Klausur SS 2011

14.09.2011

Name:		Matr.Nr.:	
Vorname:		Studiengang:	

Hinweise: (Bitte sorgfältig durchlesen!)

- Schreiben Sie auf **jedes Blatt** Ihren Namen und Ihre Matrikelnummer.
- Die Aufgaben können in der Regel auf den Aufgabenblättern beantwortet werden. Tragen Sie Ihre Lösungen in die dafür vorgesehenen Felder ein. Reicht der Platz nicht aus, **ist für jede Aufgabe ein neues Blatt zu verwenden**.
- Am Ende der Klausur ist das Deckblatt zusammen mit den Aufgabenblättern und evtl. zusätzlich verwendeten Blättern wieder abzugeben.
- Die Bearbeitungszeit beträgt **120 Minuten**.
- Es sind **keine Hilfsmittel** erlaubt.
- Die Klausur umfasst insgesamt **120** Punkte. Zum Bestehen genügen **60** Punkte.

Mit meiner Unterschrift bestätige ich, dass ich die Hinweise zur Kenntnis genommen habe.

_____

Unterschrift

Punktespiegel:

Aufgabe	1	2	3	4	5	6	7	Σ
Erreichbare Punkte	14	13	24	23	12	22	12	120
Erreichte Punkte								

Lösung 1 (Allgemeine Grundlagen) **(4+2+8) = 14 Punkte**

a) *Skizzieren* Sie das ISO/OSI-Referenzmodell und das Internet-Referenzmodell. *Geben Sie dabei die Namen der einzelnen Schichten 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, Reihenfolge und Namen der Schichten siehe Folien.

Zuordnung: Anwendung, Transport, Vermittlung direkt, untere beiden OSI auf Host-to-Network, evtl noch Schicht 5 und 6 zu Anwendung hin, ist aber eigentlich nicht nötig.

Punkte: 3 für die Referenzmodelle, einer für die Zuordnung; fehlende Namen oder falsche Reihenfolge je 0.25 Abzug (aufgerundet auf halbe Punkte).

b) Sowohl Sicherungsschicht als auch Vermittlungsschicht des ISO/OSI-Referenzmodells ermöglichen die Kommunikation zwischen Rechnern. Worin liegt der *Mehrwert der Vermittlungsschicht*?

Die Sicherungsschicht arbeitet nur lokal, sie kümmert sich nur um die Übertragung zwischen benachbarten Rechnern (MAC-Adressen).

Die Vermittlungsschicht setzt darauf ein virtuelles Netz, arbeitet global (IP-Adressen) – sie koppelt verschiedene lokale Netze und kann Daten zwischen Netzen vermitteln.

Wichtige Aussage also: die Vermittlungsschicht koppelt Netze, ermöglicht also auch Kommunikation über Netzgrenzen hinweg **(2 Punkte)**.

c) Eine Anwendung A kommuniziere über *TCP-Sockets* mit einer anderen Anwendung B. Erläutern Sie knapp die Begriffe *Dienst, Dienstzugangspunkt und Protokoll* unter Zuhilfenahme dieses Beispiels. Geben Sie außerdem an, ob es sich bei der Kommunikation zwischen A und B um *vertikale oder horizontale* Kommunikation handelt (mit Begründung).

Vom Netz bzw. einer der Schichten bereitgestellte Funktionen werden als Dienst bezeichnet – der Dienst ist in diesem Fall also die TCP-Funktionalität, also zuverlässige Datenübertragung **(2 Punkte)**.

Der Dienstzugangspunkt ist der Socket; er stellt Funktionen zur Dienstnutzung als konkrete Instanz der Anwendung zur Verfügung **(2 Punkte)**.

Dienste werden durch bestimmte Instanzen erbracht, welche sich nach bestimmten Regeln verhalten und mit anderen Instanzen interagieren – Protokolle kann man als Implementierung dieser Regeln bezeichnen. Hier definiert TCP als Protokoll die Regeln: bestätigten Datenaustausch usw **(2 Punkte)**.

Die Anwendungen kommunizieren (virtuell) horizontal. Grund: horizontal wird immer auf der gleichen Schicht kommuniziert, aber dabei werden die Dienste unterliegender Schichten genutzt. Die Interaktion zwischen den Schichten ist vertikale Kommunikation. **0.5 Punkte für korrekte Nennung von vertikal oder horizontal, 1.5 für die zugehörige Begründung.**

Lösung 2 (Signale) **(7+3+3) = 13 Punkte**

a) Gegeben sei ein Kanal mit einer Bandbreite von 5.000 Hz und einem Signal-Rauschabstand von 30 dB. Sie wollen nun 64-QAM zur Codierung Ihrer Daten auf diesem Kanal verwenden. *Ist dies unter den gegebenen Voraussetzungen möglich*? Begründen Sie Ihre Antwort mit Hilfe der *Theoreme von Shannon und Nyquist*.

Nyquist-Theorem: $C = B \cdot 2 \cdot ld(n)$

Shannon-Theorem: $C = B \cdot ld(1 + S/N)$

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

Hier: $B = 5000Hz$ und $n = 64$

$SNR = 30dB = 10 \cdot log_{10}(S/N) <=> 3 = log_{10}(S/N) <=> S/N = 10^3$

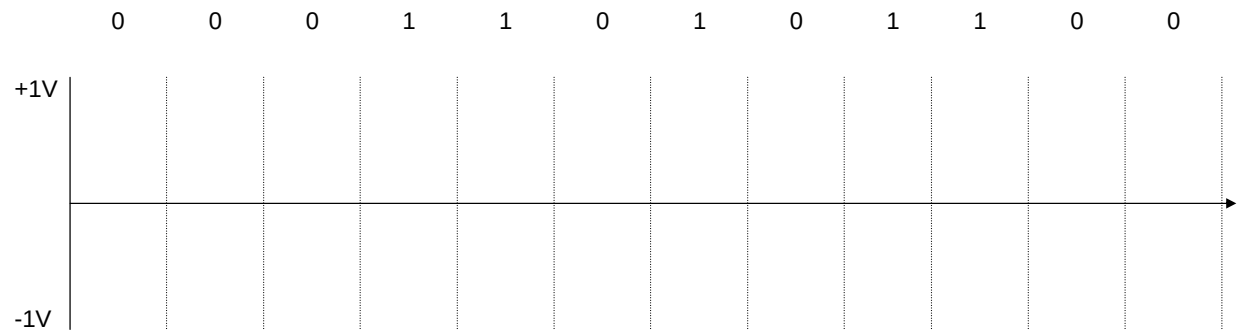
Somit:

Nyquist: $C = 5.000 \cdot 2 \cdot ld(64) = 60.000Bit/s$ **(3 Punkte)**

Shannon: $C = 5.0000 \cdot ld(1 + 1000) = 50.000Bit/s$ **(3 Punkte)**

Also: nicht möglich, da Shannon einen kleineren Wert ergibt und die Datenrate und damit auch die Zahl der möglichen Signalstufen beschränkt **(1 Punkt)**.

b) Stellen Sie die Bitfolge **0 0 0 1 1 0 1 0 1 1 0 0** im *Manchester-Code* dar.



Punkte: ach, was weiß denn ich!

c) Angenommen, es steht eine *Schrittgeschwindigkeit von 5000 baud* zur Verfügung. Geben Sie an, welche *Übertragungsrate* mit den folgenden Codes jeweils erreicht werden kann:

- Manchester-Code
- NRZ-L-Code
- 4B/5B-Code

Manchester siehe oben: je zwei Schritte pro Bit, d.h. 2500 Bit/s **(1 Punkt)**

NRZ-L: ein Bit pro Schritt, also 5000 bit/s **(1 Punkt)**

4B/5B hat effizienz von 80%, also 4000 Bit/s **(1 Punkt)**

Lösung 3 (Sicherungsschicht) **(3+6+4+6+5) = 24 Punkte**

a) Eine Aufgabe der Sicherungsschicht ist die Flusskontrolle, d.h. die Absicherung eines Empfängers mit geringer Kapazität gegen eine Überlastung durch einen Sender mit hoher Kapazität. Hierzu wird meist ein Sliding-Window-Verfahren mit einem Modulus M und einer Fenstergröße W verwendet.

Der Modulus sei mit $M = 12$ gegeben. Wie groß darf die *Fenstergröße W maximal* sein? Begründen Sie knapp Ihre Antwort.

$W = M - 1 = 11$ **(1 Punkt)**

Denn: sein $W = M = 12$. Dann könnten 12 Rahmen ohne Erhalt einer Quittung versendet werden; dies seien 0, ..., 11. Kommt nun eine Quittung mit Quittungsnummer 0 an, kann dies zwei Gründe haben: entweder ist alles quittiert (die anderen Quittungen sind nicht angekommen), oder es ist ein Duplikat einer alten Quittung für den Rahmen mit der vorherigen Nummer 11 bzw. (je nach Verfahren) ein DUP-ACK, welches den Verlust von Rahmen 0 anzeigen soll. Der Empfänger kann sich also nicht sicher sein, ob die Quittung tatsächlich die Daten quittiert oder ob Daten wiederholt werden sollten – Sender und Empfänger befinden sich nicht mehr im gleichen Zustand **(2 Punkte)**.

b) 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. *Beschreiben Sie beide Mechanismen knapp anhand der unten stehenden Fragen zum folgenden Beispiel*:

Gegeben seien ein Modulus $M = 11$ und eine Fenstergröße $W = 8$. Zum aktuellen Zeitpunkt seien die Rahmen mit den Sequenznummern 9,10,0,1,2,3 vom Sender gesendet worden, ohne dass eine Quittung eingegangen ist.

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

ii) Wie ändert sich die Situation, falls ein Rahmen mit einer Quittungsnummer (ACK) 3 empfangen wird?

iii) Was passiert, wenn stattdessen ein NAK für die Sequenznummer 0 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 8 Stück, also können in der gegebenen Situation noch die Rahmen 4, 5 gesendet werden. **(2 Punkte)**

ii.) Bei einer Quittung gilt alles bis zum vorherigen Rahmen als bestätigt, der Empfänger wartet auf Zustellung aller Rahmen ab dem dritten. In der gegebenen Situation wird das Fenster also bis zur 3 vorgeschoben, es sind fünf weitere Plätze (also 7 insgesamt) frei und wir können insgesamt 4,5,6,7,8,9 und 10 übertragen. **(2 Punkte. Wer behauptet, die 3 würde neu übertragen, da sie nicht mit quittiert wurde, wird exmatrikuliert.)**

iii). Bei einem NAK signalisiert der Empfänger, dass das bezeichnete Rahmen nicht empfangen worden ist. Laut Go-Back-N müssen alle Rahmen ab dem bezeichneten wieder neu übertragen werden. Also zumindest 0, 1, 2 – Da mit dem NAK alles vorherige quittiert ist, können auch noch 3, 4, 5, 6, 7 übertragen werden. **(2 Punkte)**

c) Eine weitere Aufgabe der Sicherungsschicht ist die Fehlererkennung bzw. -korrektur. Ein Mechanismus zur Erkennung von Übertragungsfehlern ist die *Cyclic Redundancy Checksum (CRC)*. Zwei Kommunikationspartner verwenden nun CRC und haben sich auf die Verwendung des Generatorpolynoms

$$G(x) = x^3 + x^2 + 1$$

geeinigt.

Berechnen Sie die CRC-Prüfsumme zu

1 0 1 1 0 1

und geben Sie die zu übertragende Bitfolge an.

Platz für die Polynomdivision... **(3 Punkte für die Rechnung, Abzüge nach Gefühl)**

CRC-Prüfsumme: 010

Übertragung: 101101010 **(1 Punkt)**

d) Eine Möglichkeit zur Fehlerkorrektur ist der Einsatz des *Hamming-Codes*.

Sie haben die folgenden beiden Bitsequenzen erhalten, die mit dem Hamming-Code geschützt sind. Überprüfen Sie für beide Sequenzen, ob es zu Übertragungsfehlern gekommen ist. ***Markieren*** *Sie dazu die Prüfbits, für die Sie andere Werte berechnen, und* ***unterstreichen*** *Sie diejenigen Bits, die Sie folglich als falsch identifizieren. Schreiben Sie die (korrigierten) Datenbits in die rechte Spalte der Tabelle.*

Hamming-Code									Datenbits
1	2	3	4	5	6	7	8	9	
0	[1]	0	1	1	1	1	0	0	**0 1 1 1 0**
[0]	[0]	1	[1]	0	1	1	1	1	**1 0 1 0 1**

(Für jede Bitfolge je ein Punkt für die Markierung falscher Prüfbits, ein Punkt für das Erkennen, welches Bit korrigiert werden muss, ein Punkt für korrekte Datenbitfolge.)

e) Der dritte wesentliche Aufgabenbereich der Sicherungsschicht ist die Regelung des Medienzugriffs. Das prominenteste Verfahren für lokalen 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 gleichzeitig Daten an C versenden.

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

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 fängt B an, ebenfalls zu senden **(1 Punkt)**.

ii) A hört sich selbst beim Senden zu, und erkennt durch Überlagerung seines Signals mit dem Signal von B, dass er etwas anderes hört, als er gesendet hat. 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 (falls C nicht bereits vorher auch schon an Spannungsspitzen die Kollision selbst erkannt hat) **(2 Punkte)**.

iii) Die Station muss immer noch senden, wenn das kollidierende Signal ankommt – es ist eine minimale Rahmenlänge notwendig **(2 Punkt)**.

Lösung 4 (Internet Protocol (IP)) **(6+2+6+3+5+1) = 23 Punkte**

a) Ursprünglich wurde in IPv4 ein klassenbasiertes Adressschema verwendet. Nennen Sie den *wesentlichen Nachteil*, den die Verwendung von Adressklassen mit sich bringt. Nennen und erläutern Sie außerdem *zwei Techniken, die man entwickelt hat, um mit diesem Nachteil umzugehen*.

Adressklassen: starre Einteilung des Adressraums in Netze fester Größen, keine Anpassung an tatsächlichen Bedarf möglich – was in einer Adressknappheit endet **(2 Punkte)**.

Techniken z.B.:

Subnetzmasken: Unterteilung der starren Adressräume in kleinere Netze.
NAT: zu wenig IP-Adressen verfügbar, daher nur lokale IP-Adressen (gesamtes Netz) und nur eine globale IP-Adresse nach außen..
CIDR: Effizientere Nutzung von Addressräumen durch beliebige Netzpräfixe.
Jeweils **(2 Punkte)** pro Technik.

b) Sie bekommen mitgeteilt, dass Sie in Ihrem Klasse-B-Netz die Subnetzmaske 255.255.168.0 verwenden sollen. Ist dies eine im Sinne des Standards für ihr Netz gültige Subnetzmaske? *Wenn ja: wie viele Rechner können Sie pro Subnetz installieren? Wenn nein: warum ist sie nicht gültig?*

Nicht gültig – es treten gemischt 0en und 1en auf, was nicht erlaubt ist.

c) Sie haben für Ihre Firma einen IP-Adressbereich zur Verfügung gestellt bekommen und wollen diesen in unterschiedliche Subnetze einteilen, die jeweils über 400 Hosts verfügen sollen.

i) *Welche Subnetzsmake wählen Sie innerhalb Ihrer Firma, um diese Subnetze einzuteilen?* Gehen Sie dabei davon aus, dass sich die Anzahl der Hosts in Ihren Subnetzen nie ändern wird und Sie daher nur die minimal nötige Anzahl von Bits zur Adressierung von Hosts bereitstellen müssen.

ii) Nehmen Sie nun an, dass Sie in dem Ihnen zugewiesenen Adressbereich genau 64 Subnetze der benötigten Größe einrichten können. *Welche Bits ihrer Adressen charakterisieren somit das gesamte Netzwerk, welche ein Subnetz und welche den Hostanteil?*
(Verwenden Sie für die Angabe z.B. das Format `nnnnnnnn.nnnnnnss.ssssssss.shhhhhhh`, mit `n` für Netzwerk-, `s` für Subnetz-, `h` für Hostanteil).

iii) Ihr eigener Rechner habe im obigen Netz die IP-Adresse 137.226.4.6. Geben Sie unter Verwendung der Einteilung aus (ii) den *Adressbereich des gesamten Firmennetzwerks sowie den des Subnetzes Ihres Rechners* an.

Um 400 Hosts zu adressieren, benötigt man 9 Bit ($2^9 = 512$). Daher wählen wir die Subnetzmaske 255.255.254.0 **(1 Punkt)**.

Zur Adressierung von 64 Subnetzen werden 6 Bit benötigt ($2^6 = 64$). Daher haben unsere Bits in den Adressen die folgende Bedeutung: `nnnnnnnn.nnnnnnnn.nssssssh.hhhhhhhh`. **(1 Punkt)**

Die Netzwerkmaske für das gesamte Netz ergibt sich damit zu 255.255.128.0, der Adressbereich des Firmennetzes ist also 137.226.0.0/17 (137.226.0.0 - 137.226.127.255) **(2 Punkte)**.

Die Adressbereiche der Subnetze sind gegeben durch
(137.226).0ssssss0.00000000 - (137.226).0ssssss1.11111111

Für den gegebenen Rechner ist *ssssss* = 000010, der Adressbereich des Subnetzes ist daher 137.226.4.0 - 137.226.5.255 **(2 Punkte)**.

d) IPv6 wurde eingeführt, um Nachteile zu beheben, die man bei IPv4 erkannt hatte. Benennen Sie *drei elementare Unterschiede* zwischen IPv4 und IPv6.

Elementare Unterschiede: - Größerer Adressraum / längere Adressen / mehr Adressen - Schnellere Vrerarbeitung in Routern durch bessere Headerstrukturierung (z.B. Optionen duch Erweiterungsheader) - 'Verbindungsorientierung' durch Flow Labels, nicht nur Weiterleitung auf Basis von Adressen - Integrierte Sicherheitsfunktionen bzw. generell: Unterstützung von Zusatzdiensten (wieder durch bessere Optionsverwaltung) - ...

NICHT richtig ist: - Die Header sind unterschiedlich bzw. unterschiedlich lang – das ist RESULTAT der Unterschiede! - Dotted Decimal vs. Hexadezimaler Darstellung – das ist Konvention für den Menschen, um mit den längeren Adresen klarzukommen. - IPv6 wird nicht so viel genutzt – das ist nicht wirklich ein integraler Bestandteil des Protokolls!

e) Ein Router empfange ein IP-Paket mit einer Gesamtlänge von 1500 Byte. Er ist allerdings nur in der Lage, Pakete mit einer Gesamtlänge von 480 Byte zu versenden. *Skizzieren* Sie den daraufhin eintretenden Fragmentierungsprozess und *geben Sie die enstandenden Fragmente mit ihrer Länge an*. Woran *erkennt der Empfänger*, dass eine Fragmentierung stattgefunden hat?

20 IPHeader + 1480Daten Gesamtlänge von 480 Byte: 20 Header + 460 Daten, bei Fragmentierung kann Payload aber immer nur vielfaches von 8 sein, somit maximaler payload: 456

456 * 3 = 1368, also 3 Pakete mit einem payload von jeweils 456 Byte, mit MF = 1 gesetzt, Offset: 0, 57, 114 1480 - 1368 = 112 ein Paket mit einem payload von 112, MF = 0, Offset = 171

(4 Punkte: einer für Berücksichtigung der Header, einer für Vielfaches von 8, je einen halben pro Fragment.)

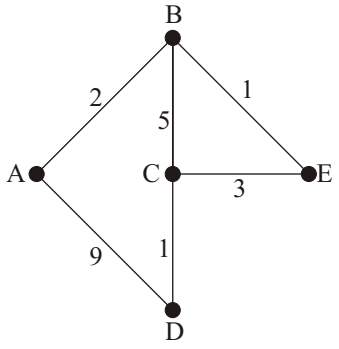
Empfänger erkennt dass Fragmentierung stattgefunden hat an MF > 0 oder MF = 0 und Offset > 0 **(1 Punkt)**

f) In einem Router werde ein Paket gelöscht, da seine Time-to-Live aubgelaufen ist. *Welches Protokoll* wird verwendet, um eine Rückmeldung über diesen Vorfall an den Sender zu geben?

ICMP

Lösung 5 (Routing) **(5+4+3) = 12 Punkte**

Gegeben sei das folgende Netzwerk, das die Router A bis E miteinander verbindet. Die Kanten sind mit der Entfernung der anliegenden Router beschriftet.



Die Betreiber der Router verwenden *Distance-Vector-Routing*. Die aktuellen Routing-Tabellen der Router sind der folgenden Tabelle (in komprimierter Form) zu entnehmen. Der Eintrag $(E, 4)$ in der Zeile B und der Spalte C bedeutet z.B., dass ein Paket mit dem Ziel C von B über E geroutet wird und dabei Kosten in Höhe von 4 anfallen.

	A	B	C	D	E
A	-	B,2	B,7	D,9	B,3
B	A,2	-	E,4	C,6	E,1
C	B,7	E,4	-	D,1	E,3
D	A,9	C,6	C,1	-	C,4
E	B,3	B,1	C,3	C,4	-

a) Alle Router seien synchronisiert und beginnen nun gleichzeitig, ihre Abstandsvektoren zu versenden. *Welche Abstandsvektoren werden in dieser Situation von den einzelnen Routern an welche anderen Router übermittelt*?

Von		An		Abstandsvektoren
A	$\rightarrow$	B,D	:	(B,2) (C,7) (D,9) (E,3)
B	$\rightarrow$	A,C,E	:	(A,2) (C,4) (D,6) (E,1)
C	$\rightarrow$	B,D,E	:	(A,7) (B,4) (D,1) (E,3)
D	$\rightarrow$	A,C	:	(A,9) (B,6) (C,1) (E,4)
E	$\rightarrow$	B,C	:	(A,3) (B,1) (C,3) (D,4)

Je 1 Punkt pro Zeile, d.h. grob 0.2 Punkte pro Abstandseintrag bzw. den Zielrechnern.

b) *Berechnen Sie für die Router C und D die nach Verarbeitung der empfangenen Abstandsvektoren resultierenden Routing-Tabellen.*

	A	B	C	D	E
C	**E,6**	**E,4**	**-**	**D,1**	**E,3**
D	**C,8**	**C,5**	**C,1**	**-**	**C,4**

Punkte: 2 pro Zeile, also ein halber pro Eintrag.

c) *Welches Problem kann bei Verwendung von Distance-Vector-Routing auftreten*? Erläutern Sie dieses beispielhaft anhand des obigen Netzwerks.

Bouncing Effect, wenn z.B. die Kante CD ausfällt: Die Routing-Tabellen schaukeln sich so lange gegenseitig hoch, bis der Pfad über A zu D kürzer wird. (Im Fall, dass ein Knoten ganz abgeschnitten wird, kann sogar Count-to-Infinity auftreten, kann hier alternativ genannt werden.)

Punkte: Nennen eines Problems 1 Punkt, Erläuterung 2 Punkte.

Lösung 6 (TCP) **(8+4+4+6) = 22 Punkte**

a) TCP arbeitet bidirektional. Welche TCP-Headerfelder werden für die *Rolle als Sender* in der Datenaustauschphase verwendet? *Geben Sie vier Felder an und begründen Sie, warum/wofür der Empfänger sie verwendet.*

Jede Menge:

- Destination-Port des Empfängers
- Sequenznummer als Kennzeichnung des 1. Bits
- Das Feld HL- berechnen und setzen
- Die Checksum wird benötigt – Über das Segment berechnen und einfügen
- PSH Flag - zur schnellen Zustellung
- (URG + Pointer)
- Ack No: Ankommende Quittungen zum verschieben des Sendefensters
- WIN - zur Bestimmung des gemeinsamen Fensters
- (Port des Senders: zum Zuordnen der Quittungen)

Nicht korrekt sind SYN- und FIN-Flag - diese betreffen Verbindungsauf- und -abbau, Sender- und Empfängerrolle gibt es nur beim Datenaustausch.

Je korrekter Nennung eines Felds 0.5 Punkte, 1.5 Punkte für die zugehörige Begründung

b) TCP implementiert das Sliding-Window-Verfahren zur Flusskontrolle. Normalerweise wird das Fenster während der Übertragung gleichmäßig verschoben. Erläutern Sie knapp, warum es aber auch zu *ruckartigen Verschiebungen* des Fensters kommen kann.

TCP quittiert jedes empfangene Segment (und zwar direkt). Daher sollte das Fenster sich eigentlich gleichmäßig verschieben. Allerdings können Quittungen verloren gehen – in diesem Fall bleibt das Fenster erst einmal stehen. Quittungen sind allerdings kumulativ: sobald ein Segment quittiert wird, sind dadurch auch alle vorherigen quittiert, somit kann sich das Fenster bei der ersten durchkommenden Quittung ruckhaft verschieben.

Oder auch: Verwendung von Selective Reject / Selective Repeat, bei denen direkt kumulative Quittungen gegeben werden können bzw. gezielt einzelne Segmente angefordert werden können, nach deren Neuübertragung eine kumulative Quittung kommen kann.
Oder halt durch die Einmischung der Congestion Control.

c) Gegeben sei ein Übertragungskanal mit einer Datenrate von 100 MBit/s und einer Round-Trip-Time von 10ms auf TCP-Ebene. *Berechnen Sie die Fenstergröße*, die notwendig ist, damit bei Verwendung von TCP die gesamte Datenrate ausgenutzt werden kann.

100 MBit pro Sekunde heißt, dass in 10 ms 1 MBit übertragen werden können muss. Also muss dies als Fenstergröße gewählt werden – in Byte, als eine Größe von 125000.

d) Beschreiben Sie knapp den *Slowstart-Mechanismus* bei TCP. *Warum* wird dieser Mechanismus *zusätzlich zum Sliding-Window-Verfahren verwendet*? Welchen Sinn hat die Einführung eines *Thresholds*?

Slowstart: übertrage zunächst nur ein Segment maximaler Größe. Falls vor einem Timeout eine Quittung ankommt, übertrage zwei weitere Segmente. Übertrage nun für jede ankommende Quittung zwei weitere Segmente, d.h. in jedem 'Schritt' Verdopplung der übertragenen Segmente und so exponentielle steigerung der Datenrate **(4 Punkte)**.

Wird zusätzlich verwendet, um eine Überlastung des Netzes zu vermeiden (Sliding-Window vermeidet nur Überlastung des Empfängers) **(1 Punkt)**.

Threshold: soll verhindern, dass man irgendwann zu große Steigerungen vornimmt und damit das Netz spontan überflutet (nur noch lineare Steigerung) **(1 Punkt)**.

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

a) Sie verwenden *RSA* als asymmetrisches Verschlüsselungsverfahren und haben $p = 5$ and $q = 3$ gegeben. *Ist* $< 7, 15 >$ *ein gültiger geheimer Schlüssel?* Begründen Sie Ihre Antwort.

Berechne zunächst $\phi(n)$ mit $n = p * q = 15$: $\phi(n) = (p-1) * (q-1) = 8$ (**1 Punkt**).

Wähle dann e relativ prim zu 8 und $d = 7$ as multiplikativ Inverses $mod\ 8$. D.h.: gibt es ein e mit $e * 7 mod 8 = 1$? Teste alle möglichen Werte für e (es sind sehr wenige): für $e = 7$ gibt es eine Lösung.

Dann kann man entweder sagen, dass der Schlüssel gültig ist, da es ein Inverses gibt, oder dass er nicht gültig ist, da es blödsinnig ist, den öffentlichen und den geheimen Schlüssel gleich zu wählen.

Vielleicht begründen die Leute auch mathematisch ganz anders.

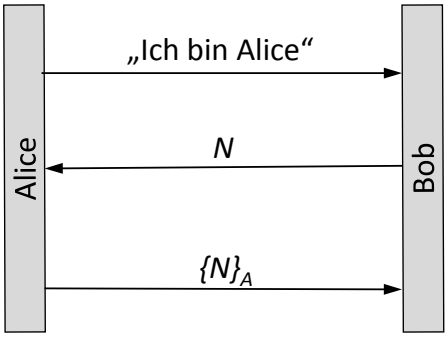
Begründung/Rechnung insgesamt 4 Punkte.

b) Bei Authentifizierungsverfahren wird üblicherweise eine Nonce benutzt. Einige Sicherheitsprotokoll-Implementierungen nutzen Zeitstempel als Nonces. *Was ist ein Nonce und warum sind Zeitstempel eine schlechte Wahl für eine Nonce*?

Nonce: ein nur einmal verwendeter Zufallswert **(1 Punkte)**.

Nonces sollen einen Nachrichtenaustauch, z.B. zur Authentifizierung, unvorhersehbar machen. Daher müssen sie zufällig sein. Zeitstempel sind nicht zufällig genug, daher können später verwendete Nonces bei einen einmal bekannten Nonce berechnet werden. (Diese fehlende Zufälligkeit wurde schon mißbraucht, um Sicherheitsprotokolle erfolgreich zu attackieren.) **(2 Punkte)**

c) $Alice$ (A) authentifiziert sich gegenüber Bob (B) mittels des folgenden Challenge-Response-Verfahrens:



Dabei ist N ein von Bob gewähltes Nonce und N_A bezeichne die Verschlüsselung von N mit dem privaten Schlüssel von $Alice$. *Welches Problem kann bei dieser Authentifizierung auftreten? Wie kann man es lösen?*

Problem: zuverlässiges Erlangen des öffentlichen Schlüssels von A. Man-in-the-Middle-Attacke möglich **(2 Punkte)**.

Lösung: KDC / CA/ Trusted 3rd party **(2 Punkte)**.