentication and Authorization.

--

Diagram illustrating a 3x2 grid of squares. The columns are labeled 0, 1, and 2 from left to right.

To make the user accounts work, Bob has to store user names and passwords. You tell him that he must never store passwords in plain text, but that he should hash and salt them.

b) Explain what a rainbow table is.

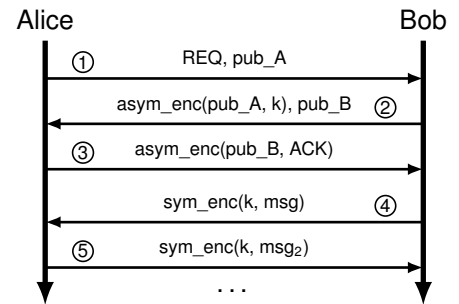
	0
	1

c) Explain how salting a password protects against attacks using rainbow tables.

	0
	1

Initially Bob wanted to implement his own protocol to secure the web traffic of his server. He came up with a simple key exchange between a user (Alice) and his self-hosted server (Bob).

In the first two messages Alice and Bob exchange public keys. Then, Bob generates a symmetric key and sends it to Alice. All further communication is symmetrically encrypted. That way, no one can access the secret key and all communication is safe... at least that's what Bob thinks.



d)* Point out the flaw of Bob's encryption strategy. Explain how a malicious actor *Mallory* can gain access to the exchanged data.

Through your explanation, you successfully convinced Bob to stick to tried and tested implementations like HTTPS with TLS. The following figures show the encryption process of the two AES variants Electronic Codebook (ECB, Fig. 6.1) and Cipher Block Chaining (CBC, Fig. 6.2) that can be part of a TLS cipher suite.

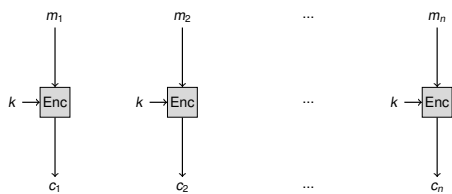


Figure 6.1: Electronic code book (ECB) mode

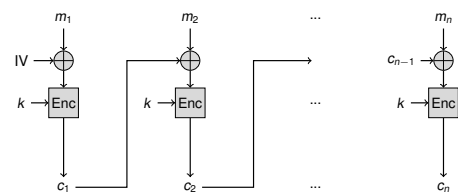


Figure 6.2: Cipher Block Chaining (CBC) Mode

e)* Why should ECB mode not be used in practice? Briefly describe what might happen.

f) Explain how CBC mode fixes the problem described in e).

Another important feature of TLS is authentication of the server using certificates. When Alice connects to Bob's server, the server returns a certificate in the TLS handshake. Obtaining the certificate itself is however not sufficient to prove authenticity. Instead, two verification steps have to be performed.

g)* Explain the two verification steps Alice has to do with the certificate.