

**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

**Klausur:** IN0010 / Retake  
**Prüfer:** Prof. Dr.-Ing. Georg Carle

**Datum:** Freitag, 6. Oktober 2017  
**Uhrzeit:** 13:30 – 15:00

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

### Bearbeitungshinweise

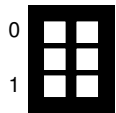
- Diese Klausur umfasst
  - **16 Seiten** mit insgesamt **6 Aufgaben** sowie
  - eine beidseitig bedruckte **Formelsammlung**.

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 90 Punkte.
- Als Hilfsmittel sind zugelassen:
  - 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 (17 Punkte)

Die nachfolgenden Teilaufgaben sind jeweils unabhängig voneinander lösbar.



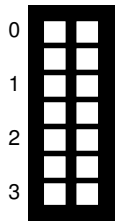
a)\* Streichen Sie **alle** Begriffe, welche **nicht** eine Schicht des ISO/OSI-Modells bezeichnen.

TCP/IP-Schicht

Verschlüsselungsschicht

Sicherheitsschicht

Benutzerschicht



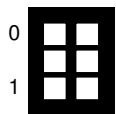
b)\* Erklären Sie detailliert die Funktionsweise von Traceroute.

Host sendet IP-Pakete mit inkrementell steigender TTL beginnend bei 1 an ein bestimmtes Ziel.

Router dekrementieren die TTL.

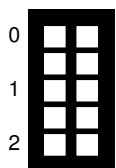
Erhält ein Router ein Paket mit TTL=1, verwirft er das Paket und sendet eine ICMP Time Exceeded / TTL Exceeded in Transit Message zurück an den Host.

Aus der Fehlernachricht kann der Host auf IP-Adressen der zwischen ihm selbst und dem Ziel liegenden Router schließen.



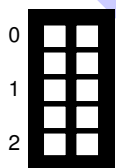
c)\* Wozu dient ARP?

Gegeben eine IPv4-Adresse, erfrage die zugehörige MAC-Adresse innerhalb der lokalen Broadcast Domain.



d)\* Erläutern Sie den Unterschied zwischen Abtastung und Quantisierung.

Abtastung ist die Diskretisierung im Zeitbereich, Quantisierung die Diskretisierung im Wertbereich.



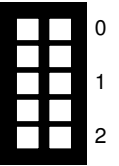
e)\* Erläutern Sie den Unterschied zwischen einem Resolver und einem Nameserver.

Nameserver sind autoritativ für eine oder mehrere Zonen und beantworten nur Anfragen diese Zonen betreffend.

Resolver lösen Anfragen iterativ an die jeweils zuständigen Nameserver auf (oder leiten sie rekursiv an einen anderen Resolver weiter) und liefern das Endergebnis an den Anfragenden zurück.

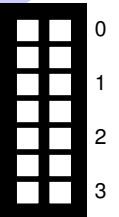
f)\* Erläutern sie das Medienzugriffsverfahren Token Passing.

Hosts sind zu einem Ring zusammengeschlossen. Ein Token zirkuliert im Ring. Der Host, der das Token gerade besitzt, darf Senden. Nach dem Senden bzw. nach einer bestimmten Zeit wird das Token weitergesendet.



g)\* Fassen Sie die 5 Netzbereiche 203.0.113.208/29, 203.0.113.216/29, 203.0.113.192/28, 203.0.113.224/29 und 203.0.113.160/27 soweit wie möglich zusammen, ohne dabei zusätzliche Netzbereiche einzuschließen.

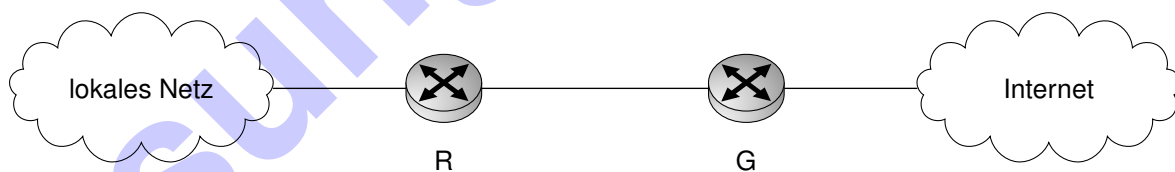
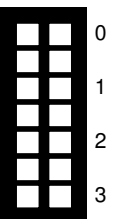
203.0.113.160/27, 203.0.113.192/27, 203.0.113.224/29



h)\* Gegeben sei die nachfolgend abgebildete Netztopologie. G stellt den von Ihrem Provider bereitgestellten Router dar (z. B. eine FritzBox!). Da Sie lieber einen eigenen Router nutzen würden, aber Ihr Provider sich weigert, Ihnen die Zugangsdaten bereitzustellen, installieren Sie kurzerhand einen eigenen Router R direkt hinter G.

Auf R konfigurieren Sie die private IP von G als Default Gateway. Weitere Konfigurationen werden nicht vorgenommen.

Im Anschluss können Sie von R aus Hosts im Internet erreichen. Ein hinter R angeschlossener Client im lokalen Netz, welcher R als Default Gateway nutzt, kann jedoch keine Verbindung zu Hosts im Internet aufbauen. Erklären Sie das Problem.



G fehlt ein Eintrag für das lokale Netz über R in seiner Routingtabelle.

## Aufgabe 2 NAT und statisches Routing (13 Punkte)

Gegeben sei die Netztopologie aus Abbildung 2.1. PC1 und PC2 sind Teil eines privaten Netzes, welches über R1 an das Internet angebunden ist. PC1 sendet eine Nachricht an den Server SRV1. Die Abbildung zeigt relevante Headerteile dieser Nachricht an drei unterschiedlichen Stellen im Netz.

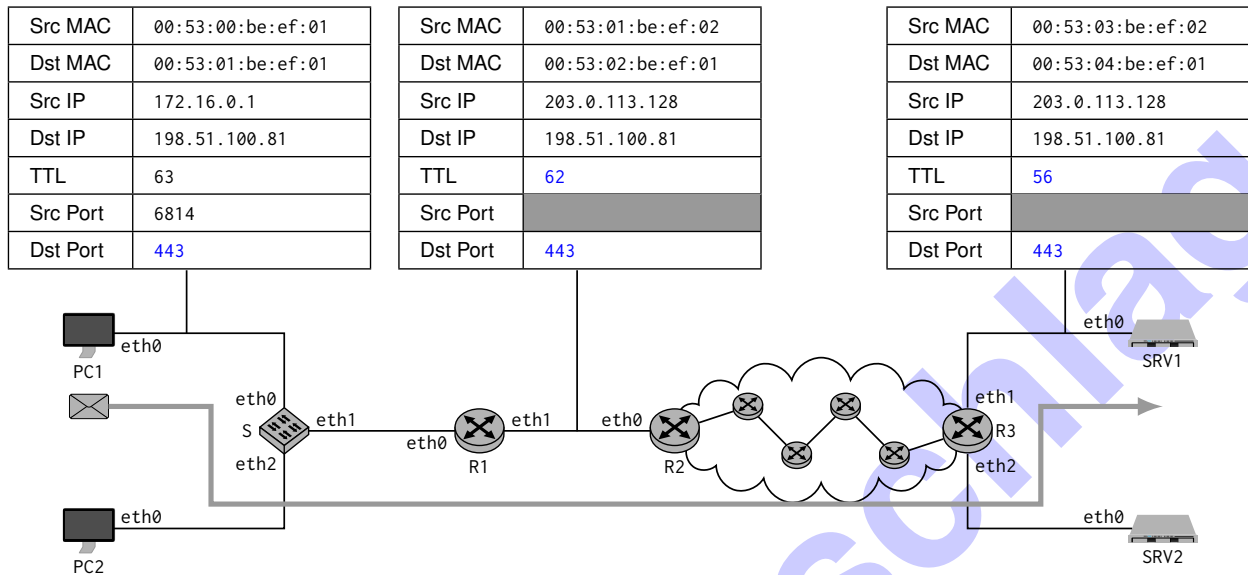


Abbildung 2.1: Netztopologie (ausgegraute Felder müssen nicht ausgefüllt werden)

a)\* Bestimmen Sie die L2- und L3-Adressen der Geräte in Abbildung 2.1. Tragen Sie die entsprechenden Adressen vollständig in der untenstehenden Tabelle ein. Adressen, die nicht aus Abbildung 2.1 hervorgehen, markieren Sie durch einen Strich (—).

	L2-Adressen		L3-Adressen	
PC1.eth0	00:53:00:be:ef:01		PC1.eth0	172.16.0.1
S.eth0	—		S.eth0	—
S.eth1	—		S.eth1	—
R1.eth0	00:53:01:be:ef:01		R1.eth0	—
R1.eth1	00:53:01:be:ef:02		R1.eth1	203.0.113.128
R2.eth0	00:53:02:be:ef:01		R2.eth0	—
R3.eth1	00:53:03:be:ef:02		R3.eth1	—
SRV1.eth0	00:53:04:be:ef:01		SRV1.eth0	198.51.100.81

b)\* Vervollständigen Sie die Time-to-Live in Abbildung 2.1.

c)\* Vervollständigen Sie den Destination Port in Abbildung 2.1 unter der Annahme, dass PC1 mit der gesendeten Nachricht eine verschlüsselte Verbindung zu einer Webseite auf SRV1 aufzubauen versucht.

Tabelle 2.1 zeigt den Inhalt der NAT-Tabelle von R1 **vor** dem Verbindungsversuch durch PC1.

d)\* Ergänzen Sie die Tabelle um den entstehenden Eintrag, sobald PC1 das erste Paket an SRV1 sendet.  
**Hinweis:** Werfen Sie noch mal einen Blick auf Abbildung 2.1. Sollte ein Eintrag nicht eindeutig bestimmt sein, treffen Sie eine sinnvolle Wahl.

Private IP	Privater Src Port	Öffentlicher Src Port
172.16.0.2	6812	6812
172.16.0.2	6813	6813
172.16.0.2	6814	6814
172.16.0.1	6814	6815

Tabelle 2.1: NAT-Tabelle von R1

e) Geben Sie Ziel-IP, Quell-Port und Ziel-Port der Antwort von SRV1 an.

**Hinweis:** Sollte ein Wert nicht eindeutig bestimmt sein, treffen Sie eine sinnvolle Wahl.

Ziel-IP: 203.0.113.128  
Quell-Port: 443  
Ziel-Port: 6815

f) Erläutern Sie im Detail, wie R1 unterscheidet, ob die Antwort für PC1 oder PC2 bestimmt ist.

Anhand des Ziel-Ports der Antwort, welcher dem öffentlichen Quellport in der NAT-Tabelle entsprechen muss, kann R1 die korrekte private IP-Adresse ermitteln.

g) Erläutern Sie im Detail, welche Modifikationen R1 an der Antwort von SRV1 vornehmen muss.  
(Angabe konkreter Werte sofern eindeutig bestimmt)

Die Ziel-IP der Antwort wird durch die private Adresse 172.16.0.1 ersetzt, der Ziel-Port durch den privaten Quell-Port 6814.  
(Checksumme muss angepasst werden, TTL wird dekrementiert)

### Aufgabe 3 Dynamisches Routing (19 Punkte)

Gegeben sei das in Abbildung 3.1 dargestellte Netzwerk. Als Routingprotokoll werde RIP verwendet. Die Tabellen neben / oberhalb der Router stellen die Routingtabelle des jeweiligen Routers dar. Dabei stehen **Dst** für den jeweiligen Ziel-Router, **NH** für den jeweiligen NextHop und **Cost** für die Kosten zum jeweiligen Ziel.

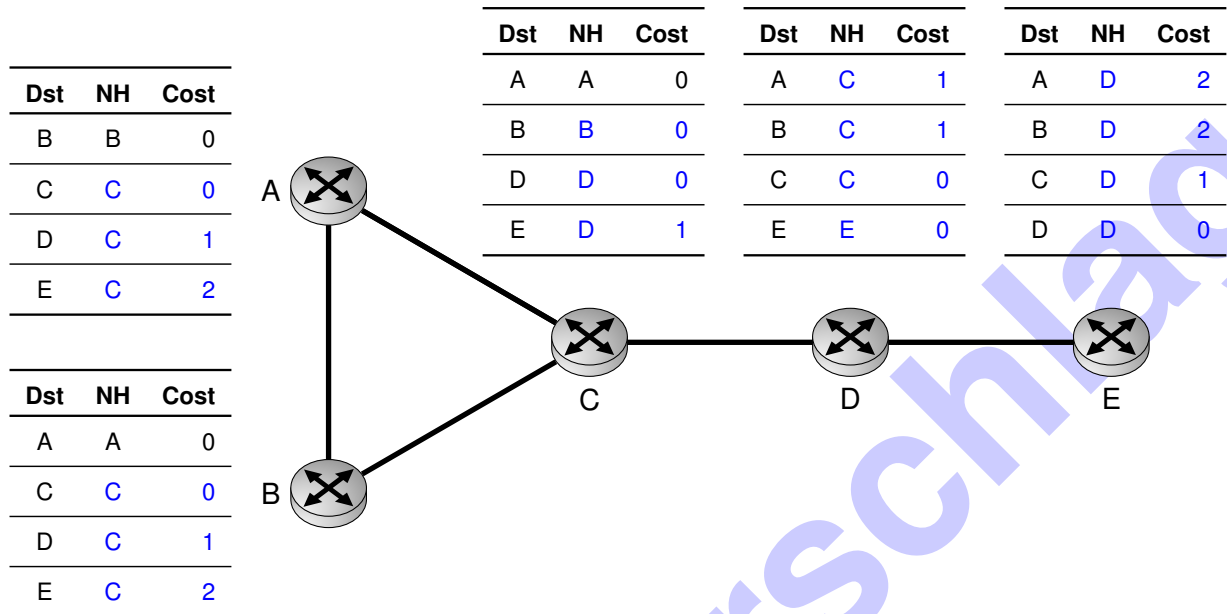


Abbildung 3.1: Topologie

a)\* Welche Metrik verwendet RIP? (Ohne Begründung)

HopCount

b)\* RIP ist ein Distanz-Vektor-Protokoll. Erläutern Sie den Unterschied zu Link-State-Protokollen.

DV-Protokolle kennen nur NextHop und Distanz zum Ziel , LS-Protokolle haben Kenntnis der Netztopologie.

c)\* RIP gehört zur Klasse der Interior-Gateway-Protokolle. Erläutern Sie den Unterschied zu Exterior-Gateway-Protokollen.

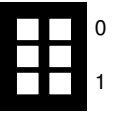
IGPs werden innerhalb autonomer Systeme eingesetzt , EGPs zwischen autonomen Systemen.

d)\* Inwiefern sind Netzwerke, deren Router ausschließlich RIP als Routingprotokoll verwenden, in der Größe beschränkt?

RIP interpretiert Ziele, die 15 Hops oder weiter entfernt sind, als unerreichbar. Dementsprechend sind Netze im Durchmesser (d. h. der maximalen Pfadlänge) beschränkt.

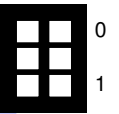
e)\* Welche Information enthalten Routingupdates bei RIP?

Erreichbare Ziele eines Nachbarn und Distanz zum jeweiligen Ziel .



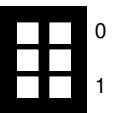
f)\* Begründen Sie, ob RIP stets die kürzeste Route (im Sinn zwischen Quelle und Ziel liegender Router) wählt.

Ja, da die einzige Metrik für RIP die Anzahl der Hops zwischen sich selbst und Ziel liegender Hops ist.



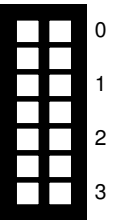
g)\* Begründen Sie, ob RIP stets die schnellste Route (im Sinn von Übertragungsrate) zu einem Ziel wählt.

Nein, weil die Anzahl der Hops nichts über die Datenrate zwischen diesen aussagt.



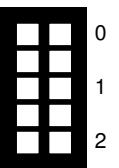
h) Vervollständigen Sie die Routingtabellen der Router in Abbildung 3.1 (ohne Angabe von Zwischenschritten), so dass ein Netzwerk kürzester Pfade gemäß der Metrik von RIP entsteht.

Es falle nun der Link zwischen Router D und E aus. Router D bemerkt den Ausfall offensichtlich sofort. Beantworten Sie die nachfolgenden Fragen in der gegebenen Reihenfolge.



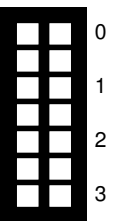
i) Router D sendet ein periodisches Update. Beschreiben Sie die Auswirkungen auf die Router A, B und C.

C wird über den Ausfall informiert, woraufhin C die Route zu E löscht. A und B haben davon noch keine Kenntnis.



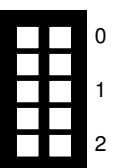
j) Router A sendet nun ein periodisches Update. Beschreiben Sie die Auswirkungen auf die Router B, C und D.

Da A noch immer eine Route zu E über C hat, wird diese an C propagiert. (da nur Ziel und Distanz berücksichtigt werden, weiß C nicht, dass diese Route über ihn selbst läuft)  
C akzeptiert diese und denkt, E über A erreichen zu können. Auf B hat das Update keinen Einfluss, da B (genau wie A) noch die alte Route zu E über C kennt. D erhält das Update von A nicht.



k) Beschreiben Sie das auftretende Problem sowie dessen Lösung.

Count-to-Infinity: Die fehlerhafte Route zu E wird zwischen A, B und C zirkulieren bis sie Kosten 15 erreicht hat (RIP Tombstone).  
Lösung ist mit RIP nur bedingt möglich, z. B. mittels Split Horizon (propagiere eine Route nicht an den eigenn NextHop für genau diese Route).



## Aufgabe 4 Huffman (22 Punkte)

In dieser Aufgabe betrachten wir eine vereinfachte Version des ITU T.30 Protokolls, bekannt als Telefax. Dieses verwendet eine Kombination aus Lauflängenkodierung (RLE) und Huffman-Code. Die Lauflängenkodierung soll beginnend bei „weiß“ abwechselnd die Anzahl der weißen und schwarzen Pixel angeben. Wir betrachten zunächst die Pixelgrafik in Abbildung 4.1.

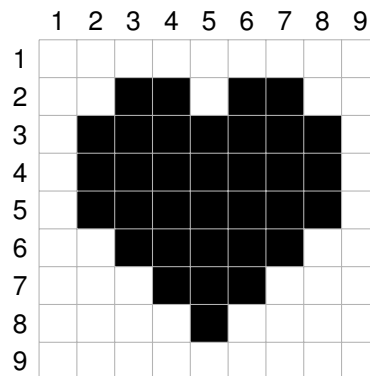
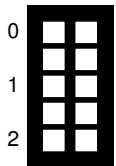
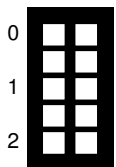


Abbildung 4.1: Pixelgrafik



a)\* Bestimmen Sie das Ergebnis der Lauflängenkodierung.

11, 2, 1, 2, 3, 7, 2, 7, 2, 7, 3, 5, 5, 3, 7, 1, 13

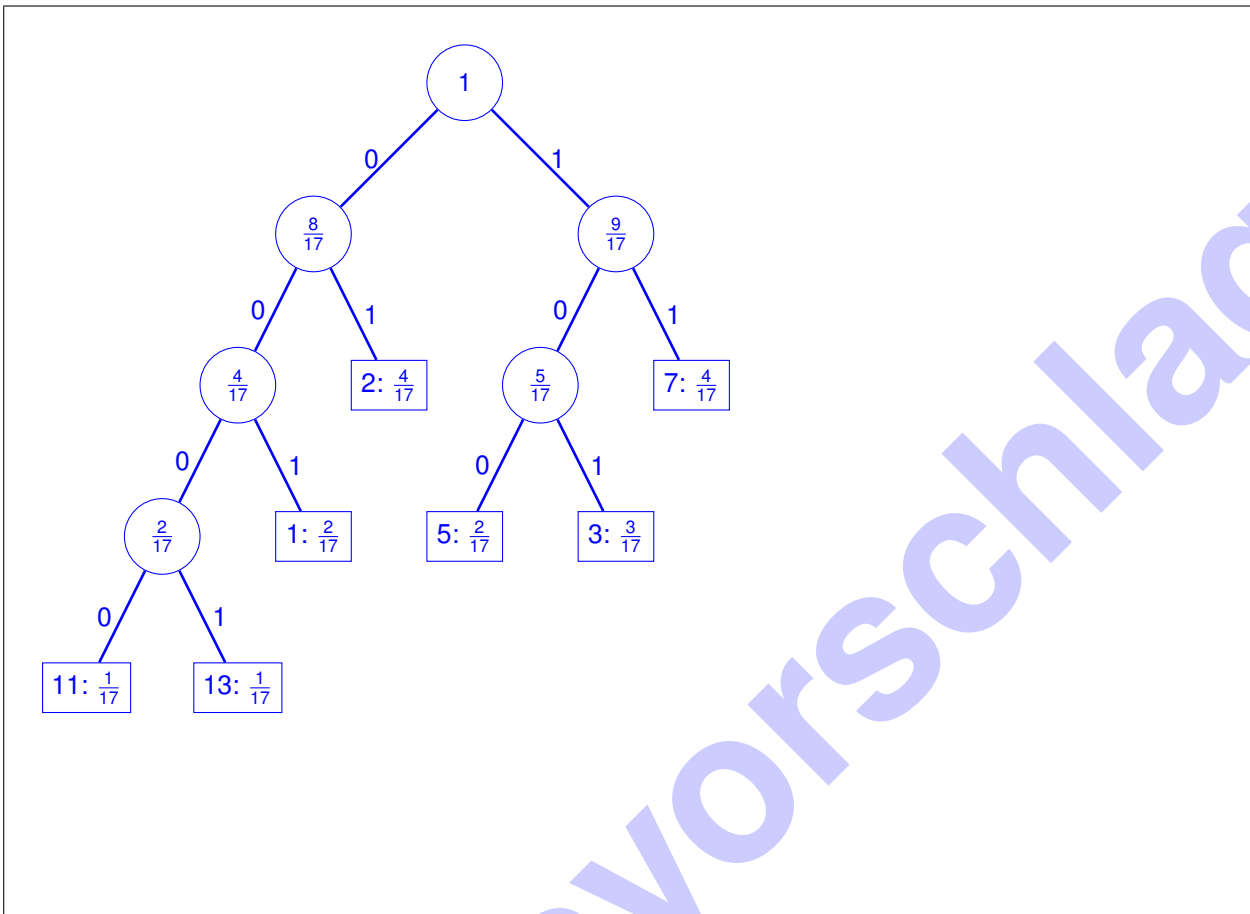
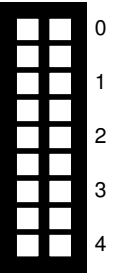


b) Bestimmen Sie die Auftrittswahrscheinlichkeiten  $p_i$ , der einzelnen RLE-Codewörter.

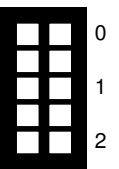
RLE	$p_i$
1	$\frac{2}{17}$
2	$\frac{4}{17}$
3	$\frac{3}{17}$
5	$\frac{2}{17}$
7	$\frac{4}{17}$
11	$\frac{1}{17}$
13	$\frac{1}{17}$



c) Erstellen Sie einen passenden binären Huffman-Code. Beschriften Sie die Blätter mit den entsprechenden RLE-Codewörtern, **alle** Knoten mit den entsprechenden Wahrscheinlichkeiten und weisen Sie den Kanten passende Abschnitte der Huffman-Codewörter zu.

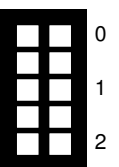


d) Erstellen Sie ein Codebuch für den Huffman-Code.

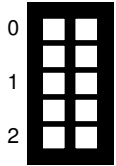


RLE	Huffman
1	001
2	01
3	101
5	100
7	11
11	0000
13	0001

e) Kodieren Sie die Pixelgrafik mit dem erstellten Huffman-Code.



0000 01 001 01 101 11 01 11 01 11 101 100 100 101 11 001 0001



f) Bestimmen Sie den Kompressionsfaktor gegenüber einer direkten Übertragung, bei der jedes Pixel mit 1 bit („schwarz“ oder „weiß“) übertragen wird.

$$\frac{81 \text{ bit}}{45 \text{ bit}} = \frac{9}{5} = 1,8$$

Wir betrachten nun im Folgenden den Huffman Baum aus Abbildung 4.2. Wir gehen davon aus, dass dieser benutzt wird, um eine gedächtnislose Quelle mit dem Alphabet  $\mathcal{A} = \{a, b, c\}$  zu kodieren. Die Auftretswahrscheinlichkeiten  $p_i$  der Zeichen  $i \in \mathcal{A}$  sind ebenfalls in der Abbildung eingezeichnet.

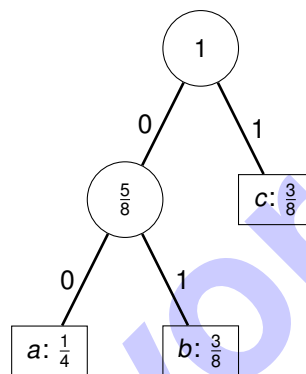
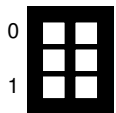
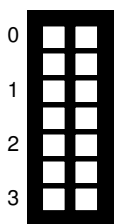


Abbildung 4.2: Huffman Baum



g)\* Begründen Sie, wieviel bit ein uniformer Code durchschnittlich zur Kodierung eines Zeichens benötigt.

$$\lceil \log_2(3) \rceil = 2 \text{ bit}$$



h)\* Bestimmen Sie den Informationsgehalt  $I(p_i)$  der Zeichen  $i \in \mathcal{A}$

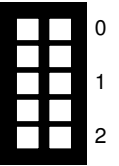
**Hinweis:** Alle Ergebnisse sind vollständig auszurechnen. Nutzen Sie ggf. die Plots am Cheatsheet zur Bestimmung von Zahlenwerten.

$$I\left(\frac{1}{4}\right) = -\log_2\left(\frac{1}{4}\right) = \log_2(4) = 2 \text{ bit}$$

$$I\left(\frac{3}{8}\right) = -\log_2\left(\frac{3}{8}\right) = -\log_2(3) + 3 \approx -1,6 \text{ bit} + 3 = 1,4 \text{ bit}$$

i) Bestimmen Sie die Entropie der Quelle.

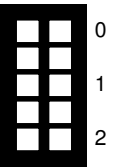
**Hinweis:** Alle Ergebnisse sind vollständig auszurechnen.



$$\begin{aligned}\sum_{i \in A} p_i \cdot l(p_i) &= \frac{1}{4} \cdot 2 \text{ bit} + 2 \cdot \frac{3}{8} \cdot 1,4 \text{ bit} \\ &= 0,5 \text{ bit} + \frac{3}{4} \cdot 1,4 \text{ bit} \\ &= 0,5 \text{ bit} + 0,75 \text{ bit} + 0,3 \text{ bit} \\ &= 1,55 \text{ bit}\end{aligned}$$

j)\* Bestimmen Sie die durchschnittliche Huffman-Codewortlänge.

**Hinweis:** Alle Ergebnisse sind vollständig auszurechnen.



$$\begin{aligned}\sum_{i \in A} p_i \cdot l_i &= \frac{1}{4} \cdot 2 \text{ bit} + \frac{3}{8} \cdot 2 \text{ bit} + \frac{3}{8} \cdot 1 \text{ bit} \\ &= 0,5 \text{ bit} + 0,75 \text{ bit} + 0,375 \text{ bit} \\ &= 1,625 \text{ bit}\end{aligned}$$

## Aufgabe 5 Wireshark (12 Punkte)

Gegeben sei das Netzwerk aus Abbildung 5.1. PC1 und PC2 sind über den Ethernet-Switch S mit Router R verbunden.

Srv sende nun ein Paket an PC1. Der betreffende Ethernet-Rahmen werde unmittelbar nach dem Ethernet-Interface von Srv abgegriffen und ist in Abbildung 5.2 dargestellt.

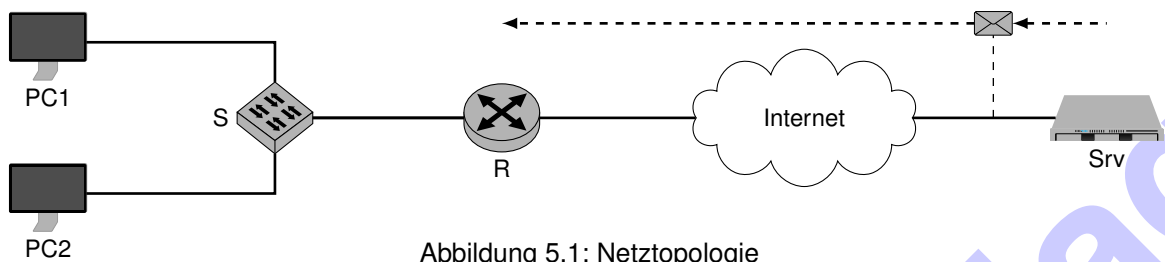


Abbildung 5.1: Netztopologie

	Receiver Address	Transmitter Address	Ethertype
0x000	f8 63 3f 16 e7 6b 58 23	8c 26 b2 44	86 dd
0x010	00 00 00 40 3a 38 2a 01	04 f8 0d 16 19 43 00 00	
0x020	00 00 00 00 00 02 20 01	4c 50 04 ac 9e 00 fa 63	
0x030	3f ff fe 16 e7 6b 81 00	20 e3 52 cf 00 0e 0d ba	
0x040	d0 59 00 00 00 00 e3 a5	06 00 00 00 00 00 10 11	
0x050	12 13 14 15 16 17 18 19	1a 1b 1c 1d 1e 1f 20 21	
0x060	22 23 24 25 26 27 28 29	2a 2b 2c 2d 2e 2f 30 31	
0x070	32 33 34 35 36 37 89 a7	1f fe	

Abbildung 5.2: Ethernet-Rahmen zwischen Srv und R inkl. Checksumme

Zu allen Teilaufgaben ist eine kurze Begründung anzugeben, z.B. Angabe oder Markierung des betreffenden Headerfelds, Hinweis auf die Bedeutung des jeweiligen Felds, etwaige Skalierung von Feldern etc.

**Hinweis:** Verwenden Sie zur Lösung die am Cheatsheet abgedruckten Header und Informationen.

a)\* Markieren und beschriften Sie alle Felder von Schicht 2 in Abbildung 5.2.

b)\* Bestimmen Sie die L2-Adressen der Geräte aus Abbildung 5.1, soweit diese aus dem L2-Header hervorgehen.

Srv: 58:23:8c:26:b2:44

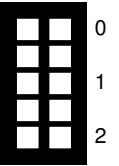
Da zwischen Srv und R das Internet liegt, gehört die Receiver Address mit Sicherheit nicht zu R sondern zum Gateway von Srv.

c)\* Der Ethertype ist 0x86dd, das IP-Versions-Feld weist auf IPv6 hin. Begründen Sie, weswegen alleine aus dem Versions-Feld ohne Kenntnis des Ethertypes nicht auf IPv6 geschlossen werden kann.

Gegeben ein Paket, welches mit 0x60 beginnt, kann nicht auf IPv6 geschlossen werden. Es könnte sich um jedes beliebige Paket beliebigen Typs handeln, das zufällig als erstes Byte 0x06 hat.

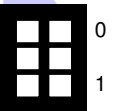
d) Bestimmen Sie die Quell- und Zieladresse auf Schicht 3 des Pakets in ihrer üblichen Schreibweise.

Quelle: 2a01:4f8:d16:1943::2  
Ziel: 2001:4c50:4ac:9e00:fa63:3fff:fe16:e76b



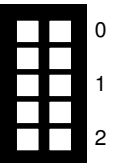
e) Begründen Sie, ob die Zieladresse aus Teilaufgabe d) die Adresse von PC1, S oder R ist.

PC1, da IPv6 verwendet wird und damit R kein NAT verwendet.



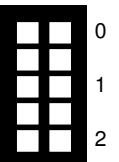
f) Bestimmen Sie die Länge des L3-Headers einschließlich evtl. Optionen oder Extension Header.

IPv6 Header hat feste Länge von 40 B. NextHeader ist 0x3a, was kein Extension Header ist.



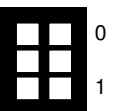
g) Bestimmen Sie die Gesamtlänge des Pakets, d. h. Header der Schicht 3 inkl. Payload.

Payload Length = 0x0040 = 64 B zzgl. des L3-Header = 104 B



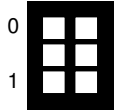
h)\* Angenommen das Paket von Srv an PC1 ist ein ICMP Echo Reply. Auf PC1 laufen zwei Instanzen einer Anwendung, die ein solches von Srv gesendetes Paket erwarten. Wie wird unterschieden, für welche der beiden Instanzen das Paket bestimmt ist?

ICMP-Identifizier, da die auf den IP-Header folgende Payload ICMPv6 mit Type=0x81, Code=0x00 ein Echo Reply ist.



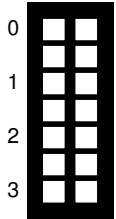
## Aufgabe 6 CRC (7 Punkte)

Gegeben sei das CRC-Polynom  $x^2 + x$  sowie die binäre Nachricht  $m = 00110001$ .



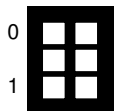
a)\* Geben Sie das CRC-Polynom in binärer Schreibweise an.

$$x^2 + x = 110$$



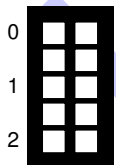
b) Bestimmen Sie die zu  $m$  passende Checksumme.

$$\begin{array}{r} 00110001 \ 00 \div 110 \\ \underline{110} \phantom{00} \\ 000001 \ 00 \\ \underline{110} \phantom{00} \\ 010 \phantom{00} \\ \underline{010} \phantom{00} \\ 000000 \end{array}$$



c) Geben Sie die gesicherte Bitfolge an, die übertragen wird.

00110001 10



d)\* Erläutern Sie, was in Teilaufgabe c) „gesichert“ bedeutet.

„gesichert“ heißt in diesem Kontext lediglich, dass die Nachricht gegen Übertragungsfehler gesichert ist. Das bedeutet nicht, dass keine solchen Fehler auftreten, sondern lediglich, dass diese mit hoher Wahrscheinlichkeit beim Empfänger erkannt werden.  
Eine Korrektur ist i. A. nicht möglich.

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

A large grid area for writing solutions, consisting of approximately 30 columns and 30 rows of small squares. A diagonal watermark reading "Lösungsvorschlag" is overlaid across the grid from the bottom-left to the top-right.

Lösungsvorschlag