

Exam

Place student sticker here

Note:

- During the attendance check a sticker containing a unique code will be put on this exam.
- This code contains a unique number that associates this exam with your registration number.
- This number is printed both next to the code and to the signature field in the attendance check list.

Grundlagen Rechnernetze und Verteilte Systeme

Exam: IN0010 / Hausaufgabe 10

Examiner: Prof. Dr.-Ing. Georg Carle

Date: Monday 15th June, 2020

Time: 14:00 – 23:59

Working instructions

- Die erreichbare Gesamtpunktzahl beträgt 61 credits.
- Bitte geben Sie bis spätestens Montag, den **13. Juli um 23:59 CEST** über TUMexam ab.
Bitte haben Sie Verständnis, wenn das Abgabesystem noch nicht reibungslos funktioniert. Wir arbeiten daran!
- Ihren **persönlichen** Link zur Abgabe finden Sie auf Moodle. Geben Sie diesen **nicht** weiter.
- Bitte haben Sie Verständnis, falls die Abgabeseite zeitweilig nicht erreichbar ist.

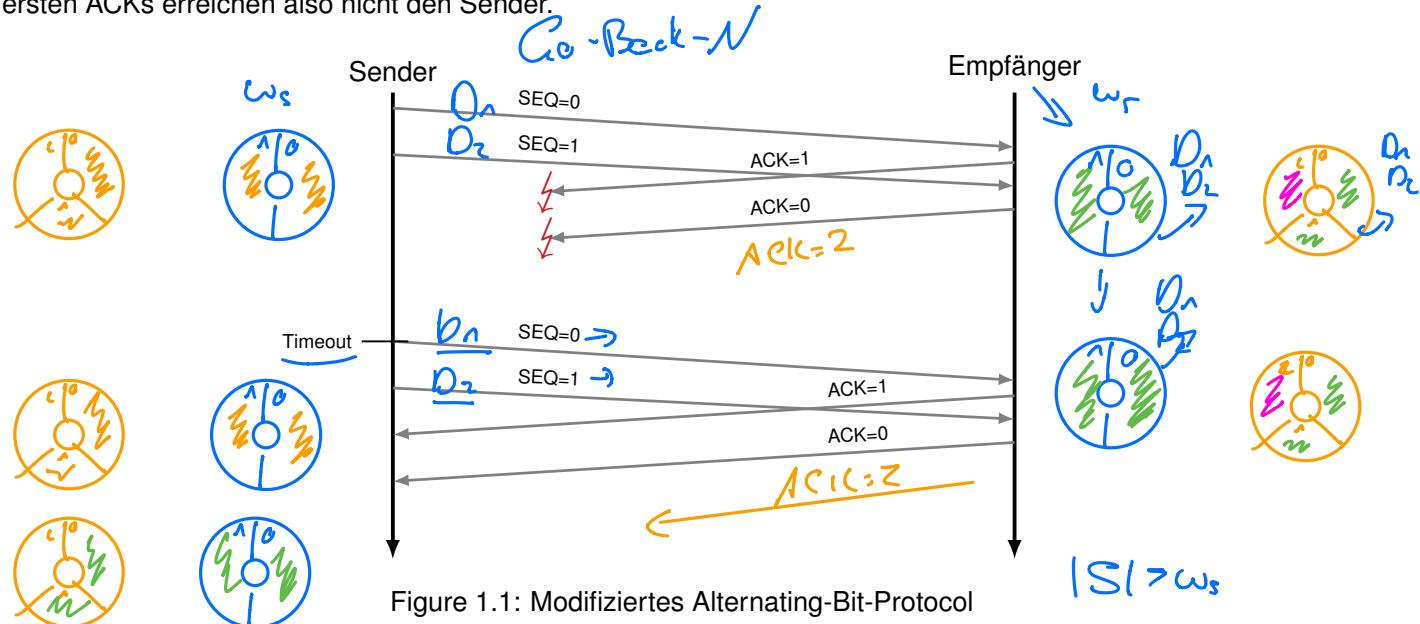
Bitte nehmen Sie die Hausaufgaben dennoch ernst:

- Neben der Einübung des Vorlesungsstoffs und der Klausurvorbereitung dienen die Hausaufgaben auch dazu, den Ablauf der Midterm zu erproben.
- Finden Sie einen für sich selbst praktikablen und effizienten Weg, die Hausaufgaben zu bearbeiten. Hinweise hierzu haben wir auf https://grnvs.net.in.tum.de/homework_submission_details.pdf für Sie zusammengestellt.

Left room from _____ to _____ / Early submission at _____

Problem 1 Schiebefensterprotokolle (10 credits)

Wir betrachten ein Sliding-Window-Verfahren, dessen Sende- und Empfangsfenster $w_s = w_r = 2$ beträgt. Der Sequenznummernraum sei $S = \{0, 1\}$. Die Fehlerbehandlung erfolge analog zu Go-Back-N. Abbildung 1.1 zeigt eine Datenübertragung, wobei die Blitze für durch Störungen verlorengegangene Segmente stehen. Die beiden ersten ACKs erreichen also nicht den Sender.



0

a)* Welches Problem tritt in dem Beispiel bei der Übertragung auf?

1
2

Es werden die Datenblitze Dn, Dz inkorrekt zweimal beim Empfänger weiter gegeben.

0

b) Passen Sie S an, so dass das Verfahren korrekt funktionieren kann. Begründen Sie Ihre Antwort.

1

Problem: Empfänger kann durch die kleinen Sequenznummern nicht merken, dass er doppelte Daten erhalten hat.

$$S = \{0, 1, 2\}$$

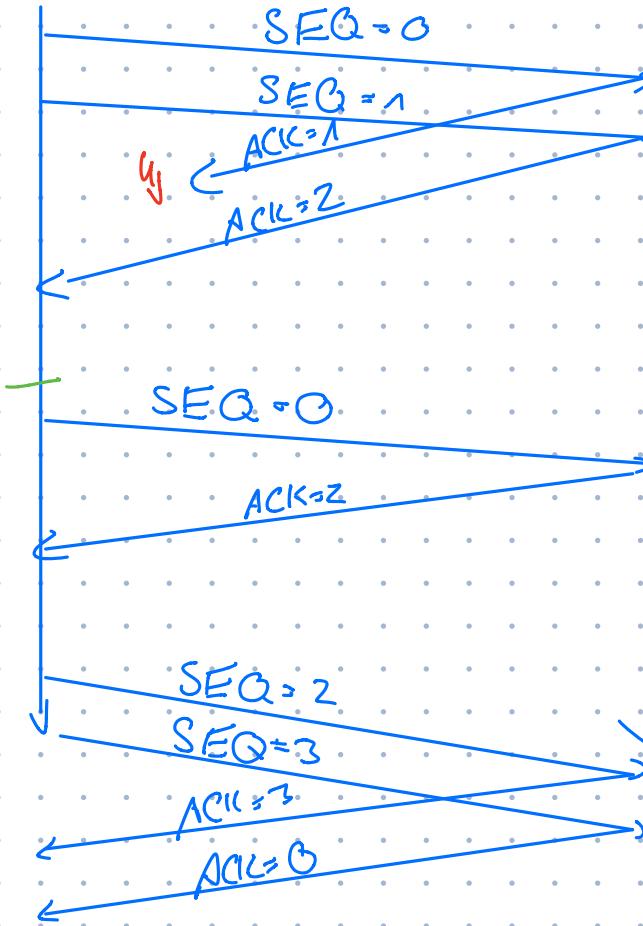
Selective Repeat

$\omega_s = 2$

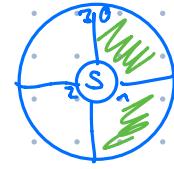


S

E



$\omega_r = 2$



Timeout



$[S] \rightarrow \frac{\omega_s}{2}$



S

E

Selective Repeat

$\omega_s = 2$



D_n SEQ = 0

D_n SEQ = 1

ACK = 1

ACK = 2

Timeout



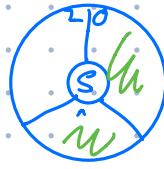
D_n SEQ = 0

D_n SEQ = 1

ACK = 2

$\omega_r = 2$

D_n
D_n ↗



D_{n+1}

y

Daten! D_n D_n D_n ...

Im Folgenden betrachten wir die beiden Verfahren Go-Back-N und Selective Repeat. Die Sequenznummern $s \in S$ haben eine Länge von 4 bit. Beantworten Sie die folgenden Fragen **sowohl für Go-Back-N als auch Selective Repeat.**

c)* Wie viele unbestätigte Segmente darf der Sender jeweils senden, um eine gesicherte Verbindung zu realisieren? Begründen Sie Ihre Antwort anhand von Beispielen. (Hinweis: Denken Sie an in möglichst ungünstigen Momenten verlorene Bestätigungen)

0
1
2
3
4

Go-Back-N (zu die nächste Sequenznummer wird akzeptiert)

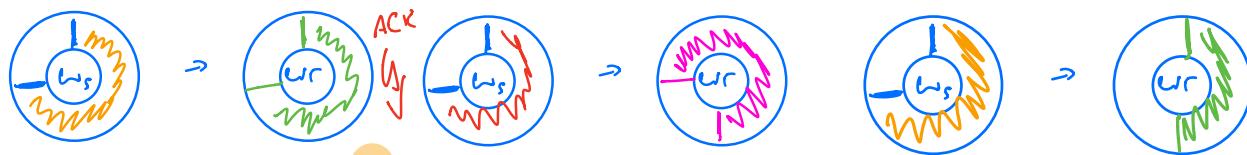
Es werden alle ab-order Segmente ignoriert.

Ungünstiger Fall: Alle Bestätigungen für erhaltene Sequenznummern gehen verloren.

Lösung: $|S| > w_s$ denn dann kann sich der Empfänger "merken", welche Sequenznummern er bereits bestätigt hat.

Selective Repeat:

Ungünstiger Fall: Bestätigungen gehen verloren.



Lösung: $\left\lceil \frac{|S|}{2} \right\rceil \geq w_s$ Denn bei Selective Repeat

werden immer w_s viele Sequenznummern unbestätigt sein. Damit Sender/Empfänger sich "merken" können, welche Sequenznummern sie gesendet haben müssen doppelt so viele Seg. wie Schiebfenster existieren.

d)* Begründen Sie, welche oberen und unteren Grenzen für das Empfangsfenster des Empfängers bei den beiden Verfahren jeweils sinnvoll sind.

0
1
2

Go-Back-N $w_r = 1$ Da immer nur das letzte Segment akzeptiert wird

Selective Repeat: $w_s \leq w_r \leq \left\lceil \frac{|S|}{2} \right\rceil$ Das Empfangsfenster muss mindestens so groß sein, wie das Schiebfenster.

- 0 e)* Für eine praktische Implementierung benötigt der Empfänger einen Empfangspuffer. Wie groß sollte dieser bei den beiden Verfahren jeweils gewählt werden?

Der Empfangspuffer sollte immer gleich groß gewählt werden

Problem 2 Fluss- und Staukontrolle bei TCP (17 credits)

Das im Internet am weitesten verbreitete Transportprotokoll ist TCP. Dieses implementiert Mechanismen zur Fluss- und Staukontrolle.

- 0 1 a)* Diskutieren Sie die Unterschiede zwischen Fluss- und Staukontrolle. Welche Ziele werden mit dem jeweiligen Mechanismus verfolgt?

Flusskontrolle: Vermeidung einer Überlast beim Empfänger
Staukontrolle: Vermeidung einer Überlast im Netz

- 0 1 b) Ordnen Sie die folgenden Begriffe jeweils der TCP-Fluss- bzw. Staukontrolle zu:

- Slow-Start ←
- Empfangsfenster
- Congestion-Avoidance ←
- Multiplicative-Decrease ←

Flusskontrolle: Empfangsfenster wird dem Sender mitgeteilt, um Überlast beim Empfänger zu verhindern.

Staukontrolle: Slow-Start und Congestion-Avoidance sind die beiden Staukontrollphasen bei TCP.
 Ablösung des Sendenfensters bei Verlust eines Segments.

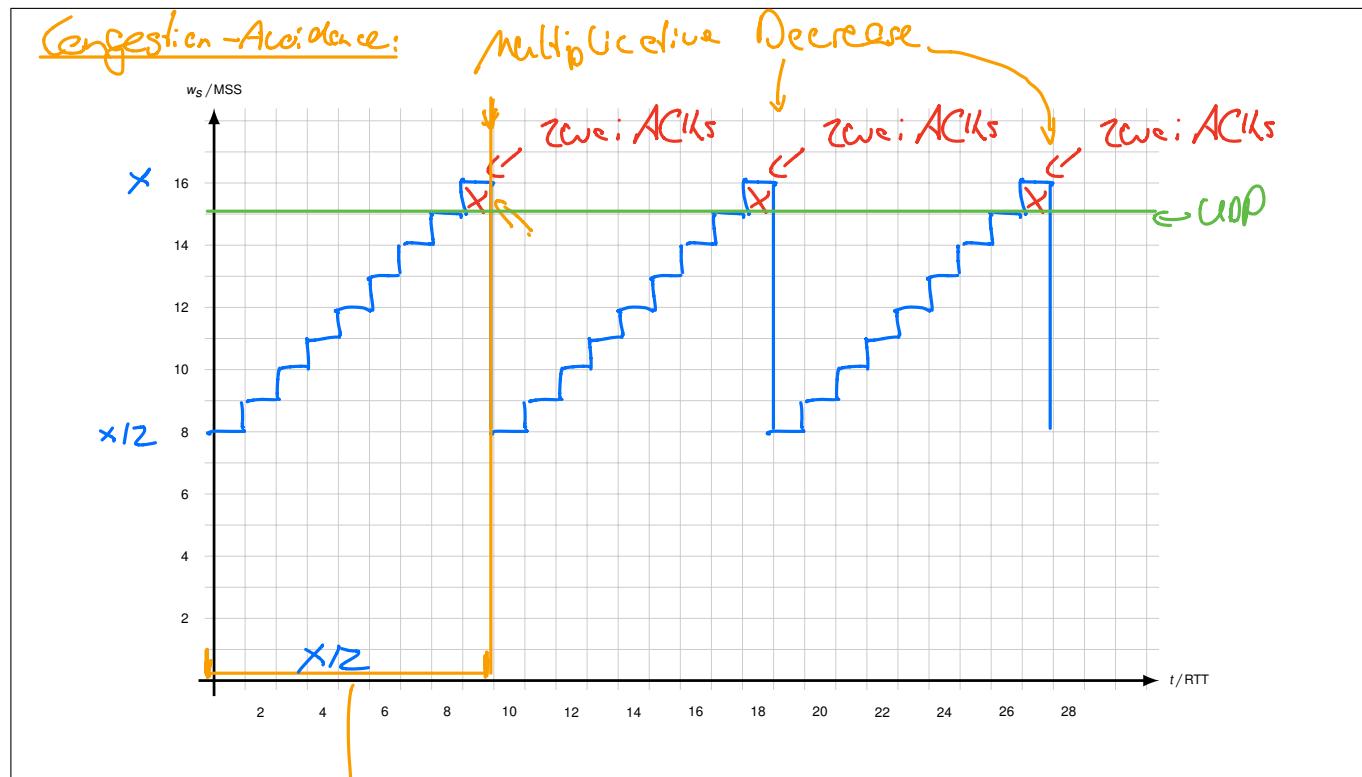
Zur Analyse der mit TCP erzielbaren Datenrate betrachten wir den Verlauf einer zusammenhängenden Datenübertragung, bei der die Slow-Start-Phase bereits abgeschlossen ist. TCP befindet sich also in der Congestion-Avoidance-Phase. Wir bezeichnen die einzelnen Fenster wie folgt:

- Sendefenster W_s , $|W_s| = w_s$
- Empfangsfenster W_r , $|W_r| = w_r$
- Staukontrollfenster W_c , $|W_c| = w_c$

Wir gehen davon aus, dass das Empfangsfenster beliebig groß ist, so dass das Sendefenster allein durch das Staukontrollfenster bestimmt wird, d.h. $W_s = W_c$. Es treten keinerlei Verluste auf, solange das Sendefenster kleiner als ein Maximalwert x ist, also $w_s < x$.

Wird ein vollständiges Sendefenster bestätigt, so vergrößert sich das aktuell genutzte Fenster um genau 1 MSS. Hat das Sendefenster den Wert x erreicht, so geht genau eines der versendeten TCP-Segmente verloren. Den Verlust erkennt der Sender durch mehrfachen Erhalt derselben ACK-Nummer. Daraufhin halbiert der Sender das Staukontrollfenster, bleibt aber nach wie vor in der Congestion-Avoidance-Phase, d. h. es findet kein erneuter Slow-Start statt. Diese Vorgehensweise entspricht einer vereinfachten Variante von TCP-Reno (vgl. Vorlesung). Als konkrete Zahlenwerte nehmen wir an, dass die maximale TCP-Segmentgröße (MSS) 1460 B und die RTT 200 ms beträgt. Die Serialisierungszeit von Segmenten sei gegenüber der Ausbreitungsverzögerung vernachlässigbar klein. Segmentverlust trete ab einer Sendefenstergröße von $w_s \geq x = 16$ MSS auf.

c)* Erstellen Sie ein Schaubild, in dem die aktuelle Größe des Sendefenster w_s gemessen in MSS über der Zeitachse t gemessen in RTT aufgetragen ist. In Ihrem Diagramm soll zum Zeitpunkt $t_0 = 0$ s gerade die Sendefenstergröße halbiert worden sein, also $w_s = x/2$ gelten. Zeichnen Sie das Diagramm im Zeitintervall $t = \{0, \dots, 27\}$.



d)* Wieviel Zeit vergeht, bis nach einem Segmentverlust das Staukontrollfenster infolge eines weiteren Segmentverlusts wieder reduziert wird?

$$T = \left(\frac{x}{2} + n\right) \cdot \text{RTT} = (8 + 1) \cdot 200 \text{ms} = 1800 \text{ms} = 1,8 \text{ s}$$

(Serialisierungszeit vernachlässigt und durch RTT approximiert)

- 0 e)* Bestimmen Sie allgemein die durchschnittliche Verlustrate θ . Hinweis: Da das Verhalten von TCP in diesem idealisierten Modell periodisch ist, reicht es aus, lediglich eine Periode zu betrachten. Setzen Sie die Gesamtzahl übertragener Segmente in Relation zur Anzahl verlorener Segmente (Angabe als gekürzter Bruch ist ausreichend).

$$n = \sum_{i=x/2}^x i = \sum_{i=1}^x i - \sum_{i=n}^{x/2-1} i = \frac{x(x+1)}{2} - \frac{(x/2-1)(x/2)}{2} = \frac{x^2+x}{2} - \frac{x^2}{8} + \frac{x}{4} = \frac{3}{8}x^2 + \frac{3}{4}x$$

Anzahl gesendeter Segmente

1 verloren Segment:

$$\Theta = \frac{1}{\frac{3}{8}x^2 + \frac{3}{4}x} \quad \leftarrow \text{Verlustrate}$$

- 0 f) Bestimmen Sie mit Hilfe der Ergebnisse aus den Teilaufgaben (c) und (e) die in der betrachteten TCP-Übertragungsphase durchschnittlich erzielbare Übertragungsrate in kB/s.

Hinweis: Verwenden Sie den exakten Wert (Bruch) aus Teilaufgabe e).

$$\begin{aligned} R_{TCP} &= \frac{n \cdot MSS}{T} (1-\Theta) = \frac{\frac{3}{8}x^2 + \frac{3}{4}x \cdot 1460 \text{ B}}{1,8 \text{ s}} (1-\Theta) \\ &= \frac{108 \cdot 1460 \text{ B}}{1,8 \text{ s}} \cdot \left(\frac{107}{108} \right) \approx 86,79 \text{ kB/s} \end{aligned}$$

- 0 g)* Bis zu welcher Übertragungsrate könnten Sie mit UDP maximal über den Kanal senden, ohne einen Stau zu erzeugen? Berücksichtigen Sie, dass der UDP-Header 12B kleiner als der TCP-Header ohne Optionen ist.

$$\begin{aligned} R_{UDP} &= \frac{15 \cdot (MSS + 12 \text{ B})}{RTT} = \frac{15 \cdot (1460 \text{ B} + 12 \text{ B})}{0,2 \text{ s}} \approx 110,4 \text{ kB/s} \end{aligned}$$

Der UDP-Header kleiner ist

Problem 3 TCP und Long Fat Networks (Hausaufgabe) (12 credits)

In dieser Aufgabe betrachten wir sog. *Long Fat Networks*. Darunter versteht man Verbindungen, welche zwar eine hohe Übertragungsrate aber insbesondere auch eine hohe Verzögerung aufweisen. Beispiele dafür sind u. a. Satellitenverbindungen in Folge der hohen Ausbreitungsverzögerungen. Wir wollen insbesondere die Auswirkungen auf die TCP-Staukontrolle untersuchen.

a)* Bei TCP wird das Sendefenster in Abhängigkeit des Empfangsfensters sowie des Staukontrollfensters gewählt. Wie lautet der genaue Zusammenhang?

<input type="checkbox"/>	0
<input type="checkbox"/>	1
<input type="checkbox"/>	2

Zwei Nutzer seien nun über einen geostationären Satelliten an das Internet mit hoher Übertragungsrate angebunden. Die RTT zwischen beiden Nutzern betrage 800 ms, die Übertragungsrate sei $r = 24 \text{ Mbit/s}$.

b)* Wie groß muss das Sendefenster (gemessen in Byte) gewählt werden, damit kontinuierlich gesendet werden kann?

<input type="checkbox"/>	0
<input type="checkbox"/>	1
<input type="checkbox"/>	2

c)* Warum ist die Situation in Teilaufgabe b) ein Problem für die TCP-Flusskontrolle?

<input type="checkbox"/>	0
<input type="checkbox"/>	1
<input type="checkbox"/>	2

d)* Lesen Sie Sektion 2 von RFC 1323 (<http://www.ietf.org/rfc/rfc1323.txt>, siehe Anhang). Beschreiben Sie die Lösung für das Problem aus Teilaufgabe c).

<input type="checkbox"/>	0
<input type="checkbox"/>	1
<input type="checkbox"/>	2

- 0 e) Bestimmen Sie den minimalen Wert für das shift.cnt-Feld der TCP-Window-Scaling-Option.

1

2

- 0 f) Geben Sie den Header des ersten TCP-SYN-Pakets an, welches die Verbindung aufbaut. Verwenden Sie dazu die konkreten Zahlenwerte aus der Angabe. Ein TCP-Header ist zur Erinnerung nochmals in Abbildung 3.1 dargestellt. Dort finden sich auch zwei Vordrucke zur Lösung.

Hinweis: Es ist nicht notwendig, den Header binär auszufüllen. Machen Sie aber bitte deutlich, ob es sich um hexadezimale, dezimale oder binäre Darstellung der Zahlen handelt.

Angenommen die Größe des Staukontrollfensters betrage derzeit die Hälfte des in Teilaufgabe b) berechneten Werts. Die MSS betrage 1200 B und die TCP-Verbindung befindet sich derzeit in der Congestion-Avoidance-Phase.

- 0 g) Wie lange dauert es, bis das Fenster die Leitung komplett ausnutzen kann?

Hinweis: Das Staukontrollfenster wird durch TCP-Window-Scaling nicht beeinflusst.

1

- 0 h) Ergibt sich aus dem Ergebnis von Teilaufgabe g) ein Problem?

1

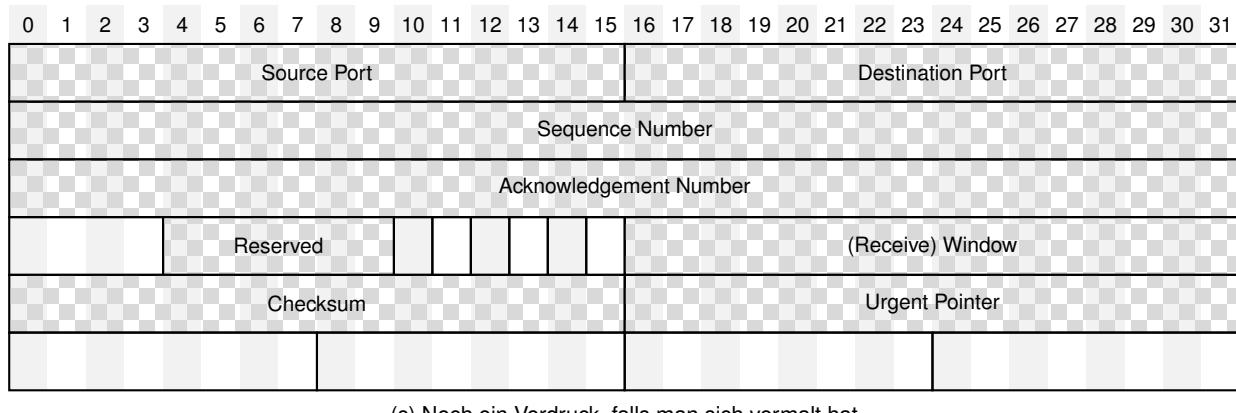
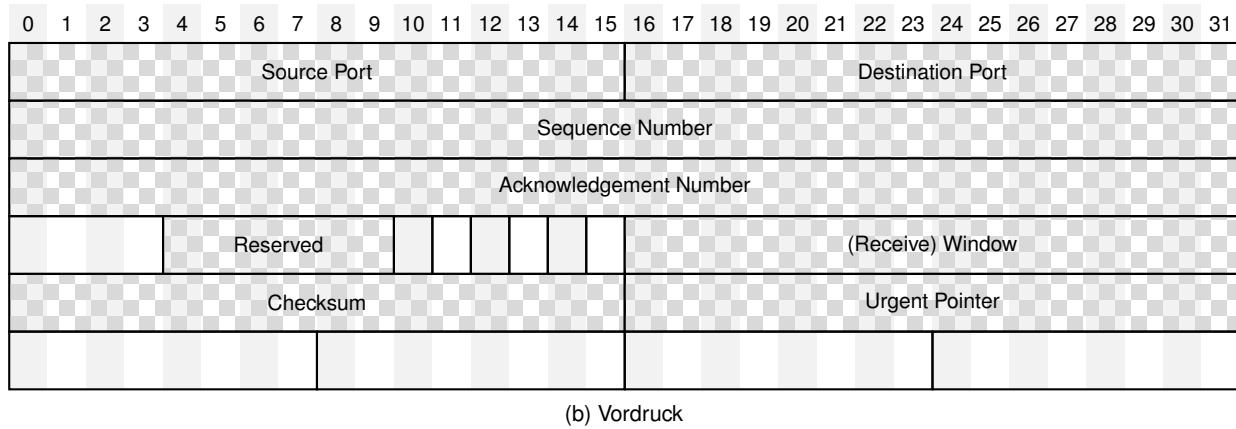
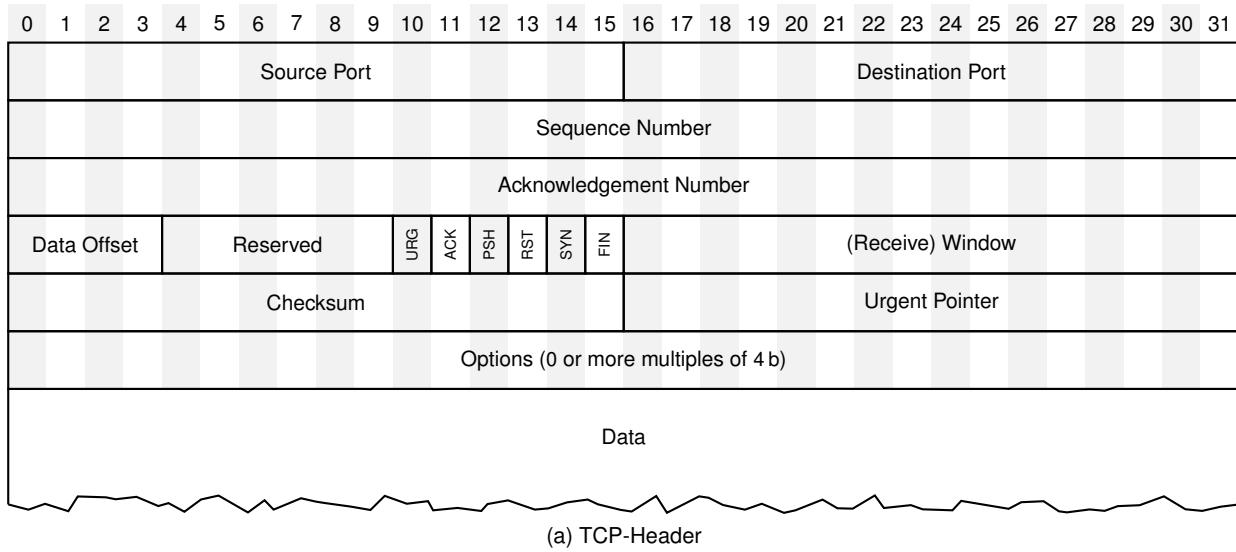


Figure 3.1: TCP-Header und Vordrucke zur Lösung von Aufgabe 3

2. TCP WINDOW SCALE OPTION

2.1 Introduction

The window scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit Window field of the TCP header (SEG.WND in RFC-793). The scale factor is carried in a new TCP option, Window Scale. This option is sent only in a SYN segment (a segment with the SYN bit on), hence the window scale is fixed in each direction when a connection is opened. (Another design choice would be to specify the window scale in every TCP segment. It would be incorrect to send a window scale option only when the scale factor changed, since a TCP option in an acknowledgement segment will not be delivered reliably (unless the ACK happens to be piggy-backed on data in the other direction). Fixing the scale when the connection is opened has the advantage of lower overhead but the disadvantage that the scale factor cannot be changed during the connection.)

The maximum receive window, and therefore the scale factor, is determined by the maximum receive buffer space. In a typical modern implementation, this maximum buffer space is set by default but can be overridden by a user program before a TCP connection is opened. This determines the scale factor, and therefore no new user interface is needed for window scaling.

2.2 Window Scale Option

The three-byte Window Scale option may be sent in a SYN segment by a TCP. It has two purposes: (1) indicate that the TCP is prepared to do both send and receive window scaling, and (2) communicate a scale factor to be applied to its receive window. Thus, a TCP that is prepared to scale windows should send the option, even if its own scale factor is 1. The scale factor is limited to a power of two and encoded logarithmically, so it may be implemented by binary shift operations.

TCP Window Scale Option (WSopt):

Kind: 3 Length: 3 bytes

+-----+	+-----+	+-----+
Kind=3	Length=3	shift.cnt
+-----+	+-----+	+-----+

This option is an offer, not a promise; both sides must send Window Scale options in their SYN segments to enable window scaling in either direction. If window scaling is enabled, then the TCP that sent this option will right-shift its true receive-window values by 'shift.cnt' bits for transmission in SEG.WND. The value 'shift.cnt' may be zero (offering to scale, while applying a scale factor of 1 to the receive window).

This option may be sent in an initial <SYN> segment (i.e., a segment with the SYN bit on and the ACK bit off). It may also be sent in a <SYN,ACK> segment, but only if a Window Scale option was received in the initial <SYN> segment. A Window Scale option in a segment without a SYN bit should be ignored.

The Window field in a SYN (i.e., a <SYN> or <SYN,ACK>) segment itself is never scaled.

Problem 4 Network Address Translation (22 credits)

In dieser Aufgabe soll die Weiterleitung von IP-Paketen (IPv4) bei Verwendung eines NAT-fähigen Routers betrachtet werden. Für die Zuordnung zwischen öffentlichen und privaten IP-Adressen verfügt ein NAT-fähiger Router über eine Abbildungstabelle, die die Beziehung zwischen lokalem und globalem Port speichert. Viele NAT-fähige Geräte speichern zusätzlich noch weitere Informationen wie die entfernte IP-Adresse oder die eigene globale IP-Adresse (z. B. wenn der Router mehr als eine globale IP besitzt). Davon wollen wir hier absehen.

Abbildung 4.1 zeigt die Netztopologie. Router R1 habe NAT aktiviert, wobei auf IF1 eine private und auf IF2 eine öffentliche IP-Adresse verwendet werde. Router R2 nutze kein NAT. PC2 habe bereits mit Server 2 kommuniziert, wodurch der Eintrag in der NAT-Tabelle von R1 entstanden ist (siehe Abbildung 4.1). Wählen Sie dort, wo Sie die Freiheit haben, sinnvolle Werte für die IP-Adressen und Portnummern.

a)* Geben Sie PC1 und Interface 1 von R1 eine passende IP-Adresse. Das Subnetz ist 10.0.0.0/24.

10. The following table summarizes the results of the study.

0
1

b)* PC1 baue nun eine HTTP-Verbindung zu Server 2 auf. Geben Sie die Felder für die Quell-IP, Ziel-IP, Quell-Port, Ziel-Port und TTL des IP- bzw. TCP-Headers für die Pakete an den drei markierten Stellen in Abbildung 4.1 an. Geben Sie außerdem neu entstehende Einträge in der NAT-Tabelle von R1 an.

Bitte in Abbildung 4.1 eintragen. Die Box dient nur dazu, Ihnen im Lösungsvorschlag eine Erklärung an dieser Stelle zukommen zu lassen!

0
1
2

c) Server 2 antworte nun PC1. Geben Sie in Abbildung 4.2 analog zur vorherigen Teilaufgabe die Header-Felder an den drei benannten Stellen sowie neu entstehende Einträge in der NAT-Tabelle von R1 an.

Bitte in Abbildung 4.1 eintragen. Die Box dient nur dazu, Ihnen im Lösungsvorschlag eine Erklärung an dieser Stelle zukommen zu lassen!

0
1
2

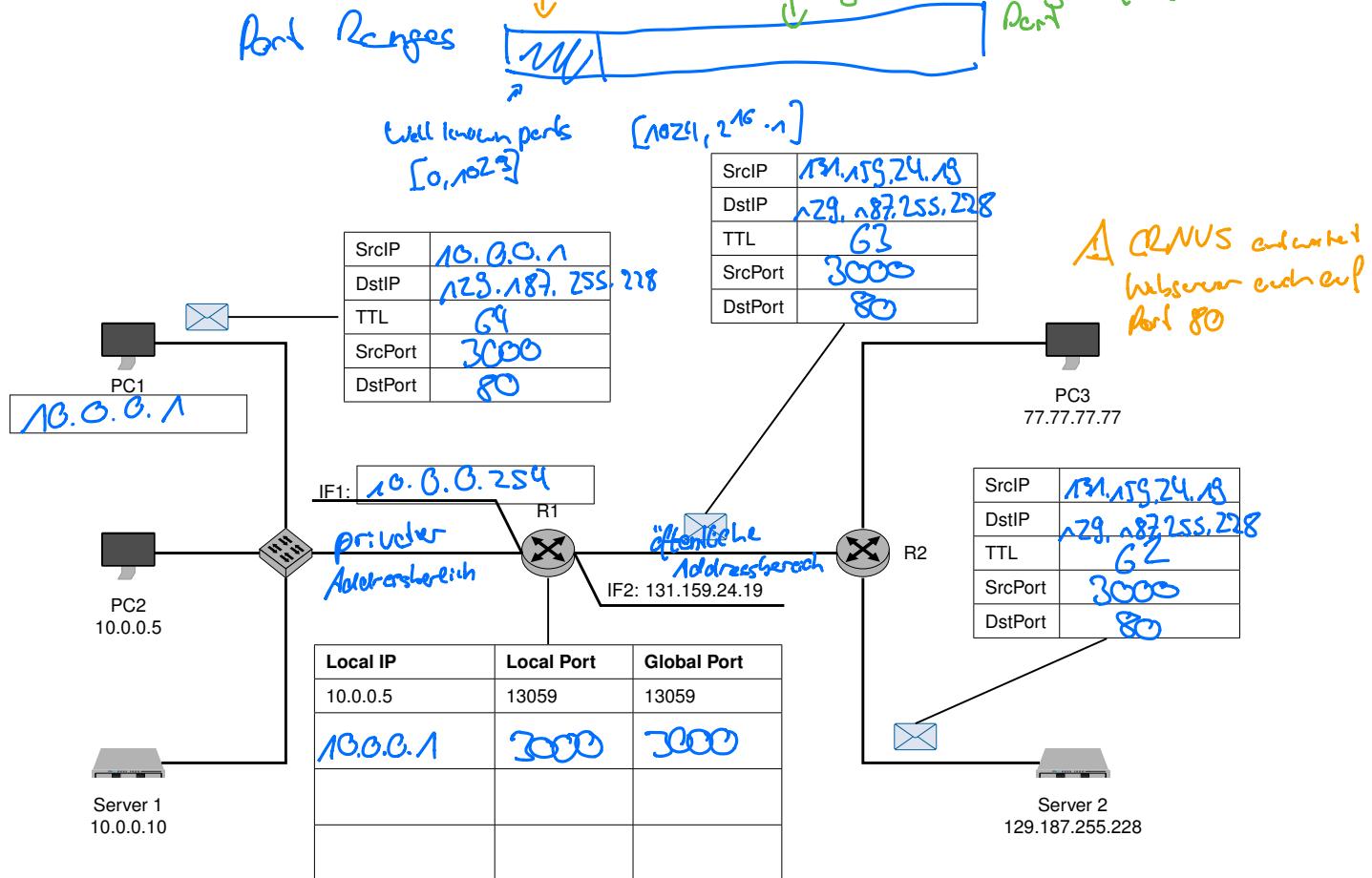


Figure 4.1: Lösungsblatt für Aufgabe 4a)/b)

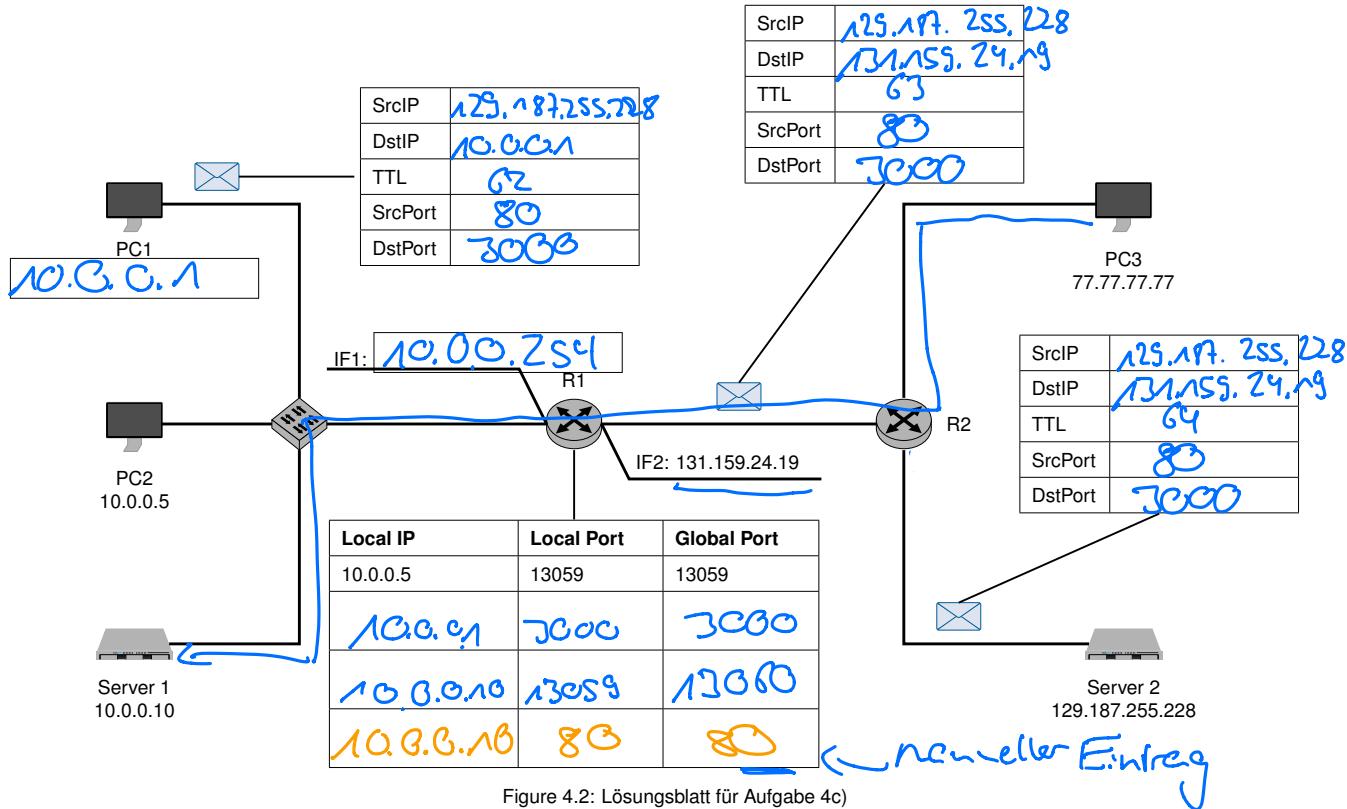


Figure 4.2: Lösungsblatt für Aufgabe 4c)

0 d)* Server 1 baut nun ebenfalls eine TCP-Verbindung zu Server 2 auf Port 80 auf. Dabei wählt er zufällig den Absender-Port 13059. Beschreiben Sie das am NAT auftretende Problem und wie dieses gelöst wird.

1 Problem: An R1 ist der gleiche Port 13055 bereits belegt.
2 Damit muss ein anderer gleicher Port für diese
Kommunikation gewählt werden. Denn der Gleiche Port
ist die einzige Zuordnungsmöglichkeit der IP-Pakete für R1.

0 e)* R1 erhält von PC3 ein an 131.159.24.19:13059 adressiertes Paket. Wie wird R1 mit diesem Paket verfahren?
Welche Probleme können sich daraus ergeben?

1 Das Paket wird an PC2 weitergeleitet.
→ PC2 erhält ein unerwartetes Paket
⇒ NAT ist keine Firewall

0 f) Ergibt sich für PC2 ein Problem, wenn dieser ein „zufälliges“ Paket mit TCP-Payload auf einem Port mit einer bestehenden Verbindung erhält?

1 Es ergibt sich nur ein Brüllen, falls PC2 folgende Informationen hat:
2 Src-IP (Server2), Dst-Port (Server2), Sequenznummer
⇒ sehr unabschöpflich

0 g)* Welche weiteren Unterscheidungskriterien könnten von einem NAT-Router verwendet werden?

- Gleiche IP des Routers (bei mehreren öffentlichen Interfaces an R1)
- Dst IP
- Dst Port
- Protokollnummer (TCP oder UDP)

0 h)* Welches Problem tritt auf, wenn PC1 einen Echo Request an Server 2 sendet?

1 Echo Requests verwenden auf Layer 4 ICMPv4/v6.
ICMP hat aber keine Portnummern!
⇒ Damit kann ein naives NAT dieses Paket nicht umsetzen

i) Beschreiben Sie eine mögliche Lösung für das in der vorherigen Teilaufgabe aufgetretene Problem.

ICMP hat keine Portnummern, jedoch ICMP Identifier.
Dieser ist für jede zusammenhängende ICMP Nachricht eindeutig (auch ZB)
Damit kann jetzt der Source Port oder ICMP Identifier zur Zuordnung des lokalen Hosts verwendet werden.

j) Welches Problem ergibt sich, wenn ein NAT-Router ICMP TTL-Exceeded Nachrichten empfängt und an den Empfänger (Absender des auslösenden Pakets) weiterleiten möchte? Wie kann dieses Problem umgangen werden?

Da die TTL-Exceeded Nachricht nicht von NAT "erzeugt" wurde, kann diese nicht direkt an einen lokalen Host weitergeleitet werden, da ICMP keine Portnummern enthält.
Aber in der ICMP Payload befindet sich der auslösende IP-Header, sowie die ersten 8B des Paketgruns.
In diesen 8B befindet sich der Source Port des auslösenden Segments. Damit kann das ICMP TTL Paket zugeordnet werden.

k)* Nun möchte PC3 eine HTTP-Verbindung zu Server 1 aufbauen. Kann dies unter den gegebenen Umständen funktionieren? (Begründung!)

Nun, da PC3 eine Verbindung zum R1 auf Port 80 aufbauen wird. R1 hat jedoch keine NAT Eintrag auf dem öffentlichen Port 80.

l) Wie könnte das Problem unter Beibehaltung des NATs umgangen werden?

Durch einen manuellen Eintrag in der NAT Tabelle von R1, wie folgt:

Gelockt IP	Lokaler Port	Globale Port
192.0.0.10	80	80

↑
Lokale IP von Server 1

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

A large grid of squares, approximately 20 columns by 25 rows, intended for students to write their solutions. The grid is composed of thin black lines on a white background.