Chair of Distributed Systems and Security
Department of Computer Engineering
Technical University of Munich

E0051
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:**	Wednesday 19th February, 2025
Examiner:	Prof. Dr.-Ing. Stephan Günther Prof. Dr.-Ing. Georg Carle	**Time:**	14:00 – 15:30

Sample Solution

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 (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 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.

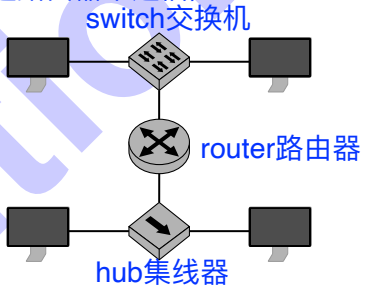
Mark correct answers with a cross ☒
To undo a cross, completely fill out the answer option ■
To re-mark an option, use a human-readable marking ×■

a)* The internet is based on the . . .

☐ DARPANET. ☒ ARPANET. ☐ Usenet. ☐ CIVILNET.

只有路由器 Router能隔离广播域（也就是说，不同的广播域之间必须经过路由器来通信）

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



☐ 4 ☐ 6 ☐ 5 ☐ 1 ☐ 3 ☒ 2

网络中哪些位置是“可能发生冲突的独立区域

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

Hub 后面无论连几台主机都是同一个冲突域

☐ 6 ☐ 5 ☒ 4 ☐ 3 ☐ 2 ☐ 1

d)* Which of the following statements about hubs and switches are correct?

☒ Switches operate at Layer 2 and makes forwarding decisions based on Destination MAC addresses.

根据目标的mac地址转发

☐ Switches operate at Layer 2 and makes forwarding decisions based on Source MAC addresses.

☒ Both hubs and switches are transparent devices that do not modify the frame contents during transmission.

不修改信号内容只管转发

☐ Switches operate at Layer 1 and simply regenerate electrical signals without processing frame information.

/24 表示 IP 地址的前 24 位是网络位，剩下 8 位是主机位

e)* Consider an IPv4 network with an address range 192.168.1.0/24 is divided into four subnets of size (/26). Which statements are true about these subnets?

因为 4 = 2²，所以你要把原来主机位的 8 位里，再拿出 2 位来做子网编号,主机位就变成了6,每个子网ip数变成2的次方

☒ Each subnet has 62 usable addresses.

再减去网络地址和传播地址 剩下了62

☐ The first usable IP address in the third subnet is 192.168.1.128.

☐ The subnet mask for each subnet is 255.255.255.224.

计算子网掩码: 比如前缀是24 32位的地址 前24个是1后面是0 8个一组 换成10进制

☒ The broadcast address for the second subnet is 192.168.1.127.

网络地址和广播地址占头和尾,其他就是可用的

f)* Which IP header fields change while packets get routed from one endpoint to another (assuming no NAT or other protocol modifications)?

☐ IHL ☐ Protocol ☐ Fragment Offset ☐ Version

☐ Flow label ☒ TTL ☒ Header Checksum ☐ Destination IP Address

每经过一个路由器，就会减 1,0就丢失这个包 防止死循环

TTL改变了头部也改变 checksum也改变

最大传输单元

g)* In an IPv6 network, large packets must be fragmented to travel across links with an MTU of 1280 bytes. Which of the following statements are true?

IPv6 中，默认不允许路由器对数据包进行分片（这是跟 IPv4 最大的不同）

☐ IPv6 fragments can be further fragmented by routers.

所有的分片（fragmentation）都必须在发送端完成（由源设备负责）

☐ IPv6 fragments are reassembled at intermediate routers.

IPv4 和 IPv6 都一样，不会在中间的路由器进行重组,只会在最终主机集合

1表示后面还有片段,0表示这是最后一片

☒ The More Fragments (MF) flag in the Fragment Header indicates whether more fragments are to follow.

☒ IPv6 fragmentation is handled by the sending device, not intermediate routers.

Sample Solution

SLAAC（Stateless Address Autoconfiguration） 是 IPv6 的一种自动地址配置机制

h)* What privacy issues arise when SLAAC generates an IPv6 address based on the device's MAC address?

如果 MAC 地址不变 → IPv6 地址的后缀也不变,设备可以被识别出来

- ☐ The address can be spoofed by attackers.
- ☒ The generated IPv6 allows device tracking on the internet.
- ☒ It is possible to identify the network card manufacturer.
- ☐ SLAAC exposes the routing prefix of the ISP.

SLAAC 本身不直接增加被 spoof伪造的风险,伪造 IP 的能力与是否用 SLAAC 无关

路由前缀:在 IPv6 中，它通常由前 64 位组成,本来就是公开的

因为 IPv6 地址后缀用了 MAC，所以能通过 IP 推断设备来源

Internet Service Provider

i)* A network contains multiple DHCP servers. Which statements about DHCP broadcast behavior are correct?

Dynamic Host Configuration Protocol,给网络中设备自动分配 IP 地址的服务器

- ☐ Each client must request addresses from every responding server individually.
- ☒ DHCP Request broadcast simultaneously accepts one offer while notifying others of rejection.
- ☐ Using unicast during request would be more efficient as it reduces network traffic during server discovery.
- ☒ Initial broadcast enables receiving multiple offers from all the available DHCP servers.

DHCP 是广播发现（Discover),不需要挨个请求

DHCP 请求广播会同时接受一个服务器的提议，并通知其他服务器它们的提议被拒绝

客户端可能会收到 多个 Offer

unicast 单播 1对1通信 对应广播,请求阶段需要使用广播,首先客户端没有自己的ip,另外有多个服务器,不能单播

j)* A TCP connection is experiencing high packet loss due to random bit errors on an unreliable link (not congestion). Which of the following issues might arise?

因为链路质量差而发生严重丢包（注意：不是网络拥塞）

Flow control（流量控制）是 TCP 中的机制，用来确保接收方不会被发送方"发太快"而压垮

- ☐ Flow control mechanisms will prevent further data transmission until packet loss stops entirely.
- ☒ The congestion window will remain small due to frequent restarts of the slow start phase.
- ☒ TCP will incorrectly interpret packet loss as network congestion and reduce its transmission rate unnecessarily.
- ☐ TCP will automatically switch to UDP for faster retransmissions in such scenarios.

这个机制是为接收方限速 而不是congestion control

因为 TCP 一直以为"太挤了"，它不断触发"慢启动"，窗口始终无法扩大

TCP 永远不会自动切换成 UDP

TCP 看见丢包就以为"网络堵车"，实际上不是

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

请问它最有可能是在访问哪个服务

这俩表示原端口　这俩表示目标端口

看目标端口指向哪里

表示从第一行开始

```
0x0000  d0  2c  00  43
0x0040  00  26  a9  86
```

Figure 1.1: Hexdump of the UDP header.

- ☐ TFTP
- ☐ DHCP
- ☐ NTP
- ☒ BOOTP
- ☐ DNS
- ☐ HTTP

Sample Solution

Problem 2 Ethernet Physical Layer (17 credits)

In this problem we investigate two different implementations of the Ethernet Physical Layer. For now, we consider the somewhat outdated 10BASE-2. As line code the Manchester Code is being used. There is no additional channel coding. Consider the 10BASE-2 signal shown in Figure 2.1.

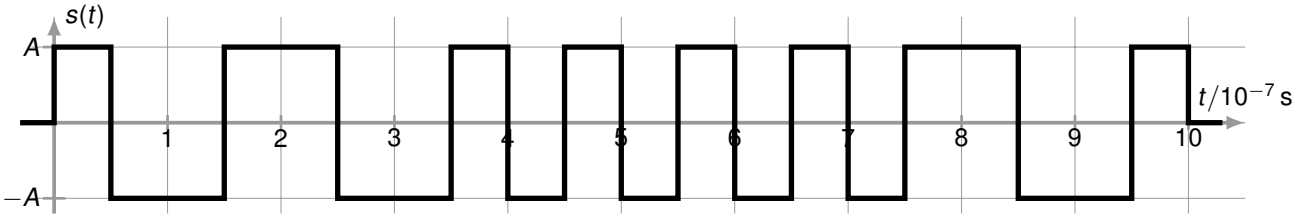


Figure 2.1: Idealized 10BASE-2 signal

0 1

a)* Is the signal time continuous or time discrete (no reasoning required)?

Time continuous 信号在任意时间点都有定义，是模拟波形的那种感觉,所以是连续的

0 1 2

b)* Determine the bit sequence transmitted in the time interval $t \in [0\,\mu s, 1\,\mu s)$.
Hint: There exist two valid solutions, stating one is sufficient.

According to IEEE 802.3: `01 01 11 11 01` 只看一个周期的开始和结束 从高到低就是0 低到高就是1
Alternative: `10 10 00 00 10`

要“串行发送一个比特”(把一个比特转换成电信号发出去)需要多长时间?

0 1

c)* How long does it take to serialize a single bit?

你要从图中找到每位所占的时间段，直接读出来

From Figure 2.1: $T = 1 \cdot 10^{-7}\,s = 0.1\,\mu s$

0 1

d)* Determine the data rate achievable by 10BASE-2 (calculation or reasoning).

bps bit per second

$$r = \frac{1\,\text{bit}}{T} = 10\,\text{Mbit/s}$$

0 1 2

e) Determine the neccessary spectral bandwith according to Hartley such that the data rate from Subproblem d) can be achieved by a binary line code.

M = 信号中可用的不同电平数量（符号数），这里的数量是2,因为是binary line code.

$$r = 2B \cdot \log_2(M)\,\text{bit} \quad \Leftrightarrow \quad B = \frac{r}{2\log_2(M)\,\text{bit}} = 5\,\text{MHz}$$

0 1

f) Reason why 10BASE-2 occupies at least a bandwidth of $B' = 10\,\text{MHz}$.

每秒传输的比特数

A bit is represented by two changes in signal with the Manchester Code. Therefore, the baud rate is doubled compared to e. g. NRZ and thus the required bandwidth also doubles.

Sample Solution

g) Reason which **other, binary** line code a higher data rate could be achieved at the same required bandwidth. 每一个符号就是一个比特

0 1

NRZ because here the baud rate corresponds to the bit rate.

h) Which significant advantage does the Manchester Code offer?

0 1

Clock recovery (and DC-freeness)

原始数据 → 4B5B 编码 → MLT-3 编码 → 信号上线

Now we consider the newer 100BASE-TX stadard, which uses MLT-3 with 4B5B coding as line code. The effective data rate is 100 Mbit/s. Figure 2.2 shows an idealized signal of a single cable core, which represents the first 4 bit of the message `0101 111101`. MLT3 遇到1就改变0就不动

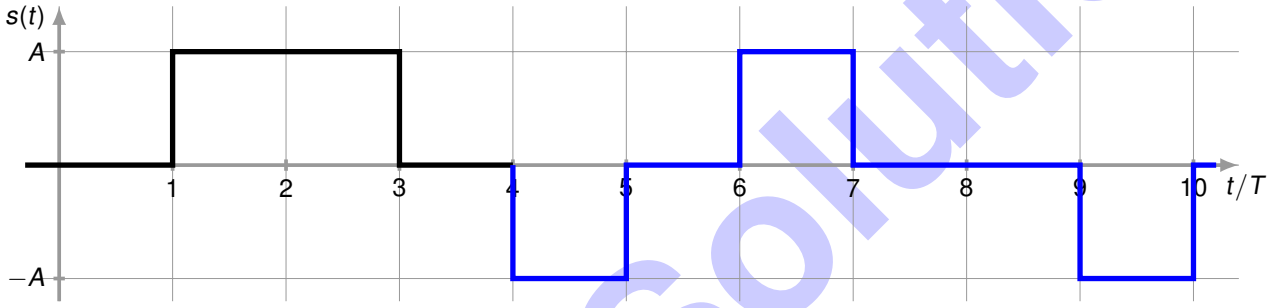


Figure 2.2: Idealized MLT-3 signals

i)* Complete the signal in Figure 2.2 such that it represents the remaining 6 bit.

0 1 2

j) Explain whether problems occur when using MLT-3 coding when recognizing long zero or one sequences.

0 1 2

Long sequences of zeros result in a constant signal.Since clock recovery is not automatically given, it is a problem.

k)* Name two advantages of 4B5B encoding.

0 1 2

Limiting the maximum length of zero sequences
Offers additional control characters

l)* How high must the bit rate actually be for 100BASE-TX in order to achieve an effective transmission speed of 100 Mbit/s?
Hint: This is only about the bit rate from the point of view of the physical layer. You therefore do not need to consider the overhead caused by protocol headers!

0 1

这是因为4B5B的编码造成的 4个要变成5个 所以要成四分之五

$$r_{\text{brutto}} = \frac{r_{\text{netto}}}{R} = 100\,\text{Mbit/s} \cdot \frac{5}{4} = 125\,\text{Mbit/s}$$

Sample Solution

Problem 3 NAT and Routing (18 credits)

Given the network topology shown in Figure 3.1. PC1 and PC2 are connected via the Access Point AP (IEEE 802.11) to the Router R1, which offers access to the Internet.

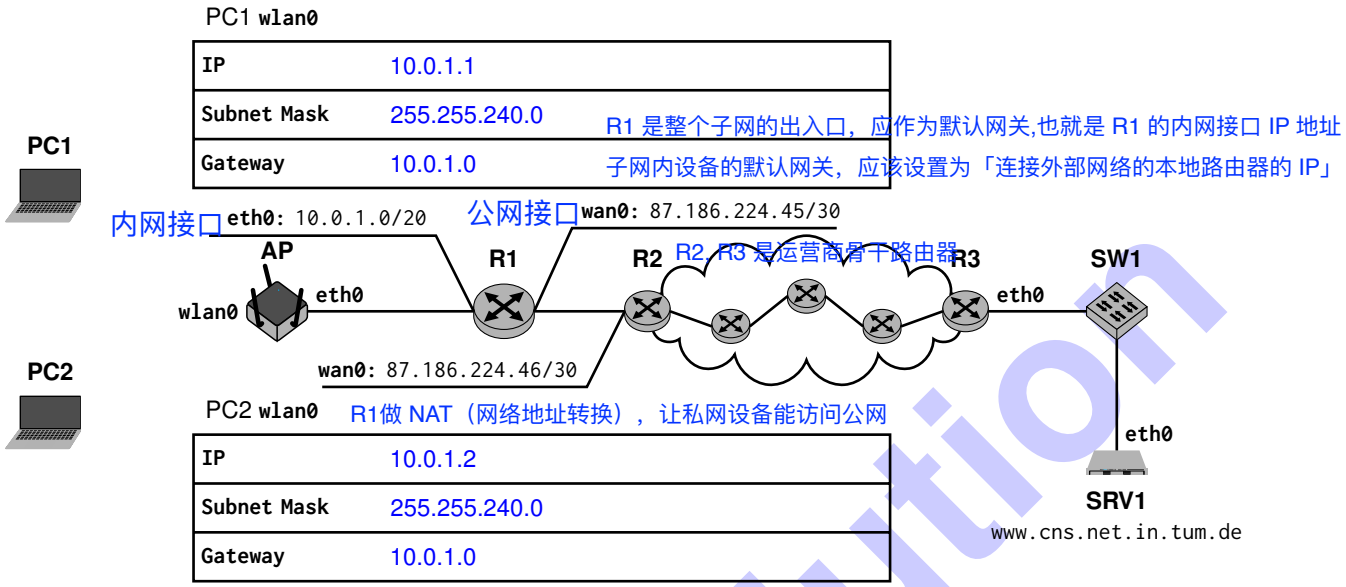


Figure 3.1: Network topology

0 1 a)* Reason wether or not the address `10.0.1.0` is useable for the given prefix. If not, assign R1 another useable address in the same subnet.

10.0.1.0 is useable in 10.0.0.0/20 because it is neither the first nor the last address.

0 1 b)* Determine the network and broadcast addresses of the subnet in which PC1, PC2, and R1 are located.

Network address 10.0.0.0
Broadcast address 10.0.15.255

子网内的任意一个ip地址和子网mask做and运算都可以计算出网络地址
把网络地址的后主机位（后 12 位）全填 1 → 就是广播地址

0 1 c) How many addresses are available to address devices in this network? Give the calculation.

The first and last address are not useable, thus:

$$2^{32-20} - 2 = 4094$$

0 1 2 d) Assign a sensible IP address, subnet mask, and gateway address to PC1 and PC2 respectively, so that they can establish a connection to the Internet. Enter the values directly in Figure 3.1. Take note of a possibly different IP of R1 from Task a).

e)* How many /20 subnets are there in the network 10.0.0.0/8? Also provide the calculation method!

0 1

$$2^{20-8} = 4096$$

Sample Solution

f)* Reason why R1 must support NAT such that PC1 and PC2 can access the internet.

0 1

PC1 and PC2 are located in a private network. Their IP addresses are not global routable.

g)* Which minimal information must R1 store in its NAT table?

0 1

Local IP of hosts, local source port, and translated (global) source port.
(The global IP of R1 is not neccessary since R1 has only one global IP.)

In the following we abbreviate IP and MAC addresses as follows: `<device name>` or `<device name>.<interface>` if the interface is not unique, e g. `PC1` or `R1.wan0`. **Note that for the following subproblems additional routers are locate between R2 and R3.**
PC1 now accesses the website `https://www.cns.net.in.tum.de`.

h)* Add for the first packet being transmitted from PC1 to `www.cns.net.in.tum.de` the header fields in the three empty boxes of Figure 3.2. If a field is not uniquely defined, choose a meaningful one.

0 1 2 3 4 5

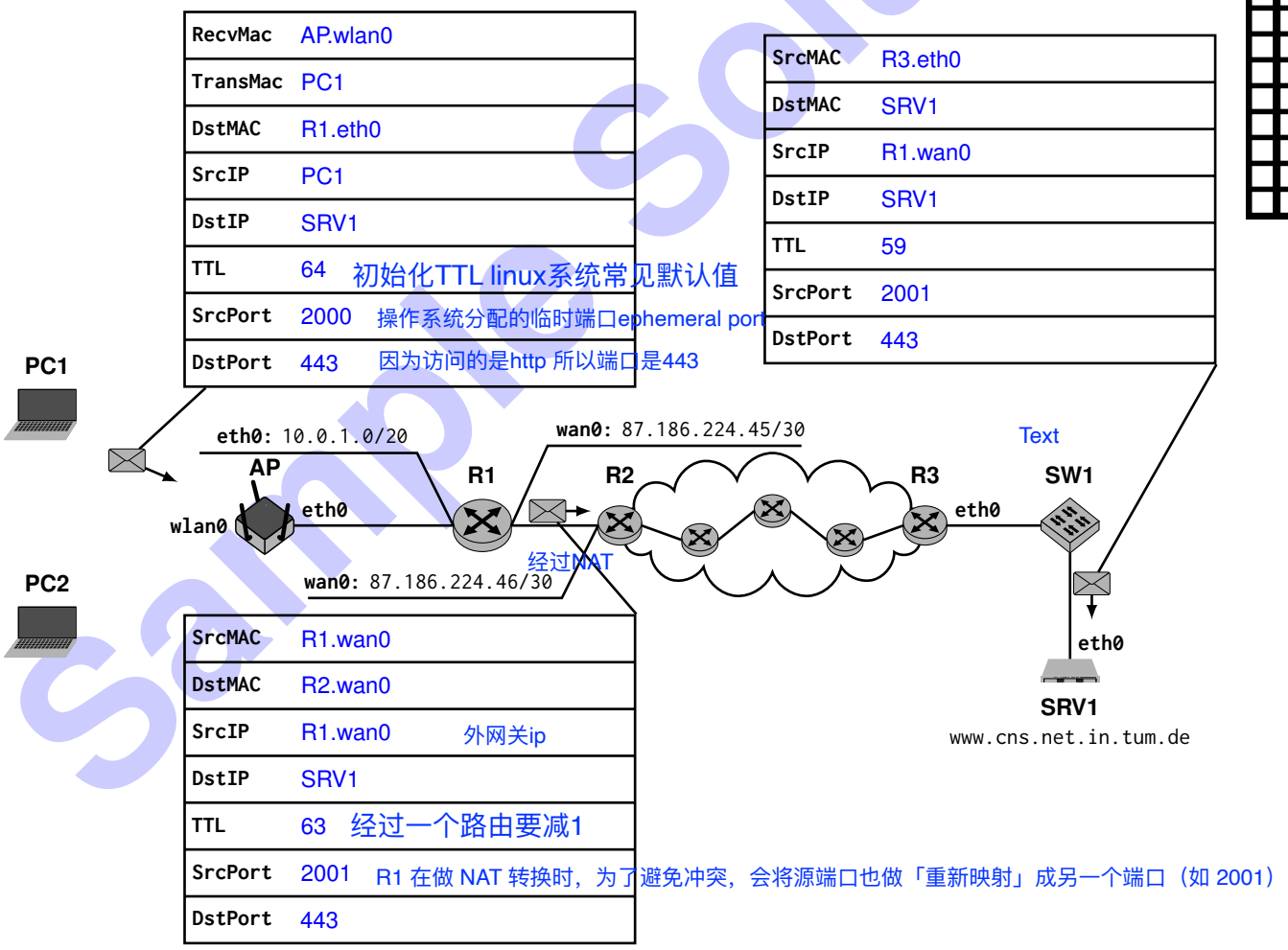


Figure 3.2: Netztopologie

Sample Solution

0
1
2
3
4
5

i) Add the header fields for the answer from [www.cns.net.in.tum.de to PC1 the header fields in the three empty boxes of Figure 3.3. If a field is not uniquely defined, choose a meaningful one.

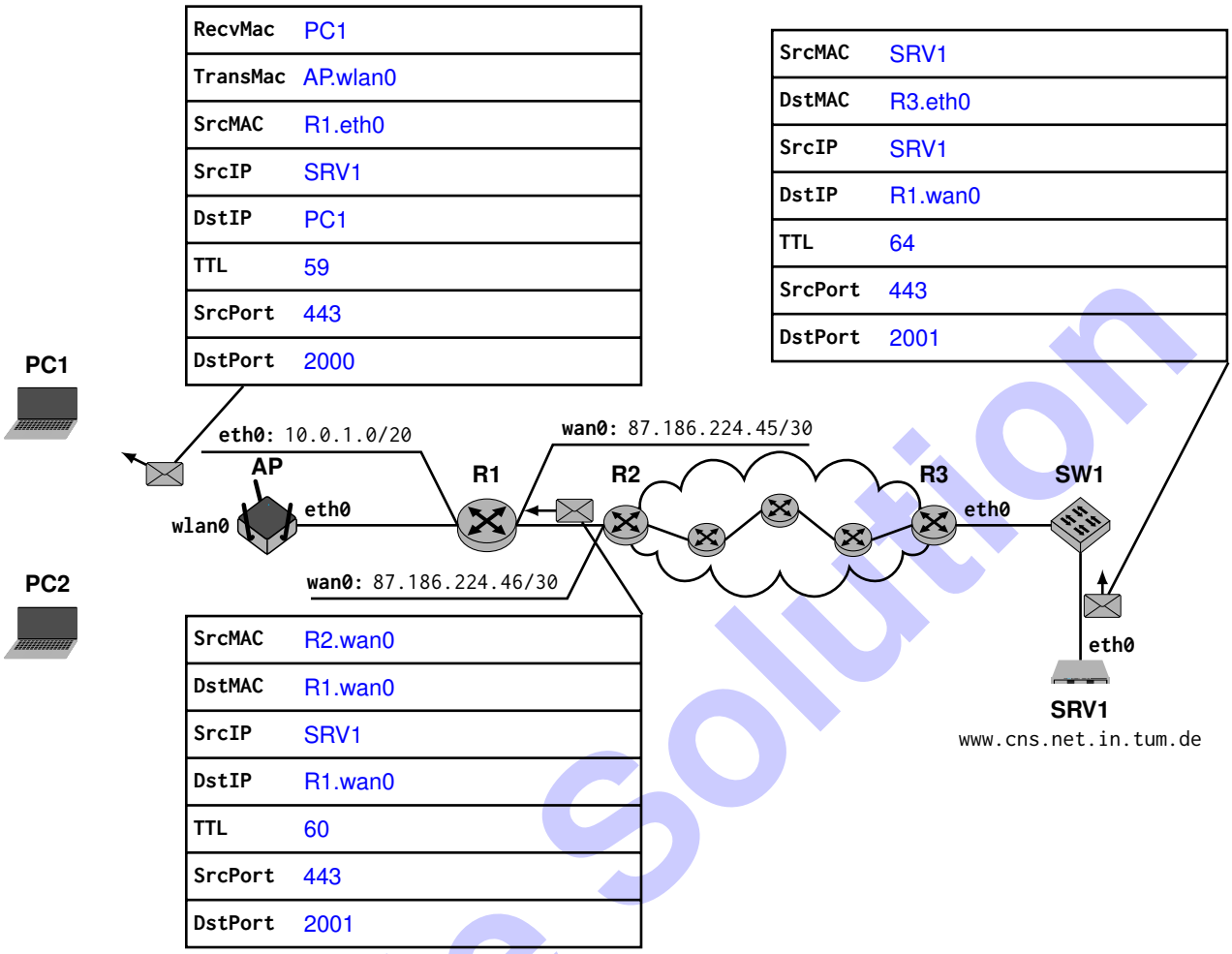


Figure 3.3: Network topology

Sample Solution

Problem 4 Recordings (14.5 credits)

Despite hopefully passing the exam, you would like to commendably repeat the contents of the lecture again after some time. You can use the lecture recordings to do this. The lecture about TCP was particularly appealing to you. The video is 512 MiB in size. Your computer is currently connected to the Internet via Ethernet and IPv6 to the Internet. The video should be accessed via HTTP 1.1. With no options are used for the underlying TCP connection. The path MTU is 1500 B.

We look at the associated TCP connection and the transmission of the segments.

a)* Show that the maximum segment size, so that no fragmentation is required, is **1440 B** in this scenario.

0
1

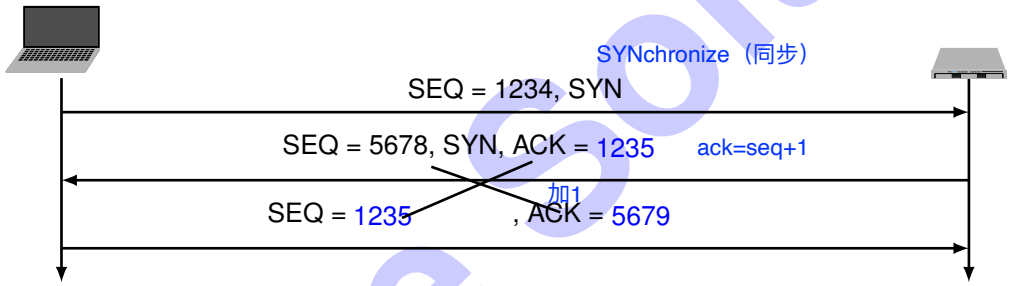
MTU - | IPv6-PCI | - | TCP-PCI |
1500 B - 40 B - 20 B = 1440 B

最大 Payload = MTU - IP 头 - TCP 头

We assume that the HTTP request 100 B in size. The first segment after the HTTP request only contains the HTTP metadata of the HTTP response, which is 500 B in size. Only the segments that follow contain the requested data. The size of the other segments was chosen to be as large as possible. Segments are acknowledged as soon as possible.

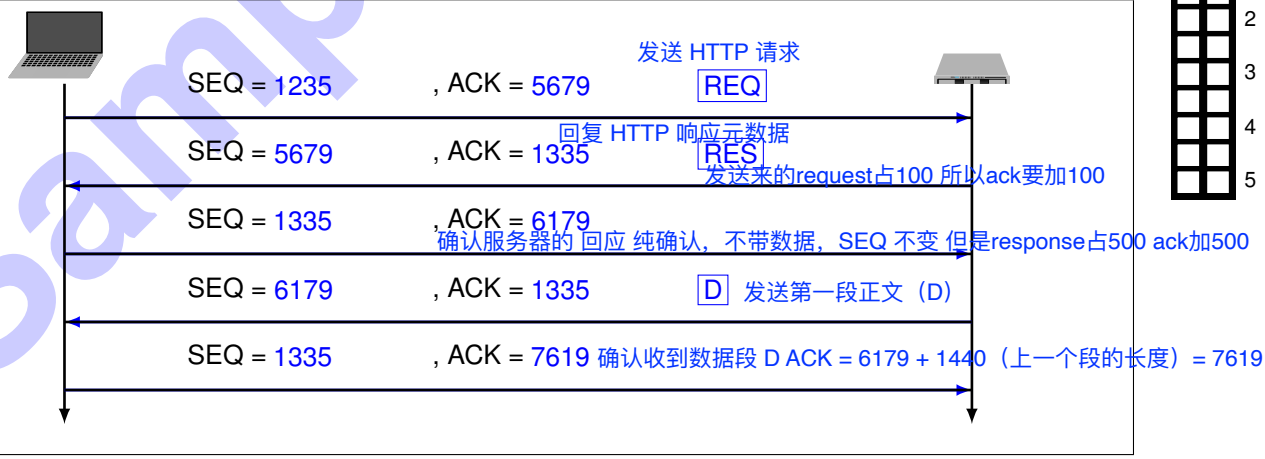
b)* Complete the TCP handshake details. Assume that no user data is transferred during the handshake.

0
1



c) Add the missing information for communication after the handshake and **add the missing arrow directions**. In the additional box of the corresponding lines, also mark segments with an HTTP request with REQ, segments with an HTTP response with RES and segments with the data with D.

0
1
2
3
4
5



Sample Solution

0 1

d) How many segments with the requested *data* will the *server* **in total** send? State your solution approach.

$$\left\lceil \frac{536870912\,B}{1440\,B} \right\rceil = 372828$$

TCP 有一套机制来根据情况自动调整传输速率

The video transmission has now started. We now assume that the simplified congestion control mechanism of TCP Reno, as presented in the lecture, is used and that we are in the congestion avoidance (CA) phase. We assume that the bandwidth of the connection allows 17 MSS/RTT and that no router has a buffer on the way to the server.

一个round trip time可以传17个max segment size

没有路由器有缓存 → 一旦超过17这个最大值，就会发生拥塞（丢包）

0 1

e)* What happens if the transmission window w_s grows to over 17 MSS?

Packet loss occurs due to the overload situation. There will be duplicated ACKs.

0 1

f) How will congestion control react to this?

congestion窗口减半 重新ca

w_c is cut in half, CA restarts

这就是fast recovery

0 1 2

g)* What is the effective throughput (in MSS/RTT) of the transmission?

$$\frac{9+10+11+12+13+14+15+16+17+17\,MSS}{10\,RTT} = 13.4\,MSS/RTT$$

Alternative solution according to cheatsheet:

$$T = \frac{18}{2} + 1 \cdot RTT = 10\,RTT, n = \frac{3}{8}18^2 + \frac{3}{4}18 = 135$$

$$\theta = \frac{1}{135}, r_{TCP} = \frac{135\,MSS}{10\,RTT} \cdot \left(\frac{134}{135}\right) = 13.4\frac{MSS}{RTT}$$

0 1

h)* Suppose your computer is very weak and is overloaded by the incoming segments. How can this situation be avoided? Name the mechanism and describe **briefly** how it works.

TCP Flow Control 通过接收方汇报接收窗口 wr，限制发送方的速率，从而防止接收端过载。

Flow control

The receiver communicates the size of its receive window w_r.

The transmitter then adjusts its transmission window and thus its transmission rate.

Sample Solution

Problem 5 DNS (14.5 credits)

You have heard from fellow students that exam solutions can be found on `grnvs.tum.de`. In the hope of finding the solution to this year's endterm, you go to the website in your browser. You are in a small home network and the router **R1** is connected to the Internet. Via DHCP, **R1** configures itself as the default resolver on your laptop **C1**. On **R1** **R2** is entered as a resolver.

配置ip 默认解析器

R1 设置了 R2（公共解析器）作为 DNS 解析器 作用是接受查询ip请求 先查自己 没有就继续查dns服务器

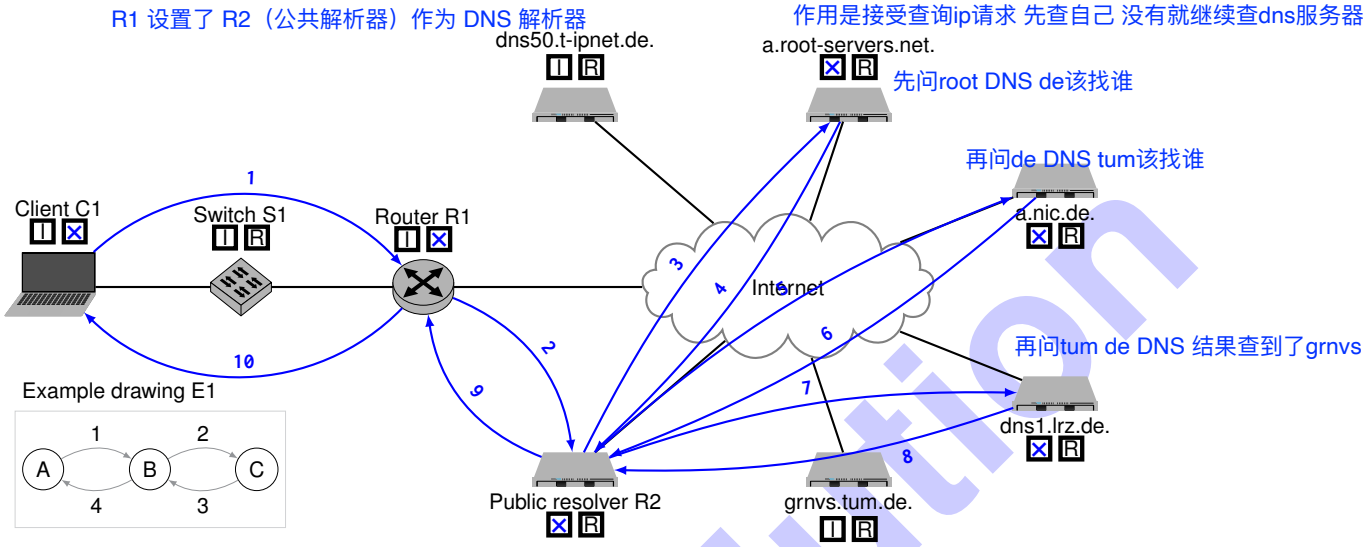


Figure 5.1: Simplified network topology

a)* Enter all DNS queries and responses that are necessary for the name resolution of `grnvs.tum.de` in Figure 5.1. Draw arrows and **number them in the order of appearance** as in the example drawing **E1**. Assume that **all caches are empty**. The following is known:

0 1 2 3

1. `a.nic.de` is the authoritative nameserver for the zone `de`.
2. `dns1.lrz.de` is the authoritative nameserver for the zone `tum.de`.

You will find an additional form at the end of the exam in Figure 6.1. Please also indicate its use in the illustration on this page if necessary.

b) For the network components used, select whether they resolve DNS queries iteratively (I) or recursively (R) by ticking the respective box. Give reasons for your choice. iteratively :服务器一步步查

0 1 2 3

recursively: 不查 转给别人

Clients and routers resolve DNS queries recursively, as they generally do not have sufficient resources (connection, computing power and memory) to perform and cache queries efficiently. Resolvers and authoritative DNS servers answer queries iteratively by definition.

解析器怎么能在没先解析 dns1.lrz.de 自己域名的情况下，就发起请求?

c)* How can the resolver make the request to `dns1.lrz.de` without first explicitly resolving its domain?

0 1 2

Using so-called glue records , a name server can send the IP addresses of another name server in addition to the NS record.

Glue Record 是和 NS 记录一起下发的 IP 地址，避免了解析器必须先去解析 NS 域名本身。

Sample Solution

You are a working student and have been given the task of creating a zone file for `grnvs.net`. Fill in the following zone file so that the requirements of the individual subtasks are met. The start of the zone file is already predefined (the `SOA` record is abbreviated for simplicity).
For the following subtasks, enter the letter of the corresponding subtask in the dotted box at the end of each line.

```
$TTL 86400 ; 1 day
grnvs.net.          IN          SOA         ns.grnvs.net. info.grnvs.net. [...]
grnvs.net.                      NS          ns.grnvs.net.
```

grnvs.net.	NS	dns2.lrz.de.	d)
ns.grnvs.net.	A	95.217.202.138.	e)
grnvs.net.	A	188.95.232.10	f)
grnvs.net.	AAAA	2a00:4700:0:9:f::	f)
grnvs.net.	MX	10 postrelay1.lrz.de.	g)
shop.grnvs.net.	CNAME	grnvs.myshopify.com.	h)

0 1

d)* `ns.grnvs.net` is already entered as the primary name server for the zone. The server `dns2.lrz.de` should act as a secondary name server for reliability. State the respective record.

0 1

e)* The primary name server should be accessible at the IP address `95.217.202.138`.

0 1 2

f)* When someone calls up `grnvs.net` in their browser, the GRNVS website should be displayed. The corresponding web server has the IP addresses `188.95.232.10` and `2a00:4700:0:9:f::`.

0 1

g) To allow students to send emails to `info@grnvs.net`, a mail server must be configured. To avoid having to operate your own mail server, the LRZ email service `postrelay1.lrz.de` should be used with priority 10.

0 1

h) To avoid having to operate your own online store, `shop.grnvs.net` should serve as an alias for `grnvs.myshopify.com`.

Sample Solution

Problem 6 Short Questions: General Knowledge (8 credits)

a)* From the lecture, the expression

$$T_{PV} = \underbrace{\frac{1}{r}\left(\left\lceil \frac{L}{p_{\max}} \right\rceil \cdot L_h + L\right)}_{①} + \underbrace{\frac{d}{\nu c_0}}_{②} + \underbrace{n \cdot \frac{L_h + p_{\max}}{r}}_{③} \tag{6.1}$$

0 1 2 3

is known for calculating the transmission time in packet switching. Briefly explain the three summands. **Note:** The question is **not** asking about the meaning of individual variables.

在链路上传输这些包所需要的总序列化时间

① Serialization time of all packets at the source including headers

信号传播延迟

② Propagation delay over the entire distance

报文在通过中间路由器时，每经过一个 hop（跳数），都需要重新将一个最大包头大小的包（含 header）序列化一次。

③ Serialization time, which occurs at n (intermediate) hops

b)* Briefly explain how Simplex and Half-Duplex differ.

0 1

单向的 不能回传数据 比如TV

Simplex refers to the unidirectional use of a medium. In contrast, with Half-Duplex, the medium can be used bidirectionally but not simultaneously by both communication partners.

双向的 但是不能同时 比如对讲机

c)* Given the 16-bit data 10101010 11001100 in Network Byte Order, the binary representation in Little Endian is:

0 1

11001100 10101010

d)* What is SLAAC used for ?

0 1

For automatic configuration of IPv6 addresses based on prefix announcement and MAC address

e)* Give one purpose of the Neighbor Discovery Protocol discussed in the lectures?

0 1

Address Resolution, Duplicate Address Detection or Neighbor Unreachability Detection

找出某个ip对应的mac地址

f)* Explain the difference between sampling and quantization ?

0 1

Sampling: Discretization in the time domain.
Quantization: Discretization in value domain.

Sample Solution

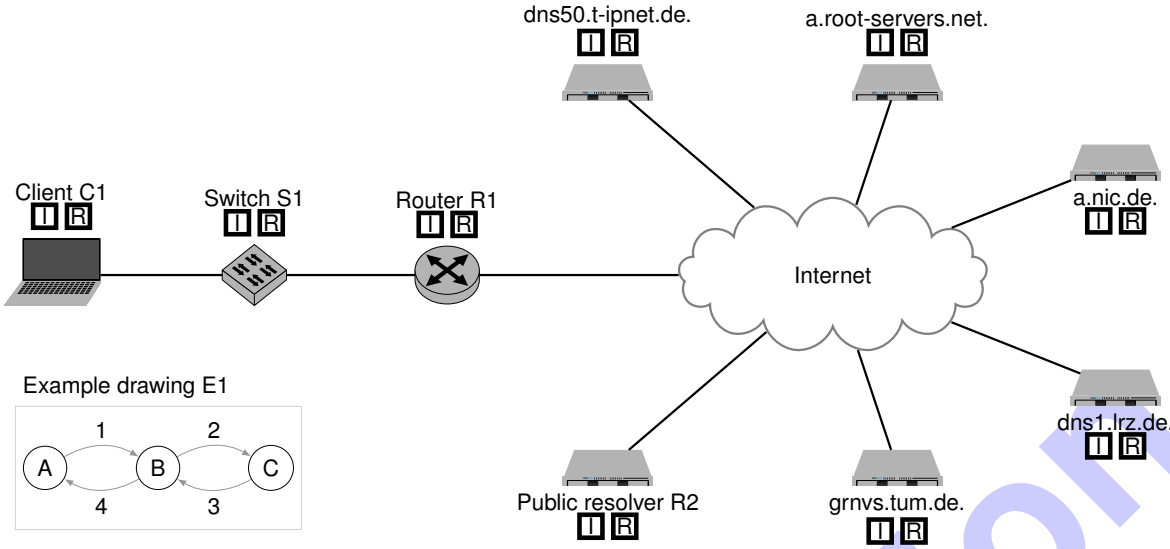


Figure 6.1: Additional preprint for Problem 5

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

Sample Solution

Sample Solution

Sample Solution

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

Sample Solution

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 ✕■

机密性 完整性 可用性

a)* Which of the following are security goals according to the lecture?

- ☐ Useability
- ☐ Performance
- ☒ Controlled Access (控制访问权限)
- ☐ Routeability
- ☐ Deployability
- ☒ Data Integrity
- ☐ Volatility
- ☒ Authenticity
- ☐ Advertisability
- ☐ Agility
- ☒ Confidentiality (机密性)
- ☐ Sustainability

128位 16字节

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 . . . (Internet Protocol Security)

- ☒ policy based (给予配置规则控制哪些流量加密)
- ☐ only available for IPv4 (IPV6也可以)
- ☐ a layer 4 protocol (layer 3)
- ☐ insecure since the protocol was broken in 2009 (错误,目前还是安全的)

前向保密性

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. 即使攻击者将来获得了你的长期密钥，也无法解密过去的通信内容。

Authenticated Encryption with Associated Data

f)* Which of the following is an AEAD cipher? (Advanced Encryption Standard)

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

Galois/Counter Mode 可以验证数据是否被篡改

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

- ☒ Timeouts (如果超时未收到 ACK，TCP 会收缩窗口，降低速度)
- ☐ Max. data rate on Layer 1
- ☒ Acknowledgements (收到一个ack 就可以再发下一个 滑动窗口)
- ☒ RTT (Round Trip Time 往返时间大 窗口就得大)
- ☒ Receive window (接收方告诉发送方：我现在还能接多少)
- ☐ Number of hops

Sample Solution

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
- [x] DNS
- [ ] SSH
- [ ] HTTPS

Fully Qualified Domain Name 完整域名 IPv4 的反向记录是放在名为 in-addr.arpa 的特殊域名下,将ip倒过来写

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

pointer record:通过ip查域名

- [ ] 24.311.0.302.in-addr-arpa.
- [ ] 302.0.311.21.in-addr.arpa.
- [x] 42.113.0.203.in-addr.arpa.
- [ ] 203.0.113.42.in-addr-arpa.

网关协议（又叫路由协议）是让不同网络之间的路由器知道“我该把数据包往哪送”的协议

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

- [x] EIGRP
- [x] BGP
- [ ] RIP
- [ ] OSPF
- [ ] IGRP

Border Gateway Protocol 内网关:校园网 外网关:不同isp

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

- [ ] 3
- [x] 4
- [ ] 7
- [ ] 2
- [ ] 5

接收方 发送方 最终接收方 中继点

Cyclic Redundancy Check 循环冗余效验

l)* What is CRC used for in Ethernet?

用于 检测数据是否在传输过程中发生了错误（比如比特翻转）

- [ ] Error Forwarding
- [x] Error Detection
- [ ] Error Correction
- [ ] Error Propagation

m)* What does QAM modulate? 正交振幅调制, Quadrature Amplitude Modulation

- [ ] Density of the signal
- [x] Phase of the signal 相位
- [x] Amplitude of the signal
- [ ] Speed of the signal

调节信号的振幅

Sample Solution

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.

`udpchat <source port> <destination IP> <destination port>`

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.

The server listens on all its interfaces on port 6112.Clients still need to know its IP address, but the server does not need to know the IPs of its clients in advance. It will learn their addresses once messages are incoming on port 6112.

0 1 2

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

They do not need to specify a source port anymore:they can choose a random ephemeral port. The server will learn the necessary port number just like it does with the IP addresses of clients.

0 1 2

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

Both need only a single socket.Since UDP is stateless, one socket can be used to send data to and receive data from arbitrary remotes.

Sample Solution

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

No, the server still awaits incoming messages (connection requests) on a specific port. Remote ports and addresses are learned dynamically.

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

0 1 2

$N + 1$, namely N for the clients and one additional as listening socket for incoming connection requests.

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

0 1 2

1. Disconnected clients can easily be identified
2. Messages are guaranteed to be received (as long as the connection holds)

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

0 1 2

1. The server must hold more state
2. Handling disconnects by getting exceptions / errors while reading from or writing to sockets can be tricky

Sample Solution

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.**

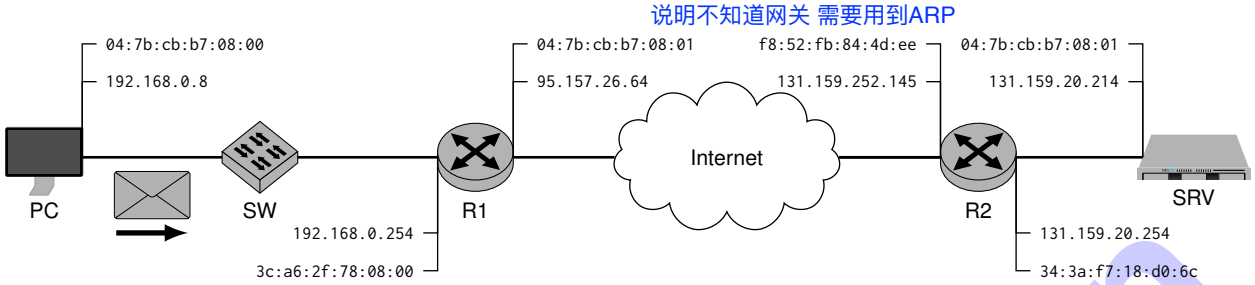


Figure 3.1: Network topology

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.

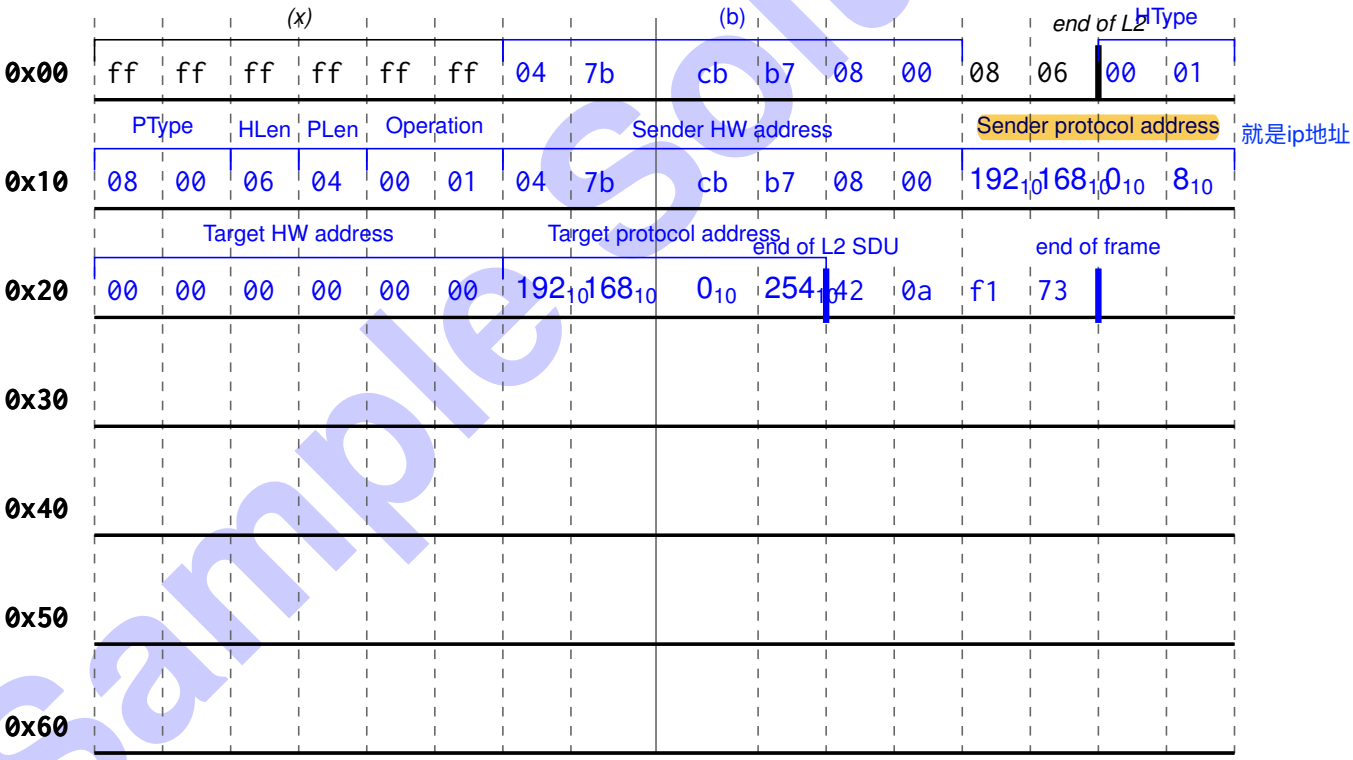


Figure 3.2: Preprint for the frame's hexdump

0 1 a) Who is (in general) being addressed by the given receiver address?

Any node on the broadcast domain.

Destination MAC address已经给出是ffff..,所以是全广播地址

0 1 b)* Fill in the transmitter address of layer 2 in Figure 3.2.

Sample Solution

c)* What is the type of the L2 SDU? service data unit上层传来的数据

ARP (Request), given by the Ethertype `0x0806`.

0
1

d) What is the purpose of this frame? 根据ip,找到mac地址

Determining the router's MAC address given its IP address.

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.

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

It would be a neighbor solicitation.

IPV6种 ARP已经被取代 使用 Neighbor Discovery Protocol（NDP）

0
1
2
3
4
5
6
7
8

0
1

Sample Solution

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.**

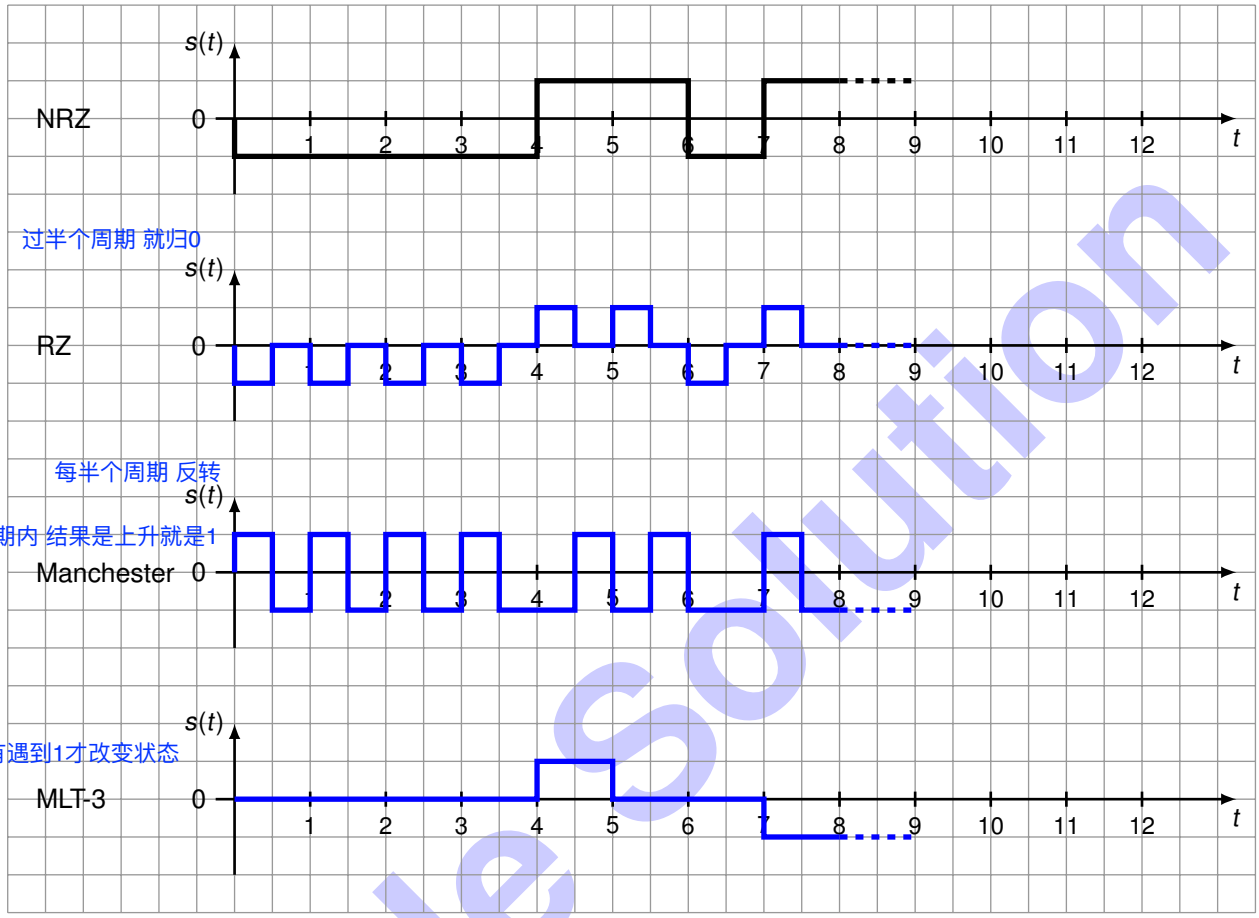


Figure 4.1: Preprint for signals

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.

Both RZ and Manchester have two signal changes per line code symbol and thus require more bandwidth than NRZ.

0 1 2

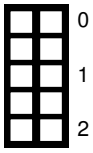
e) Reason which of the four line codes allow(s) for clock recovery / automatic synchronization?

RZ and Manchester since they require a voltage change per symbol.

0 1 2

Sample Solution

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.



For instance, 4B5B encoding can be used together with MLT-3 to guarantee a change in the signal every several bits.

Sample Solution

Problem 5 Dynamic Routing (19 credits)

RIP（Routing Information Protocol） 是一种动态路由协议

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	C	0
D	C	1
E	C	2

Dst	NH	Cost
A	A	0
C	C	0
D	C	1
E	C	2

Dst	NH	Cost
A	A	0
B	B	0
D	D	0
E	D	1

Dst	NH	Cost
A	C	1
B	C	1
C	C	0
E	E	0

Dst	NH	Cost
A	D	2
B	D	2
C	D	1
D	D	0

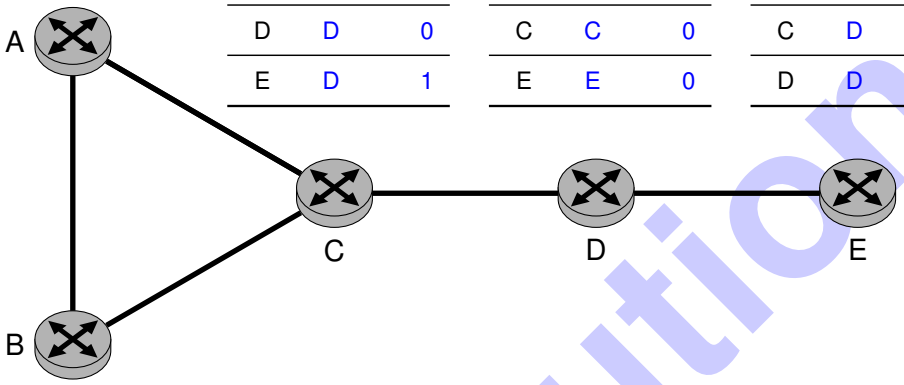


Figure 5.1: Topology and initial routing tables at boot time

度量 开销

0
1

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

Hop Count 跳跃count

0
1
2

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

The routers only know the next hop and distance for a destination whole link state protocols have detailed view of the network (or parts of it).

RIP只知道下一跳的距离 link state知道整张网络的结构

0
1
2

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

内部网关用于自治系统内部 比如校园网

IGPs are used within a single autonomuous system while EGPs are used between autonomuous systems.

外部网关用于不同的as系统 比如不同的isp之间

0
1

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

The maximum hop count for RIP is 15, thus the “diameter” of those networks cannot be larger than that.

Sample Solution

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

0 1

Solely the reachable destinations and the cost.(In particular not the next hop.)

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

0 1

Yes, hop count is RIP's sole metric. 只看跳的次数 唯一标准

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

0 1

No, the number of hops does not tell anything about available bandwidth.

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

C is informed about the fail and will remove the route to E via D.A and B do not receive the update from D.

AB还是以为能通过c到E

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

0 1 2 3

Since A still assumes there is a route to E via C, it is included in the update.B will ignore that since it also thinks there is still a route to E via C.
However, C now wrongly assumes that there is a route to E via A with cost 3 and installs this new route.

C看到A能到E 就记住了错误的信息

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

0 1 2

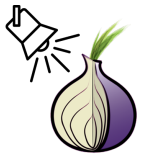
Count-to-Infinity: the non-existing route to E will circulate between A, B, and C until the tombstone of 15 is reached.
Possible solutions include split horizon, poison reverse, and triggered updates (where the latter only speed up the process at cost of network traffic).

直接发送cost=16

Sample Solution

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


visiblewiki.what.       IN A            131.159.122.12
www.visiblewiki.what.   IN CNAME        visiblewiki.what.
visiblewiki.what.       IN MX 1         visiblewiki.what.
```

Correction: 1pt for left column, 0.5pt for type(+prio), 1pt for right column. If trailing dot (fqdn) is missing, -0.5pt for each occurrence

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

Sample Solution

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

0 1 2

The A record is a glue record. It is necessary as the name server's IP is listed in the `visiblewiki.what.` zone file, but to reach that zone file, we have to query the nameserver that holds it. To break the bootstrapping cycle, the name server's IP is listed in the zone above (`what.`).

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

A resolver extracts information from the DNS by iteratively querying name servers. It interacts with our name server as soon as information from the zones it is authoritative for is to be extracted.

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

As DNS in its basic form does not provide any authentication or integrity, a client cannot trust the responses. If a malicious name server delegates to another malicious name server, the query queries a malicious subtree and returns attacker controlled information. Additionally, responses can be modified in-flight by a man-in-the-middle since the messages are unencrypted and unauthenticated. Points awarded for any reasonable explanation that is correct. Students might go into details about the hierarchy of trust here, or about DNSsec, …

DNS Security Extensions 网址签名机构

Sample Solution

Additional pre-print for Problem 4:

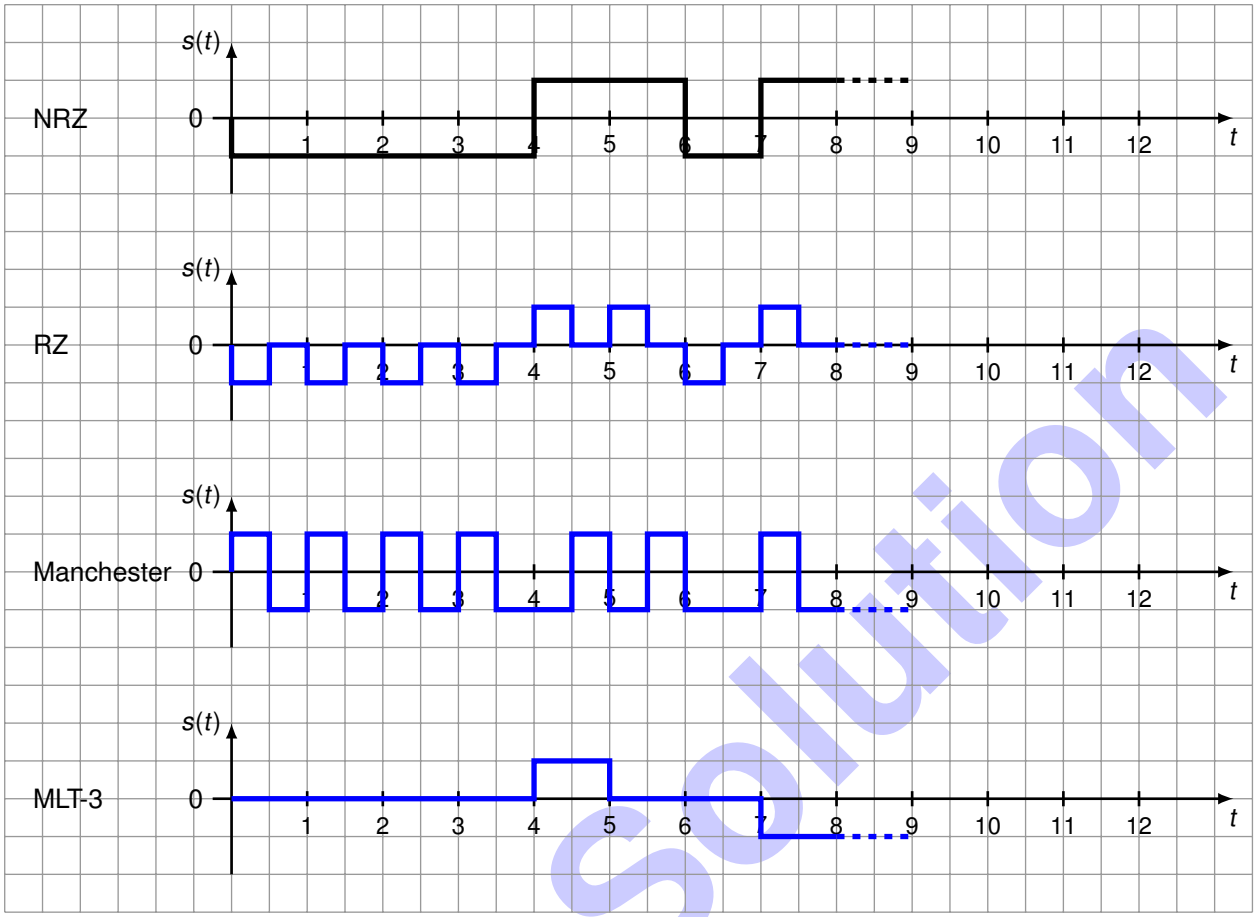


Figure 6.2: Preprint for signals

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

Sample Solution

Sample Solution

Sample Solution

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 Leander Seidlitz, M.Sc.	**Time:**	13:00 – 14:30

Sample Solution

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
- ☒ The user is not part of the model
- ☐ In general, protocols implement functions of only one layer
  协议并不只限制在一层，很多协议跨层设计很常见
- ☒ The Layer 3 SDU is the Layer 4 PDU
  PDU（Protocol Data Unit） 协议数据单元，就是这一层要发送的数据
  SDU（Service Data Unit） 是从上一层“拿来”的数据

b)* Given a message "AABB ABBB AABB AABA" ∈ {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? 内部网关协议

- ☒ RIPv2
- ☐ BGP
- ☐ CSR
- ☒ OSPF

d)* Which of the following statements regarding Layer 2 adresses in IEEE-like protocols are true?
L2就是mac地址

- ☐ Can be resolved over the Internet
  mac地址只在局域网内有效 互联网无法解析
- ☒ 6 B long
  mac地址是6 字节
- ☐ Used for routing over the Internet
  路由用的是ip而不是mac地址
- ☒ Compatible between different IEEE standard
  不同标准下兼容
- ☐ Divided into network and host part
  这说的是ip mac是硬编码在设备里的唯一地址
- ☐ 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
  载波监听多路访问 / 冲突检测
- ☒ CSMA/CD ensures fairness
  以太网用的机制
- ☐ CSMA/CD is used in wireless networks
  无限网络用的是CSMA/cA
- ☐ Token Passing is nondeterministic
- ☐ CSMA/CD is deterministic 是随机的
- ☒ Token Passing ensures fairness
  轮流发言 谁有token谁发言

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

- ☐ bb:bb:bb:bb:bb:bb
- ☐ 00:00:00:00:00:00
- ☒ ff:ff:ff:ff:ff:ff
  以太网的广播地址: 所有比特都是 1 的 MAC 地址，表示“这个帧是发给所有人的”
- ☐ 33:33:ff:ff:ff:ff

g)* Which of the following are valid 802.11 operating modes?
指的是无线网络设备（电脑、路由器等）在 Wi-Fi 网络中工作的方式/角色

- ☐ MDF (Multi-Frequency-Drift) mode
- ☒ ad-hoc mode
  对等模式 设备之间不需要 AP，彼此直接通信
- ☒ infrastructure mode
  设备之间不能直接通信，必须经由 Access Point,比如家庭路由器
- ☐ multicast mode
  所有模式都可能支持多播，但它不是模式本身

h)* What is correct regarding IPv6?

- ☒ Source and Destination address are 128 bits long
  16字节
- ☒ The IPv6 header including its extension header must always be a multiple of 8 B
- ☐ The header contains a CRC32 checksum IPv6 不再包含任何校验和
- ☐ Fragmentation is handled the same way as in IPv4 错 IPv6不再允许路由器分片

Sample Solution

Network Address Translation

i)* NAT...

- [ ] is equivalent to a firewall.
- [x] translates private IPv4 addresses to an external address and back. 把私有 IPv4 地址翻译成公网地址，反过来也可以,NAT核心作用
- [ ] adds 4 B overhead to the Ethernet header. NAT 是在 IP 层（L3）工作的，不会改动以太网帧（L2）
- [ ] does not work with IPv4 fragmentation. 可以

j)* Which of the following are TCP phases? 还包括快速充传 快速恢复

- [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`? 只能选最长的0缩写

- [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? 迭代查询 只会告诉你下一步找谁

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

递归查询 一直找到答案为止

m)* Which of the following are DNS record types? DNS 的记录类型

- [x] A
- [ ] RPT
- [x] MX
- [ ] SDR
- [ ] AAAAAA 应该是四个A
- [ ] NSS

n)* What is true regarding ECC? Elliptic Curve Cryptography:椭圆曲线加密法 非对称

- [x] For a comparable security level the key size is smaller compared to RSA 密钥短
- [ ] ECC algorithms are resistant against quantum computers
- [ ] ECC stands for Extreme Curve Cryptography
- [ ] The private key is equal to the public key 不一样 这是非对称加密

以下哪些哈希算法容易受到“长度扩展攻击”?

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

Sample Solution

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.

Sample Solution

建立安全加密的通信通道,vpn技术

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. 只包含内网通信 不保护外网通信

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:

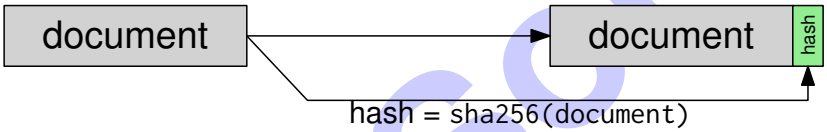


Figure 2.1: The proposed signing scheme as **Block Diagram**.

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`.

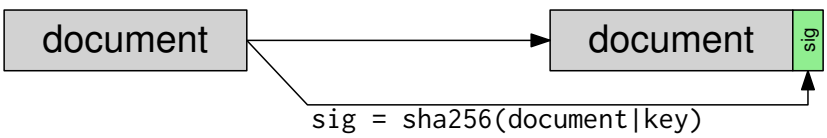


Figure 2.2: The reworked signing scheme. | denotes concatenation.

Sample Solution

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.

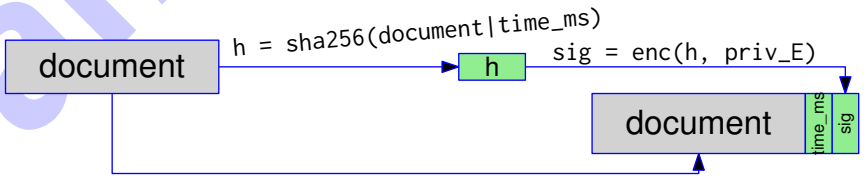
f)* How many shared secrets are necessary given there are n such parties. **Do not justify your answer.**

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

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

Sample Solution

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).

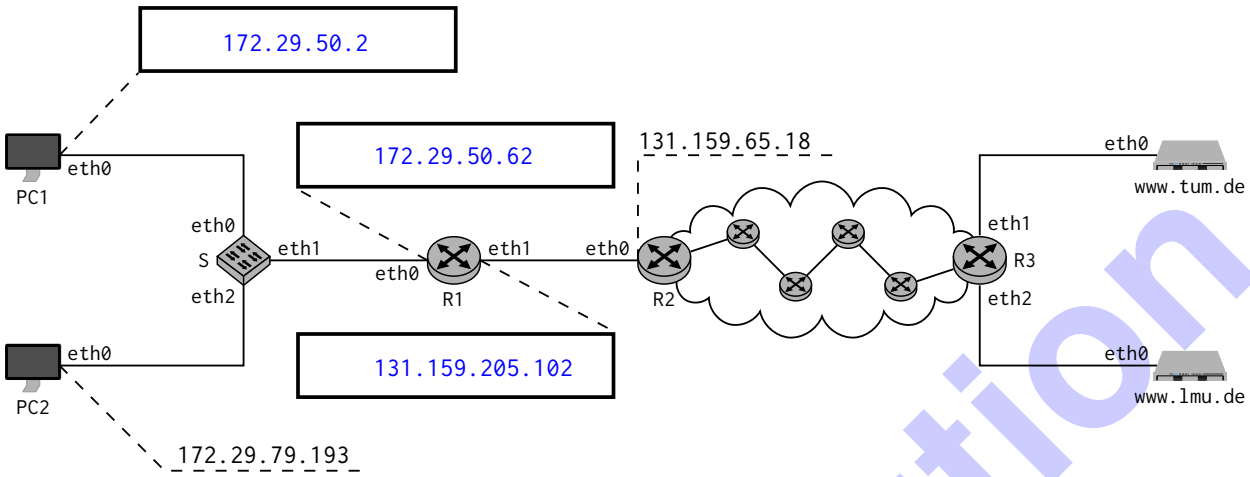


Figure 3.1: Network topology

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.

Sample Solution

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

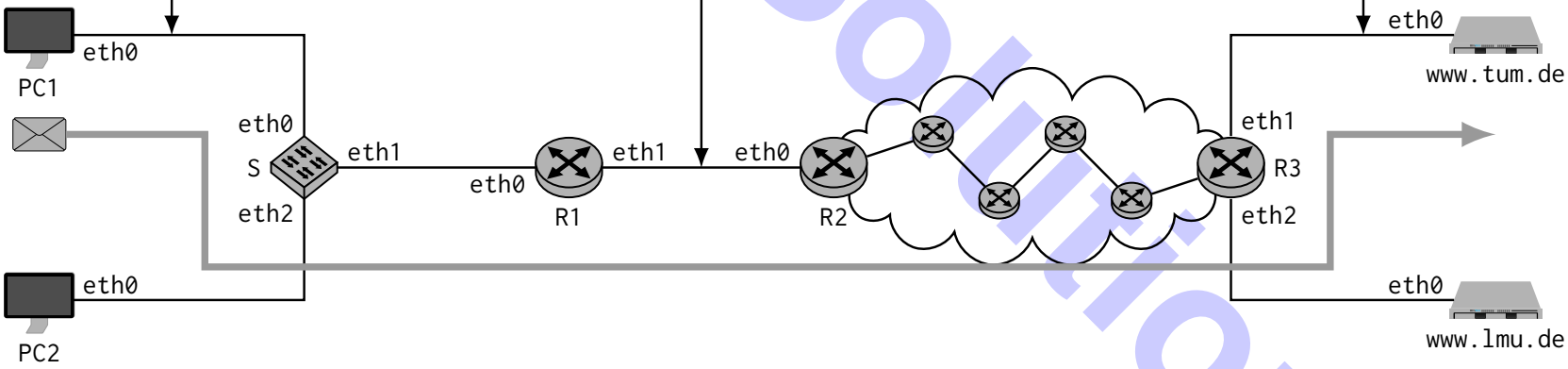


Figure 3.2: Preprint for Subproblem f)

sample solution

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

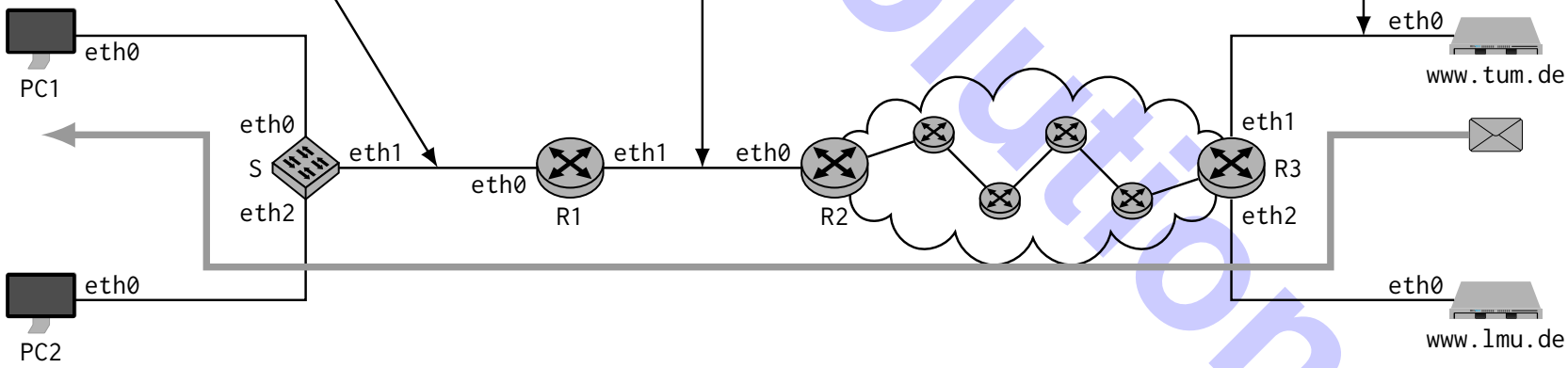


Figure 3.3: Preprint for Subproblem g)

Sample solution

Text

[Ethernet Header]
[IP Header (IPv4 or IPv6)]
[Transport Header (TCP/UDP)]
[Application Data (可选)]

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.

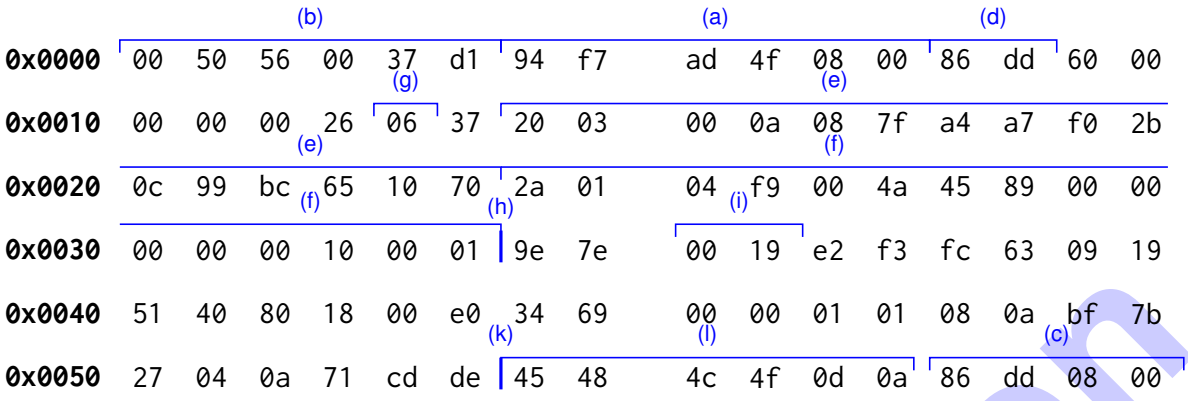


Figure 4.1: Ethernet frame including checksums.

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

offset表示某个字段（或协议）的“起始位置”

ethernet header占14b ipv6 header占40b 总共加起来是54 就是ox0036

Sample Solution

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`

Sample Solution

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.

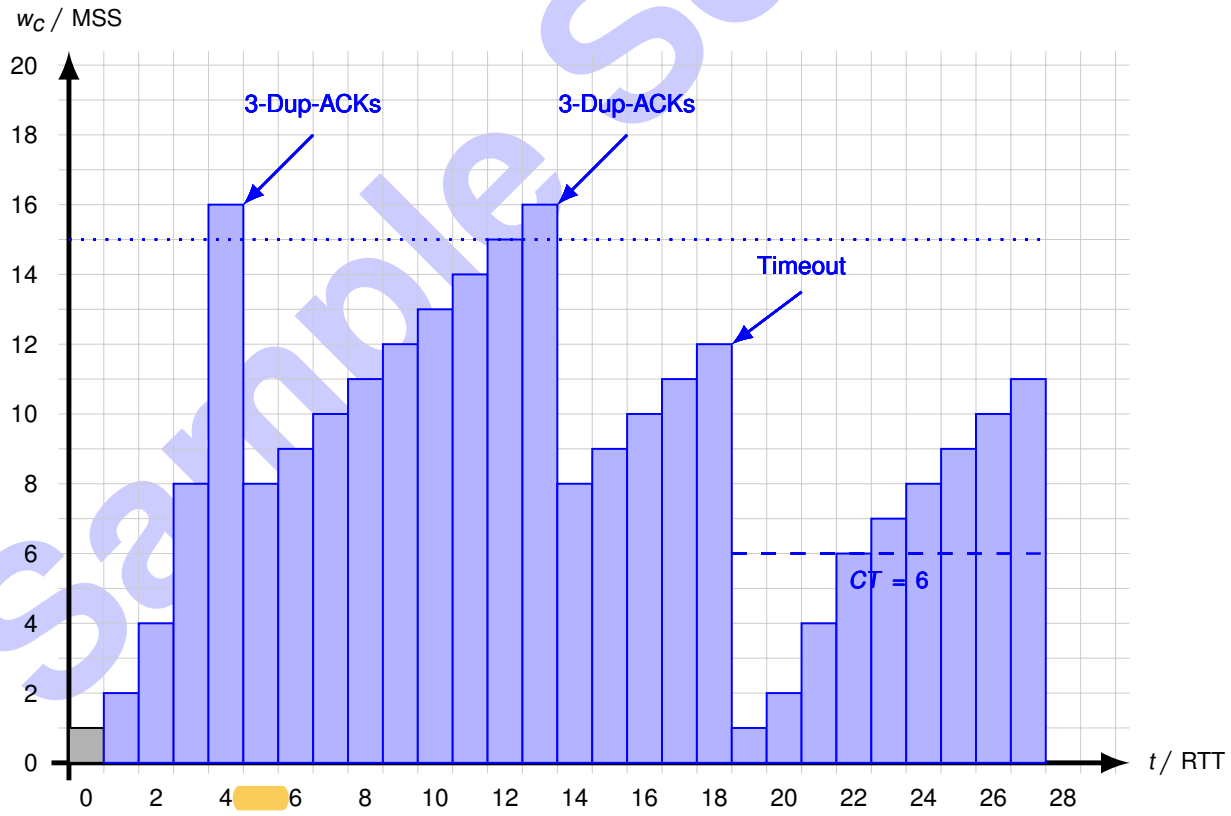


Figure 5.1: Preprint for Subproblems c) and g). An addition preprint can be found at the end of the exam. **Clearly strike out invalid solutions.**

Sample Solution

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 $r_{TCP} = \frac{108\,\text{MSS}}{9\,\text{RTT}} \cdot (1 - \frac{1}{108}) \approx 11,89\,\frac{\text{MSS}}{\text{RTT}}$.

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?

timeout啥都收不到
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.

Sample Solution

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.

hub上广播 switch是选择性发 和connected的发

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.

Sample Solution

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

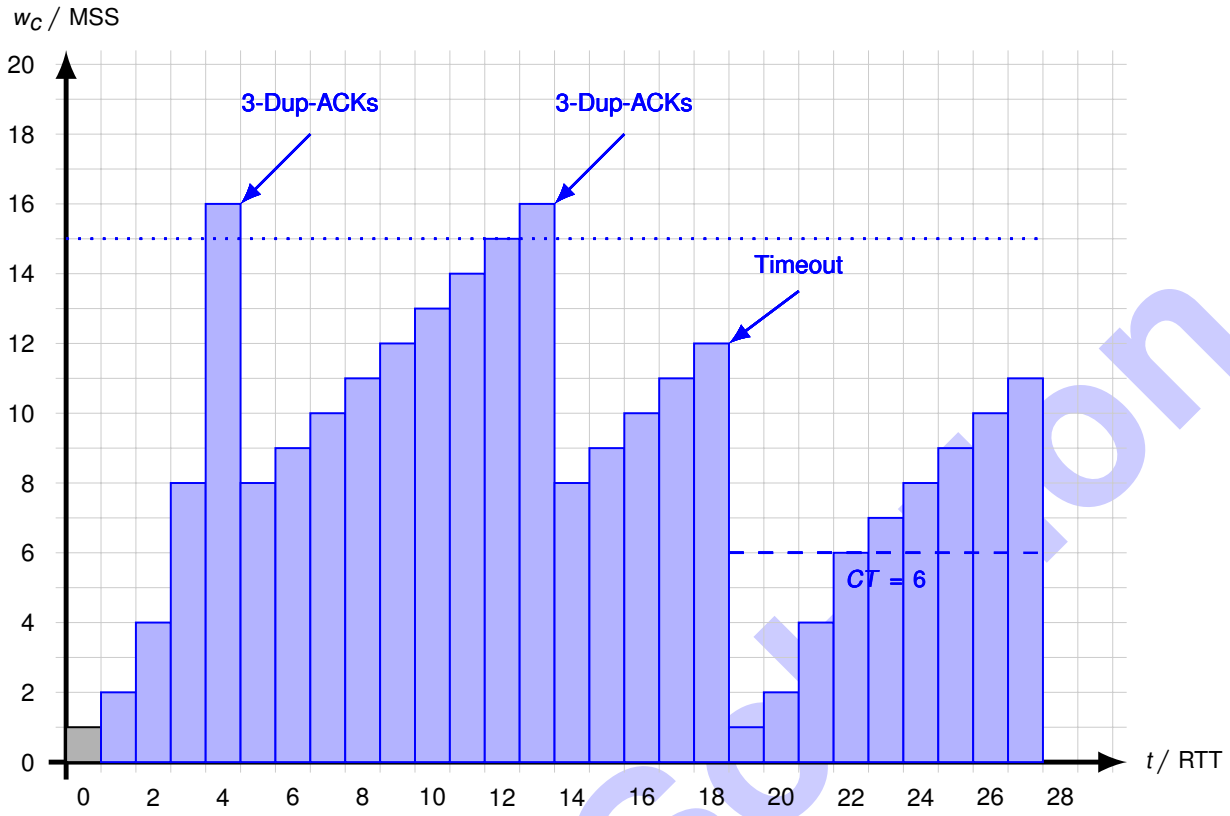


Figure 6.1: Preprint for Subproblems 5 c) and g). **Clearly strike out invalid solutions.**

Sample Solution

Sample Solution

Chair of Distributed Systems and Secuirty
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 / Endterm	**Date:**	Thursday 16th February, 2023
Examiner:	Prof. Dr.-Ing. Stephan Günther	**Time:**	14:00 – 15:30

Sample Solution

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 ✕■

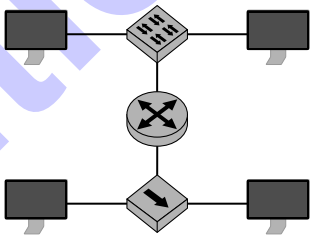
a)* Which statesments regarding MLT-3 are correct?

把比特序列变成线缆中的电信号 是把原始数据做压缩 去除冗余 直流分量为 0

- ☒ 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

是为了纠错、抗干扰而增加冗余的编码方式 1 symbol - 1 bit

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

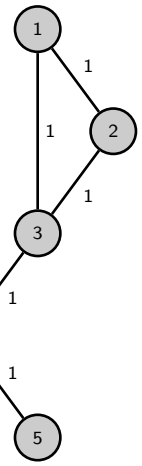


- ☐ 3 ☐ 6 ☐ 1 ☐ 5 ☒ 2 ☐ 4

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. 相连 标记1



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

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?

最多需要走几步（n）才能从任意点走到所有其他点？ 这里就是1-5的最短路径
这其实是在问图的 直径（diameter），也叫最长的最短路径

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

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

只在UDP中使用

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

发送和接收 UDP专用 其他都是通用的 TCP专用

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

只有一个字节 大小段序都一样

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

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

Sample Solution

私有地址段（192/172/10），还有 link-local（169.254）

这个地址不能直接上网

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

- [x] 169.254.0.72
- [ ] 142.251.36.174
- [ ] 131.159.15.24
- [x] 172.16.12.1
- [ ] 129.187.255.109
- [ ] 9.9.0.1

交换方式

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

电路交换 专线连接

- [x] Circuit Switching
- [ ] Lane Switching

把信息分成小包发送

- [x] Package Switching

一次性发整段消息

- [x] Message Switching
- [ ] Parcel Switching
- [ ] Multi-Track Switching

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

- [x] IP Header Length
- [ ] Integrated Header Length
- [ ] Informative Header Length

以下哪些协议没有校验和

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

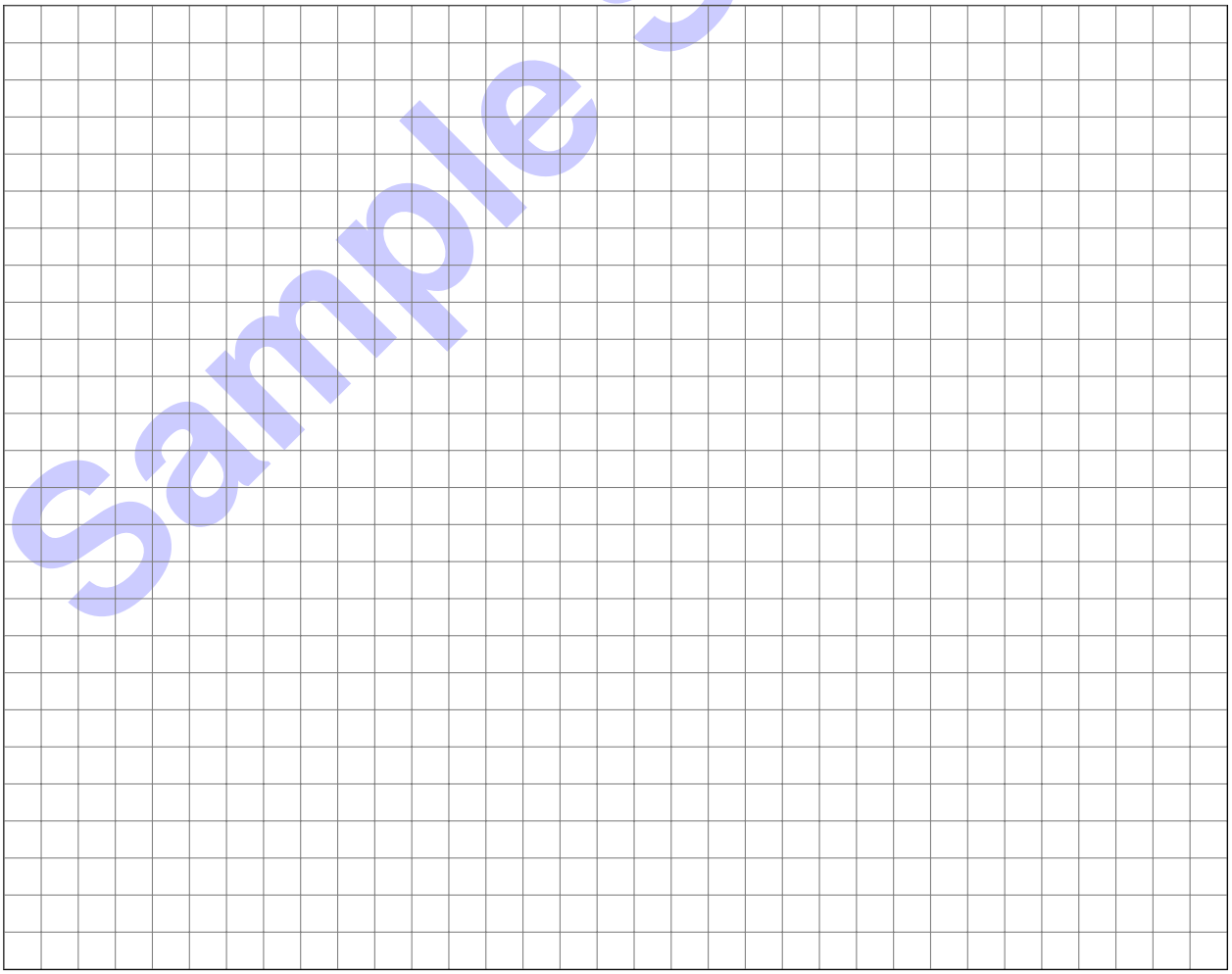
Address Resolution Protocol 地址解析 将ip换成mac

- [ ] IPv4
- [ ] UDP
- [x] ARP
- [x] IPv6
- [ ] TCP
- [ ] Ethernet

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

- [ ] GET
- [ ] HEAD
- [ ] DELETE
- [ ] POST
- [x] DISCARD 没有这个指令
- [ ] PUT

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



Sample Solution

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?

No, as the server and client can differentiate based on the L4 protocol.

0 1

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

An (unused) port number ranging from 1024 to 65 535 (ephemeral port).

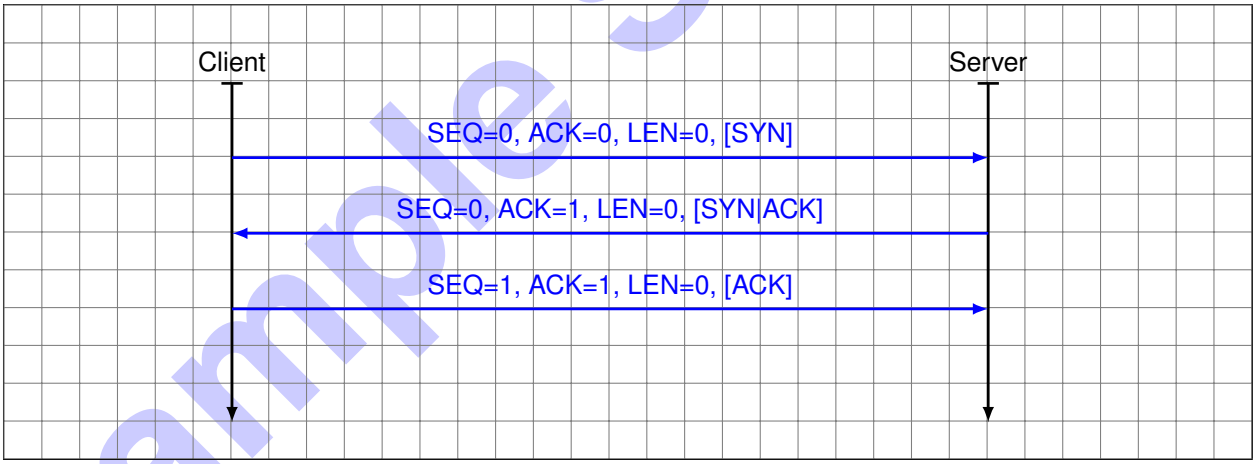
0 1

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

Port 80 (well-known port for HTTP)

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

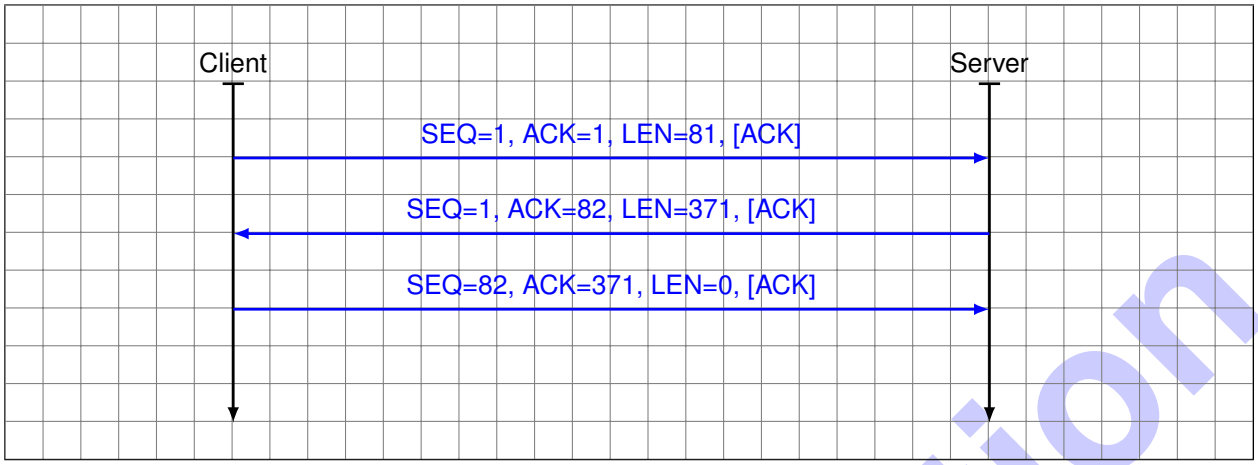
e) What is the payload (protocol and type, action, or method) of the next segment sent by the client?

HTTP GET (requesting `cns.net.in.tum.de`)

Sample Solution

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

In particular, the response code 301 means that the destination is no longer available but a redirect exists.
In that case, the redirect is simply to `https://...`, i. e., making the website reachable via unsecured HTTP by immediately redirecting to a TLS-based connection.

Sample Solution

Problem 3 DNS (13.5 credits)

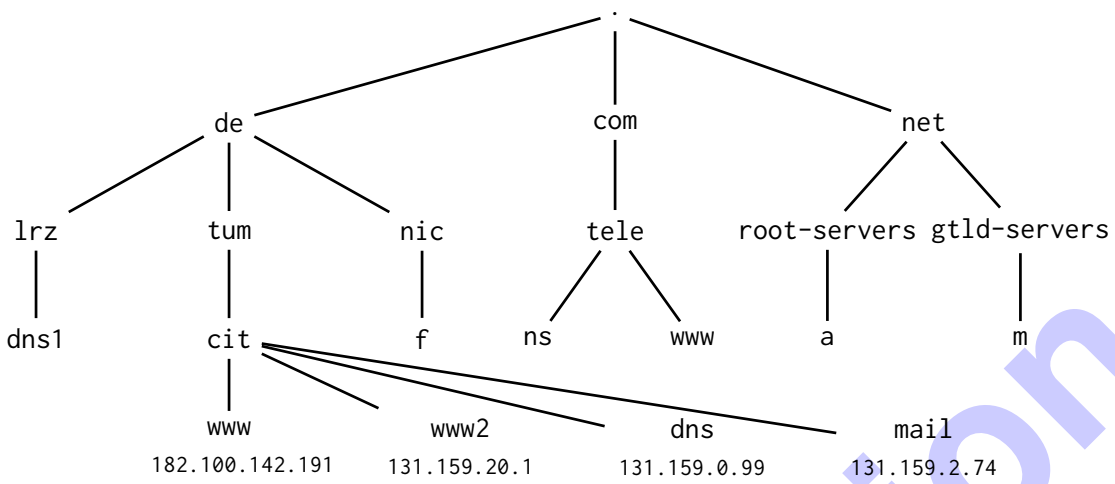


Figure 3.1: A part of the DNS.

0 1

a) Briefly describe the purpose of DNS.

The mapping between FQDN and IP addresses.

0 1

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

A fully qualified domain name starts at the root, denoted by the ".".
A non-fully qualified domain name starts at an intermediary node of the DNS.

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     dns.cit.tum.de.
 7  cit.tum.de.          IN     MX     20  mail.cit.tum.de.
 8
 9  dns.cit.tum.de.      IN     A      131.159.0.99
10  mail.cit.tum.de.     IN     A      131.159.2.74
11  www.cit.tum.de.      IN     A      182.100.142.191
12  www2.cit.tum.de.     IN     A      131.159.20.1
```

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.

Sample Solution

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

0 1

A resolver might cache the result for the amount of time specified in the TTL.After the time has expired it must query the authoritative nameservers again.

f)* What purpose does a zone transfer serve?

0 1

The zone file is synchronized onto secondary nameservers, which are authoritative for the same zone so that the latter have the up to date information.

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

0 1

An authoritative nameserver for a zone holds the zone records for this zone and answers queries it.

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

0 1

When the request is larger than 512 B.

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

The root nameservers serve as a root of trust, as a resolver knows their IP addresses without querying the DNS.Starting at the root nameservers, only nameservers that are contained in the zone files will be contacted.Therefore, assuming the root is trusted, only trusted servers are contacted.An untrusted nameserver is therefore never contacted as no server points to it.

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

0 1 2

With recursive resolution, only one request for a resource record is made to a configured resolver, which returns the final response.
With iterative resolution, the FQDN is instead resolved starting at the root zone (or the last known SOA) by querying the authoritative name servers for the respective zones.Their answers contain either the FQDN of an authoritative name server of the next lower zone or the final resource record if the queried name server is authoritative for it.

Sample Solution

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.

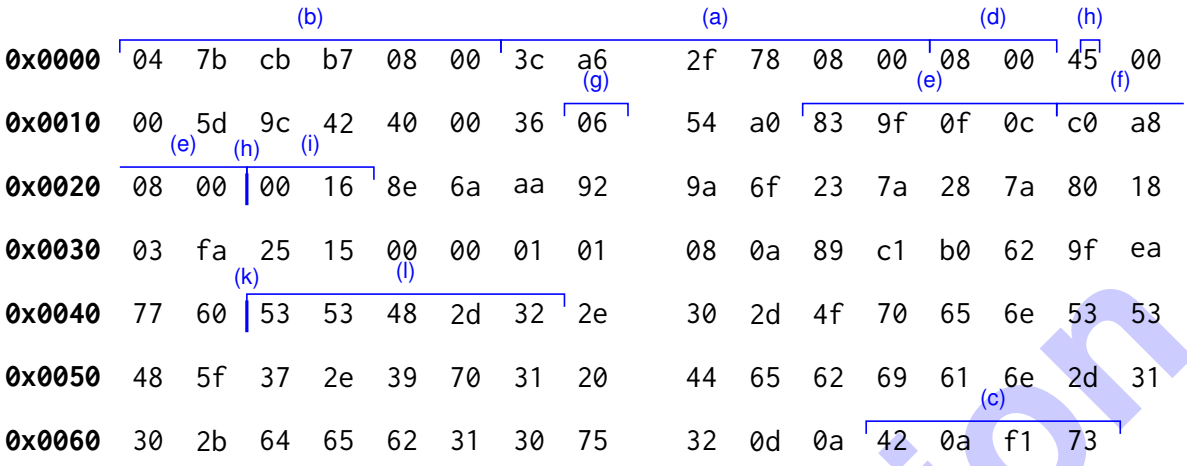


Figure 4.1: Ethernet frame including checksums.

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.

0 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.

IPv4

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

131.159.15.12

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

192.168.8.0

0 1 2 g) What protocol is used as L4 PDU? Mark the respective header field in in Figure 4.1.

TCP

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

Offset: 0x0022 Reason: IHL = 0x5 ⇒ 20 B IP header / no options

Sample Solution

i) What type is the layer 7 protocol probably?

The destination port is an ephemeral port.However, the source port 22 suggests that it is SSH.

0 1 2

j) For what purpose is that protocol used?

Encrypted remote control of computers.

0 1

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

Offset: `0x0042` Reason: Offset = `0x8` $\Rightarrow$ 32 B TCP header

0 1 2

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

ASCII coded string starting at offset `0x0042`: `0x53 0x53 0x48 0x2d 0x32` = `SSH-2`

0 1 2

Problem 5 Short Questions: Security (20 credits)

a)* Differentiate Authentication from Authorization.

Authentication is the process of proving an entities identity.
Authorization determines which privileges an entity has.

0 1 2

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

In such scheme, an asymmetric scheme is used to establish a secret. This solves the problem of not having a shared secret in the beginning as a key can be encrypted with the receiver's public key and only the receiver can decrypt it using its private key.
After key establishment, a symmetric scheme is used. This is as symmetric ciphers have a higher throughput as they are cheaper to calculate.

0 1 2

Sample Solution

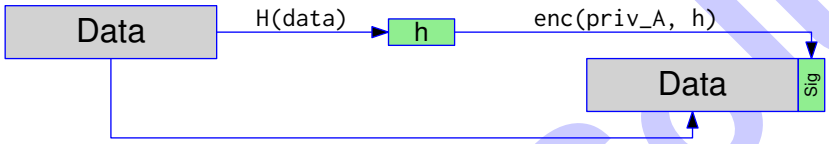
0 1 2 3

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

1. Pre-Image Resistance:
   Given a hash value, it is hard to find an input that results in the same hash.
2. Second Pre-Image Resistance:
   Given a message, it is difficult to find another input that results in the same hash.
3. Collision Resistance:
   It is difficult to find a pair of two different messages that result in the same hash.

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)`.



- General idea makes sense and reflects a signature scheme
- Signature cannot be forged without secret (= not a checksum)
- Signature is only over the hash of the message (= efficient to calculate)

0 1 2

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

A CA is responsible to issue the certificate for the requesting entity after the RA has checked the entities identity and relayed the request to the CA.

0 1

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

A predictable random number generator results in lower entropy, leading to weaker or even broken keys / encrypted material. Keys and cypher streams might thus become predictiable.

Sample Solution

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

0 1 2

ESP offers confidentiality, authenticity as well as integrity protection for its own headers and the IPsec payload.
AH only offers authenticity and integrity protection, but additionally for the preceding IP header.

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

0 1

Since IPsec encrypts the layer 4 header, the port numbers cannot be used for NAT. Therefore, a dummy UDP header is inserted which only serves the purpose of traversing the NAT.

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

0 1

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

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

0 1

The same plain text results in the same cipher text. Therefore, patterns in the plain text propagate into the cipher text.

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

0 1 2

A Merkle-Damgård based scheme outputs the entire internal state of the hash function as digest. Therefore, the digest can be loaded back into the hash function, and further blocks be hashed. This allows breaking e. g. the signature scheme `sig=hash(key|msg)`.

Sample Solution

Problem 6 Short Questions: General Knowledge (8 credits)

0 1

a)* What are well-known ports?

TCP/UDP ports with port numbers smaller than 1024.

0 1

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

OSPF has knowledge of the network topology, therefore it can detect loops.

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.

$$
\begin{aligned}
SNR_{dB} &= 10 \log_{10} SNR \Rightarrow SNR = 10^{\frac{45}{10}} = 10^{4.5} \\
r_{\max} &= B \log_2 (1 + SNR)\,\text{bit} \\
&= 35 \cdot 10^6 \text{Hz} \log_2 \left(1 + 10^{4.5}\right)\,\text{bit} \\
&\approx 523.2\,\text{Mbit/s}
\end{aligned}
$$

0 1

d)* Which purpose does ARP serve?

Resolution of layer 2 addresses to layer 3 addresses.

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.

- 2 bit $\Rightarrow N = 4$ signal levels
- Level width $\Delta = \frac{b-a}{N} = \frac{3}{2}$
- Maximum quantization error $e_{\max} = \frac{\Delta}{2} = \frac{3}{4}$
- Signal levels: $-2.25, -0.75, 0.75, 2.25$

Sample Solution

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:** Thursday 6th April, 2023
Examiner: Prof. Dr.-Ing. Stephan Günther **Time:** 14:00 – 16:00

	P 1	P 2	P 3	P 4	P 5	P 6
I						
II						

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 **16 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 _____

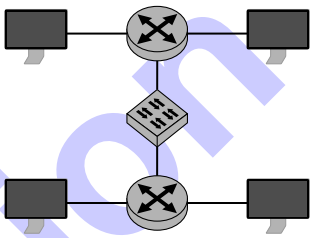
Sample Solution

Problem 1 Multiple Choice (14 credits)

The following subproblems are multiple chouce / multiple answer, i. e., at least one answer per subproblem is correct. Sub problems 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)* How many broadcast domains does the network to the right contain?

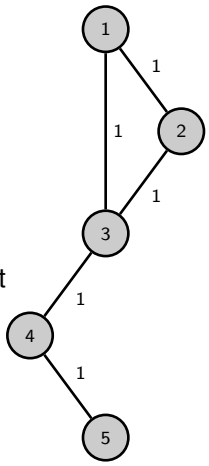


☐ 3 ☒ 6 ☐ 1 ☐ 5 ☐ 2 ☐ 4

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

☐ 4 ☐ 2 ☐ 3 ☐ 1 ☒ 6 ☐ 5

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

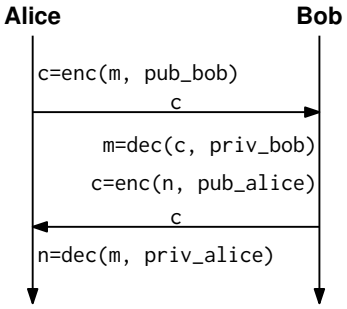


☐ $\begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix}$ ☐ $\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$ ☒ $\begin{bmatrix} 0 & 1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

d)* 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?

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

e)* Assume that Bob and Alice know each others public key. What is the scheme on the right vulnerable to? 公钥通信 这种通信方式容易受到哪些攻击



☐ Eve can impersonate Bob
☒ **No** forward-secrecy
一旦 Alice 或 Bob 的私钥被泄露，攻击者可以解密历史上的所有通信，没有前向保密性
☐ Man-in-the-Middle and thereby full message decrypt
☒ Replay Attacks
重放攻击

f)* Which **three** of the following claims are true?

☐ In AES-CBC, later blocks influence previous ones 前面的影响后面的
☐ ECC is robust against quantum computers
☐ RSA is robust against quantum computers
☒ AES is robust against quantum computers
☐ Common key lengths for AES are 2048 bit and 4096 bit AES 的密钥是 128、192、256 比特
☒ SHA-256 is vulnerable to length-extension attacks
☒ Cipher text blocks in AES-ECB can be cut and pasted unnoticeable
☐ SHA-3 is vulnerable to length-extension attacks

Sample Solution

g)* What is the AES-CTR scheme?

- [ ] A hash function
- [ ] A block cipher
- [x] A stream cipher
- [ ] A key exchange

在可信计算中，每一个启动环节验证前一个的可信性，形成一个完整的链式信任。

h)* A chain of trust is used in. . .

- [ ] Trusted fourth parties
- [ ] Trusted Memory
- [x] Trusted computing
- [ ] Your trusted bike lock

i)* The domain name system. . . 是域名到ip

- [ ] has a mapping from every single IP address to a domain name
- [x] translates domain names to IP addresses

不是完全可信的

- [ ] is inherently trustworthy

DNS是分布式系统

- [ ] has a single, central authority

j)* The congestion avoidance phase of TCP Reno. . .

- [x] increases the traffic control window linearly
- [ ] is the first phase active in a new connection

slow start是指数增长

- [ ] increases the traffic control window exponentially
- [ ] follows the rapid start phase

k)* In 802.11. . .

WEP协议下的管理帧是明文发送的

- [x] management frames are unprotected when using WEP
- [ ] traffic cannot be sniffed by attacker when not in line of sight

如果攻击者不在视野范围内，就无法嗅探数据流量.错 信号可以穿墙

在 802.11 MAC 帧结构 中，最多可能出现 4 个 Layer 2 地址

- [ ] only two layer 2 addresses are contained in the header
- [ ] arbitrary errors are corrected using the FCS (Frame Correction Sum)

Frame Check Sequence

Sample Solution

Problem 2 Short Questions: Security (14 credits)

0 1 2

a)* Differentiate Authentication from Authorization.

Authentication is the process of proving an entities identity.
Authorization determines which privileges an entity has.

0 1 2

b) Argue whether an man-in-the-middle attacker can be passive and/or active. Describe a scenario for each applicable property.

A MitM attacker can be both, active and passive.
An attacker eavesdropping on traffic would be passive, while actively replaying traffic puts them into an active position(for explanation).

0 1

c) How is a password hash function different from SHA-256?

A password hash function is built to be intentionally slow/expensive to calculate, thereby hindering brute-force attacks.

0 1 2 3

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

1. Pre-Image Resistance:
   Given a hash value, it is hard to find an input that results in the same hash.
2. Second Pre-Image Resistance:
   Given a message, it is difficult to find another input that results in the same hash.
3. Collision Resistance:
   It is difficult to find a pair of two different messages that result in the same hash.

Sample Solution

e) Briefly describe a scenario in which the IPsec tunnel mode is used.

0 1

A company connects two of its sites (and therefore the two networks) over the public internet.

f) Differentiate a block cipher from a stream cipher.

0 1

A block cipher encrypts entire blocks of data, the plain text has to be padded to a multiple of the block length.
In contrast, a stream cipher generates a key-stream using the underlying block cipher, and can therefore be used to encrypt data byte-wise.

g) Differentiate symmetric encryption from asymmetric encryption. Elaborate on the usage of keys.

0 1 2

Asymmetric encryption uses a key pair, consisting of private and public key, to encrypt and decrypt data. Data that has been encrypted using the public key can only be decrypted using the private key, and vice-versa.
Symmetric encryption is based on a shared secret — the same key is used for encryption and decryption.

h) Describe three functions of a TPM.

0 1 2

- A hardware random number generator
- A way to generate and store keys on the TPM without them ever leaving it
- A way to attest (= identify) a system based on the hardware and software running
- Using the TPM keys to encrypt/decrypt and sign data
- It can be asked to store keys, such as disk encryption keys
- The TPM usually is a separate hardware on the motherboard
- The root key of the TPM is burned into the hardware during production

Sample Solution

Problem 3 CRC (14 credits)

In this problem we consider the binary message `00100110` which should be protected by a CRC as we introduced it for Ethernet-based networks in the lecture. We assume the reduction polynomial $r(x) = x^2 + 1$.

0 1

a)* Briefly explain what CRC is used for in the context of Ethernet.

Detection of bit errors at the receiving node.

0 1

b)* What is the reduction polynomial being used for?

Mapping of a message of arbitrary length to a fixed length checksum.

0 1

c)* What does it mean if the reduction polynomial is *irreducible*.

It cannot be represented as the product of two other polynomials of degree strictly less than deg$r(x)$.

0 1 2

d)* Reason whether or not CRC requires an irreducible reduction polynomial.

It does not: using an irreducible reduction polynomial leads to finite field. However, the purpose of CRC is primarily error detection.Reduible polynomials may have desireable properties such as being able to detect all bit errors of odd length if the factor $(x + 1)$ is contained in the reduction polynomial.

0 1

e)* Show whether or not $r(x)$ is irreducible.

$r(x) = x^2 + 1 = (x + 1)^2 \quad \Rightarrow \quad$ it is reducible

0 1

f)* Assuming Ethernet, what is the reaction of the receiving node when a bit error is detected.

The frame is dropped without further action.

Sample Solution

g)* Determine the CRC checksum for the given message (see beginning of the problem).

0 1 2 3 4

```
00100110 00 : 101 = 101101
  101|||  ||
  ---|||  ||
  00111|  ||
    101|  ||
    ---|  ||
    0100  ||
     101  ||
     ---  ||
     001  00
       1  01
       -  --
          1
```

Checksum is 01.

h) Explicitly state the transmitted message.

0 1

```
00100110 01
```

Let us assume a different message (including its checksum): 1110110100101110**01**. Assume that this message is transmitted and arrives as 1110110100101111**00** at the receiver.

i)* Argue whether or not the error is being detected.

0 1 2

It is not detected sind the error is 101, which is a multiple of the reduction polynomial.

Sample Solution

Problem 4 Wireshark (19 credits)

We consider the network topology depicted in Figure 4.1. 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.

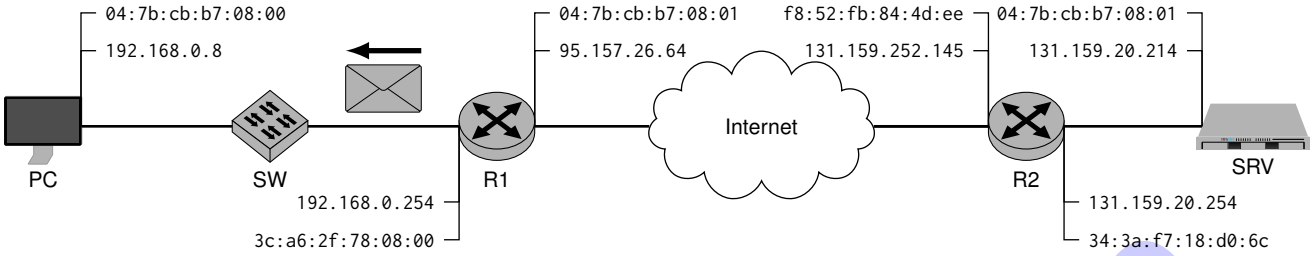


Figure 4.1: Network topology

We consider the frame sent from R1 to the PC as depicted in Figure 4.1, which is the first message from SRV **after** the TCP handshake has completed.

In the following we want to derive the **hexdump of that frame** based on the information given in Figure 4.1 and the following subproblems. Fill in the contents step by step in Figure 4.2. **Make sure to mark to which subproblem your solution belongs**, e. g. by using colors or writing the respective subproblem above your solution. As an example, the L2 receiver address is already filled as answer to some (not existing) Subproblem x).

Notes: There may be some gaps in the final hexdump as we do not derive all contents of that frame. The cheatsheet handed out together with this exam contains any headers and translations you need.

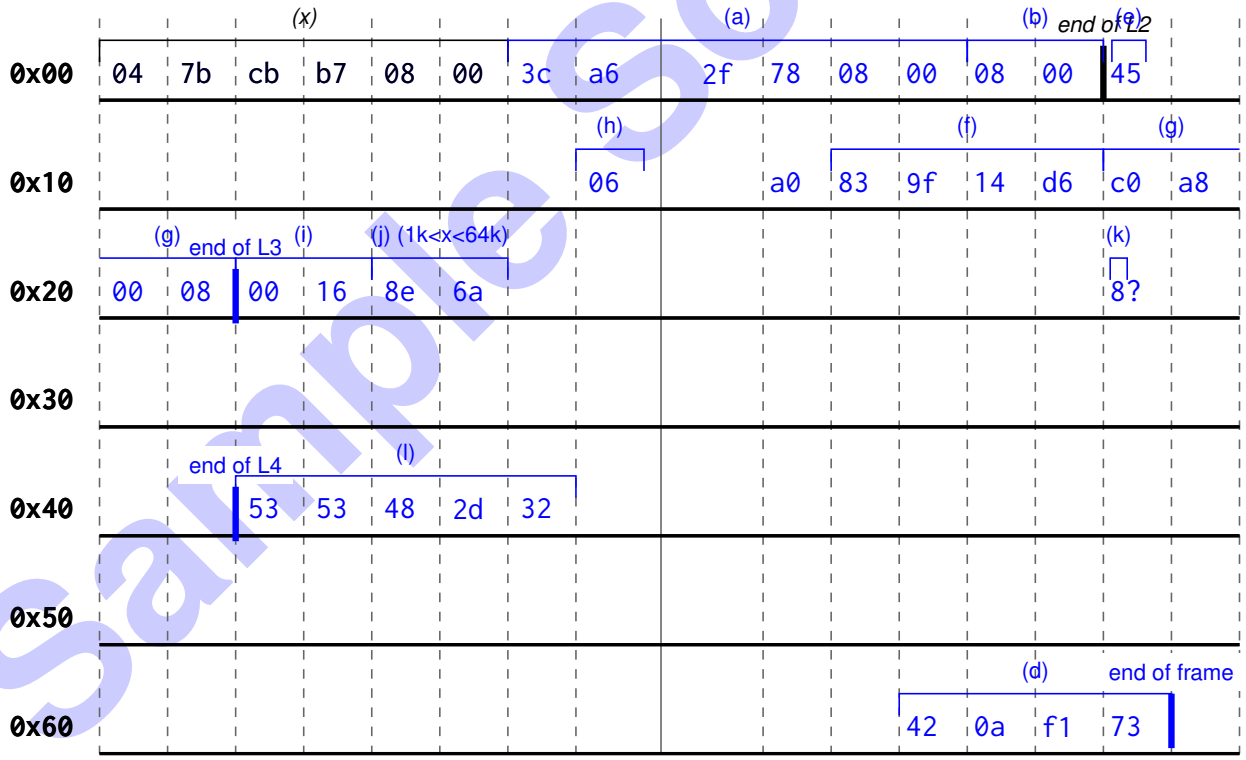


Figure 4.2: Preprint for the frame's hexdump

0

a)* Fill in the transmitter address of layer 2 in Figure 4.2.

b)* Fill in the value of the field specifying the type of the L3 PDU in Figure 4.2.

0
1

Sample Solution

Before we continue to fill out the hexdump, we want to mark the end of different headers. Assume that

- the L3 header does not use any options,
- the L4 header uses 12 B options, and
- the total frame length (including checksum) is 111 B.

c)* Mark **the end** of the **L3** and **L4 headers** as well as of the **frame iteself** in Figure 4.2. As an example, the end of the L2 header is already marked.

d) Fill in the frame check sequence given as `42 0a f1 73` in Figure 4.2.

We now start with filling in different fields of the L3 header. The start of the L3 header is already given in Figure 4.2. **Do not forget to mark to which subproblem your fill ins belong.**

e)* Fill in the field specifying type and length of the L3 header.

f)* Fill in the L3 source address.

g)* Fill in the L3 destination address.

h)* Fill in the value of the field specifying the type of the L3 SDU.

We now continue with filling in different fields of the L4 header. In case a value is not defined, make a reasonable assumption. **Do not forget to mark to which subproblem your fill ins belong.**

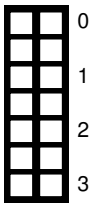
i) Fill in the source port.

j) Fill in the destination port.

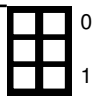
k) Fill in the value of the field specifying that offset in the L4 header.

Finally, we come the application layer of the frame's content which is the ASCII encoded string "`SSH-2.0-OpenSSH_9.2p1 Debian-2`".

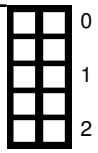
l) Fill in the first 5 B of the L7 PDU.



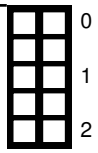
e)



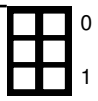
f)



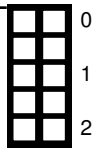
g)



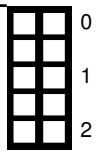
h)



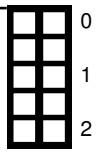
i)

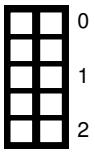


j)



k)





What is the purpose of this problem?

In this problem students show that they understood

- *how frames are made up of headers of different leayers,*
- *how the beginning/end and type of headers are determined, and*
- *how MAC and IP addresses are used for addressing.*

In addition, they demonstrate that they understood the purpose of MAC and IP addresses as well the basic concept of NAT.

The problem is an exact copy from the CNS Endterm 2023. The only difference is that we do not parse the given hexdump, but create the hexdump from information given in the problem statement.

Given the cheatsheet belonging to this exam, there is no need to remember any specific header layouts.

Sample Solution

Problem 5 DNS (13 credits)

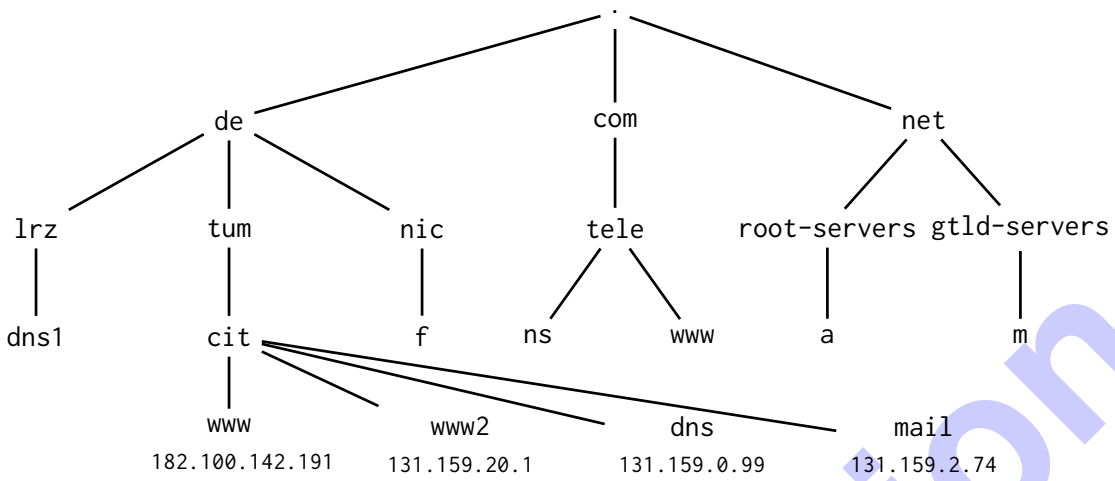


Figure 5.1: A part of the DNS.

0 1 a) Briefly describe the purpose of DNS.

The mapping between FQDN and IP addresses.

0 1 b) Briefly describe the difference between a fully and non-fully qualified domain name, also regarding their notation.

A fully qualified domain name starts at the root, denoted by the ".".
A non-fully qualified domain name starts at an intermediary node of the DNS.

Figure 5.1 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
 7  mail.cit.tum.de.      IN  A    131.159.2.74
 8  www2.cit.tum.de.      IN  A    131.159.20.1
 9  dns.cit.tum.de.       IN  A    131.159.0.99
10  www.cit.tum.de.       IN  A    182.100.142.191
11  cit.tum.de.           IN  MX    20 mail.cit.tum.de
12  cit.tum.de.           IN  NS    dns.cit.tum.de
```

Figure 5.2: DNS zone file on nameserver `dns.cit.tum.de`

0 1 2 3 c)* Add all other missing data in the zone file depicted in Figure 5.2 based on the information from Figure 5.1.

Sample Solution

d)* Distinguish a resolver from a nameserver.

0 1

A resolver is contacted by a client to query the DNS. The resolver then contacts the authoritative nameservers of the zones in order to extract the requested information.

e)* Briefly describe the purpose of a zone's SOA record.

0 1

The SOA (Start of Authority) record defines the root of the zone, as well as the authoritative nameserver.

f)* What does "authoritative" mean in the context of DNS?

0 1

An authoritative nameserver for a zone holds the zone records for this zone and answers queries it.

g)* Determine the PTR record of the address 11.42.43.12. You do not need to reason your answer.

0 1

`12.43.42.11.in-addr.arpa.`

h)* Describe the components of the url `https://www.cit.tum.de/webmail?user=user&pwd=pass`.

0 1 2

1. `https`: the protocol is TLS secured HTTP
2. `www.cit.tum.de`: domain name
3. `/webmail`: path requested on the server
4. `user=user&pwd=pass`: URL parameters / variables, probably a login

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

0 1 2

With recursive resolution, only one request for a resource record is made to a configured resolver, which returns the final response.
With iterative resolution, the FQDN is instead resolved starting at the root zone (or the last known SOA) by querying the authoritative name servers for the respective zones.Their answers contain either the FQDN of an authoritative name server of the next lower zone or the final resource record if the queried name server is authoritative for it.

Sample Solution

Problem 6 Side-Channel Information Stealing (16 credits)

You have breached the data center of a large cloud hosting provider. You intend to extract their private key of 4096 bit length. The key is derived from perfect, uniform randomness. As a very strict network policy is employed there is no way you will be able to do this via the network.
Therefore, you have come up with another way: The cloud hosting provider streams their data center via a live cam (24 frames per second), seemingly to show off their hardware. This stream includes a view of the hard drive activity LED of the relevant server. You can control the LED — and decide to extract the private key by encoding it through LED blink patterns, which you can decode by viewing the live stream.

0 1 2

a)* What is the maximum data rate achievable on the channel?

The LED has two states: on and off. Therefore, each frame shows one of two symbols. Each state therefore encodes $\log_2 2 = 1$ bit.
We can detect a different state with each new frame, therefore the maximum channel rate is 24 symbols per second.
This results in a maximum data rate of $r = 24\,\text{bit/s}$.

To properly detect the LED being on or off, a **pulse length of at least** 100 ms is needed.

0 1 2

b) What is the resulting transmission rate? How long does it take to transmit the private key?

We can transmit $\frac{1\,\text{s}}{100\,\text{ms}} = 10$ symbols per second, therefore have a transmission rate of 10 bit/s.
It takes $4096/10 \approx 409.6\,\text{s}$ to transmit the key.

There is still one problem remaining: you have to properly synchronize the transmission on sender and receiver side. To achieve this you decide to employ a new *8b11b* coding scheme. In this scheme, 8 bit of payload are coded to 11 bit of channel word. The coding transforms a byte to a channel word by prepending a start sequence, thereby marking the start of each channel word recognizeable. This start sequence is **three bits** long, and consists of all ones: **111**.
To not confuse frame starts with actual data, all left-most occurrences of `11` in the data are replaced with `110`. This process is called bit-stuffing. On the receiving side, this process is reversed, thus replacing `110` by `11`.
You can neglect any padding that would become necessary for all following sub tasks!

0 1 2 3

c)* Determine the expected length **increase** of the actual transmitted data. Note, that the bit-stuffing is done on the payload!

Let $k \in \{0,1\}^{4096}$ be uniformly random.
We define $X_i = \begin{cases} 1 & s_i s_{i+1} = 11 \quad \text{for } 1 \le i \le n-1 \\ 0 & \textit{else} \end{cases}$

The length increase is equal to $X = \sum_{i=1}^{n-1} X_i$

Thereby, $\mathbb{E}[X] = \mathbb{E}[\sum_{i=1}^{n-1} X_i] = \sum_{i=1}^{n-1} \mathbb{E}[X_i] = \sum_{i=1}^{n-1} \mathbb{P}[X_i = 1] = \sum_{i=1}^{n-1} \frac{1}{4} = \frac{n-1}{4} = 1023.75$

Sample Solution

If you were unable to solve subproblem c), use 1024 bit **as the expected length increase.**

d) Using the expected length increase, determine the expected code rate.

0 1 2

A frame start sequence of 3 bit is added for every octett.
Additionally, we have to stuff the 11 bit sequences, as determined prior.
Therefore:
Expected length: $L = 4096 + \lfloor \frac{4096}{8} \rfloor \cdot 3 + 1023.75 = 6655.75\,\text{bit}$
And by that:
$R = \frac{4096}{6655.75} \approx 0.62$

e)* Argue whether it is realistic to calculate the key by brute-force, rather than extracting it via the side-channel.

0 1

No, brute-forcing 4096 bit is not realistically doable, even given multiple years of time.

You decide that your current approach is too inefficient.

f) Propose an approach to reducing the overhead while maintaining the synchronization properties.

0 1

E. g. instead of using the 8b11b coding, we can use a 256b259b coding to synchronize sender and receiver. By doing so we reduce the overhead.

Sample Solution

While testing your approach you realize that there is still a $\frac{1}{200}$ chance left that you read a given bit **incorrectly**. Given this, you decide to add redundancy to your coding, extending the *8b11b* coding to the **8b11b_v2** coding. Again, each 8 bit long word of data is translated to 11 bit of channel word. In contrast to before, the coding scheme employed, which shall not be explained in detail, allows for synchronization **without** the use of special symbols. Bit-stuffing is therefore not longer necessary.

0 1 2

g) How long is the resulting data sent? Is this coding on average more efficient than the previous approach?

We have $\frac{4096}{8} = 512$ data words, which are translated to 512 channel words, each 11 bit long.
The total (constant) length therefore is $L_{new} = \frac{4096}{8} \cdot 11\,\text{bit} = 5632\,\text{bit}$
Therefore this approach is more efficient than the previous approach ($5632\,\text{bit} < 6655.75\,\text{bit}$).This is as we no longer require bit-stuffing.

The new coding additionally allows you to **detect and correct** one flipped bit in each **channel word**.

0 1 2 3

h) What is the probability Pr[incorrect] that the transmission cannot be decoded correctly?
Note: For this sub task, **round to four digits of accuracy**. You are allowed to calculate using rounded interim results

Let X_i be the number of flipped bits in channel word i.
We can recover the word correctly if zero or one bits flip. If two or more bits flip, the transmission is decoded incorrectly.
We continue with the channel words individually:
$\Pr[X_i = 0] = (1 - \frac{1}{200})^{11} \approx 0.9464$
$\Pr[X_i = 1] = (1 - \frac{1}{200})^{10} \cdot (\frac{1}{200})^{1} \cdot \binom{11}{1} \approx 0.0523$
Therefore $\Pr[\text{correct}] = \Pr[X_i = 0] + \Pr[X_i = 1] \approx 0.9987$
We cannot decode the data if one or more of the 512 channel words fail in decoding.
Therefore $\Pr[\text{incorrect}] = 1 - (\Pr[\text{correct}])^{512} \approx 1 - 0.5137 = 0.4863$
Note: without interim result rounding, the result is 0.4952!

Sample Solution

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

Sample Solution

Sample Solution