Chair of Distributed Systems and Security
Scholl 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 22nd February, 2024
Examiner:	Prof. Dr.-Ing. Stephan Günther, Leander Seidlitz M.Sc.	**Time:**	10:00 – 11:30

Working instructions

- This exam consists of **16 pages** with a total of **6 problems**.
  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 (15 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 are security goals according to the lecture?

- ☐ Useability
- ☐ Performance
- ☐ Controlled Access
- ☐ Routeability
- ☐ Deployability
- ☐ Data Integrity
- ☐ Volatility
- ☐ Authenticity
- ☐ Advertisability
- ☐ Agility
- ☐ Confidentiality
- ☐ Sustainability

b)* IPv4 addresses are 4 bytes long. How long is an IPv6 address?

- ☐ 16 bytes
- ☐ 6 bytes
- ☐ 128 bytes
- ☐ 8 bytes

c)* As of today, which of the following cryptographic hash functions are considered secure?

- ☐ MD4
- ☐ SHA-1
- ☐ MD5
- ☐ MD2
- ☐ BLAKE2
- ☐ SHA-2

d)* IPsec is . . .

- ☐ policy based
- ☐ only available for IPv4
- ☐ a layer 4 protocol
- ☐ insecure since the protocol was broken in 2009

e)* Which is the correct definition of **forward secrecy**?

- ☐ A cryptography scheme provides Perfect Forward Secrecy (PFS) if **future** encrypted sessions maintains their confidentiality in the scenario that the long-term secret, the current session keys and all sessions traffic become known to an attacker.
- ☐ A cryptography scheme provides Perfect Forward Secrecy (PFS) if **previously** encrypted sessions maintains their confidentiality in the scenario that the long-term secret, the current session keys and all sessions traffic become known to an attacker.

f)* Which of the following is an AEAD cipher?

- ☐ AES-CBC
- ☐ AES-CTR
- ☐ AES-GCM
- ☐ AES-ECB

g)* Which factors influence the sender window of TCP?

- ☐ Timeouts
- ☐ Max. data rate on Layer 1
- ☐ Acknowledgements
- ☐ RTT
- ☐ Receive window
- ☐ Number of hops

h)* You observe the UDP datagram whose header is shown in Figure 1.1. Which service is likely being addressed?

```
0x0000    d0  2c  00  35
0x0004    00  26  a9  86
```

Figure 1.1: Hexdump of the UDP header

☐ DHCP ☐ FTP ☐ HTTP ☐ DNS ☐ SSH ☐ HTTPS

i)* What is the FQDN of the PTR record for the IP address 203.0.113.42?

☐ 24.311.0.302.in-addr-arpa. ☐ 302.0.311.21.in-addr.arpa.

☐ 42.113.0.203.in-addr.arpa. ☐ 203.0.113.42.in-addr-arpa.

j)* Which of the following is an exterior gateway protocol?

☐ EIGRP ☐ BGP ☐ RIP ☐ OSPF ☐ IGRP

k)* How many L2 address types does 802.11 (WLAN) know? (Hint: source, destination, . . .)

☐ 3 ☐ 4 ☐ 7 ☐ 2 ☐ 5

l)* What is CRC used for in Ethernet?

☐ Error Forwarding ☐ Error Detection ☐ Error Correction ☐ Error Propagation

m)* What does QAM modulate?

☐ Density of the signal ☐ Phase of the signal

☐ Amplitude of the signal ☐ Speed of the signal

Problem 2 Code Demos — Chat Application with UDP / TCP (14.5 credits)

In the lecture we have written several versions of a small chat application that either uses UDP or TCP as transport layer protocol. First, we consider the original UDP chat that was intended for a 1:1 communication between two clients. In particular, this version was identical on both sides, i. e., there was no server involved.

0 1

a)* On your local computer, you were able to run the client by starting it two times with the following command lines:

- `udpchat.py 6112 127.0.0.1 6113`
- `udpchat.py 6113 127.0.0.1 6112`

Briefly explain the three arguments supplied to the application.

0 1 2

b) We have rewritten the `udpchat.py` in the lecture to act as a relay chat server that could be started as `udpchat_server.py 6112`. Explain why this single argument is sufficient in that case.

0 1 2

c) Argue whether or not clients need to specify a source port when communicating with the `udpchat_server`.

0 1 2

d)* How many sockets do `udpchat` and `udpchat_server` need, respectively? Give a reason for your answer.

After implementing the `udpchat_server`, we rewrote the application again to use TCP instead of UDP as transport protocol.

e) Did anything change regarding the arguments supplied to `tcpchat_server.py`?

0
1

f)* Argue how many sockets the server now needs to handle *N* clients?

0
1
2

g)* Name two **advantages** of the TCP variant compared to the UDP server. (Without reason)

0
1
2

h)* Name two **disadvantages** of the TCP variant compared to the UDP server. (Without reason)

0
1
2

Problem 3 Wireshark (16 credits)

We consider the network topology depicted in Figure 3.1. The PC tries to establish an SSH connection via IPv4 to the server SRV. The MAC and IP addresses of the devices' interfaces are given. **Assume that IP addresses are statically configured and the PC has not yet contacted its router since reboot.**

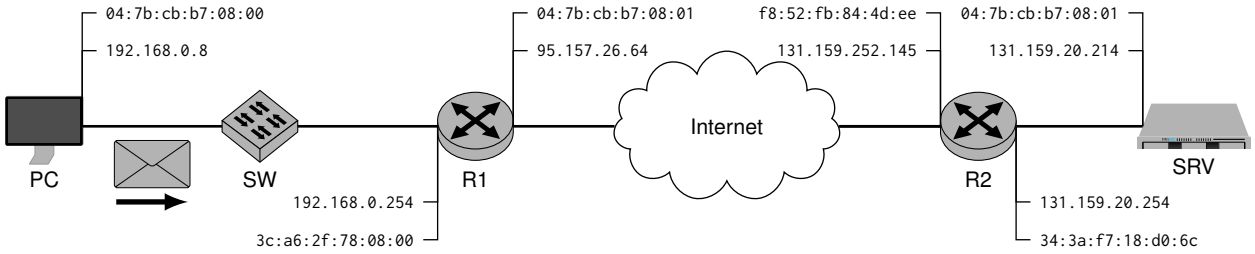


Figure 3.1: Network topology

We consider the frame sent from PC towards SW as depicted in Figure 3.1.

In the following we want to derive the **hexdump of that frame** based on the information given in Figure 3.1 and the following subproblems. Fill in the contents step by step in Figure 3.2. As an example, the L2 receiver address is already filled in as answer to some (not existing) Subproblem x).

Note: the cheat sheet handed out together with this exam contains everything you need.

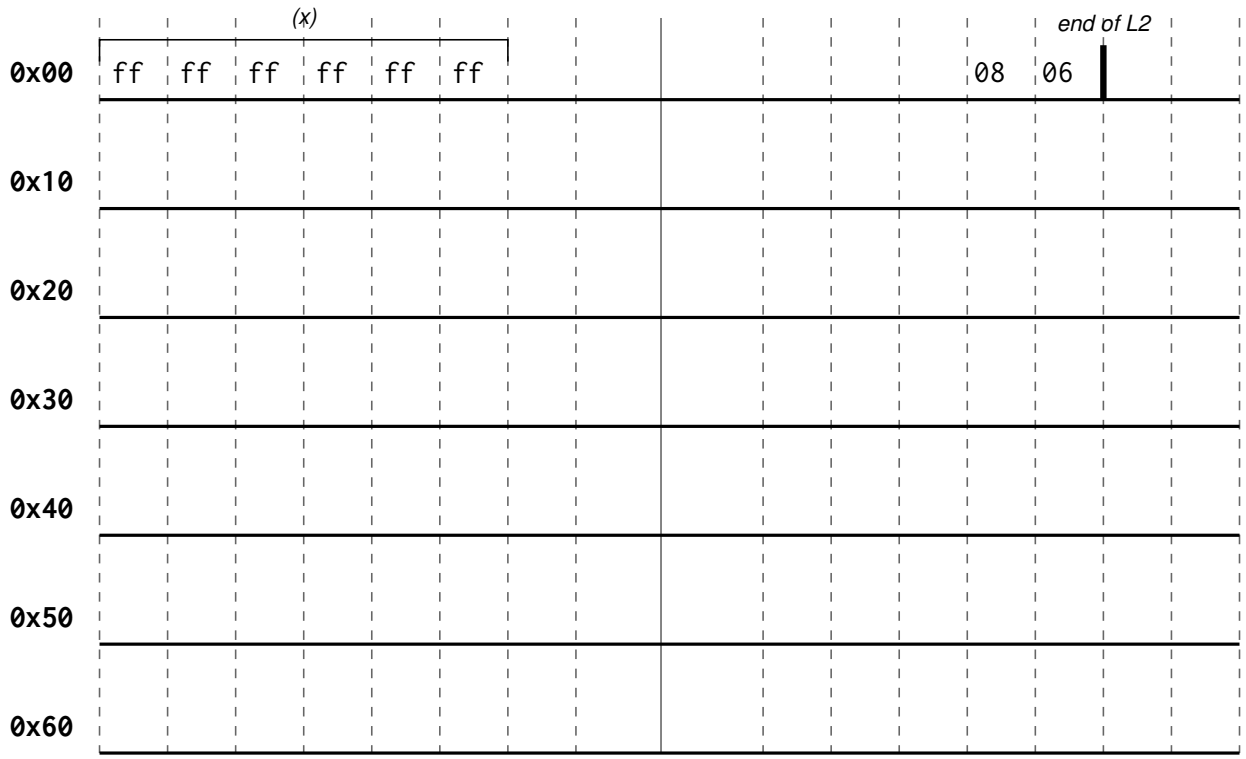


Figure 3.2: Preprint for the frame's hexdump

0 1

a) Who is (in general) being addressed by the given receiver address?

0 1

b)* Fill in the transmitter address of layer 2 in Figure 3.2.

c)* What is the type of the L2 SDU?

0 1

d) What is the purpose of this frame?

0 1

Before we continue to fill in the hexdump, we want to mark the end of the L2 payload and the end of the frame.

e)* Mark **the end** of the **L2** payload as well as of the **frame itself** in Figure 3.2. As an example, the end of the L2 header is already marked.

0 1 2

f) Fill in the frame check sequence given as `42 0a f1 73` in Figure 3.2.

After having figured out the type of the L2 payload, it should be straight-forward now to fill in the complete frame. You do not need to name the fields – just fill it in with hex digits. If IP addresses should occur, you do not need to convert them to hex – just fill it in Byte by Byte.

0 1

g) Fill in the frame's payload.

0 1 2 3 4 5 6 7 8

h) Assuming IPv6 had been used instead of IPv4. To which protocol would this frame belong to in that case?

0 1

Problem 4 Line codes (12 credits)

In this problem we want to compare the four line codes NRZ, RZ, Manchester, and MLT-3 by means of the example bit sequence `0000 1101`. Figure 6.2 gives you a template for all four different signals. You find another pre-print at the end of the exam if necessary. **Make sure to strike-out solutions that should not be graded.**

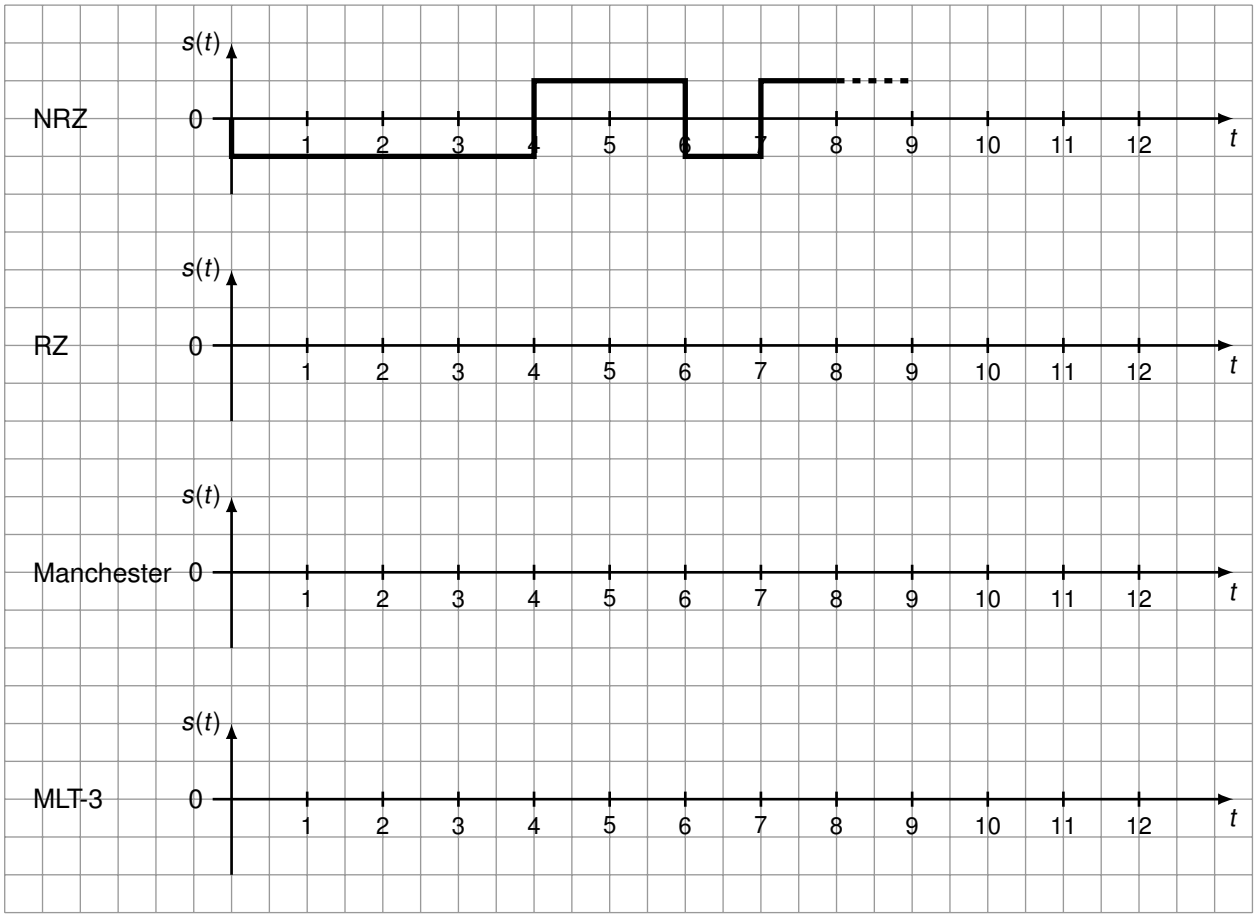


Figure 4.1: Preprint for signals

0 1 2

As an example we show the resulting signal for NRZ in Figure 6.2. Please use positive values (or turns from lower to higher voltages) to indicate a logical `1`, and vice versa for a logical `0`. Use $s(t) = 0$ as start value.

0 1 2

a)* Draw the signal for RZ in Figure 6.2.

b)* Draw the signal for Manchester in Figure 6.2.

c)* Draw the signal for MLT-3 in Figure 6.2.

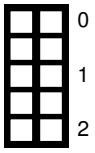
0 1 2

d) Compare NRZ to RZ and Manchester. Reason which of the signals requires the most bandwidth.

0 1 2

e) Reason which of the four line codes allow(s) for clock recovery / automatic synchronization?

f) Name an approach that can be used to allow for clock recovery even if the underlying line code does not support it on its own.



Problem 5 Dynamic Routing (19 credits)

We consider the network shown in Figure 5.1. The routers are using RIP as dynamic routing protocol. The tables next to the routers represent the (simplified) routing table of the respective router containing the destination **Dst**, next hop **NH**, and the costs.

Dst	NH	Cost
B	B	0
C		
D		
E		

Dst	NH	Cost
A	A	0
C		
D		
E		

Dst	NH	Cost
A	A	0
B		
D		
E		

Dst	NH	Cost
A		
B		
C		
E		

Dst	NH	Cost
A		
B		
C		
D		

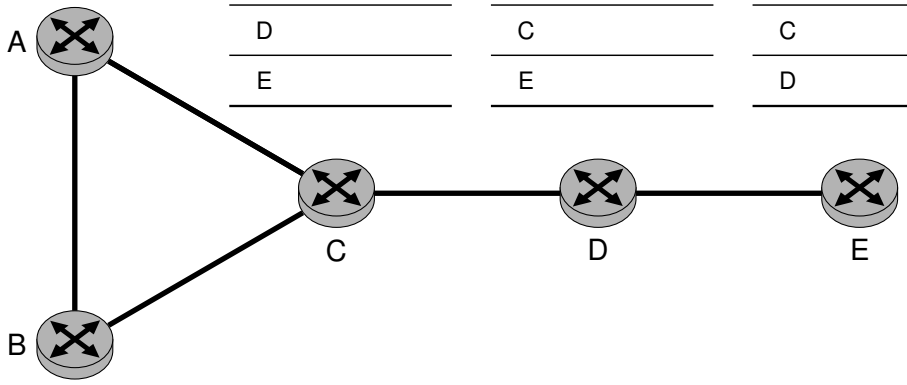


Figure 5.1: Topology and initial routing tables at boot time

0 1

a)* Which metric is used by RIP? (Without reason)

0 1 2

b)* RIP is a distance vector protocol. Explain the difference to link state protocols.

0 1 2

c)* RIP is an interior gateway protocol. Explain the difference to exterior gateway protocols.

0 1

d)* To what extent are networks limited that use solely RIP as routing protocol?

e)* Which information is contained in a routing update sent by RIP?

0 1

f)* Reason whether or not RIP always chooses the shortest path in based on the hop count.

0 1

g)* Reason whether or not RIP always chooses the fastest route in terms of bandwidth.

0 1

h) Fill in the routing tables in Figure 5.1 (without intermediate steps) such that the tables represent a converged state.

0 1 2 3

Assume the link between routers D and E fails. Router D obviously recognizes the fail. Answer the following questions in the given order.

i) Router D sends a periodic update. Describe its immediate effect on the other routers.

0 1 2

j) Now, router A sends a periodic update. Describe its immediate effect on the other routers.

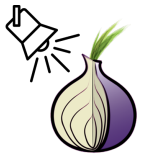
0 1 2 3

k) Describe the problem that will now arise and how it can be solved.

0 1 2

Problem 6 DNS (13.5 credits)

You are the administrator of the notorious darknet site “The Visible Wiki”, which hosts a collection of darknet links. Recently, all your servers were seized by dollarpol. You could barely escape the authorities, and are now in the process of rebuilding the site. As a first step, you set up a new nameserver at `dns.visiblewiki.what`. You start by writing a zone file.



visiblewiki’s logo

0 1 2 3 4 5 6 7

a)* You start with the basics of a DNS zone file. In the zone file below (Listing 1), add entries fulfilling the following tasks. **Do not use any record type twice!**

1. A record `visiblewiki.what.` referencing `131.159.122.12`
2. Make the website at `www.visiblewiki.what.` reachable. It is hosted on the server at `131.159.122.12`
3. Mail for `visiblewiki.what.` is also handled by the server at `visiblewiki.what.` with priority `1`.

```
$TTL            14400
$ORIGIN         visiblewiki.what.

visiblewiki.what.       IN SOA  dns.visiblewiki.what.  visiblewiki.what. (
                        2024022501      ; serial YYYYMMDDxx
                        7200            ; refresh = 4 hrs
                        1800            ; retry   = 30 min
                        604800          ; expire  = 7 days
                        3600            ; neg cache time = 1 hr
                )

;The CLASS of a record is set to IN (for Internet) for common DNS records
;involving Internet host names, servers, or IP addresses.

visiblewiki.what.       IN NS           dns.visiblewiki.what.
dns.visiblewiki.what.   IN A            131.159.122.1



_____________________   IN _____        ________________________________

_____________________   IN _____        ________________________________

_____________________   IN _____ ____   ________________________________
```

Listing 1: Zone file for `visiblewiki.what`

As you know, the DNS follows a tree structure. Your domain is part of the `what` TLD. The zone file of `what.` therefore has to reference your name server. It contains the following entries:

```
[...]

visiblewiki.what.       IN NS           dns.visiblewiki.what.
dns.visiblewiki.what.   IN  A           131.159.122.1

[...]
```

Listing 2: Part of the `what` TLD zone file

b)* Why are the entries of Listing 2 necessary? Explain the purpose of the A record of Listing 2.

0 1 2

c)* At this point, you are concerned about the resolvers that query your name server. Describe how a resolver differs from a name server and how it interacts with name servers.

0 1 2

d)* As an operator of “The Visible Wiki” you are naturally afraid of the authorities. Can a client querying the DNS trust the resolver’s response to be the actual contents of your zone file? Justify your answer!

0 1 2

Additional pre-print for Problem 4:

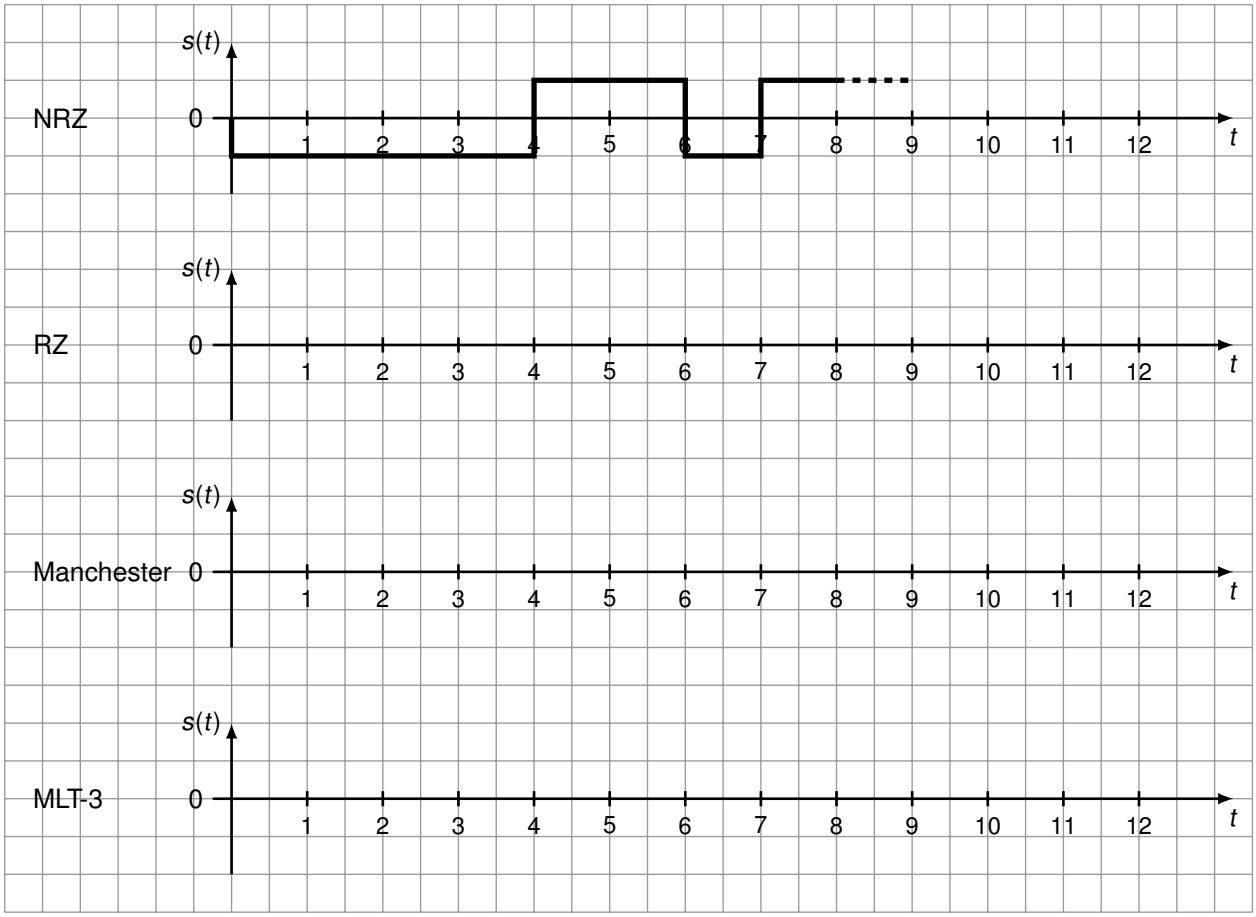


Figure 6.2: Preprint for signals

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