Chair of Distributed Systems and Security
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.

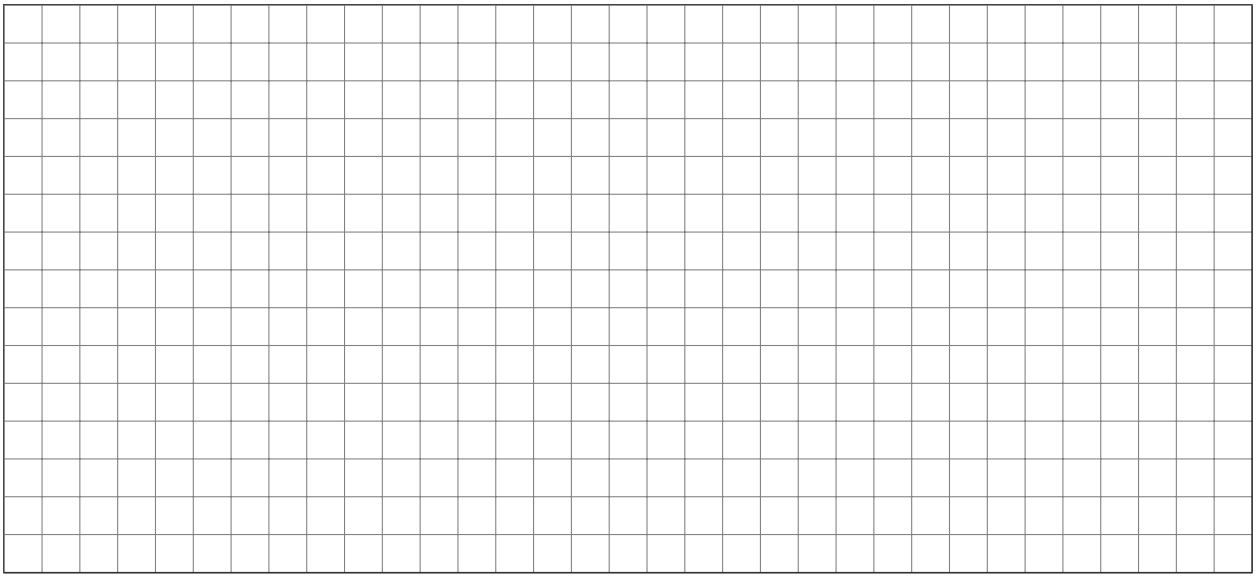
Computer Networking and IT Security

Exam:	INHN0012 / Retake	**Date:**	Wednesday 1st April, 2026
Examiner:	Prof. Dr.-Ing. Stephan Günther	**Time:**	14:00 – 15:30

Working instructions

- This exam consists of **12 pages** with a total of **6 problems**.
- The total amount of achievable credits in this exam is 90 credits.
- Detaching pages from the exam is prohibited.
- Allowed resources:
  - the **provided cheat sheet** inside the exam booklet
  - 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.

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



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 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 SNR if a signal is sent with a power of 30 mW and there is a measured noise power of 10 µW?

☐ ∼31,761 dB ☐ ∼666,67 ☐ 3000 ☐ 1.5 ☐ 1500 ☐ ∼34,771 dB

b)* What is the minimum code word length when quantizing values in the interval $I_Q = [2; 18]$ with a maximum step size of 0.5?

☐ 5 bit ☐ 32 bit ☐ 16 bit ☐ 1 bit ☐ 8 bit ☐ 6 bit

c)* A message source emits characters of the alphabet $\mathcal{X} = \{\text{“}\pi\text{”}\}$. What is the entropy of the message source?

☐ 2 bit ☐ ∞ ☐ 0 bit ☐ ∼3.14 bit ☐ unknown ☐ 1 bit

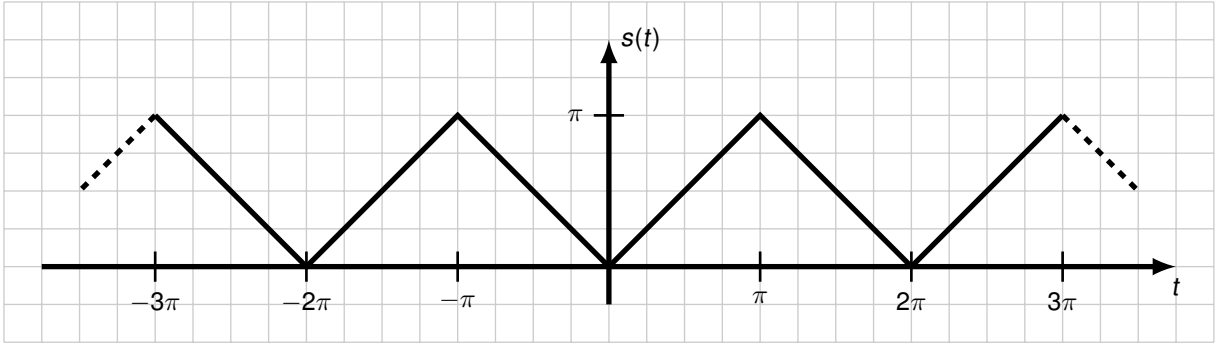
d)* Given is a link with a bandwidth of 44 Mbit/s and a propagation delay of 2 ms. What is the bandwidth delay product of the link?

☐ 44 ms ☐ 88 kbit ☐ 22 Mbit ☐ 88 Mbit ☐ 44 Mbit/s ☐ 22 Mbit/s

e)* Given is the two byte value `11001110 01011101` in little endian. What is the correct representation in network byte order?

☐ `10111010 01110011` ☐ `01011101 11001110`
☐ `01110011 10111010` ☐ `11001110 01011101`

f)* Given is the time-periodic signal shown below. The signal shall be analyzed using the fourier series.



What is correct regarding the fourier coefficients?

☐ $\forall k: b_k = 0$ ☐ $\forall k > 0: a_k = 0$ ☐ $a_0 = 0$
☐ $\exists k > 0: a_k \neq 0$ ☐ $a_0 \neq 0$ ☐ $\exists k: b_k \neq 0$

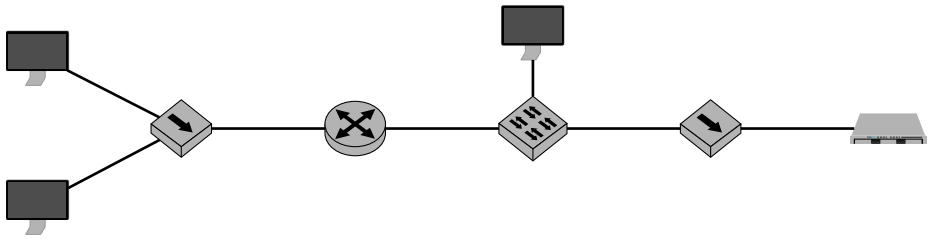


Figure 1.1: Network Topology

g)* How many collision domains are in the network topology in Figure 1.1?

☐ 5 ☐ 1 ☐ 4 ☐ 6 ☐ 2 ☐ 0 ☐ 7 ☐ 3

h)* How many broadcast domains are in the network topology in Figure 1.1?

☐ 5 ☐ 2 ☐ 4 ☐ 3 ☐ 1 ☐ 0 ☐ 7 ☐ 6

i)* What is correct regarding NAT?

- ☐ NAT replaces the src. port of incoming packets.
- ☐ NAT replaces the dst. port of outgoing packets.
- ☐ NAT replaces the dst. IP of outgoing packets.
- ☐ NAT replaces the src. IP of incoming packets.
- ☐ NAT replaces the src. IP of outgoing packets.
- ☐ NAT can translate TCP ports into UDP ports.
- ☐ NAT replaces the dst. IP of incoming packets.
- ☐ NAT provides a very high level of protection against unauthorized access.

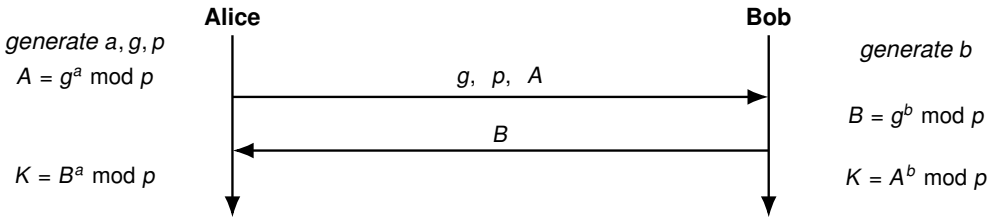


Figure 1.2: Diffie-Hellman Key Exchange

j)* What is correct regarding the Diffie-Hellman (DH) key exchange?

- ☐ The basic DH scheme is vulnerable to man-in-the-middle attacks.
- ☐ An attacker observing g, p, A, B cannot derive the shared secret without knowing a or b.
- ☐ DH requires a pre-shared secret to initiate the exchange.
- ☐ The DH parameters should be signed with short-term keys.
- ☐ Using static (non-ephemeral) DH key pairs achieves Perfect Forward Secrecy.

k)* Which of the following hash functions are considered broken?

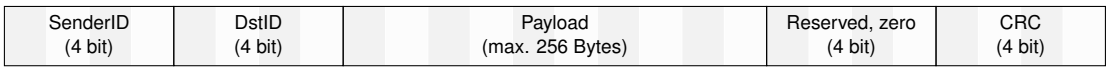
☐ MD5 ☐ SHA-1 ☐ BLAKE3 ☐ SHA-256 ☐ SHA-3 ☐ argon2

l)* Which IPsec mode encrypts the entire original IP packet, including its header?

- ☐ Tunnel mode with ESP
- ☐ Transport mode with ESP
- ☐ Transport mode with AH
- ☐ Tunnel mode with AH

Problem 2 Digital Messaging (17 credits)

In this problem we consider a simple wireless communication protocol. Each message consists of a header, some payload and a trailer that contains a checksum over everything before.
The header starts with a 4 bit sender id, followed by a 4 bit destination id. The payload consists of ASCII encoded text and is always delimited with the `NUL` character. The maximum payload length of a message is 256 B. The trailer contains four bits that are reserved and set to zero, followed by the 4 bit checksum.



Assume that the network currently consists of four nodes that are within reach of each other. The nodes have the IDs 3, 5, 6 and 9. Node 5 wants to send a message with content `CNS@HN` to node 3.

0 1 2

a)* Write the header and payload of this message in hexadecimal representation in network byte order.

0 1

b)* Assuming perfect reception, argue which nodes will receive the message sent by node 5 **and** which of those will **process or discard** the message and why.

The CRC contained in the trailer is used to detect errors during the transmission. To create the CRC, the reduction polynomial $r(x)$ = `11011` (coefficient notation) is used. After sending the message, node 5 receives the answer m = `0011 0101 0000 1111` which contains no payload.

0 1

c)* Write down the reduction polynomial $r(x)$ in the analytic notation (no reasoning required).

0 1 2 3

d)* Verify the CRC to check whether the message has changed in transit by doing the complete calculation. Note down all intermediate steps, the result and the remainder.

0 1

e) Use the calculation to argue whether there was a transmission error.

The used wireless channel has a comparatively high bit error probability of $p_e = 10^{-3}$ that results in frequent broken transmissions.

f)* Calculate the probability that a message with maximum payload length is received without error. Use the random variable X to model the number of bit errors in a message.

0 1 2

To address the relatively high bit error rate a channel code is used on layer 1. The encoder splits the full message, including header and CRC, into blocks with a size of 12 bit and adds 4 bit of redundancy to be able to detect and correct up to 1 bit error.

g)* Calculate the coderate of the encoder.

0 1

h) Calculate the number of channel words produced by the encoder for a message with maximum payload.

0 1

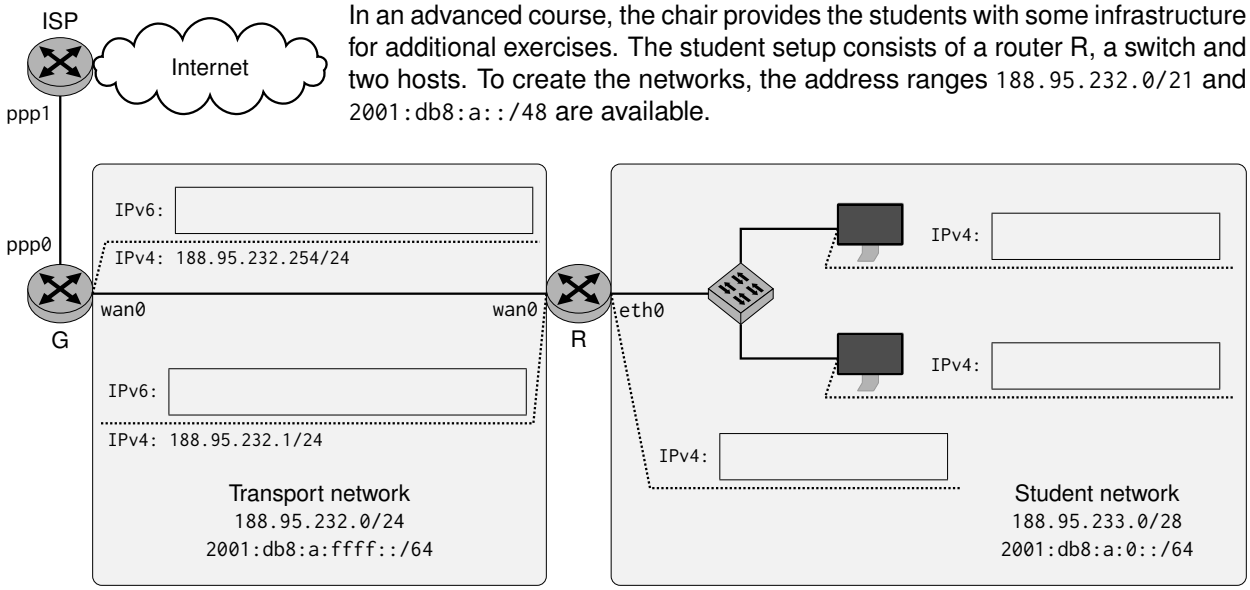
i) Calculate the probability that a single channel word can be correctly decoded at the receiver.
Give the result in percent with three decimal points.

0 1 2

j) Calculate the probability that a message of maximum length is transmitted successfully.
Give the result in percent with three decimal points.

0 1

Problem 3 IP Addressing (18.5 credits)



In an advanced course, the chair provides the students with some infrastructure for additional exercises. The student setup consists of a router R, a switch and two hosts. To create the networks, the address ranges `188.95.232.0/21` and `2001:db8:a::/48` are available.

0 1 a)* Assign valid IPv6 addresses to the router interfaces in the transport network.

0 1 b)* Assign valid IPv4 addresses to all interfaces in the student subnet. Assign `R.eth0` the highest address.

0 1 c)* Calculate the number of usable host addresses in the IPv4 student network.

0 1 The student setup should be replicated to facilitate parallel access for multiple students.

0 1 d)* Calculate the number of IPv4 addresses that are available for all student setups. Mind the `/24` network that is used as transport network and not available for student setups.

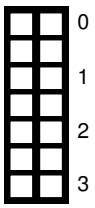
0 1 e) Calculate the total number of student setups that can be created with the available IPv4 addresses.

The resulting number of student setups is too little for the expected number of participating students. There is the option to additionally use the IPv4 network `188.95.224.0/21` to double the number of available addresses.

0 1 2 f) Is it possible to merge the new address range with the IPv4 address range already in use to get a `/20` network? Argue why it is or why it is not possible!

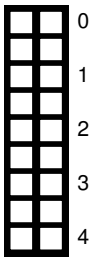
Currently, routers G and R are not fully configured. The Internet can be reached through the ISP router that is connected with router G. When everything is correctly set up, it should be possible to communicate between the student network, the transport network, the uplink between routers G and ISP, and the Internet. The ISP router has the IP addresses `131.159.35.254` and `2001:db8:4434::1/64`.

g)* Write down all necessary entries of the **IPv4** routing table of **router R**.



Destination	Next Hop	Iface

h)* Write down all necessary entries of the **IPv6** routing table of **router G**.



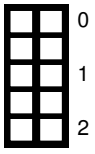
Destination	Next Hop	Iface

The used address ranges are all part of an *Autonomous System* that is controlled by the chair.

i)* Define what an autonomous system is.



j)* Differentiate the application area of Interior and Exterior Gateway Protocols.



Problem 4 **Hexagonal Wireshark (15 credits)**

While setting up your home network you discover a packet with your packet tracer Wireshark that you did not encounter before. You decide to take a closer look at the frame shown in Figure 4.1.

```
0x0000  33 33 ff c8 40 ac 46 d6   21 ee 37 0b 86 dd 60 00
0x0010  00 00 00 20 3a ff fe 80   00 00 00 00 00 00 16 16
0x0020  3d ff fe 15 f5 6b ff 02   00 00 00 00 00 00 00 00
0x0030  00 01 ff c8 40 ac 87 00   ca ff 00 00 00 00 fe 80
0x0040  00 00 00 00 00 00 00 c2   9a 4e 48 c8 40 ac 01 01
                        (x) Example
0x0050  46 d6 21 ee  37 0b
```

Figure 4.1: Ethernet frame (without FCS)

Please note: Most of the following subproblems require you to locate a header field from the hexdump. If that is the case, you MUST mark relevant parts of the hexdump – ensure that the markings are clearly associated with the subtask (see the example marking *(x)*). 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 source MAC address?

Address:

0 1 b)* What is the destination MAC address?

Address:

0 1 c)* Which network layer protocol is used?

Protocol: Reasoning:

0 1 d) What is the source IP address?

Address:

0 1 e) What is the destination IP address?

Address:

0 1 f) The destination IP address is a specific type of address. Name the type and explain how it is created.

g) What protocol is the payload of the IP packet?

0 1

Protocol:	Reasoning:

h) Inspect the payload of the IP packet and name the specific type of the message. Use relevant information from the header to justify your answer!

0 1

i) Explain the purpose of the message and when such a message is typically sent.

0 1 2

Some time later you find a different set of packets that are similar to each other. The following hexdump contains only the layer 4 header and payload of one of these packets. The layer 4 protocol is UDP.

```
0x0000  8c e7 00 35 00 28 67 f2    14 16 01 00 00 01 00 00
0x0010  00 00 00 00 04 6d 61 69    6c 06 70 72 6f 74 6f 6e
0x0020  02 6d 65 00 00 1c 00 01
```

Figure 4.2: Layer 4 header and payload

j)* Which **application layer protocol** most likely generated this message? Remember to name and mark respective fields.

0 1

Protocol:	Reasoning:

k) Determine the layer 4 payload length of this message.

0 1

Payload Length:	Reasoning:

Problem 5 DNS (15 credits)

You are a student assistant at the chair and have been given the task to configure a new teaching setup by setting up the DNS server for `grnvs.net.`. Relevant servers and their domain names and IP addresses are shown in Figure 5.1.
Fill in the following template so that the requirements of the individual subtasks are fulfilled. Enter the letter of the corresponding subtask in the box at the end of each line.

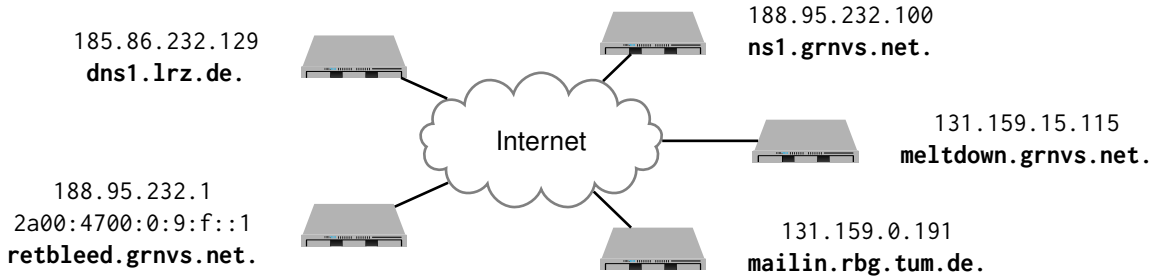


Figure 5.1: Servers relevant for the zone `grnvs.net.` with domain names and IP addresses

```
grnvs.net.          600  IN     SOA       ns1.grnvs.net.   lnt.grnvs.net.   010426
                                          3600 900 604800 900

$ORIGIN grnvs.net.

grnvs.net.                     NS        ns1.grnvs.net.

ns1.grnvs.net.                 A         188.95.232.100
```

0 1 a)

0 1 b)

0 1 c)

0 1 2 d)

0 1 e)

0 1 f)

a)* Configure `dns1.lrz.de` as an independent second nameserver for the zone.

b)* The server `meltdown.grnvs.net` should be reachable under its IPv4 address.

c)* All mail traffic for `grnvs.net` is handled by the email server `mailin.rbg.tum.de` with priority 15.

d)* The server `retbleed.grnvs.net` should be reachable under its IPv4 and IPv6 address.

e)* The domain `testbed.grnvs.net` should act as alias to `retbleed.grnvs.net`.

f)* Lastly, there should be a text record set for the `meltdown` server that contains the text `vlan=1099`.

Do not forget to reference the subproblem by its letter in the last box of each row!

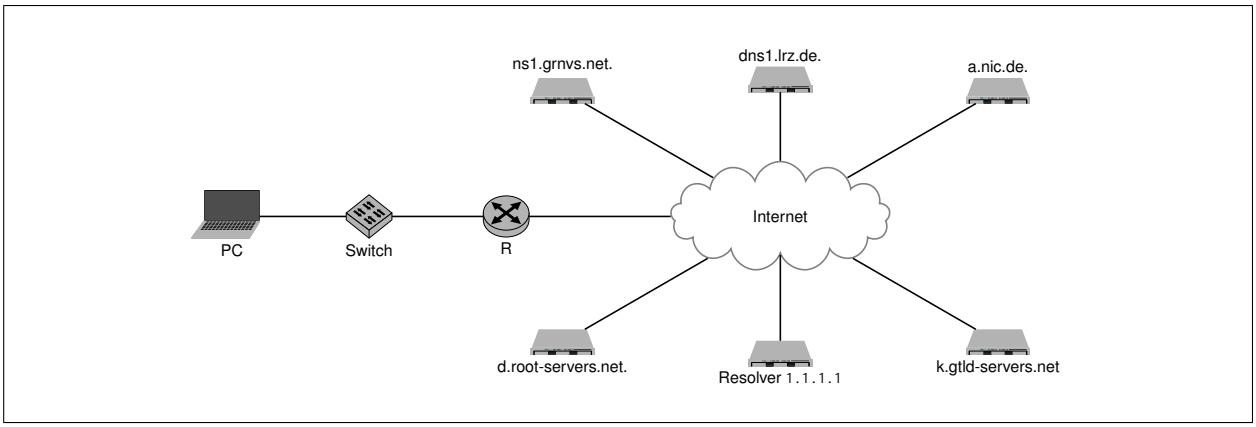
Now you test the setup by performing a lookup of the A record of the domain name `retbleed.grnvs.net` from your PC. Your PC uses the router R as resolver, which in turn uses the public resolver `1.1.1.1`. Assume that all resolver caches are empty. Table 5.1 shows relevant zones and their authoritative nameservers.

Zone	**Authoritative Name Server**
`.`	`d.root-servers.net.`
`com.`, `net.`	`k.gtld-servers.net.`
`de.`	`a.nic.de.`
`lrz.de.`	`dns1.lrz.de.`
`grnvs.net.`	`ns1.grnvs.net.` and `dns1.lrz.de.`

Table 5.1: Zones with corresponding authoritative name servers

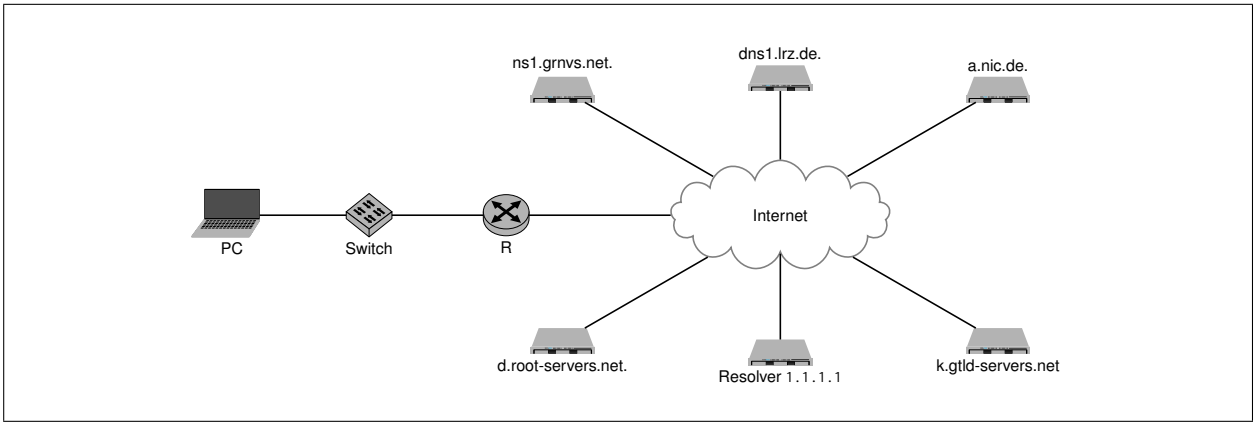
g) Draw the recursive part of the query (both request and response) in the figure using arrows.
Enumerate the individual messages (1, 2, 3, ...)!

0 1 2



h) Draw the iterative part of the query (both request and response) in the figure using arrows.
Enumerate the individual messages (1, 2, 3, ...)!

0 1 2 3



i)* Use the scenario with the primary and secondary nameserver of `grnvs.net.` to explain what a GLUE record is, when it is used and why it is necessary.

0 1 2 3

Problem 6 Websecurity (6.5 credits)

You are accessing the URL `http://tum.de`. The webserver responds with the following HTTP response:

```
HTTP/1.1 302 Found
Date: Wed, 01 Apr 2026 13:59:59 GMT
Server: Apache/2
Location: https://tum.de/
Content-Length: 239
Content-Type: text/html; charset=iso-8859-1
```

0 1 2

a)* Name three security goals that HTTPS guarantees compared to HTTP and briefly explain one of them.

0 1

b)* Given the status code, explain the purpose of the `Location` header in the response.

0 1

c)* Explain how an attacker can obtain sensitive information from an HTTP connection using an example.

After trying to access the URL, your browser displays a warning, that the connection is not secure because the certificate is self-signed. Conventionally, certificates are obtained from a trusted Certificate Authority (CA) but any entity can generate self-signed certificates.

0 1 2

d)* Explain why self-signed certificates cannot be used for secure HTTPS communication.

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