Name

Vorname

Studiengang (Hauptfach)

Fachrichtung (Nebenfach)

Matrikelnummer

Unterschrift der Kandidatin/des Kandidaten

..... Note

	I	II
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
Σ		

TECHNISCHE UNIVERSITÄT MÜNCHEN

Fakultät für Informatik

☐ **Midterm-Klausur**
☒ **Final-Klausur**

☐ **Semestralklausur**
☐ **Diplom-Vorprüfung**
☐ **Bachelor-Prüfung**
☐ .....

☐ **Einwilligung zur Notenbekanntgabe per E-Mail / Internet**

Prüfungsfach: Grundlagen Rechnernetze und Verteilte Systeme

Prüfer: Prof. Dr.-Ing. Georg Carle **Datum: 24.09.2012**

Hörsaal: ..... **Reihe:** ..... **Platz:** .....

Nur von der Aufsicht auszufüllen:

Hörsaal verlassen **von** ..... : ..... **bis** ..... : .....

Vorzeitig abgegeben **um** ..... : .....

Besondere Bemerkungen:

Nachholklausur

Grundlagen Rechnernetze und Verteilte Systeme

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München

Montag, 24.09.2012
11:00 – 12:30 Uhr

- Diese Klausur umfasst **23 Seiten** und insgesamt **5 Aufgaben** sowie ein **zusätzlich ausgeteiltes Hilfsblatt** zu Protokoll-Headern. Bitte kontrollieren Sie jetzt, dass Sie eine vollständige Angabe erhalten haben.
- Schreiben Sie bitte in die Kopfzeile **jeder Seite** Namen und Matrikelnummer.
- Schreiben Sie weder mit roter / grüner Farbe noch mit Bleistift.
- Die Gesamtzahl der Punkte beträgt 85.
- Als Hilfsmittel sind **ein beidseitig handschriftlich beschriebenes DIN A4 Blatt** sowie **ein nicht programmierbarer Taschenrechner** zugelassen. Bitte entfernen Sie alle anderen Unterlagen von Ihrem Tisch und schalten Sie Ihre Mobiltelefone aus.
- Mit * gekennzeichnete Aufgaben sind ohne Kenntnis der Ergebnisse vorhergehender Teilaufgaben lösbar.
- **Es werden nur solche Ergebnisse gewertet, bei denen ein Lösungsweg erkennbar ist.** Textaufgaben sind **grundsätzlich zu begründen**, falls es in der jeweiligen Teilaufgabe nicht ausdrücklich anders vermerkt ist.

Aufgabe 1 NAT und statisches Routing (15 Punkte)

15

Gegeben sei die Netztopologie aus Abbildung 1.1. PC1 und PC2 sind über ein gewöhnliches Ethernet-Switch mit Router R1 verbunden, welcher Zugang zum Internet ermöglicht.

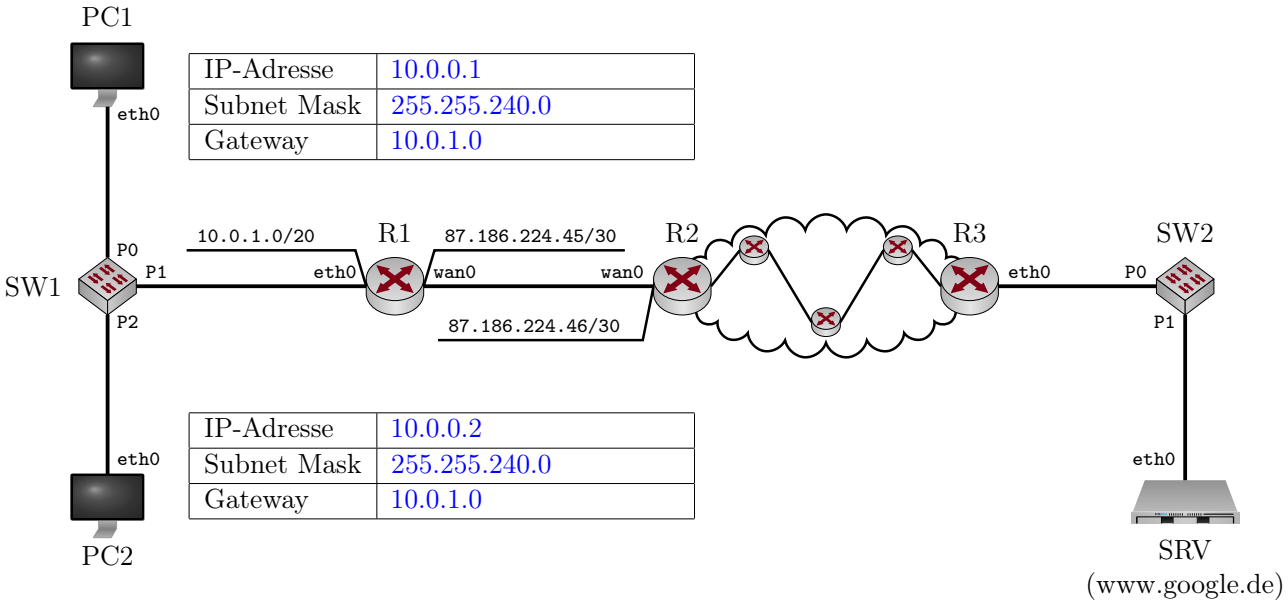


Abbildung 1.1: Netztopologie

1

a)* Begründen Sie, ob die Adresse 10.0.1.0 für das gegebene Präfix nutzbar ist. Falls nein, vergeben Sie an R1 eine sinnvolle Adresse im selben Netz.

10.0.1.0 ist eine gültige Hostadresse im Netz 10.0.0.0/20, da es sich weder um die erste noch die letzte Adresse im Subnetz handelt (sofort ersichtlich am kleinen Präfix und der 1 im 3. Oktett). ✓

1

b)* Bestimmen Sie die Netzadresse und Broadcastadresse des Netzwerks, in dem sich PC1, PC2 und R1 befinden.

Netzadresse 10.0.0.0 ✓ und Broadcastadresse 10.0.15.255 ✓

1

c)* Wieviele IP-Adressen stehen in diesem Netzwerk zur Adressierung von Geräten zur Verfügung?

$2^{12} - 2 = 4094$ ✓

1

d) Weisen Sie PC1 und PC2 jeweils eine sinnvolle IP-Adresse, Subnetzmaske und Gateway-Adresse zu, so dass diese eine Verbindung zum Internet herstellen können. Tragen Sie die Werte direkt in Abbildung 1.1 ein.

1

e)* Wie viele /20 Subnetze gibt es im Netz 10.0.0.0/8?

$2^{20-8} = 2^{24-12} = 4096$ ✓

1

f)* Begründen Sie, weswegen R1 NAT unterstützen muss, damit PC1 und PC2 mit Hosts im Internet kommunizieren können.

PC1 und PC2 befinden sich in einem privaten Netzwerk, deren IP-Adressen sind daher nicht global eindeutig. ✓

1

g)* Welche Informationen muss R1 mind. in seiner NAT-Tabelle vorhalten?

Lokale IPs der PCs, lokale Portnummer und globale Quellportnummern. (globale IP nicht notwendig, da R1 nur eine globale IP-Adresse besitzt; Zielportnummern sind für die grundlegenden Aufgaben nicht erforderlich) ✓

Im Folgenden kürzen wir IP- und MAC-Adressen nach dem Schema `<Gerätename>.<Interface>` ab, z. B. `R1.wan0`. Beachten Sie zur Bearbeitung der beiden folgenden Teilaufgaben außerdem, dass sich zwischen R2 und R3 insgesamt drei weitere Router befinden. PC1 greift nun auf die Webseite http://www.google.de zu.

4

h) Ergänzen Sie für die Anfrage von PC1 an www.google.de die Headerfelder in den drei leeren Kästen in Abbildung 1.2. Sofern ein Feld nicht eindeutig bestimmt ist, treffen Sie eine sinnvolle Wahl.

4

i) Ergänzen Sie für die Antwort von www.google.de an PC1 die Headerfelder in den drei leeren Kästen in Abbildung 1.3. Sofern ein Feld nicht eindeutig bestimmt ist, treffen Sie eine sinnvolle Wahl.

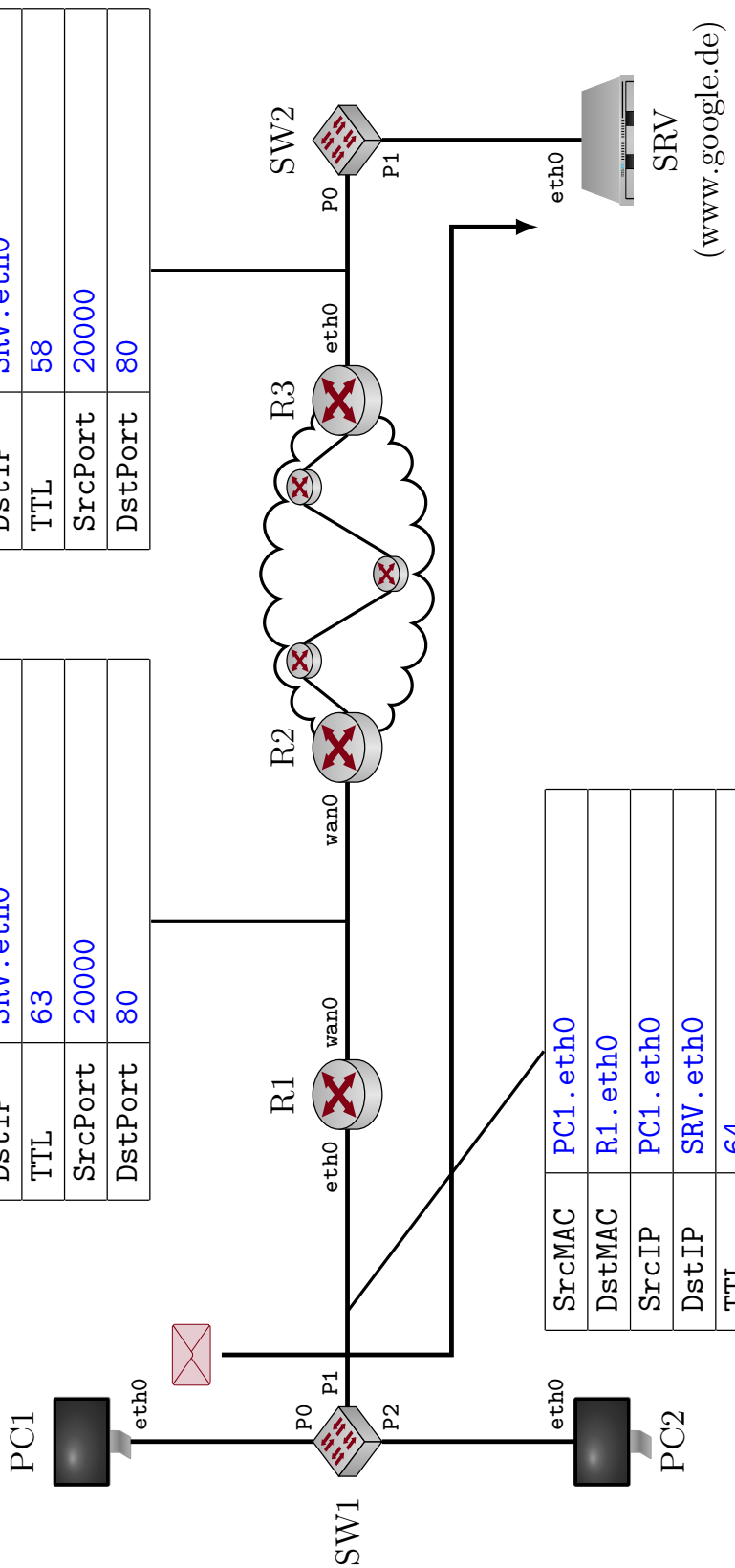


Abbildung 1.2: Netztopologie

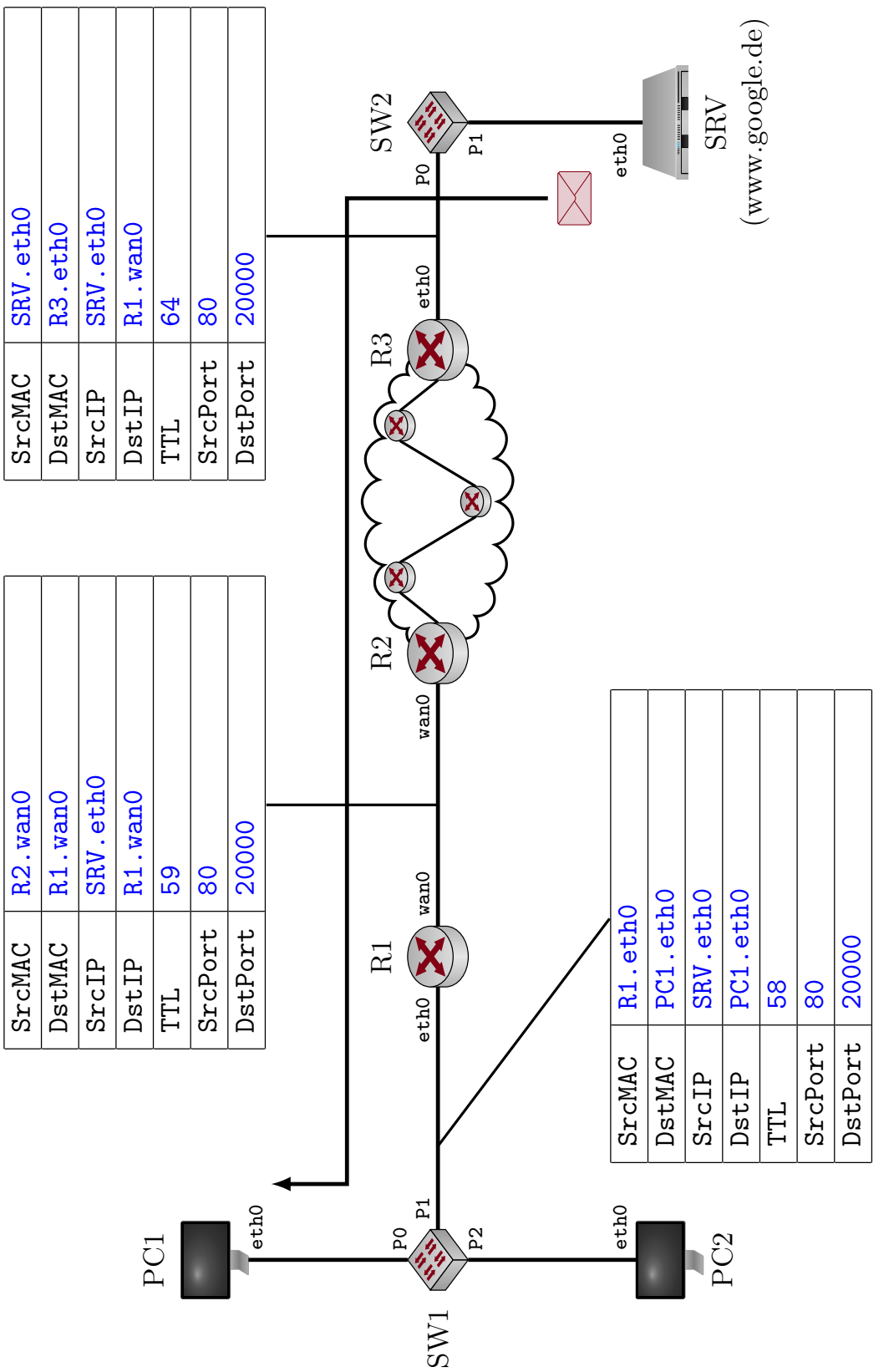


Abbildung 1.3: Netztopologie

Aufgabe 2 **Packet Pair Probing** (15 **Punkte**)

15

Gegeben sei die vereinfachte Netztopologie aus Abbildung 2.1. Knoten 1 und 4 sind mit ihren Routern jeweils über ein fullduplex-fähiges lokales Netzwerk verbunden. Die symmetrischen Datenraten betragen r_{12} bzw. r_{34}. Die beiden Distanzen d_{12} und d_{34} seien vernachlässigbar klein. Die Verbindung zwischen den Routern 2 und 3 sei bedeutend langsamer. Es gelte also $r_{23} < r_{12}, r_{34}$. Die Distanz d_{23} ist **nicht** zu vernachlässigen.
Die Übertragungsrate r_{23} soll von Knoten 1 bestimmt werden, indem möglichst wenig Last auf der ohnehin langsamen Verbindung erzeugt wird. Das Verfahren soll mit allen Knoten funktionieren, die über einen gewöhnlichen IP Stack verfügen.

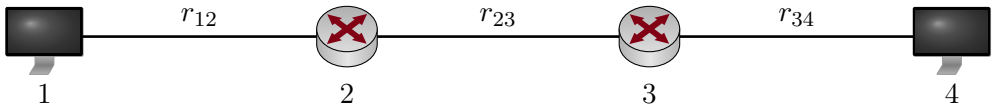


Abbildung 2.1: Vereinfachte Netztopologie

Wir leiten in dieser Aufgabe zunächst allgemein ein Verfahren her, mit dessen Hilfe Knoten 1 die fragliche Übertragungsrate bestimmen kann. Im Anschluss werten wir das Verfahren für konkrete Zahlenwerte aus.

1

a)* Geben Sie die Serialisierungszeit $t_s(i,j)$ und die Ausbreitungsverzögerung $t_p(i,j)$ zwischen zwei Knoten allgemein in Abhängigkeit der Paketgröße p, Datenrate r_{ij} und der Distanz d_{ij} an.

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

Für eine erfolgreiche und möglichst genaue Bestimmung der Rate r_{23} ist es wichtig, dass von 1 an 4 gesendete Pakete so groß wie möglich sind, aber nicht fragmentiert werden.

2

b)* Erläutern Sie kurz, wie Knoten 1 die maximale MTU auf dem gesamten Pfad nach Knoten 4 bestimmen kann.

1 sendet ein Paket mit der MTU des lokalen Segments und setzt das DF-Bit (do not fragment) im IP-Header. Sofern diese MTU größer ist als auf dem Abschnitt zwischen 2 und 3, so wird 2 das Paket verwerfen und eine entsprechende ICMP-Nachricht an 1 zurücksenden. Diese enthält die maximale MTU auf dem Abschnitt von 2 nach 3. ✓✓

Knoten 1 sende nun unmittelbar nacheinander zwei ICMP-Echo-Requests der Länge p an Knoten 4. Sie können davon ausgehen, dass sonst kein weiterer Verkehr die Übertragung beeinflusst. Die Länge p sei so gewählt, dass keine Fragmentierung notwendig ist. Eventuelle Verarbeitungszeiten an den Knoten werden vernachlässigt.

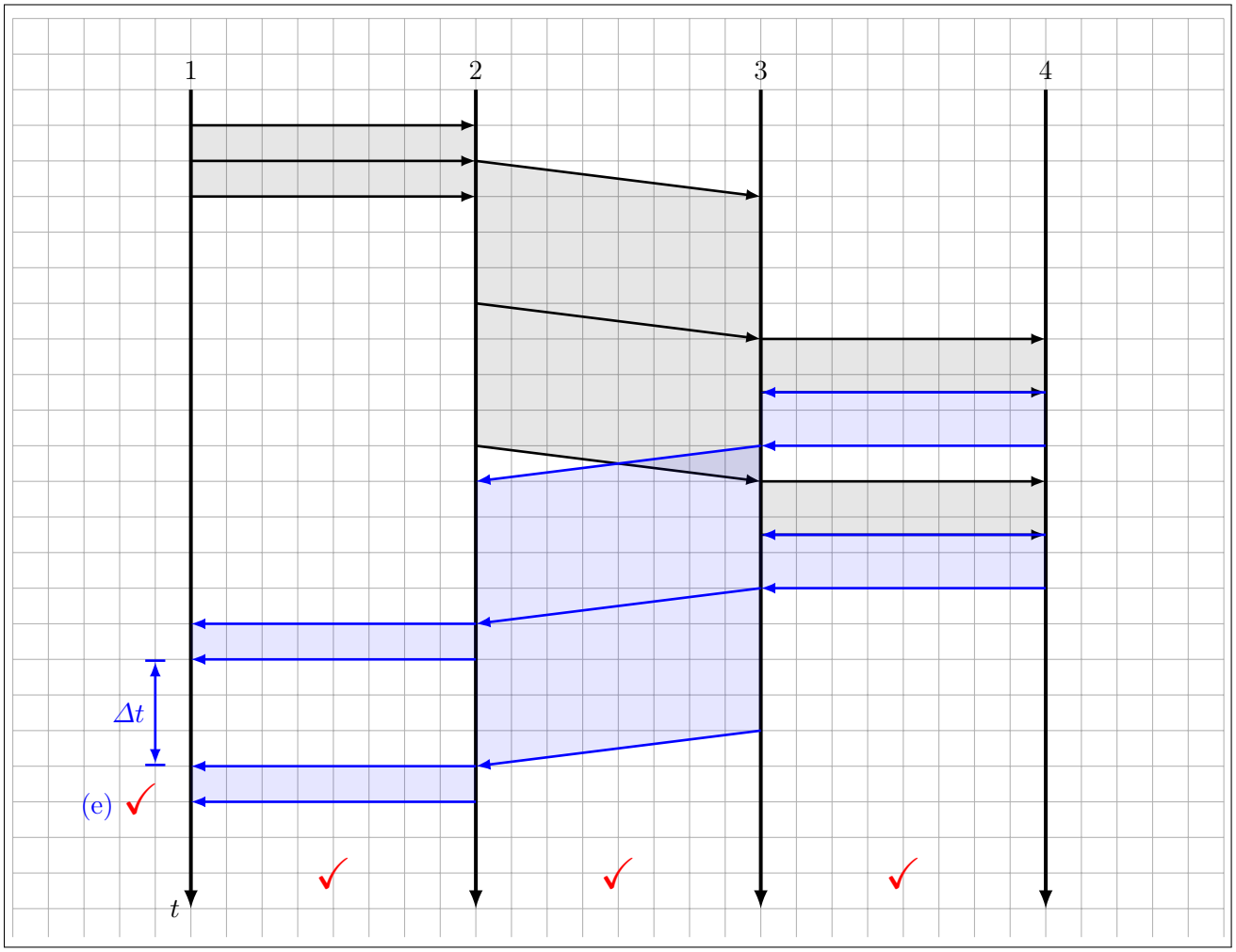
1

c)* Wie wird Knoten 4 reagieren, wenn er die ICMP-Echo-Requests von Knoten 1 erhält?

Pro Request wird (sofort) ein Reply (derselben Größse) zurückgeschickt. ✓

3

d) Ergänzen Sie das im Lösungsfeld abgebildete Weg-Zeit-Diagramm.



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 Übertragungsrate zwischen Knoten 2 und 3 verwendet werden.

1

e) Markieren Sie Δt in Ihrer Lösung von Teilaufgabe d).

f) Beschreiben Sie in Worten den allgemeinen Einfluss von r_{34} auf die Empfangspause Δt.

2

Ist r_{34} zu gering (also $t_s(3,4)$ groß), so kann es auf dem Rückweg an Knoten 3 zu einer Sendepause kommen zwischen den zwei Paketen kommen. Dies tritt allerdings erst dann auf, wenn $r_{3,4}$ kleiner ist als $r_{2,3}$. Andernfalls hat $r_{3,4}$ keinen Einfluss. ✓ ✓

g) Welche Bedingung muss r_{34} genau erfüllen, damit das Verfahren funktioniert? (Formel!)

1

$$r_{34} > r_{23} \checkmark$$

h) Geben Sie einen Ausdruck für Δt an. Vereinfachen Sie diesen soweit wie möglich.

2

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

i) Geben Sie einen Ausdruck für die gesuchte Datenrate r_{23} an. Vereinfachen Sie diesen soweit wie möglich.

1

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

Wiederholte Messungen von Knoten 1 ergeben einen Durchschnittswert $\overline{\Delta t} = 108\,\mu$s bei einer Paketgröße von $p = 1500\,$Byte. Die Übertragungsrate r_{12} betrage 1 Gbit/s.

j) Bestimmen Sie r_{23} als Zahlenwert in Mbit/s.

1

$$r_{23} = \frac{p}{\overline{\Delta t} + \frac{p}{r_{34}}} = 100\text{Mbit/s} \checkmark$$

18

Aufgabe 3 IP-Fragmentierung (18 Punkte)

In Abbildung 3.1 ist eine Anordnung von Netzkomponenten mit ihren IP- und MAC-Adressen dargestellt. Die beiden Computer PC1 und PC2 verwenden den jeweils lokalen Router als Default-Gatway. Die MTU auf dem WAN-Link zwischen R1 und R2 betrage 580 Byte. Innerhalb der lokalen Netzwerke gelte die für Ethernet übliche MTU von 1500 Byte.

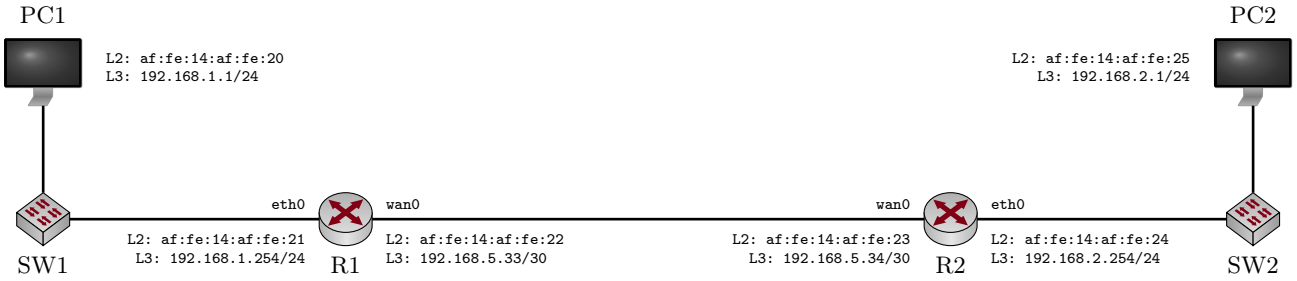


Abbildung 3.1: Netztopologie

1

a)* Begründen Sie, ob die Switches SW1 und SW2 für ihre grundlegenden Aufgaben eine eigene MAC-Adresse benötigen. Ergänzen Sie diese ggf. in Abbildung 3.1.

Kein Gerät kommuniziert direkt mit dem Switch – Switches arbeiten auf Schicht 2 und sind für die angeschlossenen Geräte transparent. ✓

2

b)* Welche Bedeutung haben die beiden Headerfelder „Identifier“ und „Fragment Offset“?

- Identifier: Eindeutige Identifikation aller zu einem Paket gehörenden Fragmente. ✓
- Fragment Offset: Ermöglicht die Reassemblierung von Fragmenten in der richtigen Reihenfolge. ✓

1

c)* Welches Protokoll dient zur Übersetzung von IP-Adressen in MAC-Adressen?

ARP ✓

1

d)* Begründen Sie, ob PC1 die MAC-Adresse von PC2 benötigt, um ein Paket an PC2 senden zu können.

Nein, er braucht nur die IP-Adresse von PC2. MAC-Adressen dienen nur der Adressierung innerhalb eines Subnetzes, nicht aber zur End-to-End Adressierung. ✓

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

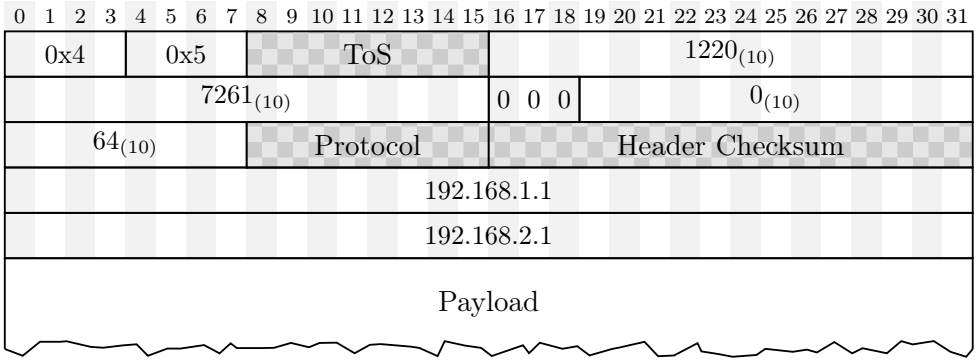


Abbildung 3.2: Schematische Darstellung des von PC1 gesendeten IP-Pakets

e)* Welche Größe besitzt der IP-Header des in Abbildung 3.2 dargestellten Pakets? 1

20 Byte ✓

f)* Wie groß ist die Payload des in Abbildung 3.2 dargestellten Pakets? 1

1220 Byte − 20 Byte = 1200 Byte ✓

g)* Welche Teile der Schicht-2-PDU zählen zur MTU? 1

Die gesamte Payload (Schicht-2-SDU), also das IP-Paket inkl. IP-Header. ✓

h)* An welcher Stelle im Netz findet die Fragmentierung statt? 1

An R1. ✓

1

i) In wieviele Fragmente wird das gesendete Paket aufgeteilt?

$$N = \left\lceil \frac{1220\,\text{Byte} - 20\,\text{Byte}}{580\,\text{Byte} - 20\,\text{Byte}} \right\rceil = 3$$ ✓

1

j)* Begründen Sie, weswegen Fragmente unabhängig voneinander weitergeleitet werden können.

Jedes Fragment erhält einen eigenen IP-Header und besitzt damit alle notwendigen Information, so dass Router Fragmente unabhängig voneinander weiterleiten können. ✓
(Argumentation über Identifier ohne Adressinformationen zu erwähnen ✓)

1

k) Aus welchem Grund kann die Reassemblierung von Paketen i. A. erst beim Empfänger stattfinden?

Einzelne Fragmente können i. A. über unterschiedliche Wege zum Empfänger weitergeleitet werden. Eine Reassemblierung ist daher erst wieder beim Empfänger möglich. ✓

Abbildung 3.3 stellt die Header der einzelnen IP-Fragmente dar (es sind ggf. mehr Fragmente abgedruckt als tatsächlich benötigt werden). Die Header-Felder TOS, Protocol und Header-Checksum können ignoriert werden.

4

l) Füllen Sie für alle Fragmente, die über die Verbindung zwischen R1 und R2 geschickt werden, die freigelassenen Header-Felder in Abbildung 3.3 aus.

2

m)* Welche Veränderungen (mit Begründung!) wurden bei der IP-Fragmentierung mit IPv6 vorgenommen?

Keine Fragmentierung beim Weiterleiten, nur noch beim Absender selbst. ✓ Dies hat Effizienzgründe: Anstatt jedes Paket auf dem Weg zum Empfänger potentiell mehrfach zu fragmentieren, wird der Sender einmal über das Problem in Kenntnis gesetzt. Dieser kann seine MTU entsprechend anpassen. ✓

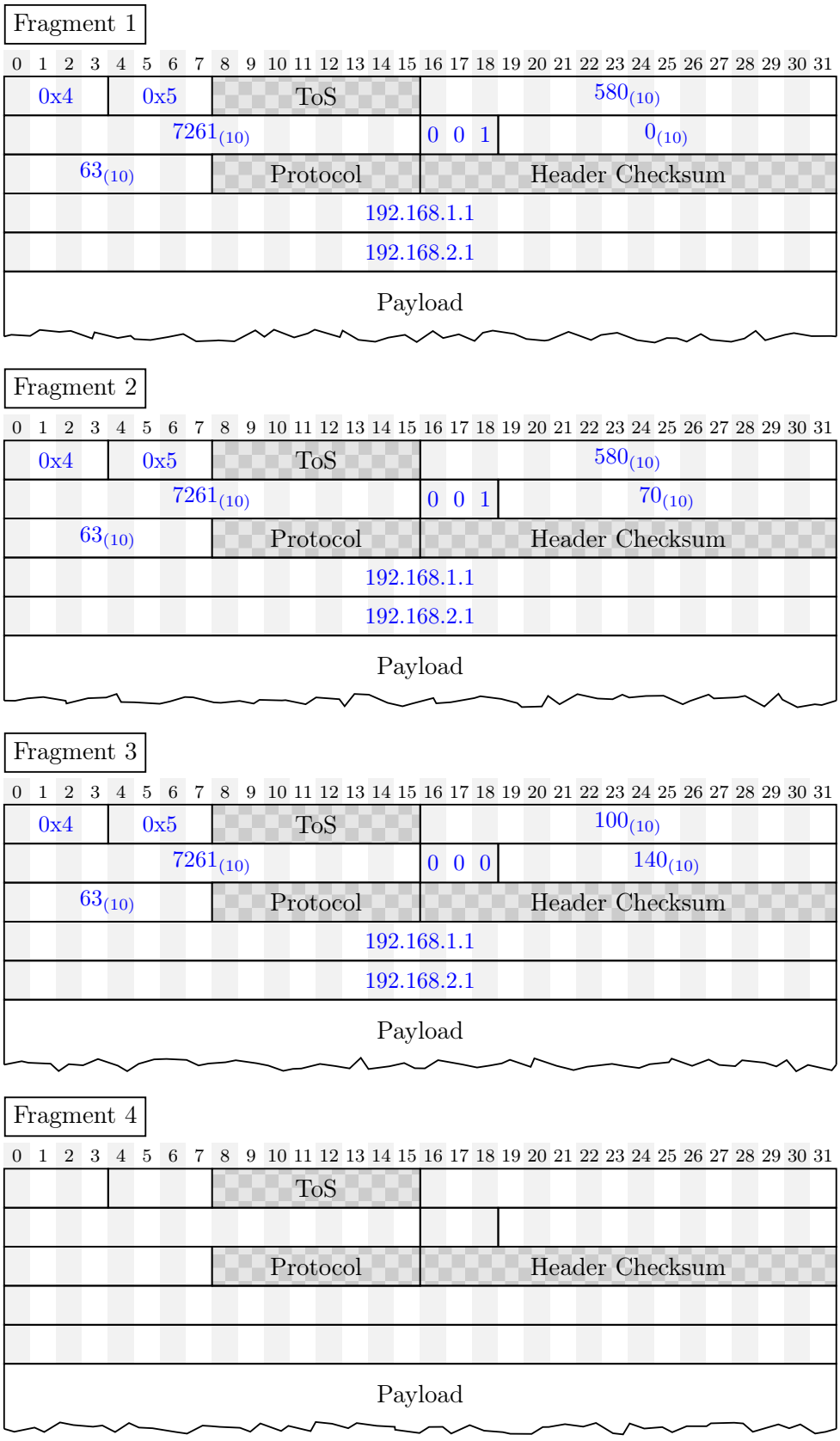


Abbildung 3.3: Lösungsvordruck für Teilaufgabe l)

23

Aufgabe 4 Protocol-Dissemination (23 Punkte)

Wir betrachten das Netzwerk aus Abbildung 4.1, welche zugunsten der Übersicht keine Switches enthält. Sie können davon ausgehen, dass alle eingezeichneten Verbindungen FastEthernet-Segmente darstellen. Sie versuchen, von PC1 aus eine TCP-Verbindung zum Server aufzubauen. Dies misslingt, obwohl Sie davon ausgehen, dass die Router RA - RD korrekt konfiguriert sind und der Server eingehende TCP-Verbindungen akzeptiert. Ein Fehler an PC1 sei ausgeschlossen.

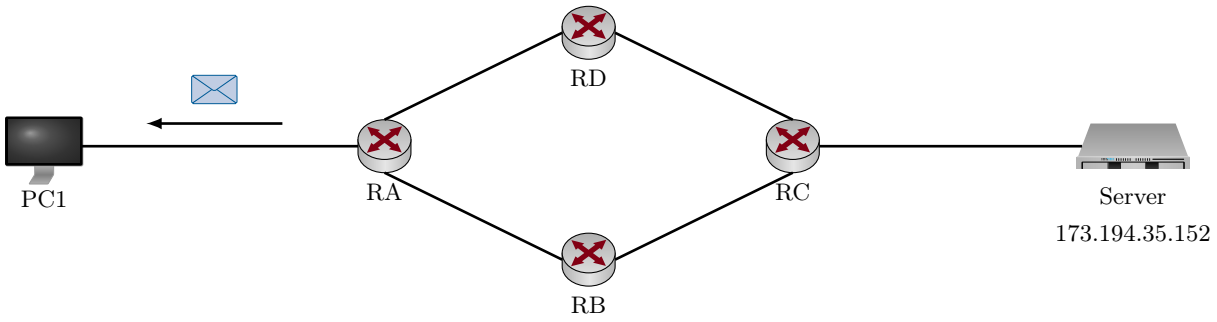


Abbildung 4.1: Vereinfachte Netztopologie (Switches zwischen den Geräten sind der Übersichtlichkeit wegen nicht eingezeichnet)

Sie beschließen deshalb, den Netzwerkverkehr an PC1 mit einem Sniffer[1] zu überprüfen, während Sie erneut versuchen, eine Verbindung zum Server aufzubauen. Dabei zeichnen sie die in Abbildung 4.1 eingezeichnete Nachricht auf, welche an PC1 adressiert ist. Diese Nachricht ist als Hexdump in Abbildung 4.2 abgedruckt. Die linke Spalte gibt den Offset (hexadezimal) in Vielfachen von Bytes an. Die beiden nachfolgenden Spalten repräsentierten die Daten (hexadezimal) in Blöcken zu je 8 Byte in Network-Byte-Order.

```
0000   28 37 37 02 32 41 00 25   90 57 1f dc 08 00 45 00
0010   00 38 b2 40 00 00 3f 01   b1 57 83 9f fc 95 83 9f
0020   14 59 0b 00 5e a4 00 00   00 00 45 00 00 40 16 17
0030   40 00 01 06 fa 4e 83 9f   14 59 ad c2 23 98 e8 fc
0040   01 bb 22 67 a5 d2
```

Abbildung 4.2: Hexdump der in Abbildung 4.1 dargestellten Nachricht (inkl. L2-Header) in Network-Byte-Order.

Im Folgenden werden wir diese Nachricht schrittweise untersuchen und herausfinden, aus welchem Grund der Server nicht erreichbar ist. **Nutzen Sie zur Lösung die auf dem Beiblatt abgegebildeten Protokoll-Header und Zusatzinformationen.**

1

a)* Erklären Sie die Begriffe “Little-Endian” und “Big-Endian”.

Unterschied: Position des höchstwertigen Bytes innerhalb eines Datums, welches länger als 1 Byte ist. Little-Ending = niederwertigstes Byte an niederwertigster Adresse, Big-Endian = niederwertigstes Byte an höchstwertiger Adresse. ✓

[1] Programm zur Aufzeichnung des Datenverkehrs, z. B. Wireshark oder tcpdump

b) Welche Byte-Order entspricht der Network-Byte-Order und welche wird von x86-basierten Computern verwenden?

1

Network-Byte-Order = Big-Endian ✓, x86-Host-Byte-Order = Little-Endian. ✓

Für die nachfolgenden Teilaufgaben ist es sicher hilfreich, wenn Sie sich Anfang und Ende der jeweiligen Header in Abbildung 4.2 markieren. **Bitte beachten** Sie, dass die nachfolgenden Teilaufgaben nur dann bewertet werden, wenn ersichtlich ist, **wie Sie auf die Antwort gegekommen sind** (z. B. Angabe der Werte der betreffenden Header-Felder).

c)* Geben Sie für das erste und letzte Byte des Ethernet-Headers den Offset vom Beginn des Rahmens an.

1

`0x0000` – `0x000D` ✓

d) Bestimmen Sie die MAC-Adresse von RA.

1

`00:25:90:57:1f:dc` ✓

e) Bestimmen Sie die MAC-Adresse von PC1.

1

`28:37:37:02:32:41` ✓

f) Welches L3-Protokoll kommt zum Einsatz (mit Begründung, woran Sie das erkennen).

1

Type-Feld im Ethernet-Header: `08 00` (Big-Endian) = IPv4 ✓

1

g) Geben Sie für das erste und letzte Byte des L3-Headers den Offset vom Beginn des Rahmens an.

`0x000E` – `0x0021` ✓

1

h) Geben Sie die L3-Adresse von PC1 in der üblichen Notation an.

PC1 = `83 9f 14 59` = 131.159.20.89 ✓

1

i) Stammt die Nachricht vom Server?

Nein, `83 9f fc 95` = 131.159.252.149 ≠ 173.194.35.152 ✓

1

j) Bestimmen Sie die TTL der Nachricht.

TTL-Feld `0x3f` = 63 ✓

1

k) Von welchem Gerät stammt die Nachricht mit hoher Wahrscheinlichkeit?

Unter der Annahme, dass Pakete mit dem Default-Wert TTL=64 verschickt werden, kommen RB oder RD in Frage. ✓ (auch korrekt: RA, wenn mit Default-Wert TTL=63 argumentiert wird)

1

l) Welches Protokoll folgt dem L3-Header?

IP-Protocol `0x01` = ICMP ✓

m) Spezifizieren Sie den Nachrichtentyp, der dem L3-Header folgt, so genau wie möglich.

1

ICMP Type 11 Code 0 (TTL exceeded in transit)

n) Beschreiben Sie in Worten (oder durch Skizze) allgemein den Inhalt der Nachricht, die auf den L3-Header folgt.

1

Direkt vom Beiblatt: IP-Header und die ersten 8 Byte der Payload desjenigen Pakets, welches die ICMP-Nachricht ausgelöst hat.

Nach der bisherigen Untersuchung besteht die Vermutung, dass diese Nachricht die Reaktion auf eine andere Nachricht ist, welche zuvor von PC1 versendet wurde. Diese Vermutung soll im Folgenden bestätigt werden.

o) Bestimmen Sie den Empfänger dieser vorangegangenen Nachricht.

1

Zieladresse = `ad c2 23 98` (Big-Endian) = 173.194.35.152 = Server ✓

p) Welche Länge hatte diese Nachricht in Bytes?

1

Total-Length - IP-Header-Length = 64 Byte − 20 Byte = 44 Byte ✓

q) Welche TTL hatte diese Nachricht zuletzt?

1

TTL = `0x01` = 1 ✓

1

r) Welches L4-Protokoll wurde in dieser Nachricht verwendet?

IP-Protocol `0x06` = TCP ✓

1

s) Geben Sie die Quellportnummer dieser Nachricht an.

Quellport = `e8 fc` (Big-Endian) = 52567 ✓

1

t) Geben Sie die Zielportnummer dieser Nachricht an.

Zielport = `01 bb` (Big-Endian) = 443 ✓

1

u) Welches Protokoll wurde auf der Anwendungsschicht verwendet?

TCP 443 = HTTPS ✓

2

v) Beschreiben Sie nun das Problem, aufgrund dessen PC1 keine Verbindung zum Server herstellen kann.

Der Server ist nur vier Hops von PC1 entfernt. Der einzige Grund (abgesehen von einer viel zu klein gewählten TTL, welche nach Aufgabenstellung ausgeschlossen ist) ist eine Routingschleife zwischen den vier Routern. Das Paket wird im Kreis weitergeleitet, bis die TTL abläuft. Hierüber wird PC1 durch eine ICMP-Nachricht von dem betreffenden Router informiert. ✓ ✓

Aufgabe 5 **Kurzaufgaben** (14 **Punkte**)

14

Die folgenden Kurzaufgaben sind **jeweils unabhängig voneinander**. Stichpunktartige Antworten sind ausreichend!

3

a)* Beschreiben Sie den Schlüsselaustausch mittels DH76 zwischen zwei Kommunikationspartnern Alice und Bob. Erklären Sie, welche Informationen ausgetauscht werden. Es ist **nicht** notwendig Formeln anzugeben. Sofern Sie Variablennamen verwenden, erklären Sie deren bedeutung!

- Alice und Bob einigen sich vorab auf eine Primzahl p und einen Generator g (primitive Kongruenzwurzel). ✓
- Alice und Bob erzeugen jeweils eine Zufallszahl a, b und berechnen mittels p, g und dieser Zufallszahlen Nonces A, B, welche über den unsicheren Kanal ausgetauscht werden können. ✓
- Alice kann nun mit a, B, p, g und Bob mit b, A, p, g das gemeinsame Geheimnis K berechnen. ✓

1

b)* Begründen Sie, ob ein Angreifer, welcher den DH76-Schlüsselaustausch beobachtet, den Schlüssel ebenfalls berechnen kann.

A und B werden nicht im Klartext übertragen. Bei richtiger Wahl von g, p nicht (zu komplex / diskreter Logarithmus). ✓

1

c)* Begründen Sie, ob sich Alice i. A. nach dem Schlüsselaustausch sicher sein kann, wirklich mit Bob zu kommunizieren.

Nein. Ein Angreifer kann sich bereits während des Schlüsselaustauschs Alice und Bob gegenüber als der jeweils andere Kommunikationspartner ausgeben (Man-in-the-Middle). ✓

1

d)* Wozu werden CRC-Summen verwendet?

Erkennung (nicht Korrektur) von Übertragungsfehlern. ✓

1

e)* Worin besteht der Unterschied zwischen Leitungs- und Paketvermittlung?

Leitungsvermittlung = Reservierung einer dedizierten Leitung (physikalisch oder logisch) zwischen Sender und Empfänger.
Paketvermittlung = Versand unabhängiger Pakete mit jeweils eigenen Adressinformationen. ✓

2

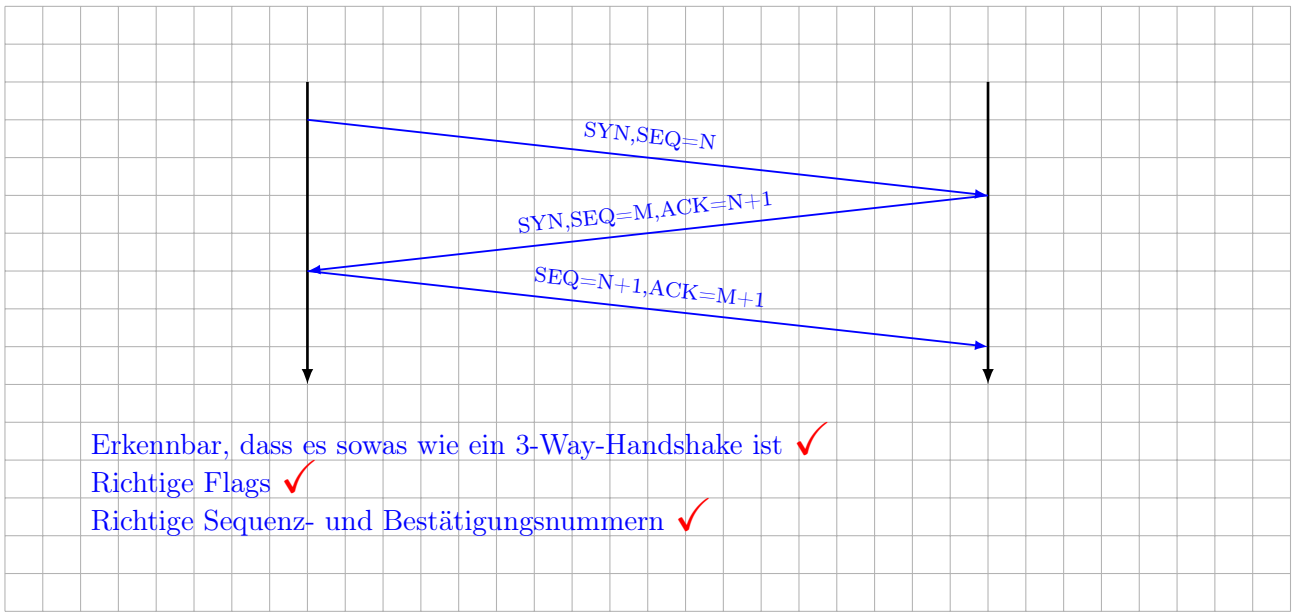
f)* Gegeben sei die zu sendende Nachricht `00101101` in binärer Schreibweise sowie das Generatorpolynom $g(x) = x^3 + x^2 + 1$. Bestimmen Sie die mittels CRC gesicherte Nachricht.

$g(x) =$ `1101`
`00101101 000 : 1101 = 0011001, Rest: 010`
$\Rightarrow$ zu senden ist `00101101 010`

- Ansatz (Anhängen von Nullen + Division durch $g(x)$ in Binärschreibweise aufstellen) ✓
- Richtiger Rest (Rechnung) ✓
- Angabe der gesamten zu sendenden Nachricht ✓

g)* Skizzieren Sie den TCP-Verbindungsaufbau (mit Angabe der Sequenznummern und Flags) als vereinfachtes Weg-Zeit-Diagramm (Serialisierungszeit und Ausbreitungsverzögerung kann vernachlässigt werden).

3



Erkennbar, dass es sowas wie ein 3-Way-Handshake ist ✓
Richtige Flags ✓
Richtige Sequenz- und Bestätigungsnummern ✓

h)* Beschreiben Sie kurz (zwei Stichpunkte genügen) das Prinzip von Token Passing.

1

- Token wird von einer Station zur nächsten weitergegeben. ✓
- Nur die Station, die das Token gerade hält, ist sendeberechtigt. ✓

i)* Wozu werden Routingprotokolle genutzt?

1

Automatisierte Bestimmung kürzester Pfade (gemäß einer bestimmten Metrik) zwischen allen Knoten in einem Netz sowie Austausch dieser Informationen zwischen Routern. ✓

Zusätzlicher Platz für Lösungen – bitte markieren Sie deutlich die Zugehörigkeit zur jeweiligen Aufgabe und streichen Sie ungültige Lösungen!