Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München

Hinweise zur Personalisierung:
- Ihre Prüfung wird bei der Anwesenheitskontrolle durch Aufkleben eines Codes personalisiert.
- Dieser enthält lediglich eine fortlaufende Nummer, welche auch auf der Anwesenheitsliste neben dem Unterschriftenfeld vermerkt ist.
- Diese wird als Pseudonym verwendet, um eine eindeutige Zuordnung Ihrer Prüfung zu ermöglichen.

Grundlagen Rechnernetze und Verteilte Systeme (GRNVS)

Modul:	IN0010	**Prüfer:**	Prof. Dr.-Ing. Georg Carle
Klausur:	Wiederholung	**Datum:**	Freitag, 30. September 2016, 15:30 – 17:00

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

Bearbeitungshinweise

- Diese Klausur umfasst
  - **19 Seiten** mit insgesamt **6 Aufgaben** sowie
  - eine beidseitig bedruckte **Formelsammlung**.

  Bitte kontrollieren Sie jetzt, dass Sie eine vollständige Angabe erhalten haben.
- Das Heraustrennen von Seiten aus der Prüfung ist untersagt.
- Mit * gekennzeichnete Teilaufgaben sind ohne Kenntnis der Ergebnisse vorheriger Teilaufgaben lösbar.
- **Es werden nur solche Ergebnisse gewertet, bei denen der Lösungsweg erkennbar ist.** Auch Textaufgaben sind **grundsätzlich zu begründen**, sofern es in der jeweiligen Teilaufgabe nicht ausdrücklich anders vermerkt ist.
- Schreiben Sie weder mit roter / grüner Farbe noch mit Bleistift.
- Die Gesamtpunktzahl in dieser Prüfung beträgt 85 Punkte.
- Als Hilfsmittel sind zugelassen:
  - ein **nicht-programmierbarer Taschenrechner**
  - ein **analoges Wörterbuch** Deutsch ↔ Muttersprache **ohne Anmerkungen**
- Schalten Sie alle mitgeführten elektronischen Geräte vollständig aus, verstauen Sie diese in Ihrer Tasche und verschließen Sie diese.

Aufgabe 1 **Kurzaufgaben (20 Punkte)**

Die nachfolgenden Teilaufgaben sind jeweils unabhängig voneinander lösbar.

0 1 2

a)* Nennen Sie zwei wesentliche Dienste, welche von der Sicherungsschicht des ISO / OSI Modells erbracht werden.

Steuerung des Medienzugriffs (unter welchen Umständen darf ein Knoten senden)
Next-Hop Adressierung (Adressierung innerhalb einer Broadcast Domain auf Basis physikalischer Adressen)

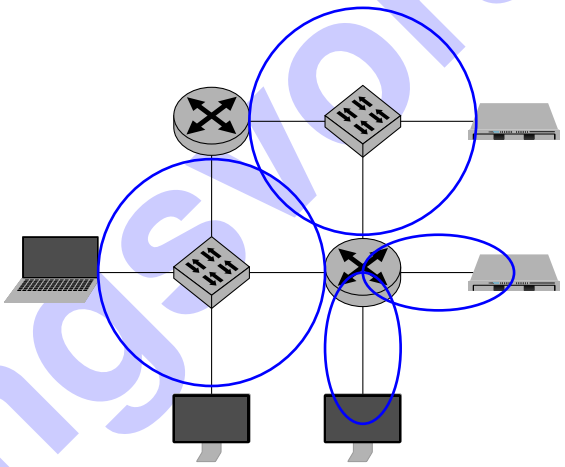
0 1

b)* Gegeben sei das 64 bit lange Datum `0x0123456789abcdef` in Network Byte Order. Wie lautet die Darstellung in Big Endian?

`0x0123456789abcdef`, da Network Byte Order bereits Big Endian entspricht.

0 1

c)* Gegeben sei das folgende Netzwerk. Zeichnen Sie alle Broadcastdomänen ein.



0 1

d)* Erläutern Sie den wesentlichen Vorteil von OSPF gegenüber RIP.

OSPF hat genaue Informationen über die Netztopologie, wodurch Schleifen auf Schicht 3 ausgeschlossen werden.

0 1

e)* Was versteht man unter *Classless Interdomain Routing*?

Die flexible Aufteilung (bzw. Aggregation) von IP-Subnetzen mittels Subnetzmasken (bzw. durch Angabe der Präfixlänge).

f)* Worin besteht der Unterschied zwischen einem Resolver und einem autoritativen Nameserver?

0 1

Ein Resolver löst beliebige DNS-Anfragen ggf. durch Weiterleitung an einen anderen Resolver (rekursive Namensauflösung) oder iterative Anfragen an die zuständigen Nameserver auf.
Ein autoritativer Nameserver beantwortet Anfragen nur für solche Zonen, für die er autoritativ ist.

g)* Begründen Sie, ob sich ein Resolver im selben Subnetz wie der anfragende Client befinden muss.

0 1

Nein, da Resolver auf Schicht 3/4 adressiert werden (IP + UDP/TCP 53).

h)* Bestimmen Sie die IP-Adresse zum Reverse-FQDN `60.50.66.128.in-addr.arpa.`.

0 1

128.66.50.60

i)* Damit ein Server eingehende UDP-Datagramme auf einem bestimmten Port liest, sind die Systemaufrufe `socket()`, `bind()` und `recvfrom()` erforderlich. Erläutern Sie kurz die Funktion der drei Systemaufrufe.

0 1 2

`socket()` erzeugt einen neuen Socket vom angegebenen Typ.
`bind()` assoziiert den Socket mit einer (oder allen) IP-Adressen des Servers sowie mit einem bestimmten Port.
`recvfrom()` versucht Daten vom Socket zu lesen und speichert Informationen über den jeweiligen Absender (IP-Adresse und Portnummer) in einer entsprechenden Datenstruktur.

j)* Bestimmen Sie den Faktor, um den sich die Größe des IPv6-Adressraums gegenüber dem IPv4-Adressraum unterscheidet.

0 1

$$\frac{\text{Anzahl IPv6-Adressen}}{\text{Anzahl IPv4-Adressen}} = \frac{2^{128}}{2^{32}} = 2^{96}$$

k)* Worin besteht der Unterschied zwischen privaten IPv4 Adressen und Link Local Adressen bei IPv6?

0 1

Private IPv4-Adressen sind innerhalb einer Gruppe von Netzen routebar, solange sie in diesen Netzen eindeutig sind (z. B. zwischen verschiedenen Netzen einer Firma).
Link Local Adressen sind ausschließlich innerhalb einer Broadcastdomäne gültig und grundsätzlich nicht routebar.
(Alternative: Link Local Adressen werden mittels SLAAC zustandslos vergeben während private IPv4 Adressen entweder statisch oder mittels DHCP Server zugewiesen werden müssen.)

0
1

l)* Worin besteht der Unterschied zwischen *Interior* und *Exterior Gateway Protokollen* hinsichtlich ihrer Verwendung?

IGPs sind eine Klasse von Routingprotokollen, welche innerhalb eines autonomen Systems verwendet werden (z. B. RIP, OSPF, IS-IS).
EGPs werden zum Austausch von Routinginformationen zwischen unterschiedlichen autonomen System verwendet (einziges praktisches Beispiel ist BGP).

0
1
2

m)* Geben Sie **zwei** Gründe an, warum moderne IEEE 802.3-Netzwerke kollisionsfrei arbeiten.

Moderne Netze sind i. d. R. vollständig geswitcht, d. h. innerhalb einer Kollisionsdomäne befinden sich höchstens ein Host sowie der jeweilige Switchport.
Da die Netze zudem Full-Duplex erlauben, kann gleichzeitig gesendet und empfangen werden.

0
1
2

n)* Gegeben sei ein Übertragungskanal der Bandbreite 20 MHz. Berechnen Sie die maximal erzielbare Datenrate bei einem Signal-Rausch-Abstand von 30 dB.

$$
\begin{aligned}
30\,\mathrm{dB} = 10\log_{10}(\mathrm{SNR}) \quad &\Rightarrow \quad \mathrm{SNR} = 10^3 \\
r_{\max} &= B\log_2(1+\mathrm{SNR})\,\mathrm{bit} \\
&= 20\cdot 10^6\,\mathrm{Hz}\log_2(1001)\,\mathrm{bit} \\
&\approx 199.34\,\frac{\mathrm{Mbit}}{\mathrm{s}}
\end{aligned}
$$

0
1
2

o)* Gegeben sei ein Alphabet mit insgesamt 64 unterschiedlichen Zeichen deren Auftrittswahrscheinlichkeit gleichverteilt ist. Begründen Sie, ob die durchschnittliche Codewortlänge bei Nutzung des Huffman-Codes größer, gleich oder kleiner 7 bit ist.

Da die Auftrittswahrscheinlichkeit der Zeichen gleichverteilt ist, haben alle Codewörter dieselbe Länge. Es entsteht ein vollständiger Binärbaum der Höhe $\log_2(64) = 6$, womit auch die durchschnittliche Codewortlänge kleiner 7 bit ist.

Aufgabe 2 Packet Pair Probing (11 Punkte)

Gegeben sei das in Abbildung 2.1 dargestellte Netzwerk. Knoten 1 und 4 sind mit ihren Routern jeweils über ein fullduplex-fähiges Netzwerk verbunden. Die symmetrischen Datenraten auf den Links betreagen r_{12} bzw. r_{34} Die Verbindung zwischen Knoten 2 und 3 ist bedeutend langsamer, d. h. $r_{23} < r_{12}, r_{34}$. Die beiden Distanzen d_{12} und d_{23} seien im Verhältnis zu d_{23} vernachlässigbar klein.

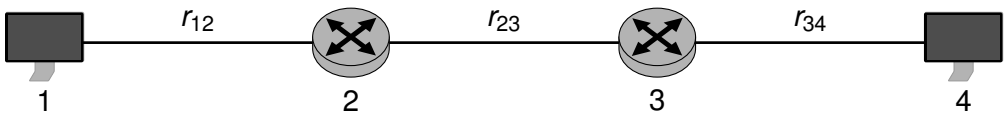


Abbildung 2.1: Vereinfachte Netztopologie

Knoten 1 soll die Datenrate r_{23} bestimmen, so dass möglichst wenig Last auf der ohnehin langsamen Verbindung entsteht. Dabei sei angenommen, dass alle Knoten über einen gewöhnlichen IP-Stack verfügen und ICMP Pakete zwischen Knoten 1 und 4 ausgetauscht werden können.

a)* Geben Sie die Serialierungszeit und Ausbreitungsverzögerung zwischen zwei benachbarten Knoten i und j in Abhängigkeit der Paketgröße p, Datenrate r_{ij} und Distanz d_{ij} an.

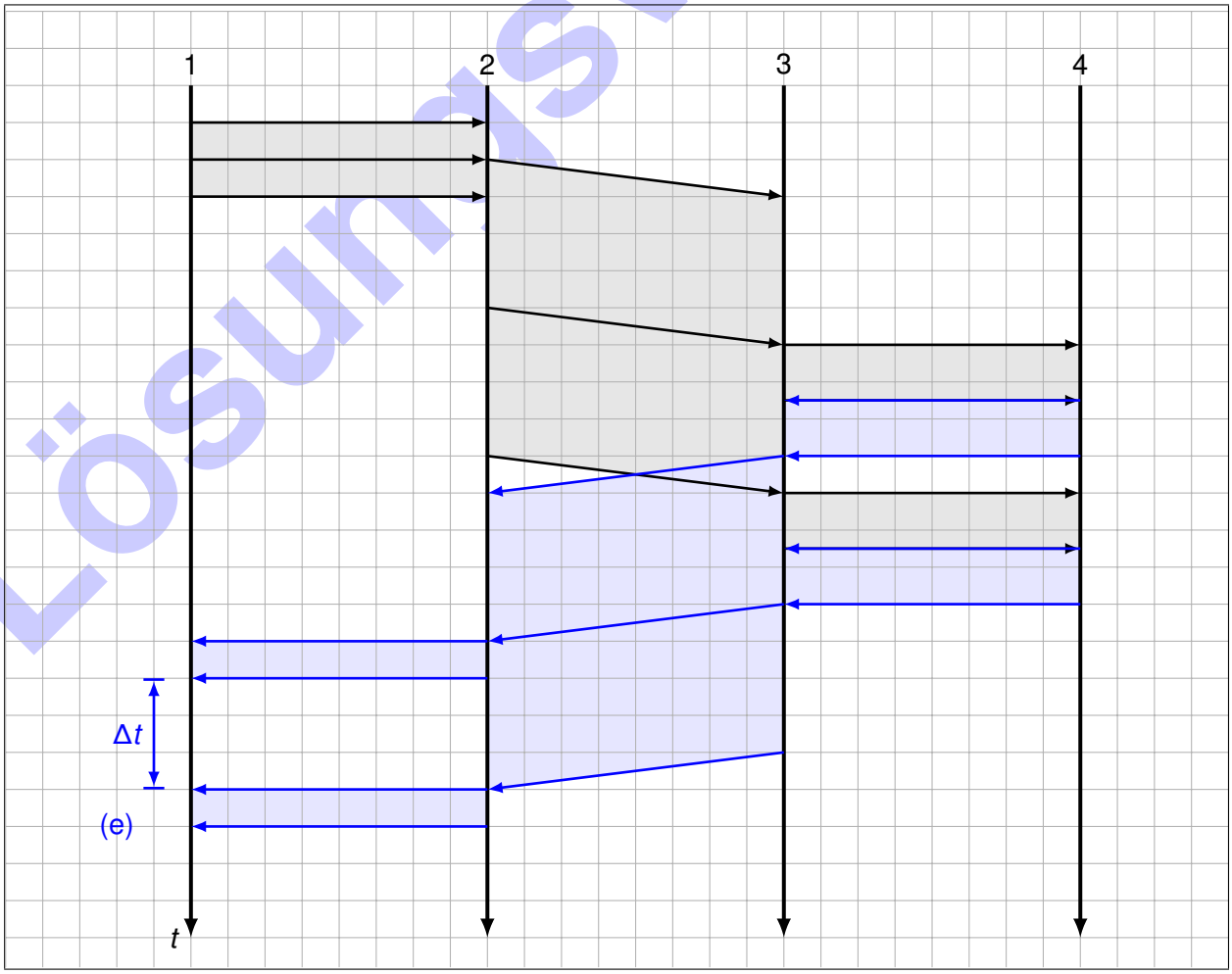
0
1

$$t_s(i,j) = \frac{p}{r_{ij}} \qquad t_p(i,j) = \frac{d_{ij}}{\nu c}$$

Knoten 1 sende nun unmittelbar nacheinander zwei ICMP-Echo-Requests der Länge p an Knoten 4. Dabei sei p genau so groß gewählt, dass entlang des Pfads zu Knoten 4 keine Fragmentierung notwendig ist. Knoten 4 wird auf jeden Echo Request mit einem Echo Reply derselben Größe p antworten. Vereinfachend seien Verarbeitungszeiten an den Knoten zu vernachlässigen.

b)* Ergänzen Sie das im Lösungsfeld abgebildete Weg-Zeit-Diagramm.
Hinweis: Bei Bedarf finden Sie am Ende der Prüfung einen Ersatzvordruck.

0
1
2
3



Durch die geringe Übertragungsrate zwischen Knoten 2 und 3 entsteht an Knoten 1 eine Empfangspause Δt. Diese kann von Knoten 1 gemessen und zur Bestimmung der gesuchten Übertragungsrate zwischen Knoten 2 und 3 verwendet werden.

0 1

c) Markieren Sie Δt in Ihrer Lösung von Teilaufgabe b).

d) Von welchen Größen hängt Δt ab, falls $r_{34} \geq r_{23}$ gilt.

0 1

p, r_{12} und r_{23}

0 1 2

e) Begründen Sie, was sich im Vergleich zur vorherigen Teilaufgabe ändern würde, falls $r_{34} < r_{23}$ gilt.

Für $r_{34} < r_{23}$ limitiert die Serialisierungszeit an Knoten 4 anstatt an Knoten 3, weswegen Δt unabhängig von r_{23} und abhängig von r_{34} wird,

0 1 2

f) Bestimmen Sie Δt allgemein für $r_{23} < r_{12}, r_{34}$. Vereinfachen Sie das Ergebnis soweit wie möglich.

$$\Delta t = t_s(2,3) - t_s(1,2) = p\left(\frac{1}{r_{23}} - \frac{1}{r_{12}}\right)$$

0 1

g) Geben Sie einen Ausdruck für die gesuchte Datenrate r_{23} an. Vereinfachen Sie das Ergebnis soweit wie möglich.

Umstellen des Ergebnisses aus Teiaufgabe f):

$$r_{23} = \frac{p}{\Delta t + \frac{p}{r_{12}}}$$

Aufgabe 3 IP-Fragmentierung (24 Punkte)

Wir betrachten das Netzwerk aus Abbildung 3.1. PC1 und PC2 kommunizieren mittels IPv4 über die beiden Router R1 und R2 miteinander.

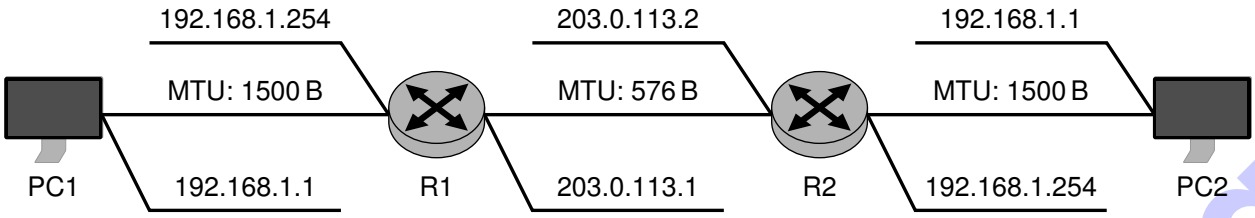


Abbildung 3.1: Netztopologie und MTU der einzelnen Abschnitte

Die drei Netzsegmente sind voneinander unabhängig und verwenden verschiedene Übertragungsverfahren auf den Schichten 1 und 2, so dass sich die in der Abbildung ersichtlichen MTUs ergeben.

a)* Erläutern Sie allgemein den Unterschied zwischen MTU und MSS.

0 1 2

Die MTU ist die maximale Größe einer L3-PDU (IP-Packet inkl. Header), welche auf Schicht 2 übertragen werden kann.
MSS hingegen ist die maximale Grösse eines TCP-Datensegments (Schicht 4, ohne Header), so dass die MTU nicht überschritten wird.

b) Wie sollte im Allgemeinen die MSS für TCP in Abhängigkeit von der MTU gewählt werden (Begründung oder Rechnung)?

0 1

MSS = MTU – TCP-Header – IPv4-Header = MTU – 40 B

c)* Begründen Sie, ob ein bereits fragmentiertes Paket nochmals fragmentiert werden kann.

0 1 2

Ja, wenn das DF Flag nicht gesetzt ist und eine Mindestpayloadgröße von 8 B nicht unterschritten wird .
Die Zuordnung erfolgt über Identifier und Fragment Offset .

0 1 2

d)* Erläutern Sie, an welcher Stelle im Allgemeinen Fragmente wieder reassembliert werden können.

Nur am Destination Host , da Fragmente unabhängig voneinander geroutet werden und im Allgemeinen erst am Empfänger wieder zusammentreffen.

0 1 2

e)* Wie erkennt der Empfänger, dass ein Paket ein Fragment eines größeren Pakets ist?

1. Der Fragment Offset 0 **und** das MF Bit ist gesetzt, oder
2. Der Fragment Offset $\neq 0$

0 1 2

f)* Was geschieht auf Schicht 3, wenn ein oder mehrere Fragmente nicht ankommen?

Alle Fragmente des betreffenden Pakets werden verworfen (und eine entsprechende ICMP Fehlermeldung an den Sender geschickt).
Eine erneute Übertragung findet **nicht** automatisch statt. Diese muss ggf. von höheren Schichten veranlasst werden.

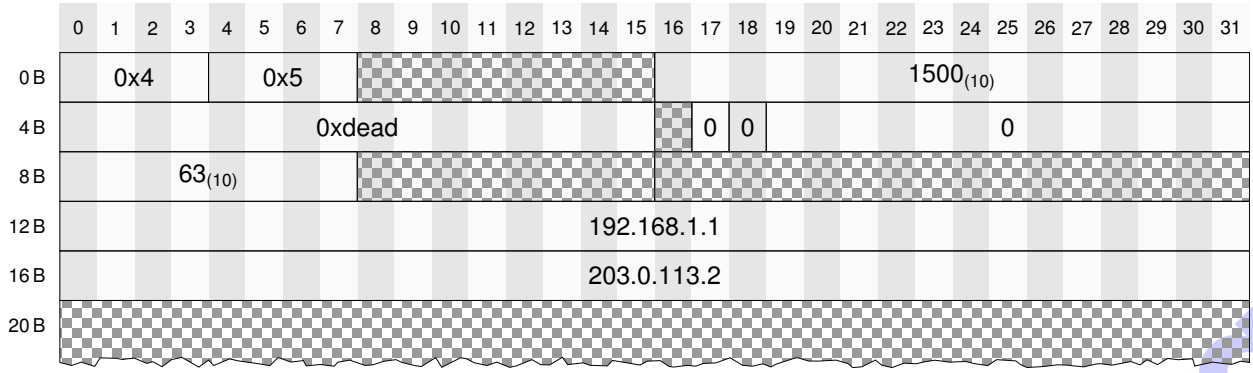


Abbildung 3.2: Darstellung des von PC1 in Richtung PC2 gesendeten IP-Pakets

Im Folgenden soll die Übertragung des in Abbildung 3.2 dargestellten IP-Pakets mit allen notwendigen Zwischenschritten nachvollzogen werden. Nutzen Sie bei Bedarf die auf dem Cheatsheet abgebildeten Protokoll-Header.

g)* Begründen Sie kurz, weswegen PC1 203.0.113.2 als Ziel-Adresse nutzt.

0 1

PC2 befindet sich in einem privaten Adressbereich, der im Allgemeinen nicht über öffentliche Netze erreichbar ist. R2 stellt NAT bereit.

h)* An welcher Stelle im Netz wird das von PC1 gesendete Paket fragmentiert?

0 1

An R1, da der Link zwischen R1 und R2 eine MTU kleiner 1500 B aufweist.

i)* Weswegen muss das erste Fragment eine Länge von 572 B anstatt der erwarteten 576 B aufweisen?

0 1 2

Der Link zwischen R1 und R2 erlaubt erlaubt eine maximale Größe von 576 B inkl. IP-Header bzw. 556 B ohne IP-Header.
Da das Fragment Offset nachfolgender Fragmente allerdings in Vielfachen von 8 B angegeben wird und 556 nicht ohne Rest durch 8 teilbar ist, muss auf das nächste kleinere Vielfache von 8 abgerundet werden.

0
1
2

j)* Bestimmen Sie die Gesamtgröße sowie Größe der Payload für alle Fragmente.

Fragment #	L3-PDU	L3-SDU	verbleibende Payload	Fragment Offset
1	572 B	552 B	928 B	0 B
2	572 B	552 B	376 B	552 B
3	396 B	376 B	0 B	1104 B

0
1
2
3
4

k) In Abbildung 3.3 sind Vordrucke für die IPv4-Header der einzelnen Fragmente gegeben. Füllen Sie die Vordrucke vollständig aus. Sollte ein Feld nicht eindeutig festgelegt sein, treffen Sie eine sinnvolle Wahl. **Hinweis:** Es sind möglicherweise mehr Vordrucke als notwendig vorhanden.

0
1

l)* Welche Veränderung wurde bei der Fragmentierung mit IPv6 vorgenommen?

Die Fragmentierung findet bei IPv6 grundsätzlich lokal beim Absender statt. Hierzu wird ein zusätzlicher Extension Header verwendet.

0
1
2

m) Aus welchem Grund ist die in Teilaufgabe l) angegebene Veränderung sinnvoll?

Erhöhte Effizienz, da so der Absender einmal die minimale MTU bestimmen muss und fortan ausreichend kleine Pakete senden kann anstelle jedes einzelne Paket von dazwischenliegenden Routern fragmentieren zu lassen. Durch Extension Header steigt die Effizienz wenn nicht fragmentiert werden muss.

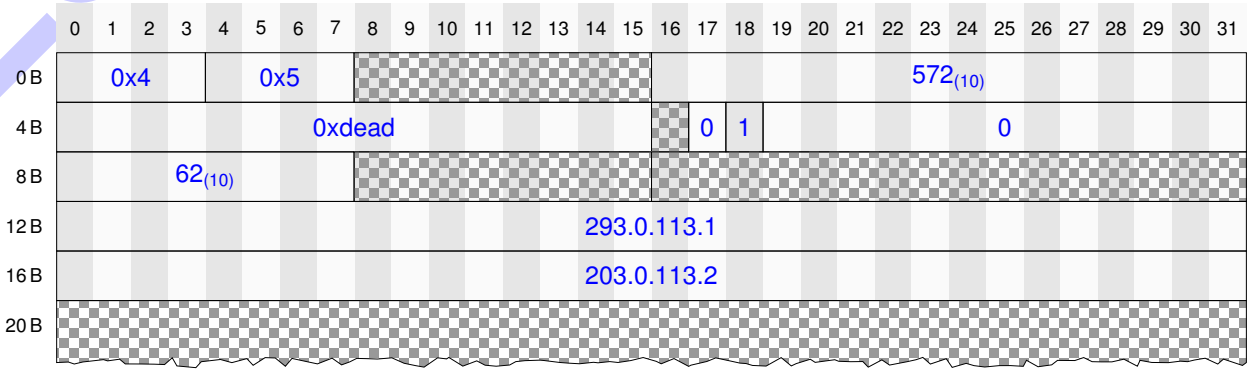


Abbildung 3.3: Vordrucke für Teilaufgabe k)

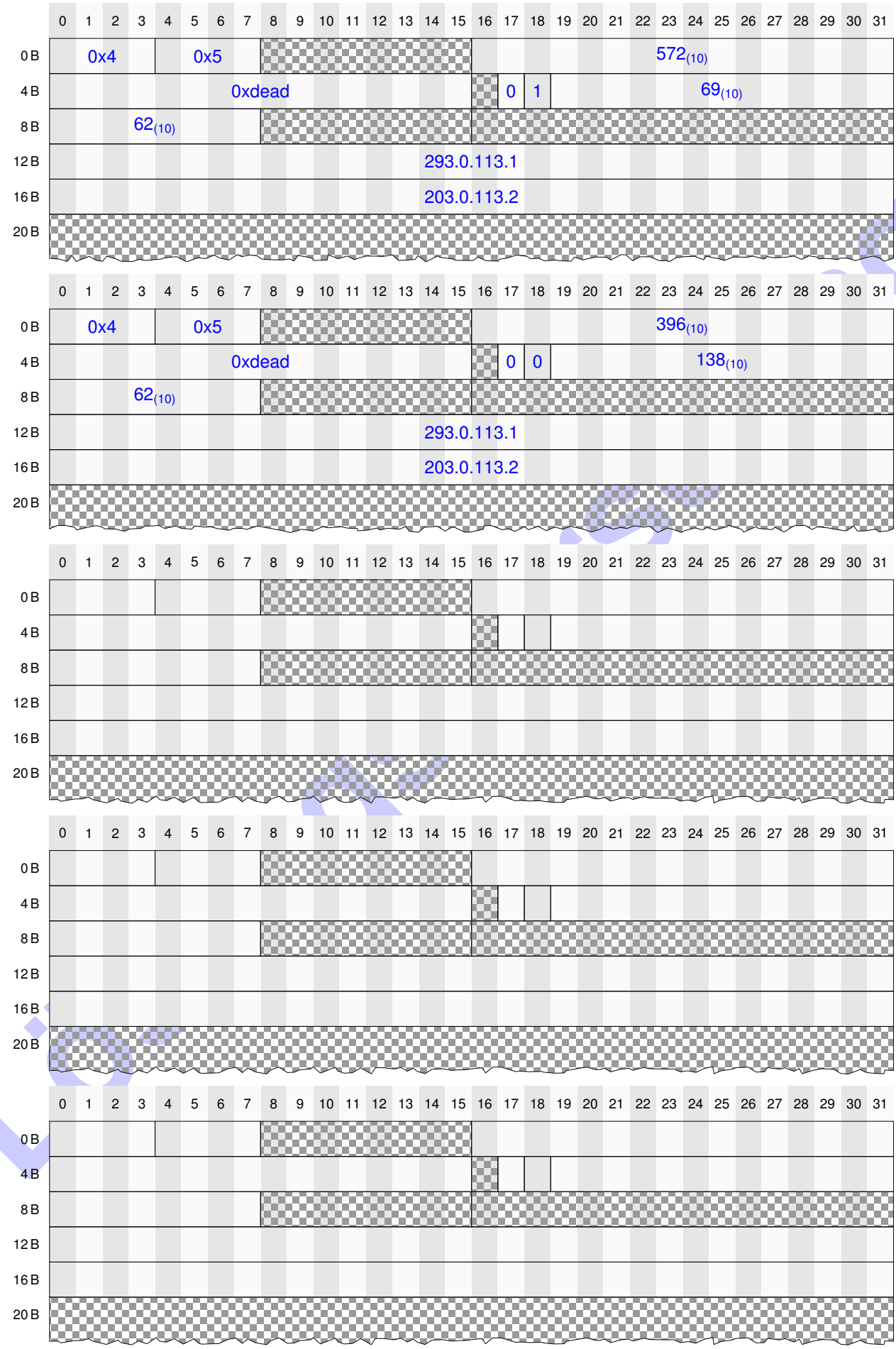
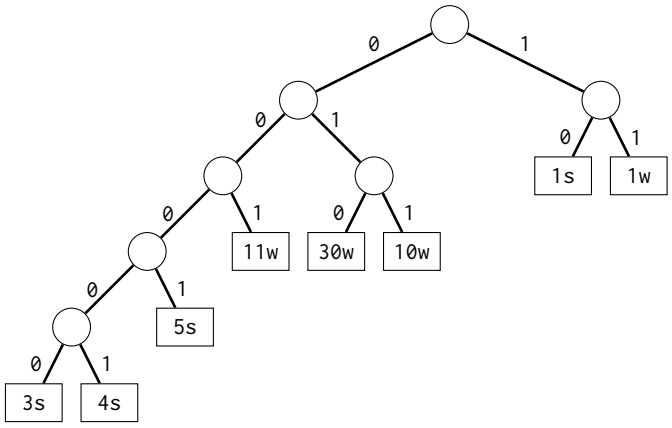


Abbildung 3.3: Vordrucke für Teilaufgabe k) (Fortsetzung)

Aufgabe 4 Datenkompression (10 Punkte)

In dieser Aufgabe betrachten wir eine vereinfachte Version des ITU T.30-Protokolls, besser bekannt als Telefax („Fax“). Dieses verwendet eine Kombination aus Huffman-Code und Lauflängenkodierung (RLE). Der zugehörige Huffman-Baum ist in Abbildung 4.1a dargestellt. Abbildung 4.1b stellt das Codebuch dar, welches die binären Huffman-Codewörter (in Teilaufgabe b) zu bestimmen) auf RLE-Codewörter abbildet.



(a) Huffman-Baum

RLE	Huffman-Codewort
1s	10
1w	11
30w	010
10w	011
11w	001
5s	0001
4s	00001
3s	00000

(b) Codebuch

Abbildung 4.1: Huffman-Baum und Codebuch

0 1 2

a)* Erklären Sie kurz den Aufbau des Huffman-Baums aus Abbildung 4.1a.

Die zu kodierenden Zeichen sind die Blätter des Baums, welche gemäß ihrer Auftrittswahrscheinlich zu Teilbäumen zusammengefasst werden. Die Differenzen der Gewichte (Summe der Wahrscheinlichkeiten aller Blätter) innerer Knoten des Baums in derselben Tiefe ist minimal.
Der Pfad von der Wurzel zu einem Blatt beschreibt Codewort, wobei die einzelnen Bitstellen von den Kanten des Baums abgelesen werden können. Häufiger auftretende Zeichen erhalten kürzere Codewörter, d. h. stehen weiter oben im Baum.

0 1 2

b) Vervollständigen Sie das Codebuch in Abbildung 4.1b.

Sie erhalten die in Abbildung 4.2 dargestellte binäre Nachricht. Diese ist zunächst mittels Huffman kodiert.

```
0100100100110000111000101100110111011101111
1100110011011101110111011101110011001101110111
1110111001100110110000011101110011010010010
```

Abbildung 4.2: Empfangene Nachricht als binärer Datenstrom

0 1 2 3

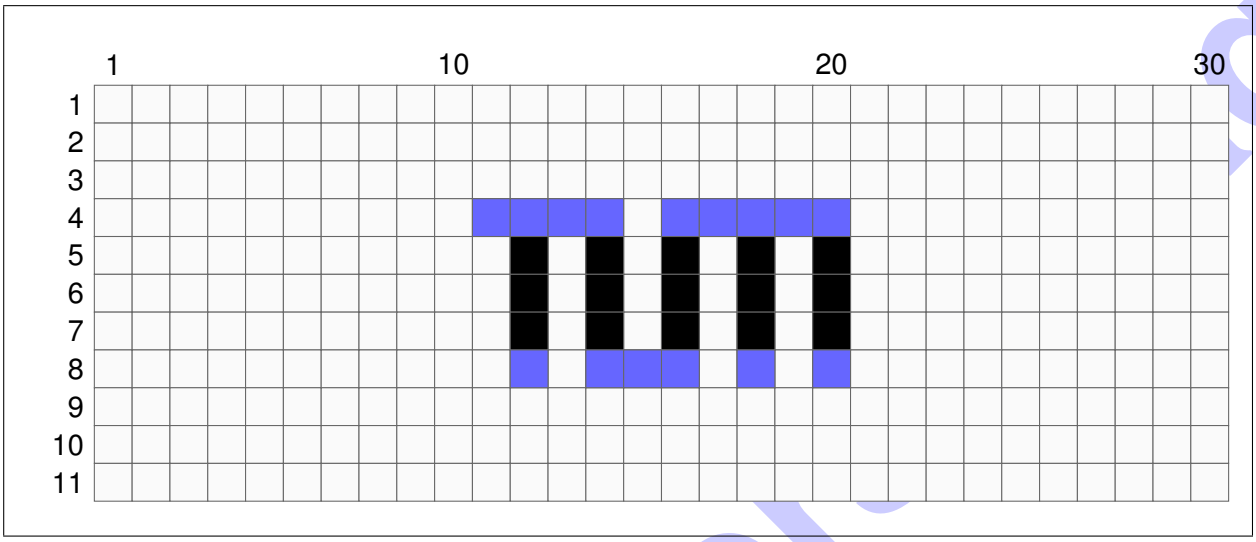
c) Geben Sie die zu den **schwarz** gedruckten Teilen des Datenstroms zugehörigen RLE-Codewörter an.
Hinweis: Das erste Bit des zweiten schwarz gedruckten Blocks stellt den Beginn eines Huffman-Codeworts dar.

```
30w 30w 30w 10w 4s 1w 5s 10w
11w 1s 1w 3s 1w 1s 1w 1s 10w 30w 30w 30w
```

Die RLE-Codewörter wiederum sind stets nach dem Schema `<Zahl><w|s>` aufgebaut. Ein RLE-Codewort gibt die Anzahl innerhalb einer Zeile aufeinander folgender weißer (`w`) oder schwarzer (`s`) Pixel an, wodurch zeilenweise eine Pixeldarstellung der Nachricht entsteht.

d) Vervollständigen Sie die Pixeldarstellung der Nachricht. 0 1 2
Hinweise:

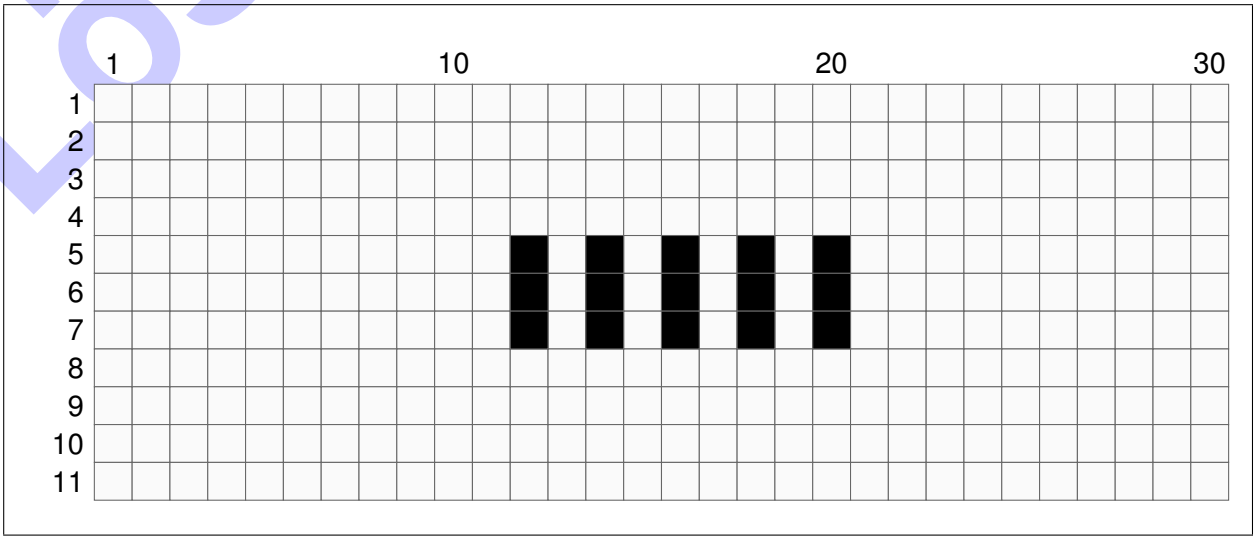
- Die Zeilen 5 – 7 entsprechen dem ausgegrauten Teil der Nachricht aus Abbildung 4.2.
- Bei Bedarf finden Sie am Ende der Aufgabe einen weiteren Vordruck.



e)* Um welchen Faktor ist die unkomprimierte Nachricht, bei der jedes Pixel binär kodiert wird (`0` = schwarz, `1` = weiß), länger als die so komprimierte Nachricht? 0 1
Hinweis: Die komprimierte Nachricht aus Abbildung 4.2 hat eine Gesamtlänge von 127 bit.

$$\eta = \frac{11 \cdot 30\,\text{bit}}{127\,\text{bit}} \approx 2.60$$

Zusätzlicher Vordruck für Teilaufgabe d). Streichen Sie ungültige Lösungen deutlich!



Aufgabe 5 Drahthai (13 Punkte)

Gegeben sei der in Abbildung 5.1 dargestellte Hexdump in Network-Byte-Order des Beginn eines Ethernet-Rahmens, welcher im Folgenden analysiert werden soll.

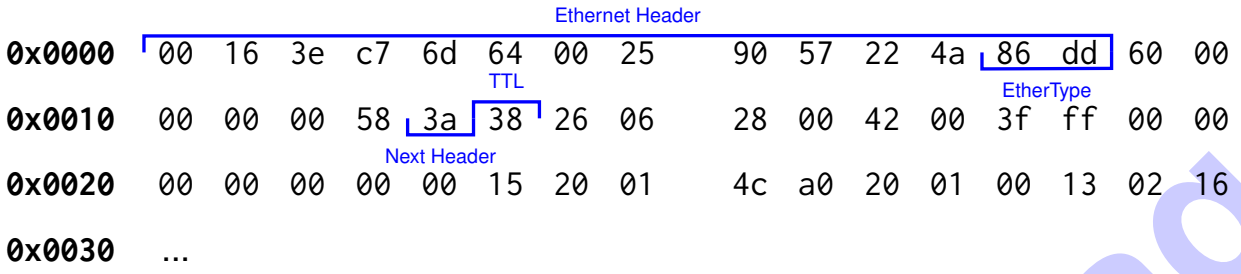


Abbildung 5.1: Hexdump eines Ethernet-Rahmens in Network-Byte-Order

Hinweis: Zur Lösung der Aufgabe sind Informationen von dem zusätzlich ausgeteilten Hilfsblatt notwendig.

0 1 a)* Markieren Sie in Abbildung 5.1 Beginn und Ende des Ethernet-Headers.

b) Begründen Sie, welches Protokoll auf Schicht 3 verwendet wird.

0 1

Ethertype `0x86dd` steht für IPv6.

c) Bestimmen Sie die Länge des Headers auf Schicht 3 (Begründung).

0 1

feste Headerlänge bei IPv6 von 40 Byte.

d) Geben Sie – sofern im Paket enthalten – TTL bzw. Hop Limit in dezimaler **und** hexadezimaler Schreibweise an.

0 1

TTL ist `0x38` = 56

e) Geben Sie die Absenderadresse der Schicht 3 in der üblichen Schreibweise an.

0 1

2606:2800:4200:3fff::15 (komprimiert)

f) Woran ist zu erkennen, dass die Payload des Pakets zu ICMPv6 gehört?

0 1

NextHeader ist `0x3a` = ICMPv6.

Wir betrachten von nun an die in Abbildung 5.2 dargestellte Payload des Pakets. Von dieser sei bekannt, dass es sich um ICMPv6 handelt.

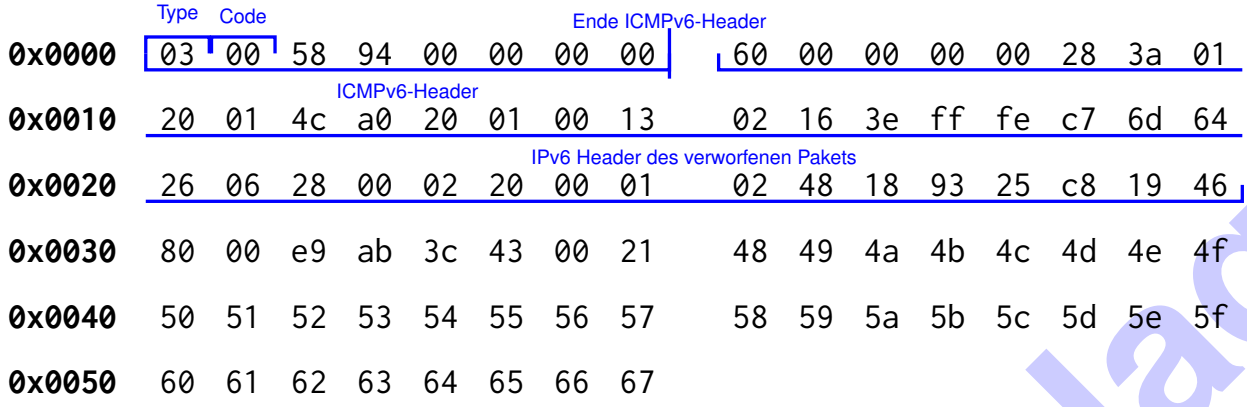


Abbildung 5.2: ICMPv6-Nachricht inklusive ICMPv6-Header in Network-Byte-Order

g)* Bestimmen Sie Typ und Code der ICMP-Nachricht.

0 1

Time Exceeded / Hop limit exceeded in transit

h) Wodurch wird eine solche Nachricht hervorgerufen?

0 1

Wenn ein Router ein Paket mit TTL=1 (bzw. bei IPv6 mit HopCount 1) erhält, welches weitergeleitet werden soll, so wird dieses verworfen und stattdessen ein Time Exceeded / Hop limit exceeded in transit an den ursprünglichen Absender des verworfenen Pakets zurückgeschickt.

i)* Markieren Sie das Ende des ICMP-Headers in Abbildung 5.2.

0 1

j) Erläutern Sie, was die Payload einer solchen Nachricht grundsätzlich enthält.

0 1 2

Die Payload enthält den IP-Header sowie die ersten 8 B der L3-SDU desjenigen Pakets, welches die ICMP TTL Exceeded Nachricht ausgelöst hat.

k)* Das Paket wurde im Rahmen eines Traceroutes aufgezeichnet. Erklären die kurz die Funktionsweise von Traceroute.

0 1 2

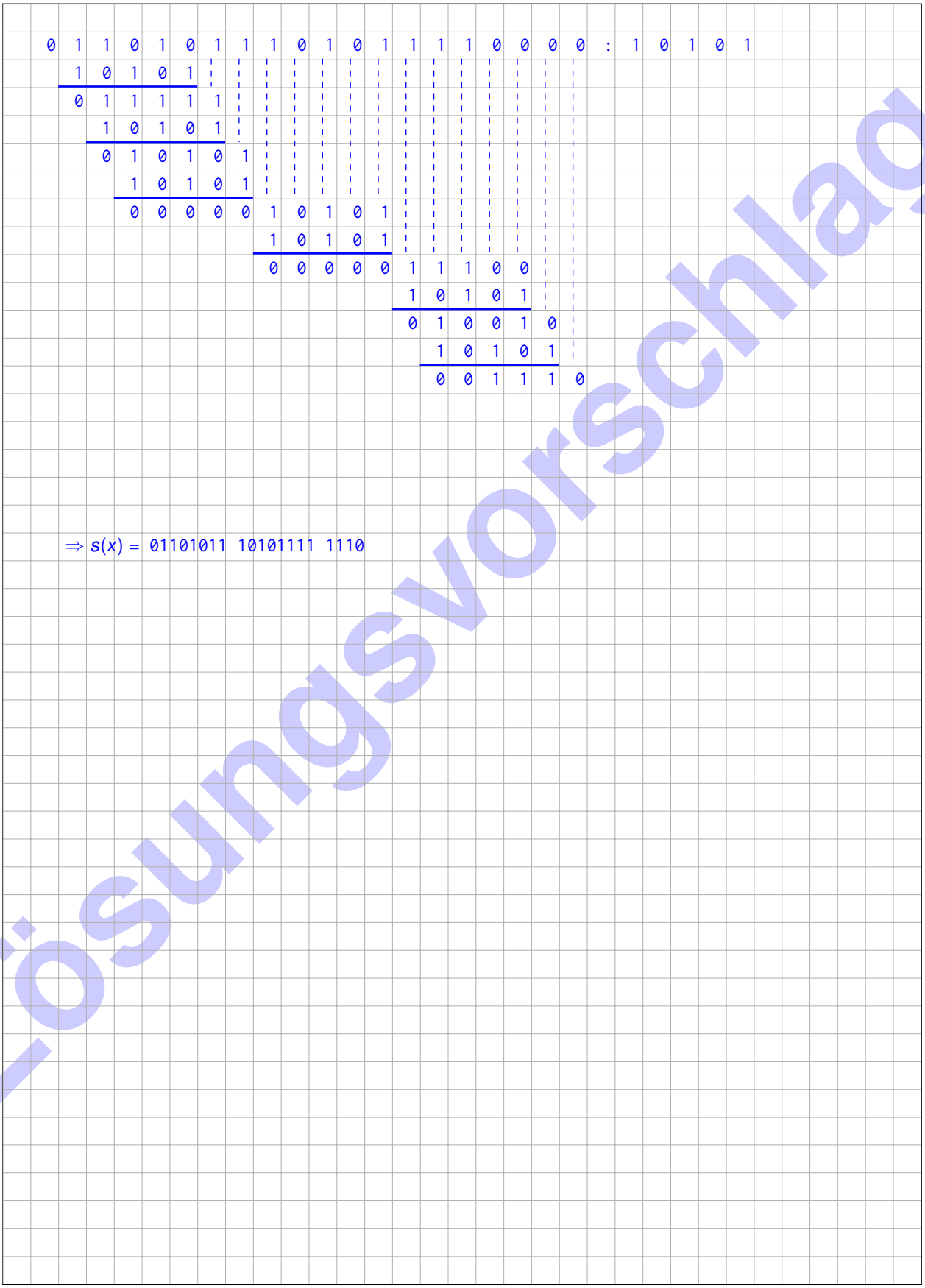
Es werden Pakete mit aufseigendem Hop Limit versendet, welche dann von den Routern verworfen werden. Hierbei werden HL Exceeded ICMP-Nachrichten versendet. An Hand der Absender Adressen der HL Exceeded ICMP-Nachrichtkann somit der „Weg“ des Pakets im Netz nachvollzogen werden.

Aufgabe 6 CRC (7 Punkte)

In dieser Aufgabe soll die zwei Oktette lange Nachricht `01101011 10101111` mittels des in der Vorlesung vorgestellten CRC-Verfahrens gesichert werden. Das Reduktionspolynom sei $r(x) = x^4 + x^2 + 1$.

0 1 2 3 4

a)* Bestimmen Sie die gesicherte Nachricht $s(x)$.



b)* Bei der Übertragung trete nun das Fehlermuster `00000000 00101010 0000` auf. Zeigen oder begründen Sie, ob der Fehler erkannt wird.

0 1 2

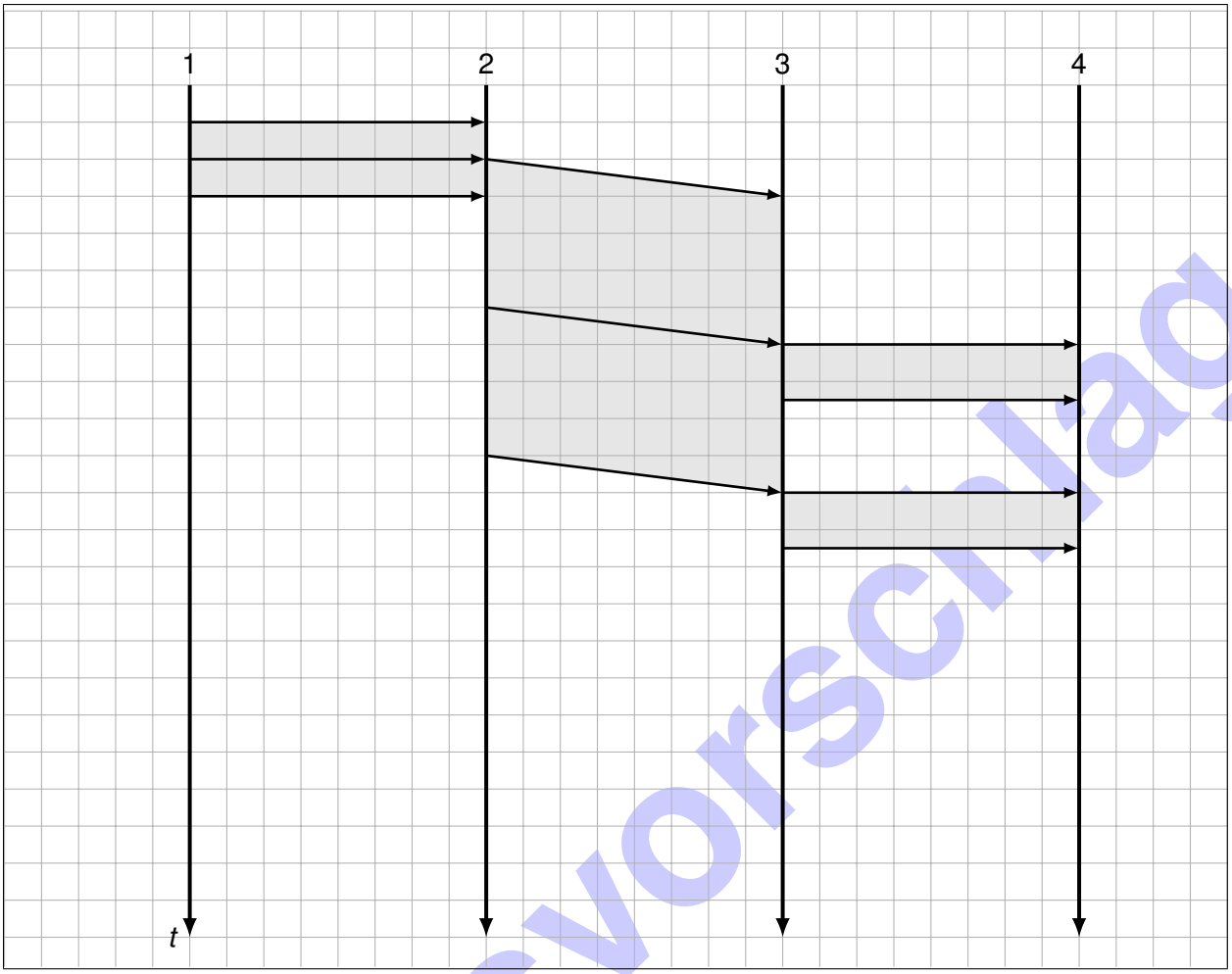
Der Fehler $e(x) = r(x)x^6$ ist ein Vielfaches des Reduktionspolynoms, weswegen der Fehler nicht erkannt werden kann.

c)* Erläutern sie kurz, welche Fehler mittels CRC korrigiert werden können.

0 1

Keine. CRC ist ein fehlererkennender Code.

Zusätzlicher Vordruck für Aufgabe 2:



Zusätzlicher Platz für Lösungen. Markieren Sie deutlich die Zuordnung zur jeweiligen Teilaufgabe. Vergessen Sie nicht, ungültige Lösungen zu streichen.