

Klausur SS 2014

08.07.2015

Name:	<u>Mustermann</u>	Vorname:	<u>Max</u>
Studiengang:	<u>Informatik, Bachelor</u>		
Matr.Nr.:	<u>999999</u>	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 ausgehängte 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 ausgehängte 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	



Aufgabe 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.*



- 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.

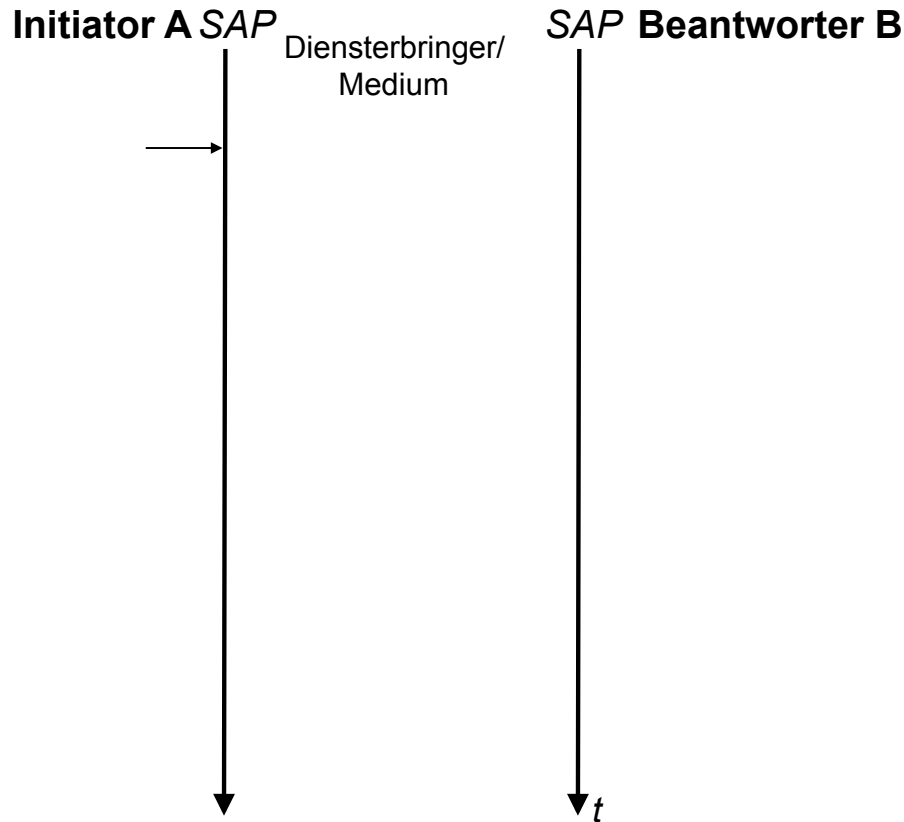


- c) Nutzer *A* möchte Daten an Nutzer *B* senden und verwendet dazu einen verbindungsorientierten Kommunikationsdienst.

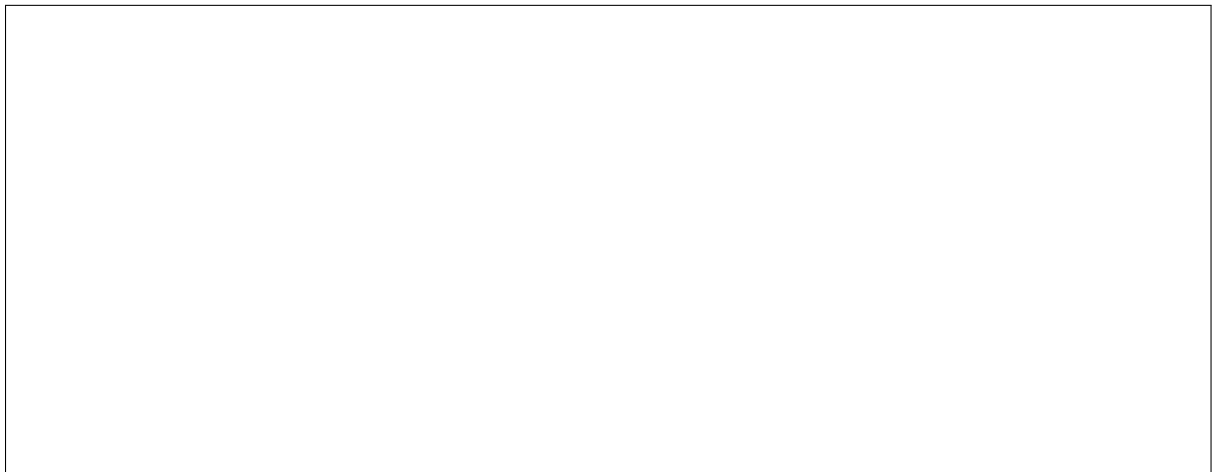
Skizzieren Sie ein Weg/Zeit-Diagramm für die drei Phasen dieses Dienstes: Verbindungsaufbau (*Connection*), Datenübertragung (*Data*) und Verbindungsabbau (*Disconnection*).

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?



Aufgabe 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

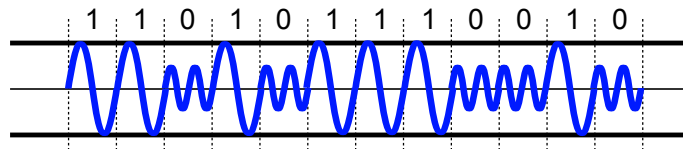
Beantworten Sie die folgenden Fragen mittels der *Theoreme von Shannon und Nyquist*:

- 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.

- 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.

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



- 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?

Aufgabe 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?*

- 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!

- 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?

Aufgabe 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)

- 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)

- 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)

- 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.

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

(1 Punkt)

- vi) Ihr Transportprotokoll soll Paketfehler durch Triple-Duplicate-Acknowledgements erkennen. Die Übertragungsverzögerung des Netzwerkes betrage $1020\ \mu\text{s}$. 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)

- 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)

- 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)

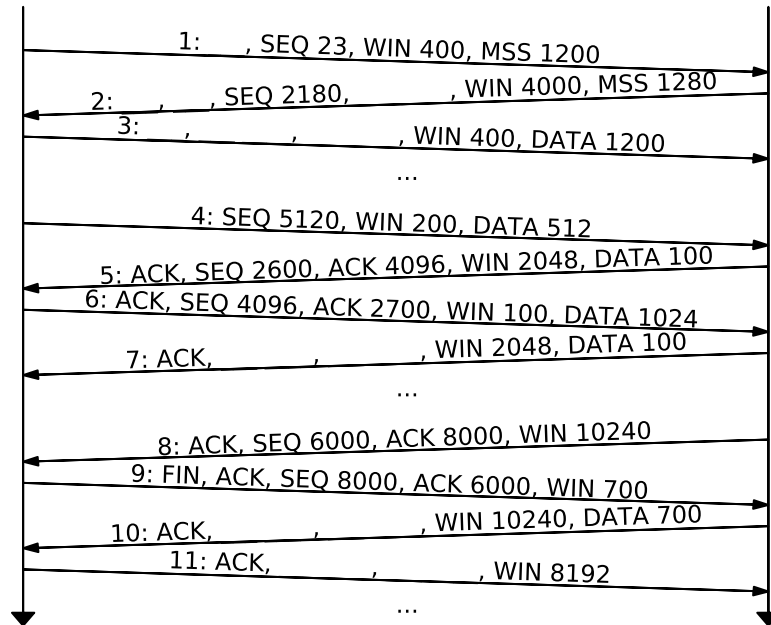
- ix) Gibt es dennoch Argumente für den Einsatz von Go-Back-N?

(1 Punkt)

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

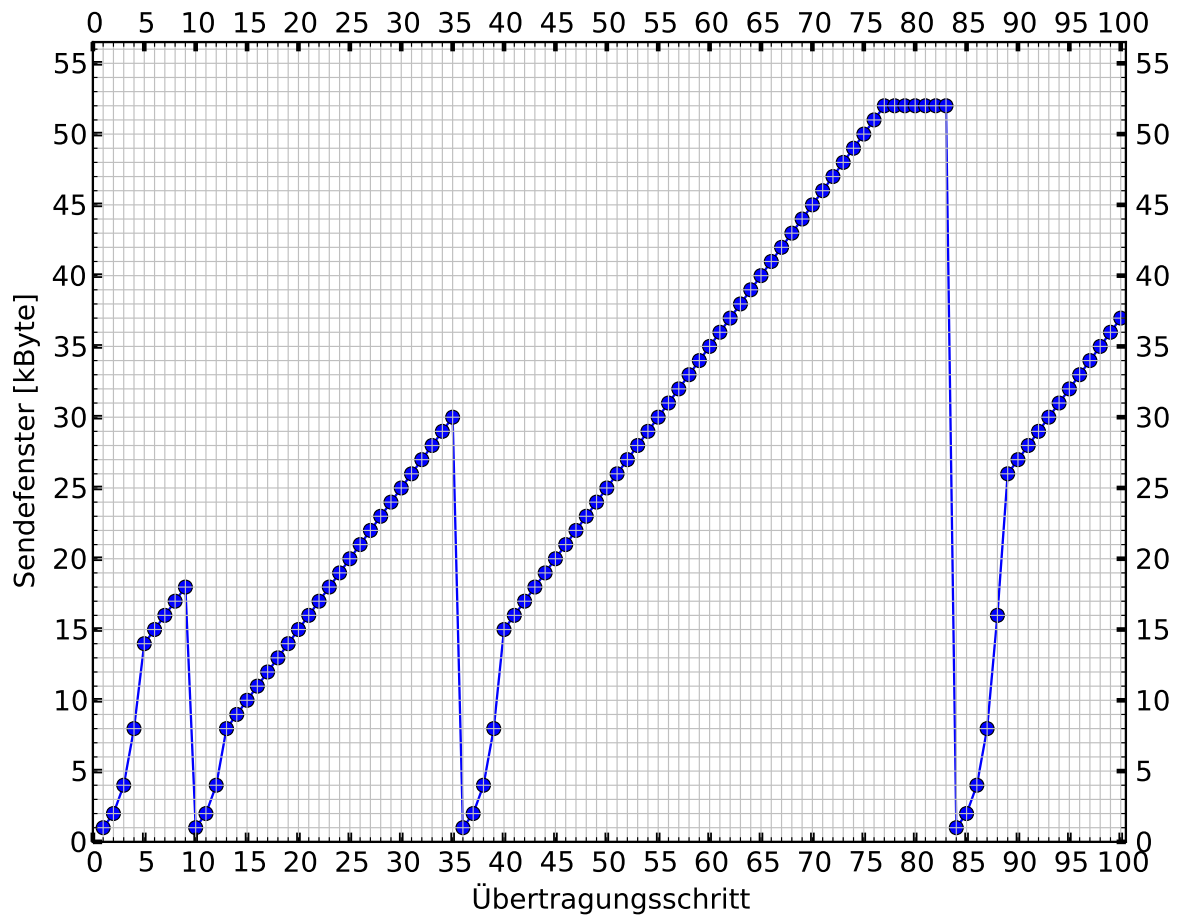
<N>: {<FLAG>,}* SEQ <S>, [ACK <A>], WIN <W>, [MSS <M>], [DATA <D>]

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.

- 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:

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

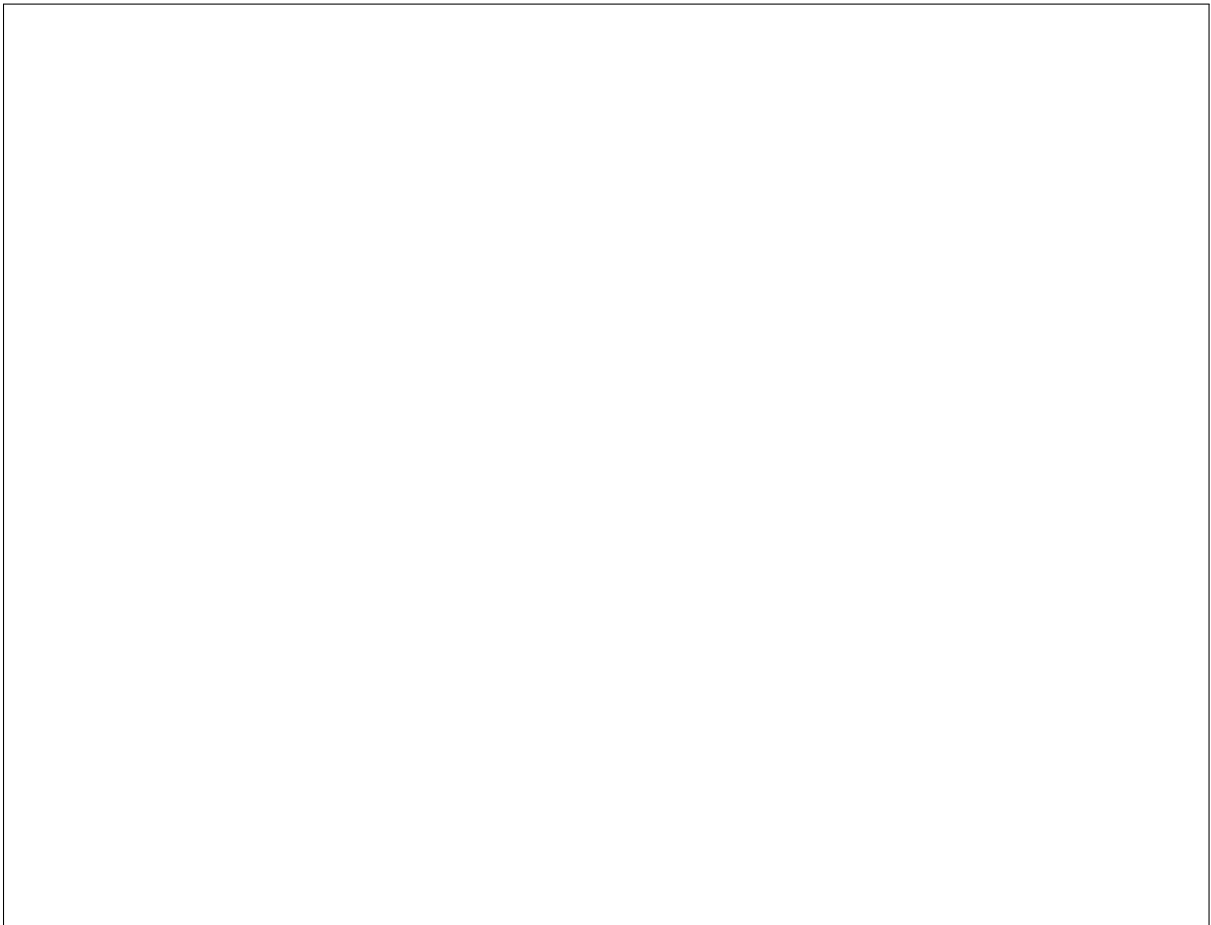
- d) In der Vorlesung haben Sie die Transportprotokolle TCP und UDP kennengelernt. Geben Sie *drei wichtige Unterschiede* der beiden Protokolle an.

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

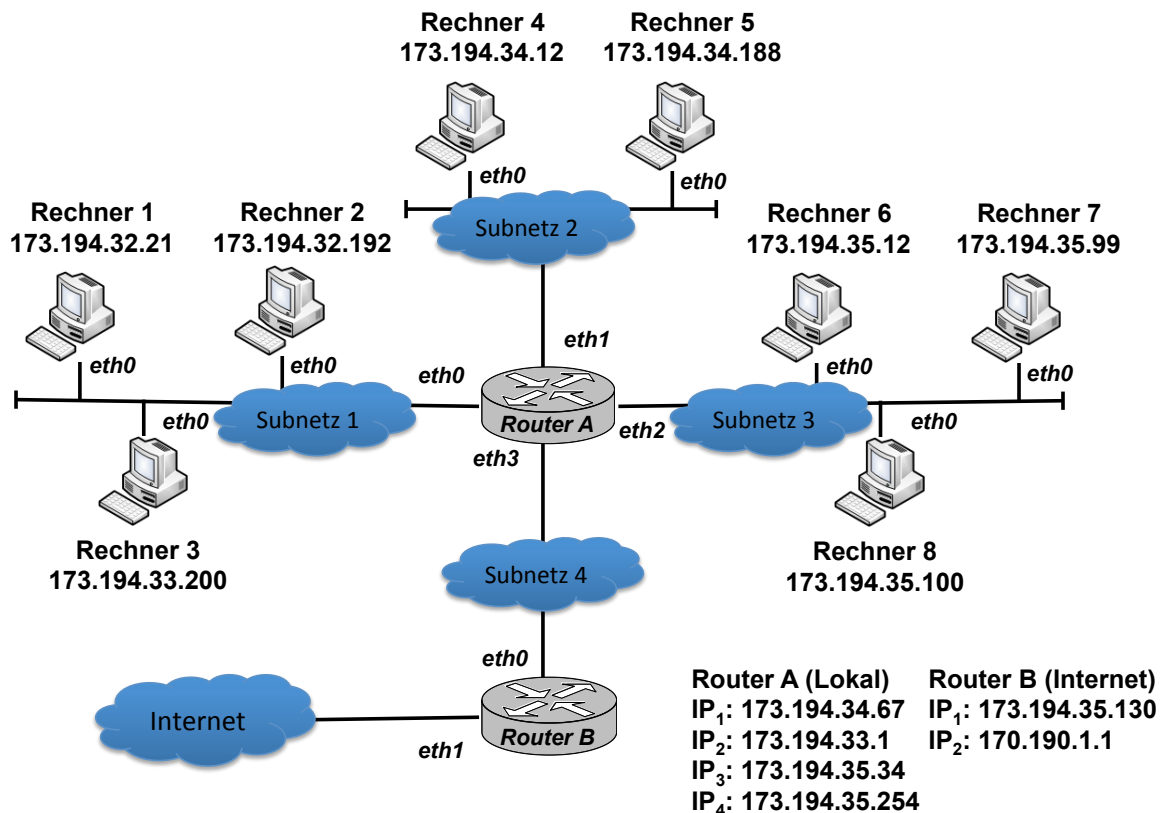
- a) IP bietet einen verbindungslosen Datagrammdienst an. *Nennen Sie zwei Probleme, die sich bei der Übertragung von Datagrammen ergeben können.*



- 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*.



- 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		
2		
3		
4		

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

Rechner	Gateway	Rechner	Gateway
1		5	
2		6	
3		7	
4		8	

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

Zielnetz	Netzwerkkarte

- (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)

- (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)

- 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?*

Aufgabe 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)			

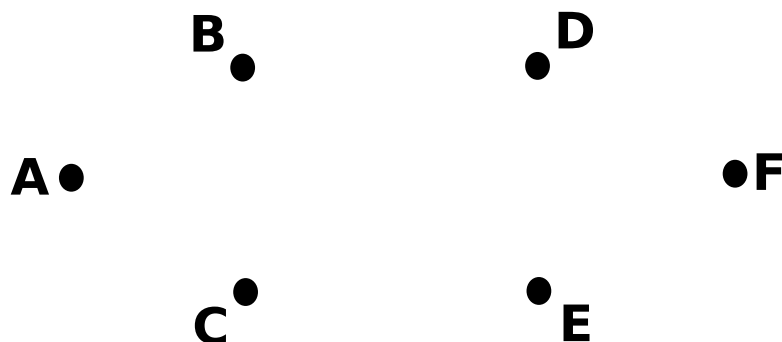
Tabelle von A

	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*?

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

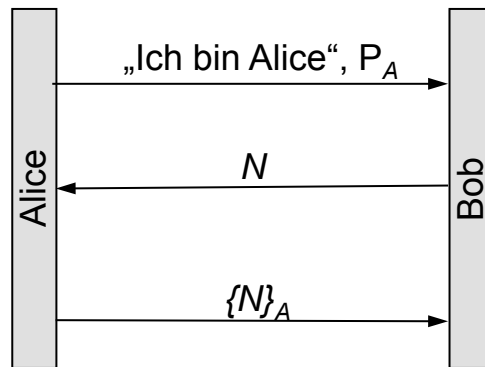


Aufgabe 7 (Sicherheit)**(5 + 3 + 4) = 12 Punkte**

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

- 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?*

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?

Platz für Nebenrechnungen

Falls Sie auf dieser Seite weitere Lösungen angeben, machen Sie bitte bei der entsprechenden Aufgabe klar, dass sich auf dieser Seite eine zu bewertende Lösung findet. Andernfalls wird diese Seite nicht beachtet!

Platz für Nebenrechnungen

Falls Sie auf dieser Seite weitere Lösungen angeben, machen Sie bitte bei der entsprechenden Aufgabe klar, dass sich auf dieser Seite eine zu bewertende Lösung findet. Andernfalls wird diese Seite nicht beachtet!

Platz für Nebenrechnungen

Falls Sie auf dieser Seite weitere Lösungen angeben, machen Sie bitte bei der entsprechenden Aufgabe klar, dass sich auf dieser Seite eine zu bewertende Lösung findet. Andernfalls wird diese Seite nicht beachtet!