Klausur SS 2014

08.07.2015

Name:	**Mustermann**	Vorname:	**Max**
Studiengang:	**Informatik, Bachelor**		
Matr.Nr.:	**999999**	Klausurnr.:	**999**

Hinweise: (Bitte sorgfältig durchlesen!)

- Die Klausur besteht aus **7 Aufgaben auf 19 Seiten**, plus 3 zusätzliche Seiten für Notizen.
- Tragen Sie Ihre Lösungen in die dafür vorgesehenen Felder auf den Aufgabenblättern ein. Reicht der Platz nicht aus, ist für jede Aufgabe ein neues Blatt zu verwenden. Dazu können die zusätzlichen Seiten am Ende des Klausurexemplars verwendet werden. Bei Bedarf wird weiteres Papier von der Klausuraufsicht gestellt. Schreiben Sie Name, Matrikelnummer und Klausurnummer auf zusätzlich ausgehändigte Blätter und machen Sie klar, zu welcher Aufgabe eine Lösung gehört.
- Die Bearbeitungszeit beträgt **120 Minuten**.
- Die Klausur umfasst **100** Punkte. Zum Bestehen genügen **50** Punkte. Ein in den Übungen erreichter Notenbonus wird nur dann angewendet, wenn in der Klausur selbst mindestens **50** Punkte erreicht wurden.
- Am Ende der Klausur sind die Klausurblätter und evtl. zusätzlich ausgehändigte Blätter abzugeben.
- **Merken Sie Sich Ihre Klausurnummer**. Die Klausurergebnisse werden unter dieser Nummer veröffentlicht. Sie können die untere linke Ecke vorsichtig abtrennen, um die Klausurnummer mitzunehmen.
- Es sind **keine Hilfsmittel** erlaubt. Mobiltelefone sind auszuschalten.
- Bitte verwenden Sie keinen roten oder grünen Stift.
- Legen Sie Ihren Studierendenausweis und einen Lichtbildausweis bereit.

Mit meiner Unterschrift bestätige ich, dass ich mich gesund genug fühle, an der Klausur teilzunehmen und dass ich die Aufgaben selbstständig bearbeitet habe.

_____

Unterschrift

Punktespiegel:

Aufgabe	1	2	3	4	5	6	7	Σ	Bonus	Note
Punkte	15	16	11	20	18	8	12	100	Noten-stufen	
davon erreicht									1	

999
Klausurnr.

Lösung 1 (Allgemeine Grundlagen) **(4 + 3 + 5 + 3) = 15 Punkte**

a) *Skizzieren* Sie das ISO/OSI-Referenzmodell und das Internet-Referenzmodell. *Geben Sie dabei die Namen der einzelnen Schichten in korrekter Reihenfolge an und ordnen Sie die relevanten Schichten der beiden Modelle einander jeweils zu.* Eine Beschreibung der Aufgaben der einzelnen Schichten ist nicht erforderlich.

7 OSI-Schichten vs. 4 TCP/IP-Schichten

OSI	**vs**	**TCP/IP**
7: Anwendung	↔	4: Anwendung/Application-Layer
6: Darstellung	↔	(4)
5: Sitzung	↔	(4)
4: Transport	↔	3: Transport-Layer
3: Vermittlung	↔	2: Internet-Layer
2: Sicherung	↔	1: Host-to-Network-Layer
1: Bitübertragung	↔	1

Anwendung, Transport und Vermittlung sind im wesentlichen gleich, untere beiden OSI-Schichten bilden auf Host-to-Network-Layer ab. Evtl. noch Schicht 5 und 6 zu Application-Layer hin, ist aber eigentlich nicht nötig.

b) HTTP ist das Anwendungsprotokoll, das zur Übertragung von Webseiten verwendet wird; es benötigt eine zuverlässige Übertragung. Es werde nun eine HTTP-PDU über Ethernet gesendet. Der Aufbau der HTTP-PDU sei wie folgt: `[HTTP-Header][Daten]`

Skizzieren Sie den Aufbau des kompletten Ethernet-Rahmens (in der Art wie oben bei der HTTP-PDU vorgegeben), wie er an die Bitübertragungsschicht weitergegeben wird, inklusive aller enthaltenen Header.
Hinweis: Header-Inhalte oder -Größen müssen nicht mit angegeben werden.

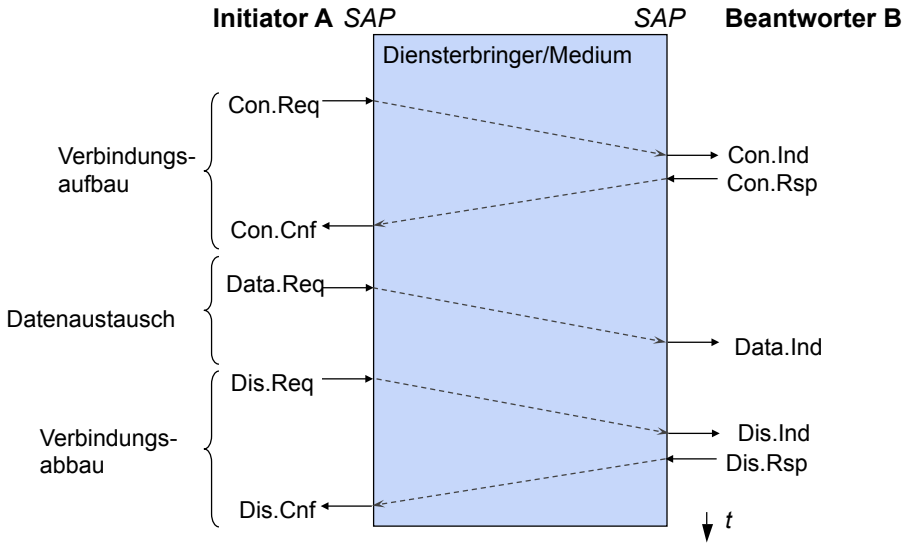
```
[Ethernet-Header] [IP-Header] [TCP-Header] [HTTP-Header] [Daten]
[Ethernet-Tail]
```

c) Nutzer A möchte Daten an Nutzer B senden und verwendet dazu einen verbindungsorientierten Kommunikationsdienst.

Skizzieren Sie ein Weg/Zeit-Diagramm für die drei Phasen dieses Dienstes: Verbindungsaufbau (Connection), Datenübertragung (Data) und Verbindungsabbau (Disconnection).

Der Verbindungsaufbau und Verbindungsabbau sind bestätigt, der Datenaustausch ist unbestätigt.

Benennen Sie die einzelnen Dienstprimitive mit der aus der Vorlesung bekannten Notation, z.B. `Con.Req` für Connection Request.



d) Nehmen Sie an, Sie wollen den Dienst aus Aufgabenteil c) in einem *Zustandsübergangsdiagramm* darstellen. *Wie viele Zustände werden mindestens benötigt, um alle Phasen darstellen zu können, und wie sind diese Zustände entsprechend zu bezeichnen?*

4 Zustände: Ruhezustand, Verbindung im Aufbau, Verbindung aufgebaut (Datenaustausch), Verbindung im Abbau.

Lösung 2 (Bitübertragungsschicht) **(10 + 2 + 1 + 3) = 16 Punkte**

a) Gegeben seien zwei Kanäle, die folgende Frequenzbereiche und Signal-Rauschabstände bereitstellen:

- Kanal 1: Frequenzbereich von 4000Hz bis 9000Hz mit 50dB Signal-Rauschabstand
- Kanal 2: Frequenzbereich von 20kHz bis 30kHz mit 30dB Signal-Rauschabstand

Beantworten Sie die folgenden Fragen mittels der *Theoreme von Shannon und Nyquist*:

i) Welcher der beiden Kanäle ermöglicht die *höhere theoretische Datenrate*?

ii) Es soll nun *256-QAM* zur Codierung der Daten verwendet werden. *Ist dies für beide Kanäle problemlos möglich*?

Hinweis: Versuchen Sie nicht, exakte Zahlen zu berechnen, sondern bestimmen Sie geeignete obere und untere Schranken. Die jeweils nächstgelegene Zweierpotenz könnte hierbei eine gute Wahl sein.

Mit B: Bandbreite, n: Signalstufen und $SNR = 10 \cdot log_{10}(S/N)$, $S/N = 10^{SNR/10}$

i) Berechnung der max. Datenrate nach Shannon: $C = B \cdot ld(1 + S/N)$

Kanal 1: $B = 5000Hz$, $SNR = 50dB$, $S/N = 10^5$
Somit: $C = 5000Hz \cdot ld(1 + 10^5)$.
(Dies gibt 83048.274507 Bit/s, aber ohne Taschenrechner ist das schwer zu berechnen.)
Zum Abschätzen des Logarithmus' wählt man dann am besten:
$ld(2^{16}) < ld(1 + 10^5) < ld(2^{17})$
$\Rightarrow 80000Bit/s < 5000Hz \cdot ld(1 + 10^5) < 85000Bit/s$

Kanal 2: $B = 10000Hz$, $SNR = 30dB$, $S/N = 10^3$
Somit: $C = 10000Hz \cdot ld(1 + 10^3)$. Mit Taschenrechner wären es 99672.262588 Bit/s.
Abschätzung: $ld(2^9) < ld(1 + 10^3) < ld(2^{10})$
$\Rightarrow 90000Bit/s < 10000Hz \cdot ld(1 + 10^3) < 100000Bit/s$

Die Datenrate von Kanal 2 ist also größer.

ii) Berechnung der max. Datenrate nach Nyquist-Theorem: $C = B \cdot 2 \cdot ld(n)$

Kanal 1: $B = 5000Hz$, $n = 256$
Somit $C = 5000Hz \cdot 2 \cdot ld(256) = 80000Bit/s$
$\Rightarrow 80000Bit/s < 5000Hz \cdot ld(1 + 10^5)$

Kanal 2: $B = 10000Hz$, $n = 256$
Somit $C = 10000Hz \cdot 2 \cdot ld(256) = 160000Bit/s$
$\Rightarrow 10000Hz \cdot ld(1 + 10^3) < 100000Bit/s < 160000Bit/s$

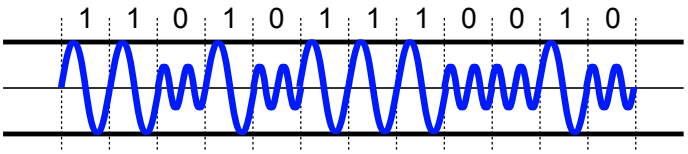
Nach Vergleich mit den Datenraten nach Shannon ist 256-QAM nur für Kanal 1 geeignet, da für Kanal 2 mit dem schlechteren Signal-Rauschabstand die hohe Datenrate mit 256-QAM nicht schafft.

b) *Erklären Sie knapp* die Bedeutung des Begriffs *Selbsttaktung* im Zusammenhang mit digitalen Leitungscodes für die Basisbandübertragung. *Nennen Sie zudem zwei in der Vorlesung vorgestellte Leitungscodes*, die Selbsttaktung sicherstellen.

Selbsttaktung bezeichnet die Fähigkeit eines Leitungscodes, die Synchronisation einer Bitfolge zwischen Sender und Empfänger ohne weitere Hilfsmittel (z.B. Taktleitung) sicherzustellen. Dazu wird in Kombination mit den zu übertragenden Daten eine Taktinformation mit in die erzeugte Signalfolge eingebettet, anhand derer der Empfänger den Takt auslesen und die Daten synchronisiert entnehmen kann.

Selbsttaktend: Manchester (Biphase-L), Differential Manchester, Biphase-M, Biphase-S, 4B/5B (oder ähnliche Codierverfahren)
NICHT selbsttaktend: NRZ*, Uni-/Bipolar RZ
QAM o.ä. wäre hier auch nicht richtig, da wir ja über Basisbandübertragung sprechen.

c) Die nachfolgende Grafik zeigt die Modulation einer Bitfolge. *Nennen Sie die Modulation(en), die hier angewendet wurde(n).*



Amplituden- und Frequenzmodulation

d) *Was ist die Kernaussage des Abtasttheorems von Shannon und Raabe?*

Angenommen, ein analoges Stereosignal wurde mit PCM digitalisiert. *Welche Datenrate ist für die Übertragung der digitalen Daten mindestens erforderlich*, wenn das Stereosignal ein Spektrum von 20Hz bis 20kHz umfasst und mit 16Bit quantisiert wird?

Die Abtastfrequenz f_A muss mindestens doppelt so hoch sein wie die höchste im abzutastenden Signal vorkommende Frequenz f_{Grenz}: $f_A \geq 2 * f_{Grenz}$

Die Grenzfrequenz ist 20kHz, also muss mit 40kHz abgetastet werden. Pro Abtastung werden 16Bit benötigt. Also $40000Hz \cdot 16Bit = 640000Bit/s$. Da wir ein Stereosignal haben, benötigen wir die doppelte Datenrate.
$2 \cdot 40000Hz \cdot 16Bit = 2 \cdot 640000Bit/s = 1.28MBit/s$

Lösung 3 (Sicherungsschicht) **(4 + 4 + 3) = 11 Punkte**

a) Ein wesentlicher Aufgabenbereich der Sicherungsschicht ist die Regelung des Medienzugriffs. Das prominenteste Verfahren für lokale Netze ist das bei Ethernet verwendete Zugriffsverfahren CSMA/CD.

In einem lokalem Netz mit Bus-Topologie seien drei Stationen A, B und C angeschlossen, die CSMA/CD verwenden. A und B möchten nun fast gleichzeitig Daten an C versenden.

i) *Woran liegt es, dass es in diesem Fall trotz CSMA/CD zu einer Kollision kommen kann?*

ii) *Woran erkennen A, B und C jeweils, dass es zu einer Kollision gekommen ist?*

iii) *Welche Voraussetzung stellt sicher, dass eine Station erkennen kann, ob ihre Daten ohne Kollision übertragen wurden?*

i) Durch Signallaufzeit kann B nicht erkennen, dass A bereits angefangen hat, zu senden (bzw. umgekehrt), und somit nimmt B an, dass das Medium frei ist und fängt ebenfalls an zu senden.

ii) A hört sich selbst beim Senden zu, und erkennt, dass er etwas anderes hört, als er gesendet hat – also eine Überlagerung seines Signals mit einem anderen Signal (dem von B) stattgefunden haben muss. Analog bei B.
C erkennt die Kollision dadurch, dass A bzw. B, sobald sie die Kollision erkannt haben, ein Jamming-Signal auf die Leitung legen. C erkennt dieses Jamming-Signal.

(Achtung: je nach Situation kann es auch sein, dass nur eine der Stationen A und B die Kollision selbst erkennt und die andere Station durch das Jamming-Signal der ersten. Oder C erkennt Spannungsspitzen und sendet direkt schon ein Jamming-Signal aus, welches A und B benachrichtigt. Wichtig ist nur, dass mindestens eine Station die Kollision durch Lauschen erkennen muss und andere Stationen durch Jamming benachrichtigt werden.)

iii) Die Station muss immer noch senden, wenn das kollidierende Signal ankommt – um sicherzustellen, dass sie auf jeden Fall so lange sendet, bis bei vorgegebener Netzausdehnung auch im Worst Case ein kollidierendes Signal angekommen wäre, ist eine minimale Sendedauer (und daraus folgend Rahmenlänge) notwendig.

b) Ein Sender möchte die folgende Bitsequenz übertragen: `10100110`. Er sichert die Sequenz mit einer *Cyclic Redundancy Checksum (CRC)* mit dem Generatorpolynom

$$G(x) = x^3 + x^1 + 1.$$

Der Empfänger empfängt die folgende Bitsequenz: `101001001100`.

i) *Ist ein Übertragungsfehler aufgetreten*?

ii) *Wie handelt der Empfänger bei Erhalt der Bitsequenz*?

Begründen Sie Ihre Antworten!

i) Offensichtlich ja. Denn die empfangenen Daten (ohne CRC) sind `101001001`, was definitiv nicht die obige Bitsequenz ist.

ii) Der Empfänger führt erst mal den CRC durch:

```
|101001001100:1011
|1011
|   1010
|   1011
|      1011
|      1011
|         000
```

Der Rest ist 0. Also geht der Empfänger von einer korrekten Übertragung aus und leitet das Paket an die nächste Schicht weiter. Wichtig ist hier, dass man erkennt, dass der Fehler eben nicht erkannt wird, Antworten wie “er verwirft den defekten Rahmen” wären also falsch.

c) Sie verwenden das *Sliding-Window-Verfahren* zusammen mit *Go-Back-N* zur Fehlerbehandlung. Es seien sowohl positive Quittungen (ACK) als auch negative Quittungen (NAK) möglich.

Gegeben seien ein Modulus $M = 16$ und eine Fenstergröße $W = 9$. Zum aktuellen Zeitpunkt seien die Rahmen mit den Sequenznummern 11,12,13,14,15 vom Sender gesendet worden, ohne dass eine Quittung eingegangen ist.

Beantworten Sie die folgenden Fragen mit knapper Begründung:

i) *Welche Rahmen dürfen in dieser Situation ohne jede Quittung gesendet werden*?

ii) *Wie ändert sich die Situation, wenn ein Rahmen mit einer Quittungsnummer (ACK) 14 empfangen wird*?

iii) *Was passiert, wenn anstelle des ACK 14 ein NAK für die Sequenznummer 12 empfangen wird*?

i) Sliding-Window erlaubt es, mehrere Rahmen zu schicken, ohne für die vorherigen eine Quittung empfangen zu haben. Die Fenstergröße gibt vor, wie viele Rahmen versendet werden können, bevor man auf Quittungen warten muss. Im Beispiel sind dies neun Stück, also können in der gegebenen Situation noch vier weitere Rahmen – 0, 1, 2 und 3 – gesendet werden.

ii) Bei einer Quittung gilt alles bis zum vorherigen Rahmen als bestätigt, der Empfänger wartet auf Zustellung aller Rahmen ab dem vierzehnten. In der gegebenen Situation wird das Fenster also bis zur 14 vorgeschoben, es sind drei weitere Plätze (also 7 insgesamt) frei und wir können insgesamt 0 bis 6 übertragen.

iii) Mit einem NAK signalisiert der Empfänger, dass der bezeichnete Rahmen nicht empfangen worden ist. Laut Go-Back-N müssen alle Rahmen ab dem bezeichneten wieder neu übertragen werden. Also 12, 13, 14 und 15 – und da mit dem NAK alles vorherige quittiert ist, kann auch das Fenster um eine Position vorgerückt werden und noch 0 bis 4 übertragen werden.

Lösung 4 (Transportschicht) **(11 + 4,5 + 3 + 1,5) = 20 Punkte**

a) Für ein Transportprotokoll möchten Sie ein geeignetes ARQ-Verfahren auswählen. Dazu wollen Sie die durchschnittliche Datenrate von Go-Back-N und Selective Repeat unter bestimmten Bedingungen berechnen. Führen Sie hierzu die im folgenden angegebenen Schritte durch.

Hinweise:

- Die Angaben in den einzelnen Schritten gelten auch für die folgenden Schritte.
- Sollten Sie einen Teil nicht bearbeiten können, geben Sie in den folgenden Teilen eine Formel für die Berechnung des Ergebnisses an. Nutzen Sie dazu die Variablenbezeichnungen aus der Aufgabenstellung der vorherigen Teile. Vereinfachen Sie die Formel soweit wie möglich.

i) Der Kanal habe eine Datenrate von 100 MBit/s. Die Paketgröße (inklusive aller Header) betrage 900 Byte. *Wie groß ist die Sendedauer t_S für ein Paket*? (1 Punkt)

Teile Paketgröße durch Datenrate:

$$t_\mathrm{S} = \frac{900\,\mathrm{Byte} \cdot 8\,\mathrm{Bit/Byte}}{100\,\mathrm{MBit/s}} = 72\,\mu\mathrm{s}$$

ii) Die Bitfehlerrate liege bei $1 \cdot 10^{-5}$. Geben Sie einen Ausdruck an, um die *Paketfehlerrate* auszudrücken, und vereinfachen Sie diesen soweit Ihnen das ohne Taschenrechner möglich ist. (1 Punkt)

Rechne BER in PER um:

$$1 - (1 - 10^{-5})^{900 \cdot 8} = 1 - 0,99999^{7200}$$

Das sind dann 6,9 %, kann man aber ohne Taschenrechner nicht ausrechnen.

iii) Nehmen Sie zur Vereinfachung der Rechnungen eine Paketfehlerrate von 10 % an. Wie groß ist die *mittlere Anzahl N korrekt übertragener Pakete* zwischen zwei defekten Paketen? (1 Punkt)

Wenn 1 von 10 Paketen defekt ist, liegen im Mittel 9 heile zwischen 2 defekten.

iv) Der Kanal sei unbelegt. Der Sender kann nun beginnen, eine Folge von Paketen abzusenden. Einige dieser Pakete werden erfolgreich empfangen, andere nicht. Welche Zeit t_1 wird *im Mittel* benötigt, bis das erste Paket versendet wurde, das später erfolgreich empfangen wird? (1 Punkt)

Hinweis: Wenn es keine Paketfehler gäbe, entspräche t_1 genau der Sendedauer.

Für 10 Pakete (korrekte und defekte gemischt) benötigen wir 720 µs. Davon sind im Mittel 9 korrekt. Also schaffen wir in 720 µs 9 korrekte Pakete. Das sind $t_1 = 80\,\mu\mathrm{s}$ für ein korrektes Paket.

v) Wie lange dauert es folglich im Mittel (t_3), drei Pakete zu versenden, die korrekt empfangen werden? (1 Punkt)

$t_3 = 240\,\mu s$.

vi) Ihr Transportprotokoll soll Paketfehler durch Triple-Duplicate-Acknowledgements erkennen. Die Übertragungsverzögerung des Netzwerkes betrage 1020 µs. *Wie lange dauert es* (t_e) *ab dem Zeitpunkt, an dem das Absenden eines Rahmens R abgeschlossen ist, bis der Sender den Verlust von R erkennt?* Nehmen Sie an, dass Bestätigungen ohne Verzögerungen abgesendet werden können, keine Sendedauer benötigen und nicht verloren gehen können. (1 Punkt)

Wir müssen nach dem defekten Paket drei weitere Pakete korrekt verschicken, um drei Dup-ACKs zu triggern. Dafür benötigen wir (s.o.) 240 µs. Dann muss das letzte Paket aber noch zum Empfänger und das DUP-ACK zurück. Also:

$$t_e = 240\,\mu s + 2 \cdot 1020\,\mu s = 2280\,\mu s$$

vii) *Bestimmen Sie nun die mittlere Datenrate D_G bei Verwendung von Go-Back-N.*
Gehen Sie vereinfachend davon aus, dass der Sender sofort die Übertragungswiederholung initiiert, sobald er einen Paketverlust erkennt. Eventuell laufende Übertragungen werden sofort abgebrochen. (2 Punkte)

Das ist jetzt recht einfach: Eine Periode besteht aus: N Pakete korrekt verschicken, 1 defektes Paket verschicken, auf das Triple-DUP-Ack warten. N ist im Mittel 9, der erste Teil dauert also im Mittel $9 \cdot 72\,\mu s$. Der zweite Teil dauert 72 µs. Der dritte Teil dauert 2280 µs. Alles zusammen dauert also:

$$9 \cdot 72\,\mu s + 72\,\mu s + 2280\,\mu s = 3000\,\mu s$$

Was übertragen wir in dieser Zeit? 9 Pakete, also $9 \cdot 7200\,\text{bit}$. Also ist die Datenrate:

$$D_G = \frac{9 \cdot 7200\,\text{bit}}{3\,\text{ms}} = 21,6\,\text{Mbit/s}$$

viii) *Wie groß wäre die mittlere Datenrate D_S bei Verwendung von Selective Repeat?*
Hierbei soll die laufende Übertragung *nicht* abgebrochen werden, wenn ein Paketverlust erkannt wird. (2 Punkte)

Da wir hier bei Verlust eines Paketes nur das verlorene Paket neu übertragen, müssen wir nur ausrechnen, wie viel Zeit wir mit dem Versenden defekter Pakete verbringen. Das sind bei einer PER von 10 % natürlich 10 % der Zeit. Also erreichen wir 90 % der maximalen Datenrate, also $D_S = 90\,\text{Mbit/s}$.

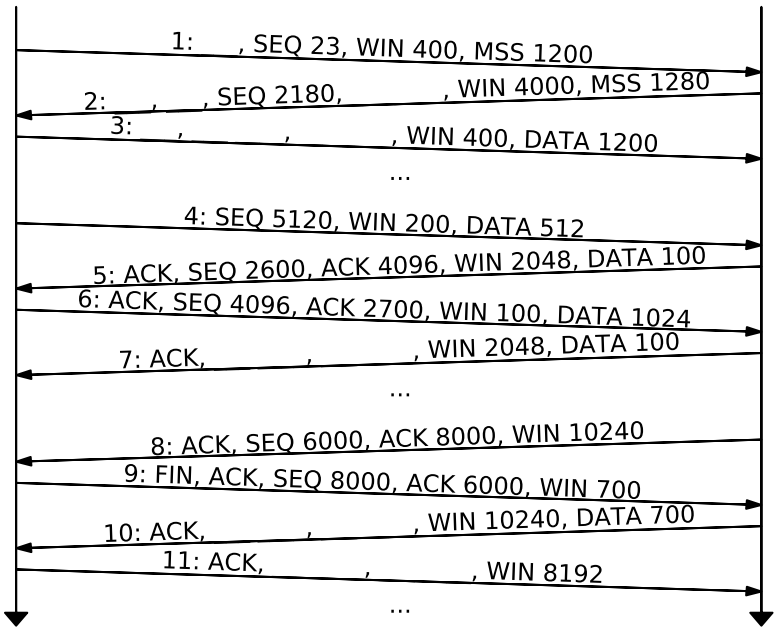
ix) *Gibt es dennoch Argumente für den Einsatz von Go-Back-N?* (1 Punkt)

Der Empfänger benötigt im vorherigen Szenario sehr große Puffer, damit Selective Repeat korrekt implementiert werden kann. Da der Sender schon 3 ms benötigt, um einen Paketverlust zu erkennen und das Paket neu zu übertragen, müssten wir mindestens die Daten, die in den 3 ms anfallen, zwischenspeichern können. Das sind allein schon 37,5 kB. Wenn das Delay größer wäre, wäre es noch deutlich mehr.
Also: für den Einsatz von Go-Back-N spricht der geringe Pufferbedarf auf Empfängerseite.

b) Gegeben sind die unten stehenden Auszüge einer TCP-Verbindung. Das Format ist dabei:

`<N>: {<FLAG>,}* SEQ <S>, [ACK <A>,] WIN <W>, [MSS <M>,] [DATA <D>]`

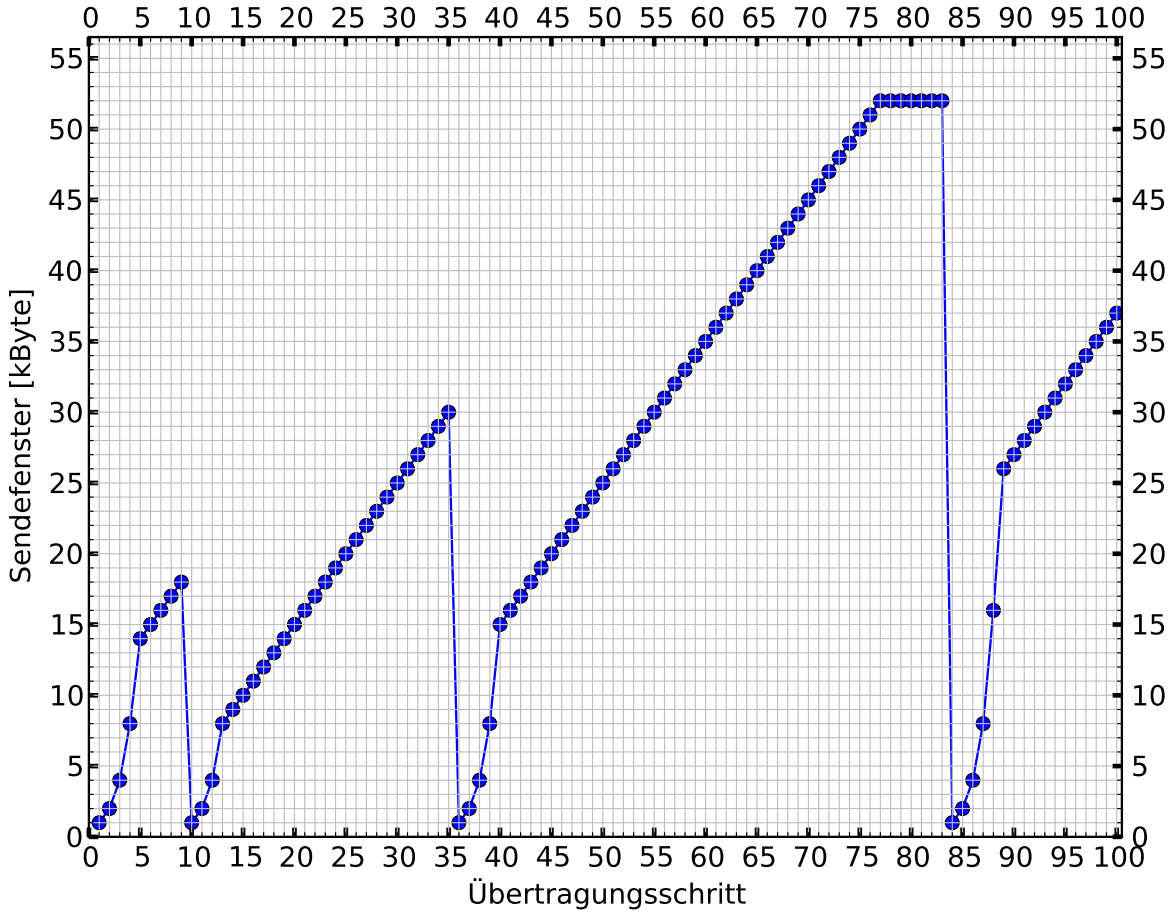
wobei `N` die Segmente lediglich zu Referenzzwecken durchnummeriert. Mit `FLAG` werden die Flags SYN, ACK und FIN genau dann angegeben, wenn sie gesetzt sind. `S` ist die Sequenznummer, `A` die Bestätigungsnummer sofern gesetzt, `W` die Window Size und `M` die Maximum Segment Size sofern gesetzt. Wenn `DATA <D>` angegeben ist, enthält die Nachricht `D` Byte Payload. "..." steht für beliebig viele Segmente, die hier nicht dargestellt sind. Das Auslesen von Daten aus den Empfangspuffern durch die Applikationen ist hier nicht dargestellt.



Ergänzen Sie die fehlenden Informationen.

- 1: SYN
- 2: SYN, ACK, ACK 24
- 3: ACK, SEQ 24, ACK 2181
- 7: SEQ 2700, ACK 5632
- 10: SEQ 6000, ACK 8001
- 11: SEQ 8001, ACK 6700

c) Gegeben ist das folgende Diagramm einer TCP-Datenübertragung, in der vereinfachend davon ausgegangen wird, dass die Übertragung in einzelnen Schritten stattfindet. Das Diagramm zeigt für jeden Schritt die Menge an Daten, die der Sender versenden darf.



Beantworten Sie folgende Fragen:

i) Wie heißt der Algorithmus, der hier benutzt wird?
ii) Wie groß ist der initiale Threshold?
iii) Wie groß ist der Threshold im 85. Übertragungsschritt?
iv) In welchen Übertragungsschritten liegen Paketverluste vor?
v) Wie groß muss der Puffer des Empfängers mindestens sein?
vi) Wie groß ist die maximal erreichbare Datenrate, wenn die RTT 13 ms beträgt?

i) Slow-Start-Algorithmus (mit Congestion Avoidance)
ii) 14 kB
iii) 26 kB
iv) 9, 35, 83
v) 52 kB
vi) $\frac{52\,\mathrm{kB}}{13\,\mathrm{ms}} = 32\,\mathrm{Mbit/s}$

d) In der Vorlesung haben Sie die Transportprotokolle TCP und UDP kennengelernt. Geben Sie *drei wichtige Unterschiede* der beiden Protokolle an.

Zum Beispiel:

Kriterium	TCP	UDP
zuverlässige Übertragung	ja	nein
Flusskontrolle	ja	nein
Staukontrolle	ja	nein

Lösung 5 (Internet Protocol (IP)) **(1 + 5 + 11 + 1) = 18 Punkte**

a) IP bietet einen verbindungslosen Datagrammdienst an. *Nennen Sie zwei Probleme, die sich bei der Übertragung von Datagrammen ergeben können.*

Zum Beispiel: ein Datagramm

- kann verloren gehen,
- kann andere Datagramme überholen (keine Reihenfolgetreue),

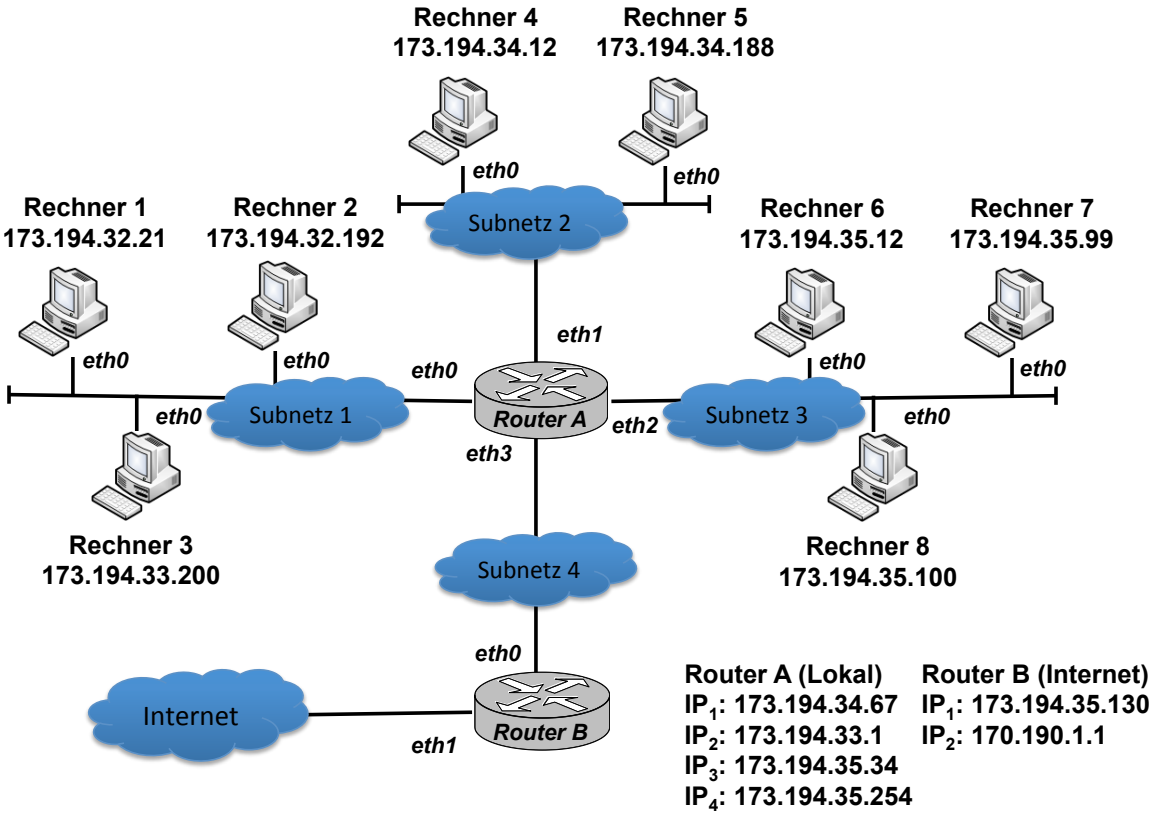
b) Ursprünglich wurde in IPv4 ein klassenbasiertes Adressschema verwendet. Nennen Sie den *wesentlichen Nachteil*, den die Verwendung von Adressklassen mit sich bringt. *Nennen* Sie außerdem *zwei Techniken*, die entwickelt wurden, um den Nachteil zu umgehen, und *beschreiben Sie jeweils knapp die Idee dieser Techniken*.

Wesentlicher Nachteil von Adressklassen: Starre Einteilung des Adressraums in Netze fester Größen, keine Anpassung an tatsächlichen Bedarf möglich – Adressbereiche liegen brach, Adressknappheit ist die Folge.

Techniken:

- Subnetzmasken: Unterteilung der (großen) starren Adressräume in kleinere Netze.
- NAT: Zu wenig IP-Adressen verfügbar, daher nur lokale IP-Adressen im gesamten lokalen Netz und eine globale IP-Adresse nach außen für alle internen Rechner.
- CIDR: Effizientere Nutzung von Adressräumen durch beliebige Netzpräfixe (so dass auch kleinere Netze zu größeren zusammengefasst werden können).

c) Ein Netzbetreiber hat den Adressbereich `173.194.32.0/22` zugewiesen bekommen und sein Netz wie in der folgenden Abbildung dargestellt konfiguriert:



Das Netz ist in vier Ethernet-Subnetze unterteilt, welche durch einen lokalen Router (Router A) miteinander verbunden sind. Ein weiterer Router (Router B) verbindet das gesamte Netzwerk mit dem Internet. Für jeden Rechner und Router sind in der Abbildung jeweils die IP-Adressen sowie die Namen der vorhandenen Netzwerkkarten angegeben. Da Router über mehrere IP-Adressen verfügen, sind diese schlicht mit IP_x durchnummeriert, allerdings ist keine Zuordnung zu den Netzwerkkarten angegeben.

Beantworten Sie die folgenden Fragen zur Konfiguration des Netzes:

(i) Welche *Basisadresse (Netz-ID) und Subnetzmaske* werden in den vier Subnetzen jeweils verwendet? (4 Punkte)

Subnetz	Netz-ID	Subnetzmaske
1	**173.194.32.0**	**/23 oder 255.255.254.0**
2	**173.194.34.0**	**/24 oder 255.255.255.0**
3	**173.194.35.0**	**/25 oder 255.255.255.128**
4	**173.194.35.128**	**/25 oder 255.255.255.128**

(ii) Welche *Gateways (Default-Router)* müssen Rechner 1 – 8 jeweils eintragen? (2 Punkte)

Rechner	Gateway	Rechner	Gateway
1	**173.194.33.1**	5	**173.194.34.67**
2	**173.194.33.1**	6	**173.194.35.34**
3	**173.194.33.1**	7	**173.194.35.34**
4	**173.194.34.67**	8	**173.194.35.34**

(iii) Welche *Einträge* muss *Router A* in seiner Tabelle vornehmen? Beschränken Sie sich dabei auf Angaben zu Zielnetz und Netzwerkkarte. (2 Punkte)

Zielnetz	Netzwerkkarte
173.194.32.0/23	**eth0**
173.194.34.0/24	**eth1**
173.194.35.0/25	**eth2**
173.194.35.128/25	**eth3**
0.0.0.0/0	**eth3**

(iv) Wäre es *zulässig*, Router A auf der Netzwerkkarte `eth2` die IP-Adresse `173.194.35.127` zu geben? Begründen Sie Ihre Antwort. (1 Punkt)

Nicht zulässig, da es sich um die Broadcastadresse des Netzes handelt.

(v) *Wie viele Einträge in seiner Routing-Tabelle* muss *ein beliebiger Router im Internet* für die obigen vier Subnetze anlegen? *Erhöht sich die Anzahl der Einträge, wenn Subnetz 1 in weitere Subnetze aufgeteilt würde*? Begründen Sie Ihre Antwort. (2 Punkte)

Ein beliebiger Router benötigt *einen Eintrag*. Die interne Struktur ist hinter Router B verborgen und spielt nur intern eine Rolle.

Nur der lokale Router (Router A) muss die Struktur von Subnetz 1 kennen, daher erhöht sich die Anzahl nicht.

d) Angenommen, ein Router habe ein valides IP-Paket zur Vermittlung erhalten und hat festgestellt, dass er es in sein eigenes Subnetz weiterleiten muss. Außerdem hat er festgestellt, dass er zum ersten mal ein IP-Paket an den Zielrechner weiterleiten muss. *Was muss der Router nun unternehmen, um das Paket im Subnetz zuzustellen? Welches Protokoll wird dazu benutzt?*

Zunächst muss der Router die MAC-Adresse des Rechners ermitteln, dem die entsprechende IP-Adresse zugewiesen ist.

Dazu wird ARP benutzt.

Lösung 6 (Routing) **(0,5 + 7,5) = 8 Punkte**

Angenommen, ein Provider betreibt ein autonomes System mit sechs Knoten *A, B, C, D, E, F* und verwendet Link-State-Routing. In den unten stehenden Tabellen sind die kürzesten Pfade von *A* und *D* zu jedem anderen Knoten im Netzwerk angegeben.

	Schritt					
Knoten	0	1	2	3	4	5
A	(0,-)					
B	∞	12,A	11,C	11,C	11,C	(9,E)
C	∞	(2,A)				
D	∞	∞	∞	(6,F)		
E	∞	∞	11,C	7,F	(7,F)	
F	∞	∞	(5,C)			

Tabelle von A

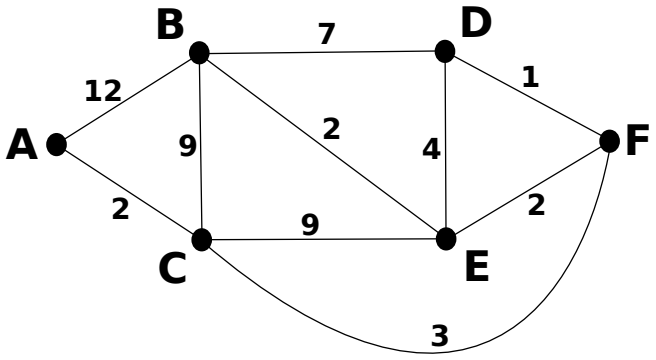
	Schritt					
Knoten	0	1	2	3	4	5
A	∞	∞	∞	∞	6,C	(6,C)
B	∞	7,D	7,D	5,E	(5,E)	
C	∞	∞	4,F	(4,F)		
D	(0,-)					
E	∞	4,D	(3,F)			
F	∞	(1,D)				

Tabelle von D

a) *Welche Kosten hat der günstigste Pfad* zwischen *C* und *D*?

Die minimalen Kosten zwischen C und D sind 4.

b) Vervollständigen Sie die Topologie des Netzwerkes, indem Sie die Kanten einzeichnen und mit den zugehörigen Kosten beschriften.



Lösung 7 (Sicherheit) **(5 + 3 + 4) = 12 Punkte**

a) Sie verwenden *RSA* als asymmetrisches Verschlüsselungsverfahren und haben $p = 7$ und $q = 13$ gegeben. *Ist* $< 7, 91 >$ *ein gültiger geheimer Schlüssel?* Begründen Sie Ihre Antwort.

Berechne zunächst $\phi(n)$ mit $n = p \cdot q = 91$: $\phi(n) = (p-1) \cdot (q-1) = 72$.

Prüfe zuerst, dass $d = 7$ relativ prim zu 72 ist (z.B. mittels euklidischem Algorithmus zeigen $\mathrm{ggT}(d, n) = 1$). Oder durch scharfes Hinsehen.

Jetzt bleibt zu klären: Gibt es ein e mit $e \cdot 7 \mod 72 = 1$ (also ein multiplikatives Inverses)?

Mögliche Begründung:

- Mittels erweitertem euklidischen Algorithmus $e = 31$ bestimmen.
- Erkennen, dass es ein Inverses geben muss, da d relativ prim zu $\phi(n)$ ist.

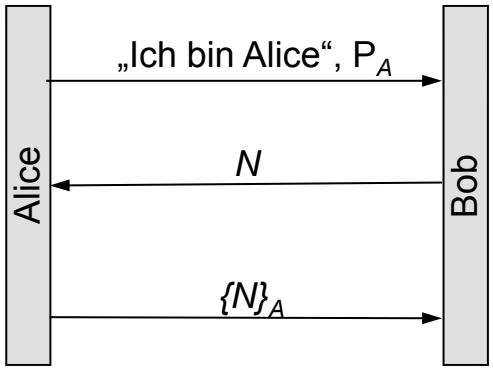
b) *Was ist eine Nonce und wofür wird sie verwendet?* Einige Sicherheitsprotokoll-Implementierungen nutzen Zeitstempel als Nonces. *Warum sind Zeitstempel eine schlechte Wahl für eine Nonce?*

Eine Nonce (Number Used Once) ist ein nur einmal verwendeter Zufallswert.

Nonces werden dazu verwendet einen Nachrichtenaustausch, z.B. zur Authentifizierung wie im nächsten Aufgabenteil, unvorhersehbar zu machen. Daher müssen sie zufällig sein. Verhindert z.B. Replay-Angriffe.

Zeitstempel sind nicht zufällig genug, daher können später verwendete Nonces bei einer einmal bekannten Nonce berechnet werden. (Je nach Verwendung der Nonces kann ein Sicherheisverfahren dadurch angegriffen werden – würde z.B. Bob im nächsten Aufgabenteil seine Nonce mit P_A verschlüsseln und Alice ihre Identität durch Entschlüsselung des Wertes sicherstellen, kann ein Angreifer durch korrektes Raten der verwendeten Nonce direkt den erwarteten Wert an Bob zurücksenden und Alice' Identität fälschen.)

c) Alice authentifiziert sich gegenüber Bob mittels des folgenden Challenge-Response-Verfahrens:



Dabei ist P_A der öffentliche Schlüssel von *Alice*, N eine von Bob gewählte Nonce und $\{N\}_A$ bezeichne die Verschlüsselung von N mit dem privaten Schlüssel A von $Alice$. *Beschreiben Sie das Problem, welches bei dieser Authentifizierung auftritt. Beschreiben oder skizzieren Sie zudem einen möglichen Angriff. Wie kann man das auftretende Problem lösen?*

Problem: In der ersten Nachricht überträgt Alice ihren öffentlich Schlüssel mit. Dieser ist nicht authentifiziert (Bob kann nicht prüfen, ob er wirklich von Alice ist).

Möglich: Man-in-the-middle-Angriff: Mallory ersetzt in der ersten Nachricht den öffentlichen Schlüssel P_A durch ihren eigenen öffentlichen Schlüssel P_M. Bob schickt die Nonce an Mallory, welche sie einfach an Alice weiterleitet, damit diese nichts merkt, und die Nonce mit dem eigenen privaten Schlüssel verschlüsselt an Bob zurücksendet. (Das Ganze als Bild dargestellt und korrekt beschriftet ist auch ok.)
Mögliche Lösungen: Zertifikate (CA), Trusted 3rd party / CA, anderer sicherer Kanal (z.B. persönliches Übergeben des Schlüssels, oder per Post).