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
- ☒ Endterm
- ☐ Wiederholung

Prüfungsfach: Grundlagen Rechnernetze und Verteilte Systeme

Prüfer: Prof. Dr.-Ing. Georg Carle **Datum:** 22.07.2014

Hörsaal: _____ **Reihe:** _____ **Platz:** _____

Nur von der Aufsicht auszufüllen:

Hörsaal verlassen **von** _____ : _____ **bis** _____ : _____

Vorzeitig abgegeben **um** _____ : _____

Besondere Bemerkungen:

Endterm-Klausur

Grundlagen Rechnernetze und Verteilte Systeme

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

Dienstag, 22.07.2014
11:30 – 13:00 Uhr

- Diese Klausur umfasst **23 Seiten** und insgesamt **6 Aufgaben**. Außerdem wird ein zusätzliches Hilfsblatt mit Protokollheadern ausgeteilt. Bitte kontrollieren Sie jetzt, ob 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.
- Halten Sie sich bei der Bearbeitung nicht zu lange mit einer (Teil-)Aufgabe auf. Wenn Sie die Aufgabe nicht sofort lösen können, machen Sie lieber mit der nächsten Aufgabe weiter.
- **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 Fourierreihe (10 Punkte)

10

Gegeben sei der in Abbildung 1.1 dargestellte, periodische Dreiecksimpuls. Dieses Signal soll im Folgenden als Fourierreihe

$$s(t) = \frac{a_0}{2} + \sum_{k=1}^{\infty} \left(a_k \cos(k\omega t) + b_k \sin(k\omega t)\right)$$

dargestellt werden. Die Koeffizienten für alle ganzzahligen $k > 0$ lassen sich, wie aus der Vorlesung bekannt, wie folgt bestimmen:

$$a_k = \frac{2}{T} \int_{-T/2}^{T/2} s(t) \cos(k\omega t)\, dt, \quad b_k = \frac{2}{T} \int_{-T/2}^{T/2} s(t) \sin(k\omega t)\, dt.$$

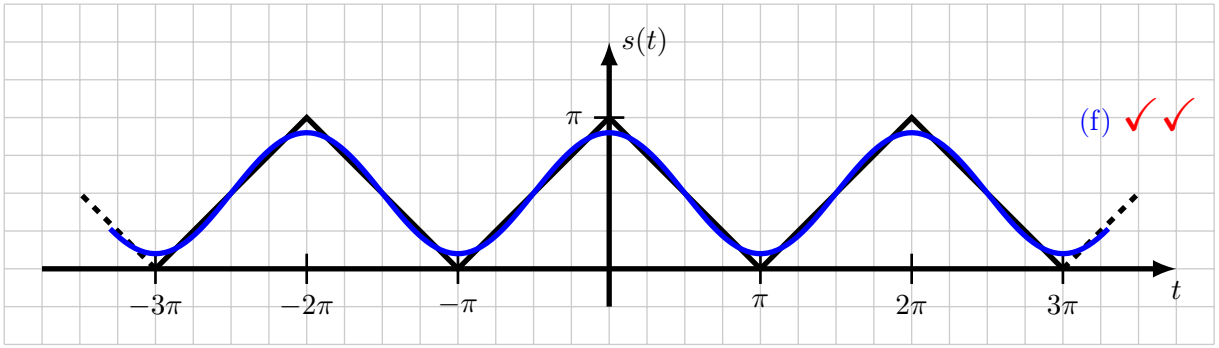


Abbildung 1.1: Periodischer Dreiecksimpuls $s(t)$

1

a)* Geben Sie einen analytischen Ausdruck für den Sendegrundimpuls an, also für das Signal $s(t)$ im Intervall $t \in [-\pi; \pi]$.

$$s(t) = \begin{cases} \pi + t & \text{für } -\pi \leq t < 0, \checkmark \\ \pi - t & \text{für } 0 \leq t < \pi. \checkmark \end{cases}$$

1

b)* Bestimmen Sie die Periodendauer T und Kreisfrequenz $\omega = 2\pi/T$ des Signals.

$$T = 2\pi \checkmark, \quad \omega = 1 \checkmark$$

1

c)* Bestimmen Sie den Gleichanteil a_0.

$$\frac{a_0}{2} = \frac{\pi}{2} \Leftrightarrow a_0 = \pi \checkmark$$

1

d)* Begründen Sie, weswegen $b_k = 0$, $\forall k \in \mathbb{N}$. (keine Rechnung notwendig)

b_k sind Sinus-Anteile. Diese müssen aber 0 sein, da $\sin(t)$ eine ungerade und $s(t)$ eine gerade Funktion ist. ✓

4

e) Zeigen Sie, dass für die Kosinusanteile gilt:

$$a_k = \begin{cases} \frac{4}{k^2\pi} & \text{für } k = 1, 3, 5, \ldots, \\ 0 & \text{sonst.} \end{cases}$$

Hinweis: Je nach Lösungsweg ist einer der beiden folgenden Hinweise hilfreich:

$$\int t\cos(kt)\ dt = \frac{kt\sin(kt) + \cos(kt)}{k^2} + const \tag{1}$$

$$\int_a^b f'(t) \cdot g(t)\ dt = [f(t) \cdot g(t)]_a^b - \int_a^b f(t) \cdot g'(t)\ dt \tag{2}$$

Lösung mittels partieller Integration:

$$\begin{aligned} a_1 &= \int_{-T/2}^{T/2} s(t)\cos(k\omega t)\ dt \ ✓ \\ &= \frac{2}{\pi}\int_0^{\pi} (\pi - t)\cos(kt)\ dt \\ &= \frac{2}{k\pi}\Big[(\pi - t)\sin(kt)\Big]_0^{\pi} + \frac{2}{k\pi}\int_0^{\pi} \sin(kt)\ dt ✓ \\ &= \frac{2}{k^2\pi}\Big[-\cos(kt)\Big]_0^{\pi} \\ &= \begin{cases} \frac{4}{k^2\pi} & \text{für } k = 1, 3, 5, \ldots, \ ✓ \\ 0 & \text{sonst.} \ ✓ \end{cases} \end{aligned}$$

2

f)* Zeichnen Sie das approximierte Signal $s'(t) = \frac{a_0}{2} + a_1\cos(\omega t)$ in Abbildung 1.1 ein.

Aufgabe 2 PHY und MAC bei PCIe (16 Punkte)

16

Das ISO/OSI-Modell ist nicht nur auf Kommunikationsvorgänge im Internet anwendbar. Vielmehr ist es ein abstraktes Modell für beliebige Kommunikationsvorgänge. In dieser Aufgabe betrachten wir die Anwendung auf PCIe (Peripheral Components Interconnect express), welcher heute den Standard zum schnellen Datenaustausch zwischen Geräten innerhalb eines Computers darstellt. Beispielsweise werden in heutigen Computern praktisch alle internen Erweiterungskarten (Grafikkarten, Netzwerkkarten, Soundkarten, etc.) sowie viele integrierte Geräte wie SATA-Controller über diese Schnittstelle angeschlossen. PCIe selbst ist ein serielles, geswitchtes Netzwerk zwischen diesen Geräten.

1

a)* Begründen Sie, welchen Vorteil geswitchte Verbindungen gegenüber einem Bussystem haben.

Durch die Nutzung eines Switches werden mehrere Punkt-zu-Punkt Verbindungen zwischen jeweils zwei Geräten zur selben Zeit möglich. ✓Bei einem Bus gäbe es konkurrierenden Zugriff auf ein gemeinsames Medium, d.h. es könnte zu jedem Zeitpunkt jeweils nur ein Gerät senden. ✓

Auf der physikalsichen Schicht nutzt PCIe pro Lane[1] zwei Datenleitungen pro Richtung, auf denen Signale jeweils differentiell kodiert übertragen werden. Ein Beispiel ist in Abbildung 2.1 dargestellt. Das Empfangssignal ergibt sich aus Addition beider Einzelsignale, d.h. $s(t) = s^+(t) + s^-(t)$.

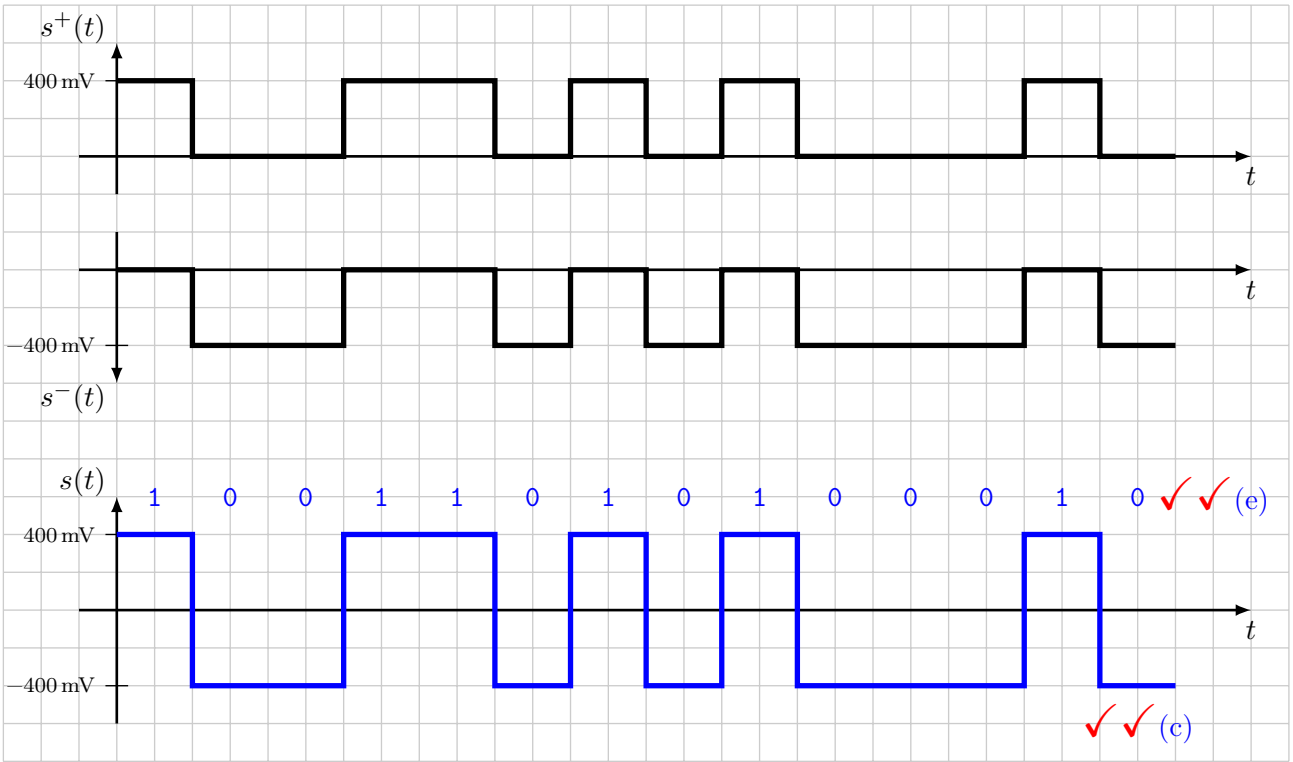


Abbildung 2.1: Differentiell kodierte Signale $s^+(t)$ und $s^-(t)$ sowie Empfangssignal $s(t) = s^+(t) + s^-(t)$.

[1] Wir betrachten hier nur PCIe mit einer Lane, also PCIe x1.

2

b)* Zeichnen Sie in Abbildung 2.1 das Empfangssignal $s(t)$ ein.

1

c) Welchen Sendegrundimpuls verwendet PCIe offensichtlich?

NRZ (no return to zero) ✓

2

d) Geben Sie in Abbildung 2.1 die übertragene Bitfolge an. Tragen Sie Ihre Lösung direkt in Abbildung 2.1 ein. **Hinweis:** Es gibt zwei äquivalente Lösungen.

1

e)* Nennen Sie einen Vorteil der differentiellen Übertragung in diesem konkreten Fall.

- Es ist kein Massebezug notwendig. ✓
- Die Differenz zwischen einer logischen '1' (400 mV) und einer logischen '0' (−400 mV) ist das doppelte der Amplitude auf jeder Leitung. Es ist so leichter, die Signalpegel zuverlässig auseinander zu halten.

1

f)* Als Leitungscode verwendet PCIe die 8B10B-Kodierung. Nennen Sie zwei Vorteile, die sich daraus ergeben.

- Taktrückgewinnung ✓
- zusätzliche Steuerzeichen ✓
- (Gleichstromfreiheit)

1

g)* Die Bruttodatenrate beträgt 2,5 $\frac{\text{Gbit}}{\text{s}}$ pro Lane und Transferrichtung. Bestimmen Sie die Nettodatenrate unter Berücksichtigung der 8B10B-Kodierung.

$$r_{netto} = \frac{8}{10} \cdot 2{,}5 \frac{\text{Gbit}}{\text{s}} \checkmark = 2{,}0 \frac{\text{Gbit}}{\text{s}} \checkmark$$

Auf der Sicherungsschicht verwendet PCIe 32 bit lange CRC-Checksummen. Vereinfachend nehmen wir an, dass jeder Rahmen eine 8 bit lange Sequenznummer trägt, welche vom Sender für jeden gesendeten Rahmen um 1 inkrementiert wird. Die Sende- und Empfangspuffer betragen auf beiden Seiten 4 Rahmen. Als Flusskontrolle kommt Go-Back-N zum Einsatz.

Der Empfänger quittiert (ACK) erfolgreich übertragene Rahmen, wobei Bestätigungen stets die nächste erwartete Sequenznummer enthalten. Ferner wird der Sender über fehlerhaft übertragene Rahmen mittels negativer Bestätigungen (NACK) explizit informiert. Nachfolgende, korrekt übertragene Rahmen mit höherer Sequenznummer werden gemäß Go-Back-N ignoriert und nicht bestätigt.

h)* Welches Ziel wird durch die Checksummen verfolgt? 1

Erkennung von Bitfehlern in einem Rahmen. ✓

i)* Nennen Sie eine weitere Ihnen bekannte Übertragungstechnik, welche ebenfalls Bestätigungen auf der Sicherungsschicht einsetzt. 1

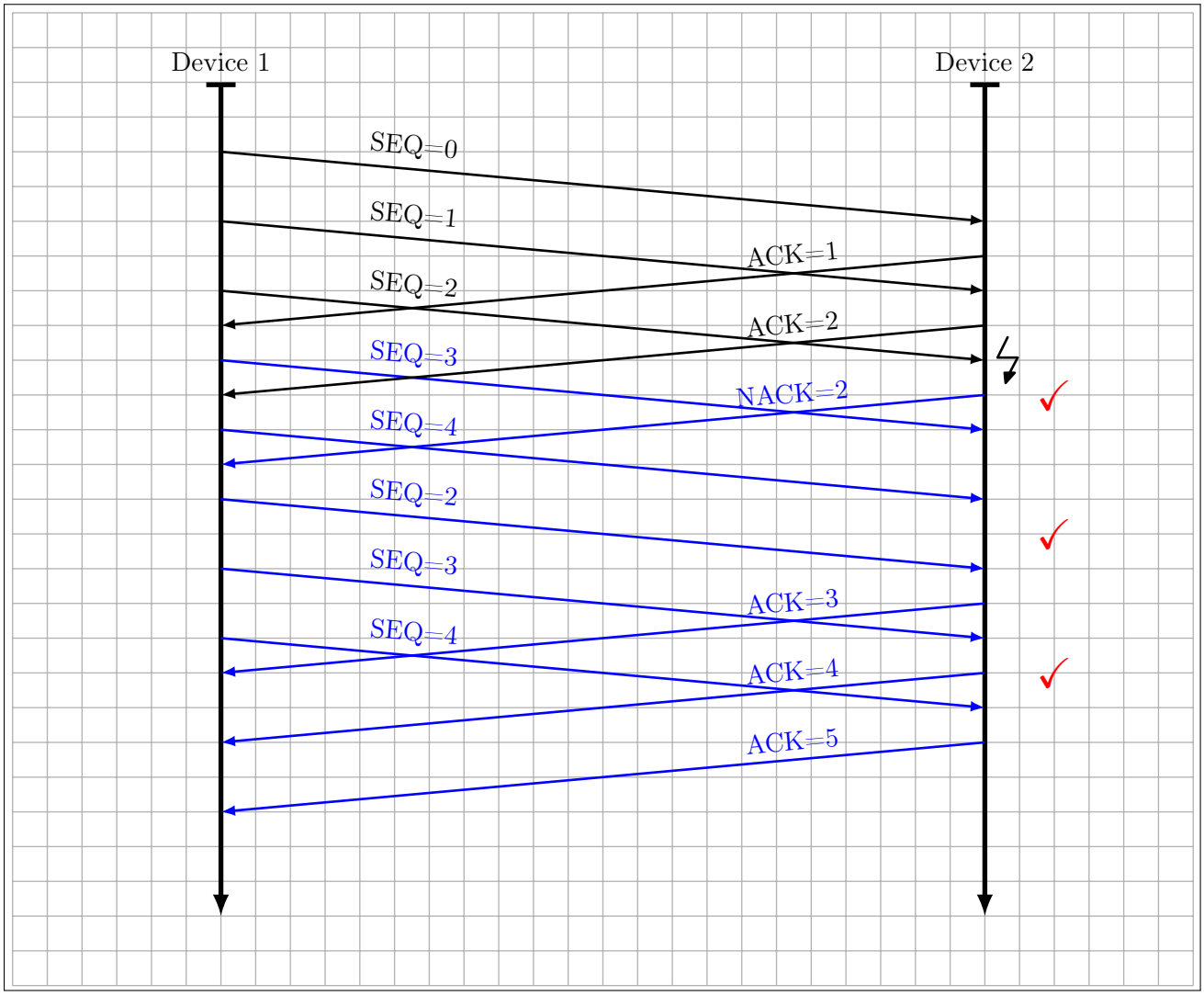
IEEE 802.11 ✓

j)* Beschreiben Sie, welches Ziel mit der Flusskontrolle verfolgt wird. 1

Verhinderung von Überlastsituationen am Empfänger. ✓

3

k)* Gegeben sei der im Lösungsfeld abgedruckte Nachrichtenaustausch. Bei dem durch einen Blitz gekennzeichneten Rahmen (SEQ=2) werde beim Empfänger ein Fehler erkannt. Vervollständigen Sie den Nachrichtenaustausch, bis SEQ=4 erfolgreich übertragen wurde. Nehmen Sie hierzu an, dass keine weiteren Fehler mehr auftreten.
Hinweis: Sie finden bei Bedarf einen weiteren Vordruck auf Seite 20. Streichen Sie bitte deutlich ungültige Lösungen.



1

l) Wie würde sich das Ergebnis von Teilaufgabe k) ändern, wenn Selective Repeat verwendet würde?

Die Rahmen mir SEQ=3 und SEQ=4 müssten nicht noch einmal wiederholt werden. ✓

Aufgabe 3 IP-Fragmentierung und Path-MTU-Discovery (19 Punkte)

19

In dieser Aufgabe betrachten wir zunächst Fragmentierung bei IPv4. Hierzu ist die Netzwerktopologie in Abbildung 3.1 gegeben.

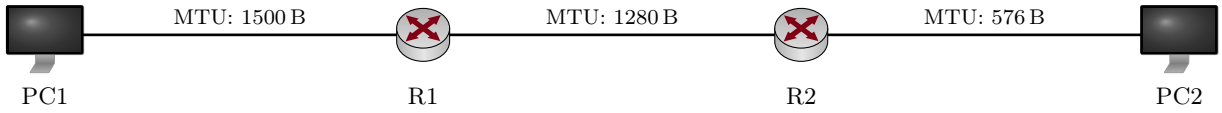


Abbildung 3.1: Netztopologie

Die Router R1 und R2 sind so konfiguriert, dass die beiden Hosts PC1 und PC2 miteinander kommunizieren können. Die drei Netzsegmente sind voneinander unabhängig und verwenden verschiedene Übertragungstechnologien, sodass sich die in der Abbildung ersichtlichen MTUs ergeben.

a)* Grenzen Sie die Begriffe MTU und MSS gegeneinander ab.

1

Die MSS gibt die Größe der TCP (Layer 4) Segmente ohne Header an ✓. Die MTU die Größe der IP (Layer 3) Pakete inklusiv IP-Header ✓.

b)* Wie sollte die MSS in Abhängigkeit von der MTU gewählt werden (Formel)?

1

$MSS = MTU - 40B$ ✓, 20B für IP-Header, 20B für TCP-Header

c)* Können Fragmente nochmals fragmentiert werden?

1

Ja ✓, die Zuordnung der Fragmente erfolgt über ID und Offset ✓.

d)* An welcher Stelle im Netzwerk werden Fragmente reassembliert (Begründung)?

1

IP-Fragmente werden erst auf dem Destination Host ✓wieder reassembliert. Die Fragmente können über unterschiedliche Pfade geroutet werden ✓.

2

e)* Woran erkennt man, dass es sich um ein vollständiges (unfragmentiertes) IP-Paket handelt?

Ein unfragmentiertes IP Paket hat das MF (More Fragments) Flag nicht gesetzt ✓ und der Fragment Offset muss 0 ✓ sein.

1

f)* Welches Problem tritt beim Empfänger beim Verlust einzelner Fragmente auf?

Das Paket kann nicht reassembliert werden ✓ und geht vollständig verloren ✓.

Gehen Sie nun davon aus, dass PC1 eine TCP-Verbindung zu PC2 aufgebaut hat. PC1 möchte nun 1460 B Nutzdaten über diese TCP-Verbindung an PC2 senden.
PC1 versendet diese Daten unter Berücksichtigung der benötigten minimalen IP- und TCP-Header. Der Router R1 kann das resultierende Paket nicht direkt weiterleiten und muss es zunächst fragmentieren.

1

g) Geben Sie die jeweilige Größe aller von R1 an R2 gesendeten IP-Pakete an.

1276 B ✓ = 20 B IP-Header + 20 B TCP-Header + 1236 B und
244 B ✓ = 20 B IP-Header + 224 B.
IP Header für beide Pakete, TCP Header nur einmal, der IP Payload von Fragmenten muss wegen dem Offset ein Vielfaches von 8 Byte sein.

2

h) Router R2 muss diese Pakete jetzt auf geeignete Weise verarbeiten. Geben Sie die jeweilige Größe aller von R2 an PC2 gesendeten IP-Pakete an.

572 B ✓ = 20 B IP-Header + 20 B TCP-Header + 532 B,
572 B ✓ = 20 B IP-Header + 552 B,
172 B ✓ = 20 B IP-Header + 152 B und
244 B ✓ = 20 B IP-Header + 224 B.
IP Header in allen Paketen notwendig, TCP Header nur einmal, der IP Payload von Fragmenten muss wegen dem Offset ein Vielfaches von 8 Byte sein, Paket darf auf R2 nicht reassembliert werden.

Als Alternative zur IP-Fragmentierung betrachten wir nun die Path-MTU-Discovery. Hierzu nutzen wir weiterhin die Netzwerktopologie aus Abbildung 3.1. PC1 möchte weiterhin über eine schon bestehende TCP-Verbindung Nutzdaten mit einer Länge von 1460 B an PC2 versenden.
Path-MTU-Discovery wird verwendet, um Fragmentierung im Netzwerk zu verhindern. Damit auch der Sender keine IP-Fragmentierung durchführen muss, kann dieser die TCP MSS entsprechend anpassen. Path-MTU-Discovery funktioniert wie folgt:

- Der Sender versendet zunächst Pakete der Größe der lokalen MTU.
- Diese Pakete dürfen im Netzwerk nicht fragmentiert werden.
- Wenn ein Router ein solches Paket erhält, es aber wegen der MTU im nachfolgenden Netzsegment nicht direkt weiterleiten kann, so schickt er eine ICMP Destination Unreachable, Fragmentation Needed (Type3, Code 4) Nachricht an den Sender.
- Diese Nachricht enthält die MTU des nachfolgenden Netzsegments und der Router verwirft das ursprüngliche Paket.
- Der Sender muss die Daten erneut unter Einhaltung dieser MTU versenden. Bei TCP ist dies durch die Anpassung der MSS möglich.
- Der Sender speichert sich die MTU für nachfolgende Pakete mit demselben Ziel.

i)* Wie stellt der Sender sicher, dass seine Pakete im Netzwerk nicht fragmentiert werden dürfen? /1

Ein gesetztes ✓DF (Don't Fragment) Flag ✓weist Router an die Pakete nicht zu fragmentieren.

j)* Wie kann der Sender im Allgemeinen bei gleichzeitiger Path-MTU-Discovery zu mehreren Zielen eine ICMP Nachricht (Typ 3, Code 4) entsprechend zuordnen? /2

Die ICMP Nachricht enthält neben dem ICMP Header auch den IP Header und die ersten 8 Payload Bytes des auslösenden Pakets. ✓ Der Empfänger der ICMP Nachricht kann den original IP-Header entpacken und über die darin enthaltene Ziel-IP die Verbindung zuordnen. ✓

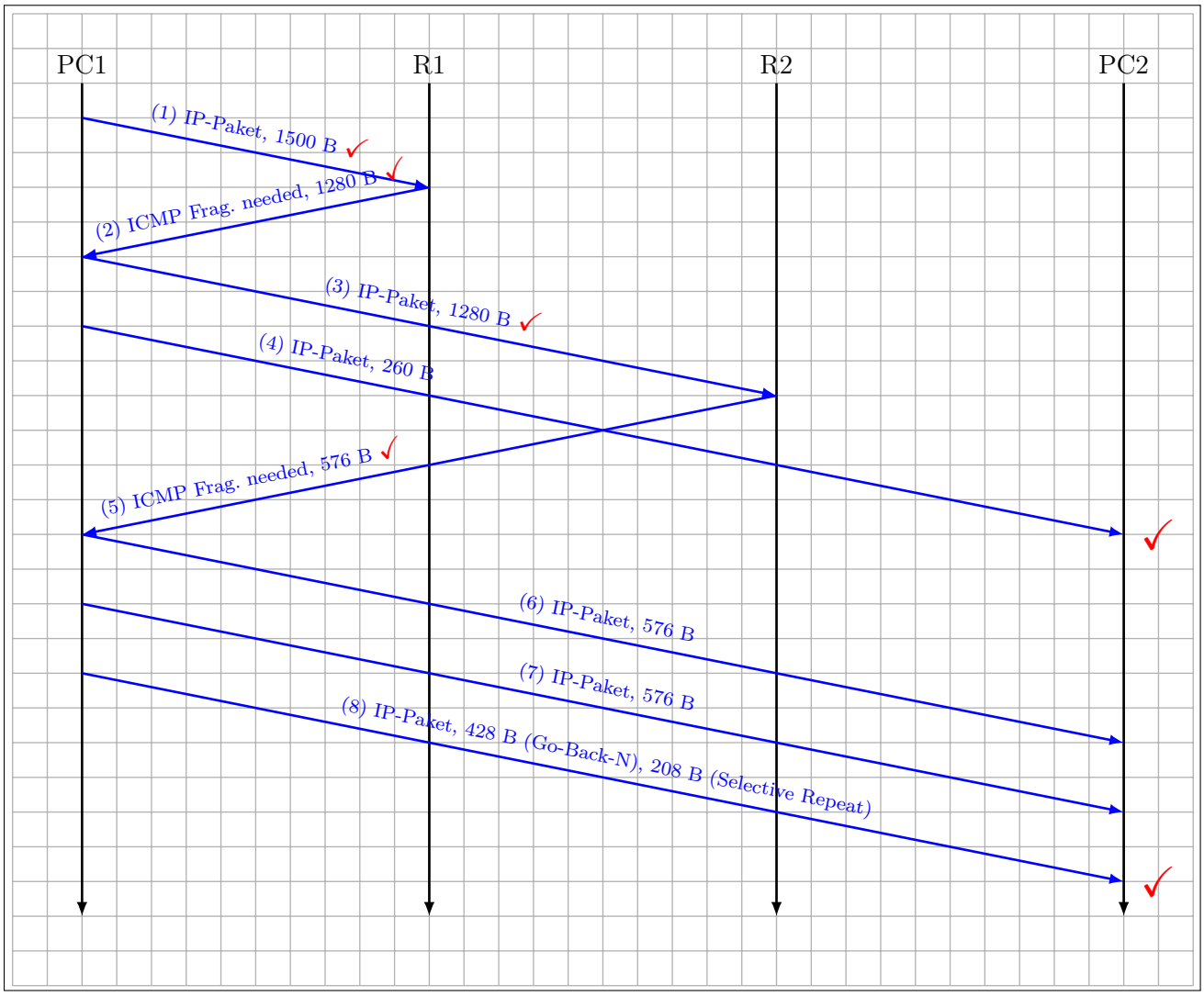
2

k) Berechnen Sie die jeweilige Größe aller benötigten IP-Pakete, um TCP-Nutzdaten mit einer Länge von 1460 B von PC1 zu PC2 ohne jedwede Fragmentierung zu übertragen. Berücksichtigen Sie hierbei alle notwendigen Header in ihrer minimalen Größe.

576 B ✓= 20 B IP-Header + 20 B TCP-Header + 536 B,
576 B ✓= 20 B IP-Header + 20 B TCP-Header + 536 B und
428 B ✓ = 20 B IP-Header + 20 B TCP-Header + 388 B.
IP- und TCP-Header in jedem Paket.

4

l) Zeichnen Sie nun ein vereinfachtes Weg-Zeit-Diagramm (Serialisierungszeit und Ausbreitungsverzögerung können vernachlässigt werden) für die Path-MTU-Discovery und das Versenden der Nachricht (1460 B TCP-Nutzdaten). Geben sie bei Datenpaketen die Gesamtgröße des IP-Pakets an („IP-Paket, 128 B“). ICMP Fragmenation Needed Pakete sind als solche zu markieren und die zurückgegebene MTU ist anzugeben („ICMP Frag. needed, 256 B“). **Hinweis:** Das initiale Congestion Window für TCP beträgt 10 MSS. Vernachlässigen Sie TCP-Acknowledgements und eventuelle Layer 2 Nachrichten.



Aufgabe 4 Routing in IP-Netzen (13 Punkte)

13

Abbildung 6.1 zeigt ein IPv4-basiertes Netzwerk. Es besteht aus einigen Hosts (H1, H2, ...), den Routern R1, R2 und R3 und dem Switch S1. Tabelle 1 zeigt die Routing-Tabellen von R1 und R2.

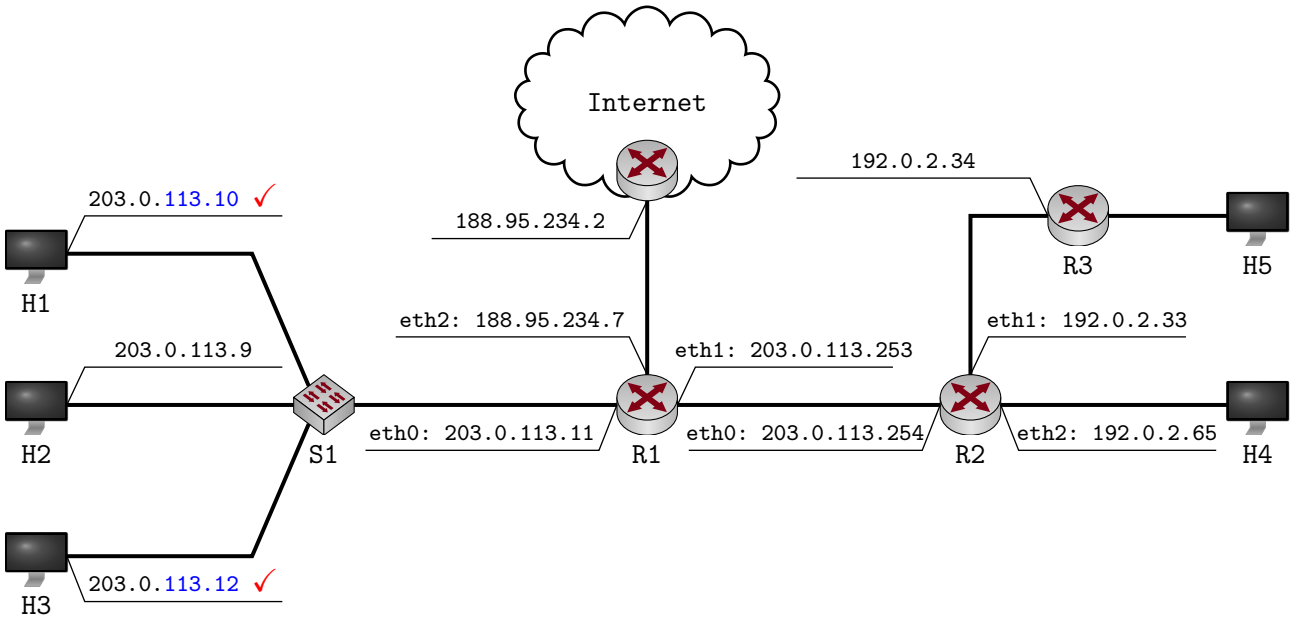


Abbildung 4.1: Netztopologie

a)* Nennen Sie die Netzadresse und die Broadcast-Adresse des Netzes 203.0.113.8/29.

1

Netzadresse: 203.0.113.8 ✓

Broadcast-Adresse: 203.0.113.15 ✓

b)* Wieviele Adressen im Netz 203.0.113.8/29 können an Hosts vergeben werden?

1

/29 $\rightarrow 2^{32-29} = 2^3 = 8$, nutzbar: $8 - 2 = 6$ Adressen ✓

c) Vergeben Sie gültige IP-Adressen an die Hosts H1 und H3. Tragen Sie Ihre Antwort direkt in Abbildung 6.1 ein.

1

Router R1

Destination	Gateway	Iface
203.0.113.8/29	—	eth0
203.0.113.252/30	—	eth1
188.95.234.7/23	—	eth2
192.0.2.32/27	203.0.113.254	eth1
192.0.2.64/26	203.0.113.254	eth1
0.0.0.0/0	188.95.234.2	eth2

Router R2

Destination	Gateway	Iface
192.0.2.32/27	—	eth1
192.0.2.64/27	—	eth2
192.0.2.96/27	192.0.2.34	eth1
203.0.113.252/30	—	eth0
0.0.0.0/0	203.0.113.253	eth0

Tabelle 1: Statische Routing-Tabellen der Router `R1` und `R2`.
(auszufüllen in Teilaufgabe (h))

d)* Wie kann ein Router bestimmen, ob die Route mit Adresse a_R und Subnetz-Maske m_R für die Adresse a_P eines Pakets in Frage kommt? 1

$a_P \odot m_R = a_R \odot m_R$
$\odot$: bitweises und

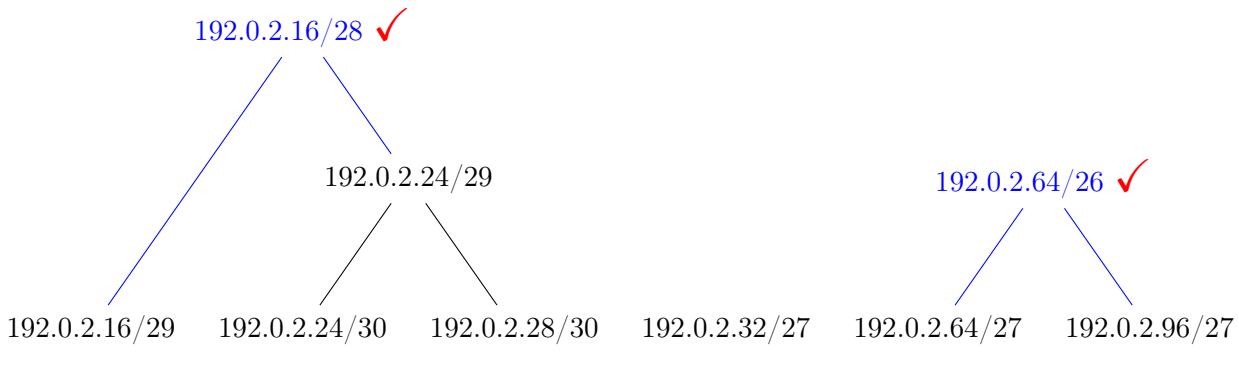
e)* Welchen Eintrag aus der Forwarding-Tabelle wählt ein Router, wenn mehrere geeignet sind? 1

den mit dem längsten Präfix (LPF) ✓

f)* Nennen Sie **zwei** Kriterien, die erfüllt sein müssen, damit ein Router zwei Einträge in seiner Tabelle aggregieren kann. 2

nebeneinander ✓ + gleich groß ✓ + Maske«1 passt ✓ + gleicher Port/Gateway ✓ (oder: Default-Gateway + X an gleichem Port)

g) Aggregieren Sie folgende Netze soweit wie möglich. Verwenden Sie dazu, wie gezeigt, eine Darstellung als Binärbaum. 2



h) Ergänzen Sie die Routing-Tabelle (Tabelle 1 auf S. 12) so, dass 4

- jeder Host jeden anderen im gegebenen Netz und im Internet erreichen kann.
- alle Einträge soweit wie möglich aggregiert sind.

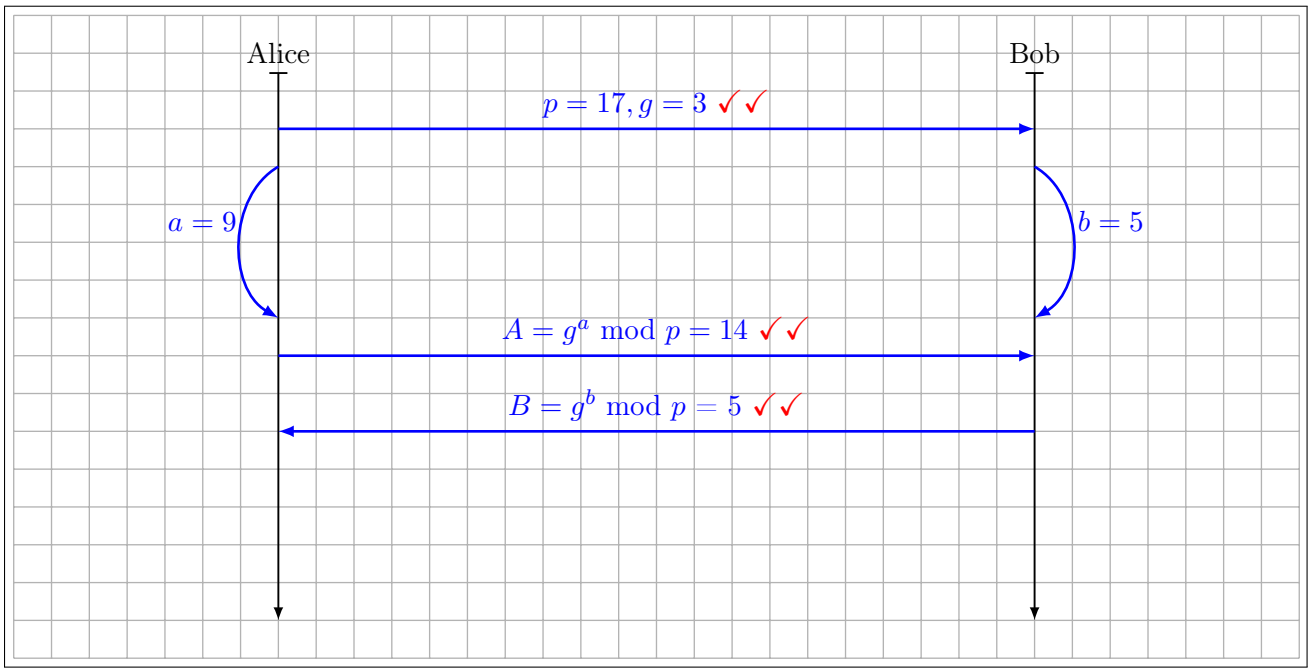
14

Aufgabe 5 Schlüsselaustausch und Anwendungen (14 Punkte)

Im Folgenden wird das Diffie-Hellman-Schlüsselaustauschverfahren betrachtet. Gegeben seien hierfür die Primzahl $p = 17$ und die Primitivwurzel $g = 3$. Alice und Bob wollen nun dieses Verfahren anwenden. Nehmen Sie an, Alice wählt $a = 9$ und Bob wählt $b = 5$ als Zufallszahl.

3

a)* Skizzieren Sie den Diffie-Hellman Schlüsselaustausch, indem Sie die notwendigen Nachrichten in das nachfolgende Diagramm einzeichnen. Beschriften Sie die Nachrichten sowohl mit den allgemeinen Formeln als auch den konkreten Werten.



1

b) Bestimmen Sie das Shared Secret („Schlüssel“), welches Bob und Alice nun berechnen können.

$K = A^b \bmod p =$ ✓$14^5 \mod 17 = 12$ ✓
$K = B^a \bmod \mathrm{p} = 5^9 \mod 17 = 12$

2

c)* Begründen Sie, ob $g = 16$ auch eine geeignete Wahl für $p = 17$ wäre (Rechnung und Begründung).

$$16^1 \mod 17 = 16$$
$$16^2 \mod 17 = 1$$
$$16^3 \mod 17 = 16$$

$16^1 \mod 17 = 16^3 \mod 17$ ✓ → 16 ist keine primitive Kongruenzwurzel und daher keine geeignete Wahl ✓

d)* Begründen Sie, ob der Diffie-Hellman-Schlüsselaustausch sicher gegen Man-in-the-Middle-Angriffe ist.

1

Nein, ✓der Verbindungsaufbau kann abgefangen und manipuliert werden bzw. sich die Kommunikationsparteien nicht gegenseitig authentisieren. ✓

e) Wie würden bei der Verwendung von El Gamal die jeweils öffentlichen und privaten Schlüssel für Alice und Bob aussehen? Verwenden Sie Ihre konkreten Werte aus den vorherigen Aufgaben.
Hinweis: Diese können direkt aus dem Diffie-Hellman-Verfahren abgeleitet werden.

1

$Bob_{priv} = b = 5$ und $Bob_{pub} = (p, g, B) = (17, 3, 5)$ ✓
$Alice_{priv} = a = 9$ und $Alice_{pub} = (p, g, A) = (17, 3, 14)$ ✓

Eine unabhängige dritte Partei X möchte nun Alice eine verschlüsselte Nachricht m senden und verwendet hierfür den öffentlichen Schlüssel A von Alice, welchen Sie bereits in einer der vorangegangenen Teilaufgaben bestimmt haben.
Hinweis: $c = k \cdot m \mod p$ mit $k = A^x \mod p$, wobei x durch die dritte Partei frei wählbar ist, mit $x \in \{1, p-1\}$. $m = k^{-1} \cdot c \mod p$ mit $k^{-1} = X^{p-a-1} \mod p$, wenn p eine Primzahl ist.

f) Alice erhält die verschlüsselte Nachricht $(X, c) = (9, 8)$. Bestimmen Sie den Klartext.

2

$m = k^{-1} \cdot c \mod p$
$= ((X^{p-a-1} \mod p) \cdot c) \mod p$
$((9^7 \mod 17) \cdot 8) \mod 17$ ✓
$m = 16$ ✓

g)* Begründen Sie, ob die Hash-Funktion $h = n \mod 5$, wobei n die Nachricht darstellt und $n \in \mathbb{N}$ gilt, über eine ausreichende kryptografische Stärke verfügt.

1

Nein, ✓die gegebene Funktion ist nicht einmal eine schwache Hash-Funktion, sodass sehr einfach ein m' bestimmt werden kann, sodass eine Kollision entsteht, d.h. es gilt: $h = m \mod 5 = m' \mod 5$ mit $m = m'$ ✓

1

h)* Schätzen Sie die allgemeine Aussagekraft eines Message Authentication Code (MAC) in Bezug auf Authentizität ein, wenn Sie den zugehörigen Schlüssel zusammen mit der Nachricht erhalten haben.

Aunthentiziät der Nachricht kann im Allgemeinen nicht gewährleitst werden, ✓da die Kopplung zwischen Inhaber und Schlüssel nicht mehr gewährleistet ist. ✓

1

i)* Begründen Sie, ob ein Message Authentication Code (MAC) wirksam gegen Replay-Angriffe, d.h. wiederholtes Einspielen von gleichen Nachrichten, ist?

Nein, ✓wiederholtes Senden gleicher Nachrichten führt nicht zu ungültigen MACs ✓

1

j)* Nennen Sie ein aus der Vorlesung bekanntes Schutzziel, welches durch kryptografische Verfahren im Allgemeinen nicht erreicht werden kann.

Verfügbarkeit ✓

Aufgabe 6 Surfen im Web (13 Punkte)

13

Gegeben sei folgende Infrastruktur. Der **Client** führt einen Browser aus, welcher auf die URL „http://web.lan/grnvs.html“ zugreift. Die im Netz versandten Ende-zu-Ende-Nachrichten werden mit gestrichelten Linien gekennzeichnet, die Pfeile bezeichnen die Senderichtung. Sie sind mit ⓐ – ⓕ beschriftet.
Gehen Sie davon aus, dass Router bereits den DNS-Server und den Web-Server im ARP-Cache hat; die Caches des Clients sind leer. Gehen Sie ferner davon aus, dass alle Dienste ihre Standardports verwenden. MAC-Adressen können Sie im Stil Host.Interface, also z.B. C.eth0, angeben.

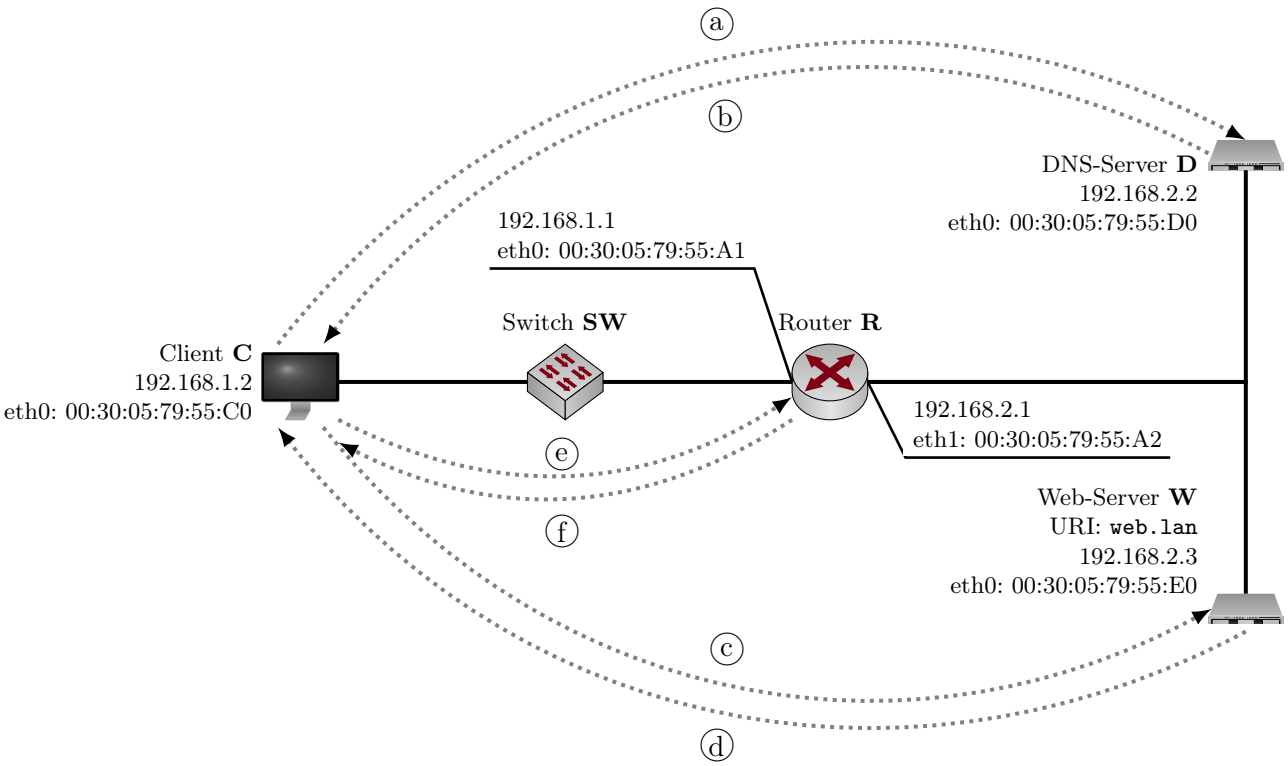


Abbildung 6.1: Netztopologie

a)* Wovon hängen die ersten drei Byte der MAC-Adresse ab?

1

Jeder Hersteller besitzt ein eindeutiges, drei Byte langes Präfix. ✓

b)* Welche Header der Nachricht vom Client zum Web-Server werden vom Switch verändert? Begründen Sie Ihre Antwort kurz.

1

Keine ✓Der Switch leitet die Nachrichten lediglich transparent weiter. ✓

2

c)* Füllen Sie Tabelle 2 vollständig aus. Geben Sie die Nachrichten ⓐ – ⓕ in *chronologischer* Reihenfolge an und nennen Sie jeweils das höchste in der Nachricht verwendete Protokoll (bezogen auf das Schichtenmodell).

Nr	Nachricht	Typ	Nr	Nachricht	Typ
1	ⓔ	**ARP**	4	ⓑ ✓	**DNS**✓
2	ⓕ ✓	**ARP**✓	5	ⓒ ✓	**HTTP**✓
3	ⓐ ✓	**DNS**✓	6	ⓓ ✓	**HTTP**✓

Tabelle 2: Ende-zu-Ende-Nachrichten

2

d) Welche IP-Pakete müssen beim Versand der Nachricht ⓐ verschickt werden? Füllen Sie in der nachfolgenden Tabelle jeweils eine Zeile für jedes Paket aus.
Hinweis: Die Tabelle enthält möglicherweise mehr Zeilen als notwendig. Ein Punkt ✓pro Zeile

MAC		IP		Port	
von	zu	von	zu	von	zu
C.eth0	R.eth0	.1.2	.2.2	1234	53
R.eth1	D.eth0	.1.2	.2.2	1234	53

2

e) Gehen Sie genauso für Nachricht ⓓ vor.
Hinweis: Auch diese Tabelle enthält möglicherweise mehr Zeilen als notwendig. Ein Punkt ✓pro Zeile

MAC		IP		Port	
von	zu	von	zu	von	zu
Web.eth0	R.eth1	.2.3	.1.2	80	5678
R.eth0	C.eth0	.2.3	.1.2	80	5678

Im Folgenden finden Sie das erste TCP-Paket, welches der Client zum Web-Server sendet.

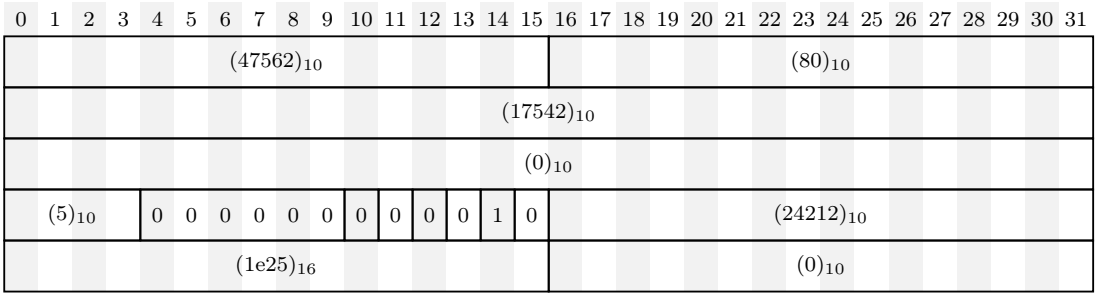


Abbildung 6.2: Erstes TCP-Paket vom Client zum Web-Server

f)* Füllen Sie die weißen Felder des TCP-Headers der Serverantwort (Abb. 6.3) korrekt aus. Beachten Sie auch, die Flags richtig zu setzen.

3

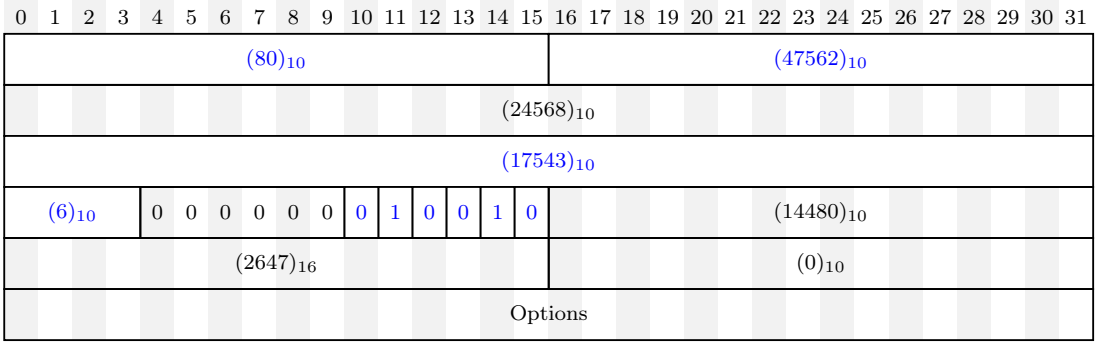


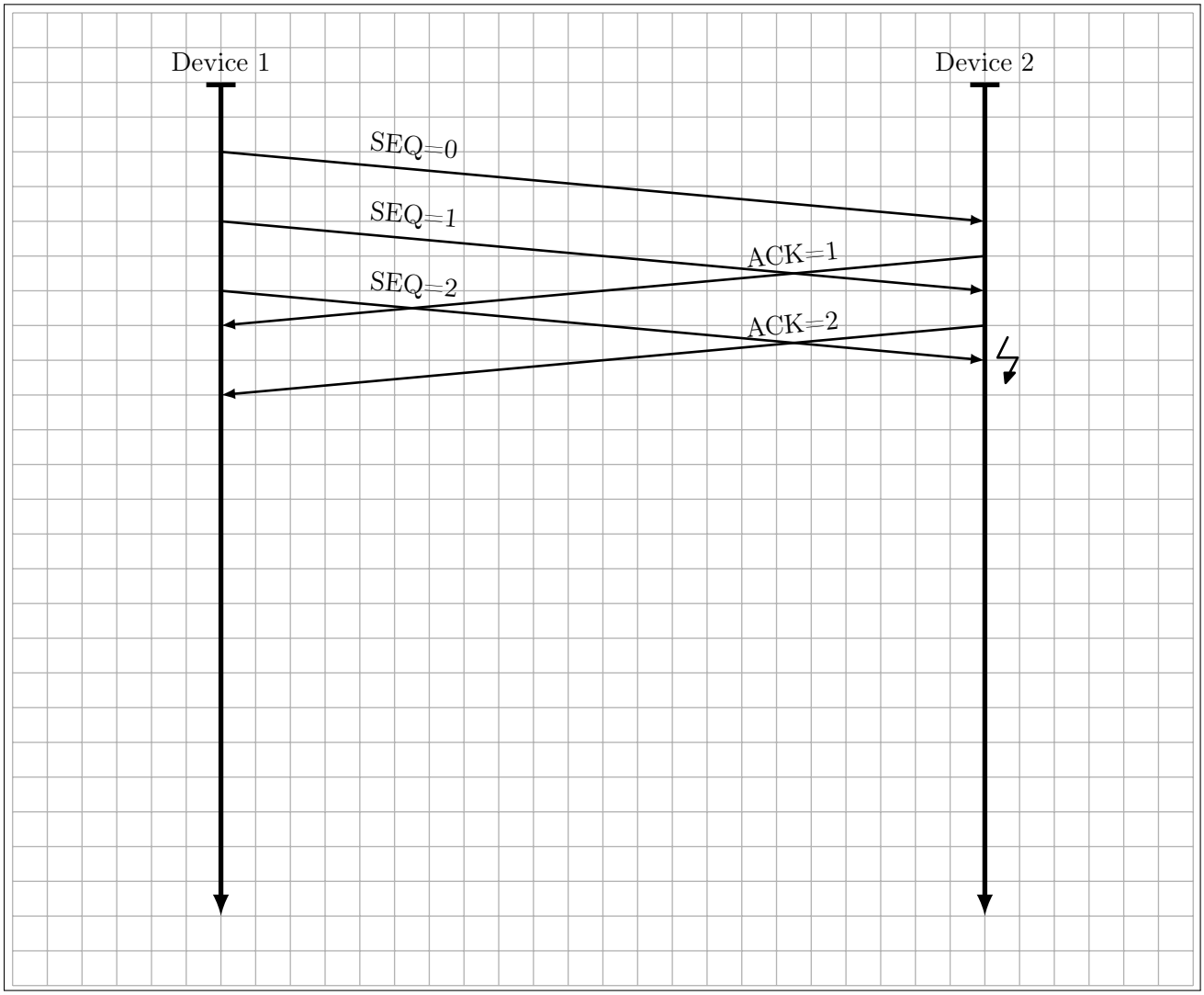
Abbildung 6.3: TCP-Header der Antwort des Web-Servers

g)* Welche Ende-zu-Ende Anfrage-Antwort-Paare in der Darstellung 6.1 können *nicht* durch TLS geschützt werden? Begründen Sie Ihre Antwort für jedes genannte Paar.

2

Die Verbindung zum DNS-Server kann nicht mit TLS geschützt werden, weil Anfragen über UDP stattfinden. Die Verbindung zum Router bei ARP-Requests, weil TLS auf einer höheren Schicht als ARP operiert.

Ersatzvordruck für Aufgabe 2k).



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