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

Eexam
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 / Endterm	**Date:**	Thursday 16th February, 2023
Examiner:	Prof. Dr.-Ing. Stephan Günther	**Time:**	14:00 – 15:30

Before we proceed with reading the processing instructions, please answer the following questions. This information helps us to examine learning success depending on participation in individual lecture components. The information is **voluntary** and **not considered for evaluation**, i. e., answers to these questions do not give credits. In order to exclude any influence, this page will not be made accessible during the correction.

a) Did you attend the lecture?

☐ 1 (regularly) ☐ 2 (sometimes) ☐ 3 (never)

b) Did you attend the tutorials?

☐ 1 (regularly) ☐ 2 (sometimes) ☐ 3 (never)

Working instructions

- This exam consists of **12 pages** with a total of **6 problems** and the cheatsheet ditributed with the exam. Please make sure now that you received a complete copy of the exam.
- The total amount of achievable credits in this exam is 90 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)

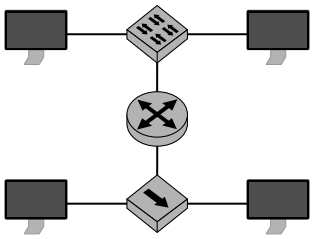
The following subproblems are multiple chouce / multiple answer, i. e., at least one answer per subproblem is correct. Subproblems with a single correct answer are graded with 1 credit if correct. Those with more than one correct answers are graded with 0.5 credit per correct answer and -0.5 credit per 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 statesments regarding MLT-3 are correct?

- ☐ It is a line code
- ☐ It is a source code
- ☐ It is guranteed to be DC-free
- ☐ It is a channel code
- ☐ One symbols encodes 3 bit
- ☐ The spectrum is narrower than Manchester

b)* How many broadcast domains does the network to the right contain?

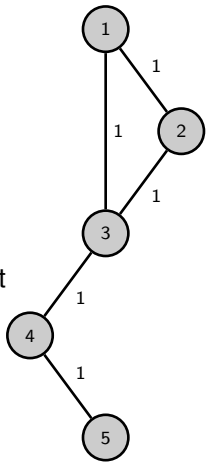


☐ 3 ☐ 6 ☐ 1 ☐ 5 ☐ 2 ☐ 4

c)* How many collision domains does the network to the right contain?

☐ 4 ☐ 2 ☐ 3 ☐ 1 ☐ 6 ☐ 5

d)* Mark the adjacency matrix for the network to the right.



☐ $\begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix}$ ☐ $\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$ ☐ $\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

e)* Given the distance matrix $\boldsymbol{D}$ for the network to the right. What is the minimum n such that $\boldsymbol{D}^n = \boldsymbol{D}^{n+1}$ holds?

- ☐ $n = 1$
- ☐ $n = 4$
- ☐ $n = 3$
- ☐ $n = 6$
- ☐ $n = 7$
- ☐ $n = 0$
- ☐ $n = 2$
- ☐ $n = 5$

f)* Given the IP address 192.0.2.42, determine the respective PTR record in DNS.

- ☐ 42.2.0.192.in-addr.arpa.
- ☐ 192.0.2.42.
- ☐ There is no PTR record
- ☐ 192.0.2.42.in-addr.arpa.
- ☐ 42.2.0.192.
- ☐ Something different

g)* Which of the following syscalls are usually **only** used with datagram oriented sockets?

- ☐ `sendto()`
- ☐ `send()`
- ☐ `bind()`
- ☐ `accept()`
- ☐ `recvfrom()`
- ☐ `recv()`
- ☐ `listen()`
- ☐ `connect()`

h)* Given the binary value `10011100` in network byte order. Determine its representation in little endian.

- ☐ `10011100`
- ☐ `00111001`
- ☐ `11001001`
- ☐ `00110110`

i)* Which of the following addresses are not routable in the Internet?

- ☐ 169.254.0.72
- ☐ 142.251.36.174
- ☐ 131.159.15.24
- ☐ 172.16.12.1
- ☐ 129.187.255.109
- ☐ 9.9.0.1

j)* Which of the following are valid types of switching?

- ☐ Circuit Switching
- ☐ Lane Switching
- ☐ Package Switching
- ☐ Message Switching
- ☐ Parcel Switching
- ☐ Multi-Track Switching

k)* What does IHL stand for in the context of IPv4?

- ☐ IP Header Length
- ☐ Integrated Header Length
- ☐ Informative Header Length

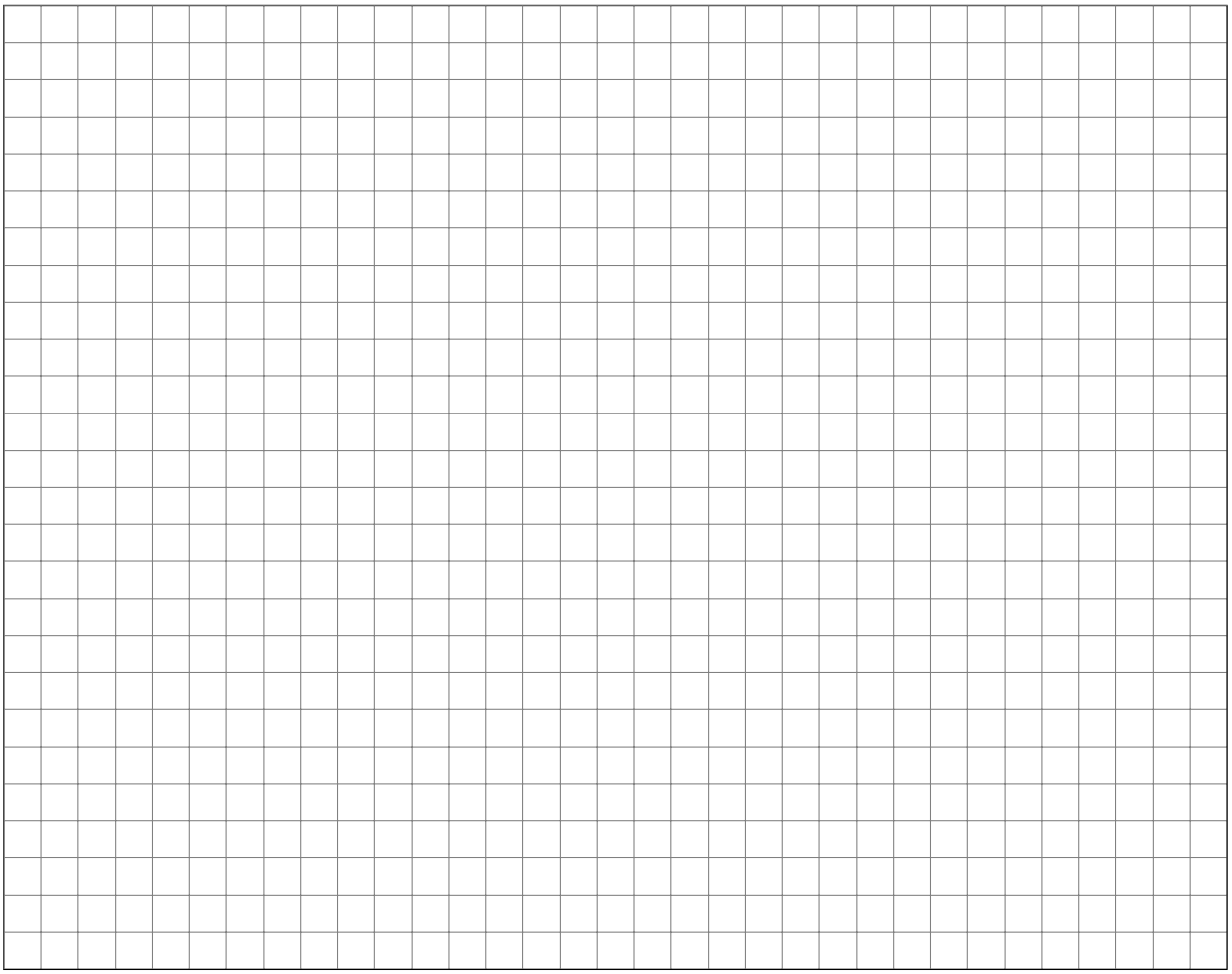
l)* Which of the following protocols **do not** feature checksums?

- ☐ IPv4
- ☐ UDP
- ☐ ARP
- ☐ IPv6
- ☐ TCP
- ☐ Ethernet

m)* Which of the following are **invalid** HTTP commands?

- ☐ GET
- ☐ HEAD
- ☐ DELETE
- ☐ POST
- ☐ DISCARD
- ☐ PUT

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



Problem 2 TCP (15 credits)

In this problem we consider the message exchange between client and server when accessing `http://cns.net.in.tum.de`.

0 1

a)* A server receives both a UDP datagram and a TCP segment from the same source address. Both feature the same port number as their source port. Is this a problem?

0 1

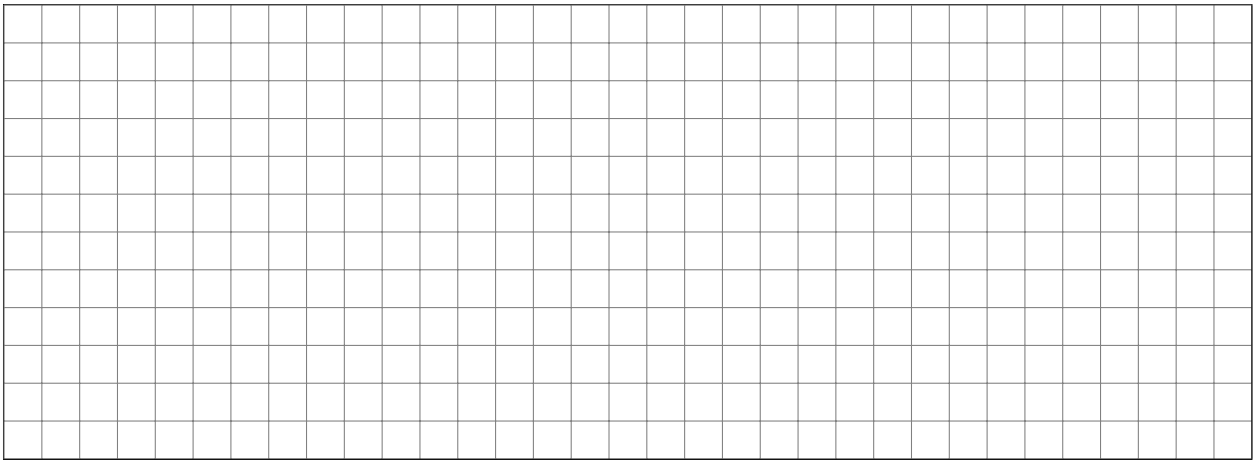
b)* Justify which port number will be used as source port by the client? Assume the client is an unprivileged process.

0 1

c)* Justify which port number will be used as destination port by the client?

0 1 2 3

d)* Sketch the connection establishment in the chart below. For each segment exchanged between client and server, state the SEQ and ACK numbers, the segment length (LEN), and relevent flags that are set.



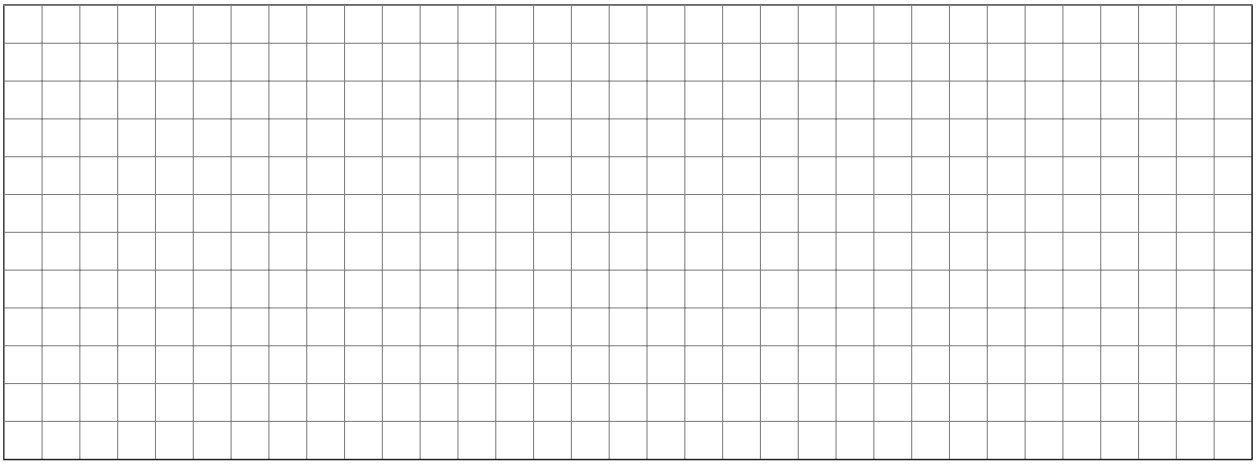
0 1

e) What is the payload (protocol and type, action, or method) of the next segment sent by the client?

The segment sent in Subproblem e) has a payload of 81 B, followed by a response of length 370 B by the server.

f) Draw the message exchange so far assuming that the MSS is not exceeded for individual segments.

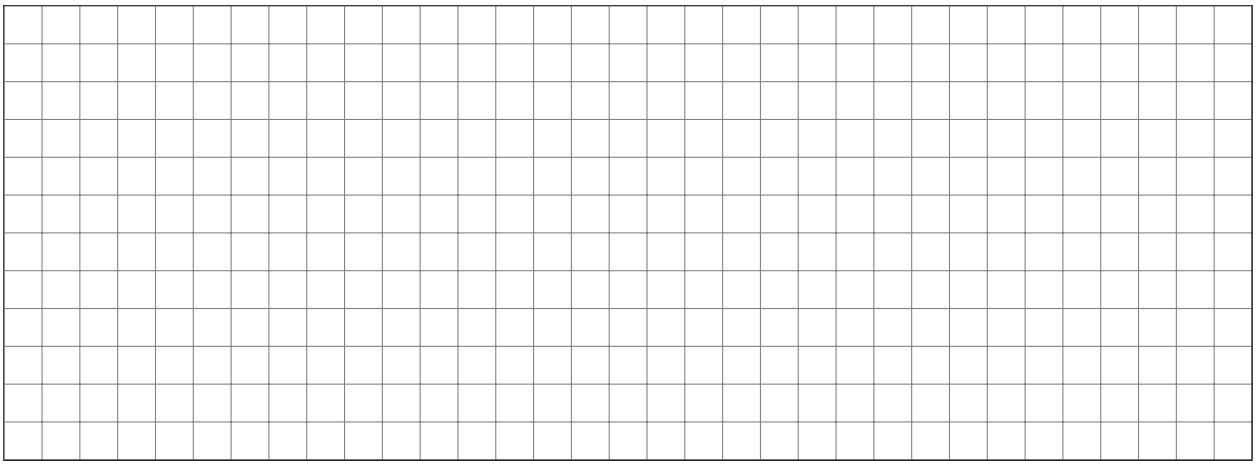
0 1 2 3



After that, the connection termination is initiated by the client and completed from both sides.

g)* Draw the message exchange during termination.

0 1 2 3



The reply from the server in Subproblem f) has the following text content:

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.18.0
Date: Thu, 02 Feb 2023 10:55:24 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
Location: https://cns.net.in.tum.de/
(...)
```

h)* What does the response mean?

0 1 2

Problem 3 DNS (13.5 credits)

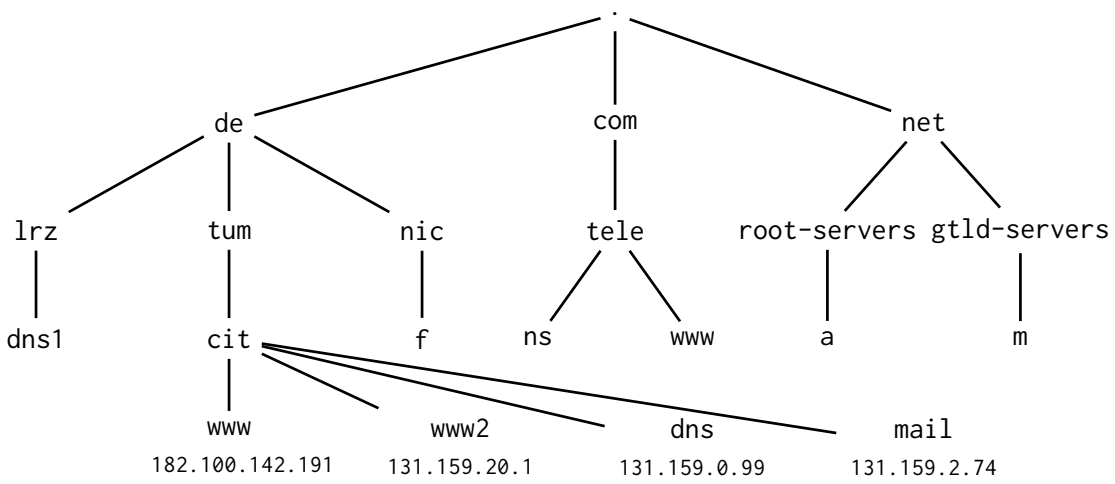


Figure 3.1: A part of the DNS.

0 1 a) Briefly describe the purpose of DNS.

0 1 b) Briefly describe the difference between a fully and non-fully qualified domain name.

Figure 3.1 shows the zone file of the authoritative name server for `cit.tum.de`.

```
 1  $ORIGIN cit.tum.de.
 2  $TTL 1H
 3
 4  @ IN SOA dns.cit.tum.de. hostmaster.cit.tum.de. (...)
 5
 6  cit.tum.de.          IN    NS     _________.tum.de.
 7  cit.tum.de.          IN    MX     __  _________.tum.de.
 8
 9  dns.cit.tum.de.      IN    A      ___________________
10  mail.cit.tum.de.     IN    A      ___________________
11  www.cit.tum.de.      IN    A      ___________________
12  www2.cit.tum.de.     IN    A      ___________________
```

0 1 Figure 3.2: DNS zone file on nameserver `dns.cit.tum.de`

0 1 2 c)* Add the mail server **`mail.in.tum.de`** to the zone file given in Figure 3.2 based on the information from Figure 3.1 and assign it preference **20**.

d)* Add all other missing records in Figure 3.2 based on the information from Figure 3.1.

e)* What purpose does the TTL of 1 h in the DNS zone file serve?

0 1

f)* What purpose does a zone transfer serve?

0 1

g)* What does “authoritative” mean in the context of DNS?

0 1

h)* When does DNS use TCP instead of UDP?

0 1

i)* How is the administrator of `dns.cit.tum.de.` ensured that no malicious server answers the requests for their zone, assuming that man-in-the-middle attacks are not possible.

0 1 2

j) Explain the difference between recursive and iterative name resolution.

0 1 2

Problem 4 **Wireshark (15.5 credits)**

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

0x0000	04	7b	cb	b7	08	00	3c	a6	2f	78	08	00	08	00	45	00
0x0010	00	5d	9c	42	40	00	36	06	54	a0	83	9f	0f	0c	c0	a8
0x0020	08	00	00	16	8e	6a	aa	92	9a	6f	23	7a	28	7a	80	18
0x0030	03	fa	25	15	00	00	01	01	08	0a	89	c1	b0	62	9f	ea
0x0040	77	60	53	53	48	2d	32	2e	30	2d	4f	70	65	6e	53	53
0x0050	48	5f	37	2e	39	70	31	20	44	65	62	69	61	6e	2d	31
0x0060	30	2b	64	65	62	31	30	75	32	0d	0a	42	0a	f1	73	

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 **are not graded**.

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

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

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

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

0
1 e) State the layer 3 source address in its usual and fully abbreviated form.

0
1 f) State the layer 3 destination address in its usual and fully abbreviated form.

0
1 g) What protocol is used as L4 PDU? Mark the respective header field in in Figure 4.1.

0
1
2 h) At which offset does the layer 4 PDU start? Give an explicit reason how you determine this offset.

Offset: Reason:

i) What type is the layer 7 protocol probably?

0 1 2

j) For what purpose is that protocol used?

0 1

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

Offset: Reason:

0 1 2

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

0 1 2

Problem 5 **Short Questions: Security (20 credits)**

a)* Differentiate Authentication from Authorization.

0 1 2

b)* Why are so-called hybrid encryption schemes employed? Describe the function of such scheme, and why each component is used.

0 1 2

0 1 2 3

c)* Name and describe the three properties of a cryptographic hash function.

0 1 2 3

d)* Sketch a simple scheme for signing data. **Sketch only the signature generation!**
Use the block diagrams you know from the lecture. **You do not need to reason your answer.**
You can use the cryptographic hash function `H(x)` and assume the signing party to possess a key pair `(key_priv, key_pub)`. For encrypting and decrypting you may use `aenc(key, msg)`, `adec(key, msg)` as well as `enc(key, msg)` and `dec(enc, msg)`.

0 1 2

e)* Describe the tasks and responsibilities of a Certification Authority (CA) and Registration Authority (RA).

0 1

f)* Why is the usage of true randomness for cryptographic purposes important.

g)* Differentiate AH from ESP in the context of IPsec.

0 1 2

h)* What problem does IPsec pose to NAT, and how does NAT-T solve it?

0 1

i)* Describe the properties offered by a cryptographic scheme implementing Perfect Forward Secrecy (PFS).

0 1

j)* What main drawback does the usage of AES-ECB come with?

0 1

k)* Describe how a length-extension attack against Merkle-Damgård-based hash functions works.

0 1 2

Problem 6 Short Questions: General Knowledge (8 credits)

0 1

a)* What are well-known ports?

0 1

b)* What is a major advantage of OSPF over RIP?

0 1 2 3

c)* Assume a channel with a bandwidth of 35 MHz. Calculate the maximum data rate given a signal to noise ratio of 45 dB.

0 1

d)* Which purpose does ARP serve?

0 1 2

e)* A time-continuous signal with unknown properties, whose signal level varies in the interval [-3, 3), shall be digitized such that the quantitization error is minimal. The resulting signal levels are encoded using 2 bit. Determine the signal levels and the maximum quantization error in the given interval.