
Allgemeines

1. **(1p) Fragmentierung:** Internetschicht
2. **(1p) Carrier Sensing:** Netzzugangsschicht(Link-Layer)
3. **(1p) Fehlererkennung in den Nutzdaten (Payload):** Transportschicht, Netzzugangsschicht(Link.Layer)
4. **(1p) Namensauflösung:** Anwendungsschicht
5. **(1p) Ports:** Internetschicht
6. **(1p) Überlastkontrolle:** Transportschicht
Überlastkontrolle ist für gewöhnlich eine Aufgabe der Transportschicht. Es existieren aber auch Überlastkontrollmechanismen in Link-Layer-Protokollen, die nicht in der VL behandelt worden sind. Daher wirkt sich ein entsprechendes Häkchen unschädlich für die Bewertung aus.

Angenommen Sie möchten Ihren Laptop mit einem lokalen Netzwerk verbinden (z.B per Ethernet oder WLAN).

Das lokale Netz ist über einen handelsüblichen "DSL-Router" mit dem Internet verbunden.

Die Konfiguration der IP-Adressen haben sie vorab statisch vorgenommen.

IP Laptop: 192.168.178.69

IP Router: 192.168.178.1

7. **Frage:** (0,5) In einem lokalen Netzwerk werden zur Adressierung sog. MAC-Adressen verwendet. Damit ihr Laptop also ein Paket bzw. Rahmen (Frame) zum Router schicken kann muss er dessen MAC-Adresse kennen, bekannt ist aber nur die IP. Welches Protokoll löst dieses Problem (Abkürzung genügt)?

Antwort: ARP

8. **Frage:** (2P) Beschreiben Sie kurz wie das oben genannten Protokoll funktioniert. Wann muss ihr Laptop diesen Prozess wiederholen?

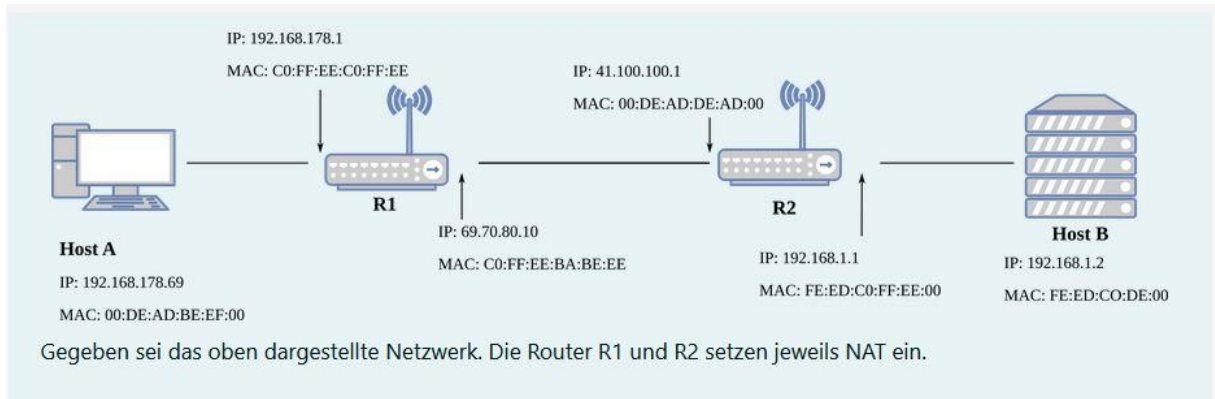
Antwort:

A sendet ARP-Anfrage als Broadcast (Adresse FF-FF-FF-FF-FF-FF) mit seiner physikalischen Adresse und der IP-Adresse von B 0.5P

B erkennt sich als Ziel an IP-Adresse in der ARP-Anfrage und sendet in ARP-Antwort seine physikalische Adresse an die physikalische Adresse von A 0.5P

A speichert die Zuordnung der Adressen von B in seiner ARP-Tabelle 0.5

Die Prozedur muss wiederholt werden sobald der TTL abläuft in der ARP-Tabelle. 0.5P



9. **Frage: (3P)** Angenommen Host A möchte eine unverschlüsselte HTTP-Verbindung zu einem Webserver auf Host B aufbauen.
Welche Adresdaten schreibt er dafür in das zu sendende Paket? Ergänzen Sie!

	Source	Destination
Ethernet	00:DE:AD:BE:EF:00	C0:FF:EE:C0:FF:EE
IP	192.168.178.69	41.100.100.1
TCP(Port)	Zufällig	80

10. **Frage: (1P)** Welche zusätzliche Konfiguration muss in R2 vorgenommen werden, damit der Webserver auf Host B überhaupt erreichbar ist?

Antwort: NAT verhindert eine Verbindungsaufnahme von außen, daher muss ein statischer Eintrag in der NAT Tabelle eingetragen werden für Port 80 auf die IP von Host B.

Es muss klar sein, was genau passiert, nur "Port-Forwarding" etc. zu ungenau. Es muss direkt oder indirekt klar sein, welcher Port betroffen ist. NAT-Tabelle sollte erwähnt oder zumindest impliziert werden

PEER to PEER

11. **Frage: (4P)** Ordnen Sie den verschiedenen Aspekten die Architektur zu, auf die diese Stärken im Allgemeinen eher zutreffen.

Antwort:

Geringere Komplexität des Gesamtsystems → Client-Server

Direktere Skalierbarkeit → Peer-to-Peer

Effizientere Auslastung der vorhandenen Ressourcen → Peer-to-Peer

Simplere Organisation → Client-Server

12. **Frage: (3P)** Welche der folgenden Aussagen über P2P Netzwerke sind wahr oder falsch?

Antwort:

WAHR	Nicht kooperative Peers sind ein fundamentales Problem für das Design von P2P Netzwerken und müssen beim Design besonders bedacht werden.
WAHR	Alle Teilnehmer eines P2P Netzwerks können die selbe Funktionalität bereitstellen.
Falsch	Wenn zu viele Teilnehmer einem P2P Netzwerk beitreten kann dieses schnell überlastet sein.

WAHR	Die gesamte verfügbare Kapazität des P2P Netzwerks kann theoretisch produktiv verwendet werden.
Falsch	P2P Netzwerke weisen keinerlei Struktur auf, da alle Peers miteinander kommunizieren können.
Falsch	Inhalte und Peers werden in P2P Netzwerken in der Regel durch menschenlesbaren Namen adressiert

13. Frage: (3P) In der Vorlesung wurden mehrere P2P Netzwerke vorgestellt, die verschiedene Mechanismen implementieren um Inhalte zu suchen

- Napster: zentrales Verzeichnis
- Gnutella: query flooding
- KaZaA: strukturiertes Overlay

Die Ansätze bringen haben jeweilige Stärken und Schwächen. Ordnen Sie den Ansätzen den Aspekt zu, in dem diese am Besten funktionieren.

Antwort:

- Gnutella (query flooding) → Dezentralisierung,
- KaZaA (strukturiertes Overlay) → Skalierbarkeit,
- Napster (zentrales Verzeichnis) → Konsistenz

Chord

Nehmen Sie ein Chord Netzwerk an, das 8 Bit Adressen verwendet und aus den folgenden Knoten besteht:

74, 110, 124, 136, 164, 179, 199, 254

Hinweis: Zur Bearbeitung der folgenden Aufgaben kann es sinnvoll sein, dieses Netzwerk als Ring zu visualisieren

14. Frage: (1P) Welcher Knoten ist für das Datum 36 verantwortlich?

Antwort: 74

15. Frage: (2P) Stellen Sie die Fingertable für Knoten 110 auf:

Antwort:

1	124
2	124
3	124
4	124
5	136
6	164
7	179
8	254

16. Frage: (1P) Wieviele Nachrichten spart die Verwendung von Fingertables, wenn Node 110 den für das Datum 36 verantwortlichen Knoten herausfinden möchte?

Antwort: 5

17. Frage: (6P)

Antwort: Knoten 93 möchte der DHT beitreten. Er sendet eine `join` Nachricht mit seiner ID an einen bekannten Knoten der DHT. Diese Nachricht wird in der DHT von Knoten an ihre Nachfolger

weitergeleitet, bis zu Knoten **110**. Dieser updatet seinen Vorgänger auf **93** und sendet Knoten 93 eine **notify** Nachricht, woraufhin dieser Knoten **110** als seinen Nachfolger einträgt.

Knoten **74** sendet **stabilize** eine Nachricht an seinen Nachfolger **110** und erhält als Antwort eine **notify** Nachricht mit einem von ihm abweichenden Vorgänger (**93**), woraufhin er seinen Nachfolger aktualisiert.

Knoten **74** sendet eine **stabilize** Nachricht an seinen Nachfolger **93**, woraufhin dieser seinen Vorgänger auf **74** setzt.

DNS – Domain Name Service

18. Frage: (3P) Geben Sie für jede der folgenden Aussagen über DNS an, ob die Aussage wahr oder falsch ist.

Antwort:

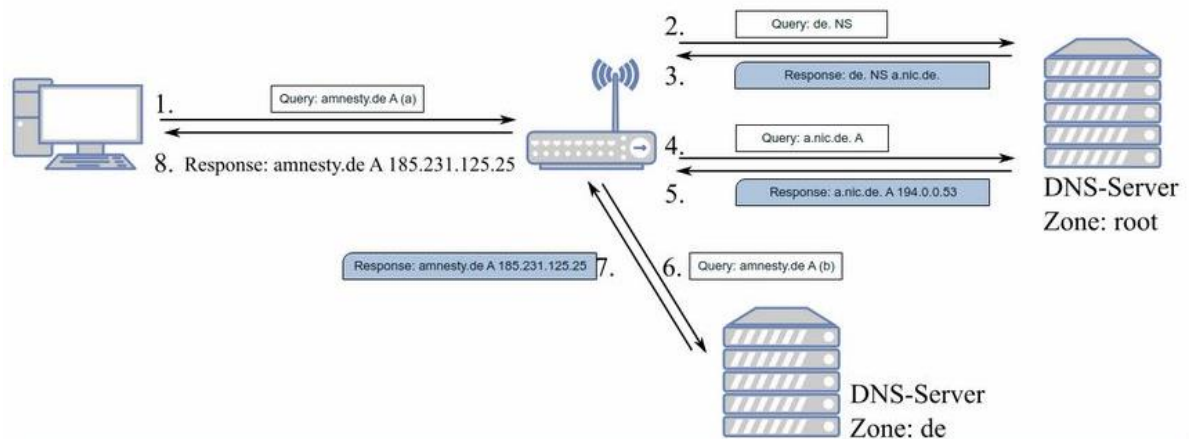
Wahr	Der DNS-Namensraum ist hierarchisch aufgebaut
Wahr	Autoritative DNS-Name-Server bilden die unterste Ebene der DNS-Hierarchie.
Falsch	Ein DNS-Resource-Record vom Typ NS beinhaltet die IP-Adresse zu einem Domainnamen.
Wahr	Der Vorteil iterativer Namensauflösung besteht darin, dass der angefragte Name-Server keine Informationen zwischenspeichern muss.
Falsch	Die Root-Name-Server bilden die unterste Ebene der DNS-Hierarchie.
Falsch	DNS ist eine zentrale Datenbank zur Auflösung von Namen in IP-Adressen.

19. Frage: (7P) Die folgende Abbildung zeigt einen PC, einen Router und zwei DNS-Server. Der Nutzer am PC möchte die Website <https://amnesty.de> aufrufen. Die Abbildung soll so vervollständigt werden, dass die korrekte Auflösung des Domain-Namens in eine IP-Adresse über das Domain Name Service Protokoll gezeigt wird.

Wählen Sie dazu die richtigen DNS-Anfragen (Query) und -Antworten (Response) aus und schieben Sie sie auf die entsprechenden Felder.

Hinweis: Es gibt eine Anfrage, die zwei mal vorkommt. Achten Sie auf die richtige Reihenfolge (erst (a), dann (b)).

Antwort:



Zeitsynchronisation

- 20. Frage: (2P)** Sie befinden sich in Berlin und auf ihrem PC läuft kontinuierlich ein Prozess zur Zeitsynchronisation mittels des NTP-Protokolls. Sie haben vier verschiedene Server konfiguriert mit denen Ihr PC sich synchronisieren kann. Mit diesen Servern wird kontinuierlich Delay und Offset gemessen. Im folgenden sind die Eigenschaften der Server so wie die Delay-Messungen aufgelistet:

ntp.example.org:										
Messung Nr.	1	2	3	4	5	6	7	8	9	10
Delay [ms]	10	20	10	11	8	10	11	10	12	10
Standort: Berlin Stratum: 3 Primäre Zeitquelle: GPS-Empfänger										
what.timeis.it:										
Messung Nr.	1	2	3	4	5	6	7	8	9	10
Delay [ms]	26	27	25	30	26	31	32	27	30	29
Standort: Frankfurt Stratum: 3 Primäre Zeitquelle: GPS-Empfänger										
clock.djxmx.net:										
Messung Nr.	1	2	3	4	5	6	7	8	9	10
Delay [ms]	40	32	28	29	28	30	29	28	30	29
Standort: Frankfurt Stratum: 3 Primäre Zeitquelle: Funkuhr										
ticktock.edu:										
Messung Nr.	1	2	3	4	5	6	7	8	9	10
Delay [ms]	100	85	91	97	75	78	88	90	102	87
Standort: Berkeley, Kalifornien Stratum: 2 Primäre Zeitquelle: Atomuhr										

Antwort:

Clock.djxmx.net

Die niedrigste Varianz im Delay

- 21. Frage: (3P)** Bewerten Sie folgende Aussagen im Kontext der Zeitsynchronisation in verteilten Systemen.

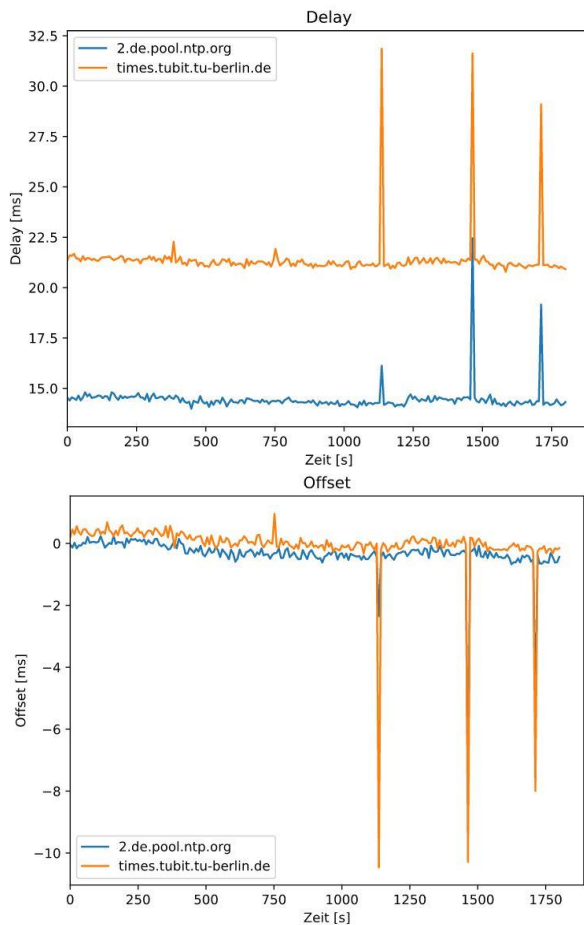
Antwort:

Falsch	Eine Uhr darf durch eine Zeitsynchronisation auf keinen Fall vorgestellt werden, da sonst die Kausalität von Ereignissen nicht mehr eindeutig ist.
Falsch	Im NTP-Protokoll wird der Round-Trip-Delay gemessen, daher hat die Verzögerung auf dem Hinweg bzw. auf Rückweg keinen Einfluss auf die Genauigkeit der Offsetberechnung. Nur die Gesamtverzögerung zählt.
Wahr	Eine exakte Zeitsynchronisation ist in einem verteilten System nicht möglich.
Wahr	Wenn zwei Ereignisse auf zwei verschiedenen Servern laut lokalem Zeitstempel sehr kurz nacheinander (< 1s) auftreten lässt sich nicht mit Sicherheit sagen welches Ereignis zu erst eingetreten ist, auch wenn beide Server sich mit dem selben Zeitserver synchronisieren.
Falsch	Ein niedrigeres Stratum eines NTP-Servers bedeutet, dass er über eine genauere Zeitquelle verfügt (bspw. eine Atomuhr anstatt eines Funkuhrempfängers).

Wahr

Der Berkeley-Algorithmus ist geeignet für Zeitsynchronisation in geschlossenen Netzwerken.

22. Frage: (3P)



Die oben dargestellten Plots sind das Ergebnis einer kontinuierlichen Delay- und Offsetmessung eines NTP-Clients zeitgleich mit zwei verschiedenen NTP-Servern. Auffällig dabei sind die starken Spitzen in den Messergebnissen, die beide Server gleichermaßen betreffen. Beantworten Sie im Freitext die folgenden Fragen:

- Was ist die wahrscheinlichste Ursache für die zeitgleich in beiden Kurven auftretenden Spitzen im Delay?
- Warum reagiert die Offsetschätzung so stark auf die Abweichungen im Delay?
- War die Verzögerung zu den Spitzen eher auf dem Hinweg der Messung stärker, bei der Antwort des Servers oder war sie gleichmäßig in beiden Richtungen? Begründen Sie!

Antwort:

1.) Stau im Netzwerk (1P)

2.) Die Offsetschätzung bei NTP geht von einer symmetrischen Verzögerung auf dem Hin- und Rückweg der Zeitmessung aus. Durch den Stau ist das nicht mehr gegeben und die Schätzung weicht stark von den vorherigen Werten ab. (1P)

3.) Wäre die Verzögerung weiterhin symmetrisch bliebe die Offsetschätzung konstant.

Bei starker Verzögerung auf dem Rückweg unterschätzt man die Verzögerung des Antwortpaketes dadurch wird der Offset negativer. Dies ist hier im Plot gut zu beobachten, daher war die Verzögerung auf dem Rückweg vermutlich größer. (1P)

23. Frage: (2P) Bewerten Sie folgende Aussagen im Kontext von Logischen Uhren:

Antwort:

Falsch	Lamport-Uhren können in der Praxis nicht genutzt werden, da man mit ihnen keine Kausalität bestimmen kann.
Falsch	Um in einem verteilten System eine konsistente Sicht auf die Reihenfolge aller Ereignisse zu garantieren, genügt es die eigene Uhr jedes Knotens mittels NTP oder ähnlichen Verfahren zu synchronisieren wenn diese genau genug sind. Logische Uhren und klassische Zeitsynchronisation sind also austauschbar.
Wahr	Die totale Ordnung von Ereignissen mit einer Lamport-Uhr entspricht nicht der physikalischen Reihenfolge der Ereignisse.
Falsch	Hat das Ereignis x von Prozess A einen höheren Wert auf der Lamport-Uhr als das Ereignis y von Prozess B, so kann man sagen y hat vor x stattgefunden.

Transportschicht

24. Frage: (3P) Bewerten Sie folgenden Aussagen als richtig oder falsch.

Antwort:

Wahr	Stop-and-Wait ist optimal in einem 100MBit/s-WLAN
Falsch	Selective-Repeat ist am besten bei kleinem Bandbreiten-Verzögerungsprodukt
Falsch	Timeout bei Stop-and-Wait ist kleiner als bei Schiebefensterprotokollen
Falsch	Selective-Repeat benötigt einen Timer am Empfänger
Wahr	Selective-Repeat erfordert Puffer beim Sender
Wahr	G-back-N erfordert keinen Puffer beim Empfänger

25. Frage: (1P) Berechnen Sie das **Bandbreiten-Verzögerungsprodukt** für folgende Parameter:

$$c = 300000000 \text{ m/s} = 3 \times 10^8 \text{ m/s}$$

$$l = 9000000 \text{ m} = 9000 \text{ km}$$

$$R = 1000000000 \text{ bit/s} = 1 \text{ Gbit/s}$$

$$\text{MTU} = 12000 \text{ byte} = 12000 \text{ bit}$$

Vergessen Sie nicht, die **Einheit** beim Ergebnis anzugeben!

Antwort: 300000000,0 bit

26. Frage: (3P) Wie groß muss der Sequenznummernraum **mindestens** sein, um Mehrdeutigkeit zu vermeiden. Wir gehen von einer Fenstergröße $W=10$ aus.

Antwort:

Stop and Wait	1
G back N	11
Selectiv Repeat	20

27. Frage: (1P) Welche der Aussagen sind korrekt?

Antwort:

- a) TCP ist ineffizient für kurzlebige Verbindungen
- b) UDP ist komplett abstrahiert vom genutzten Protokoll der Netzwerkschicht
- c) UDP kann Überlast verursachen
- d) TCP-Sequenznummern beginnen bei 1 statt bei 0

Die richtigen Antworten sind:

UDP kann Überlast verursachen
TCP ist ineffizient für kurzlebige Verbindungen

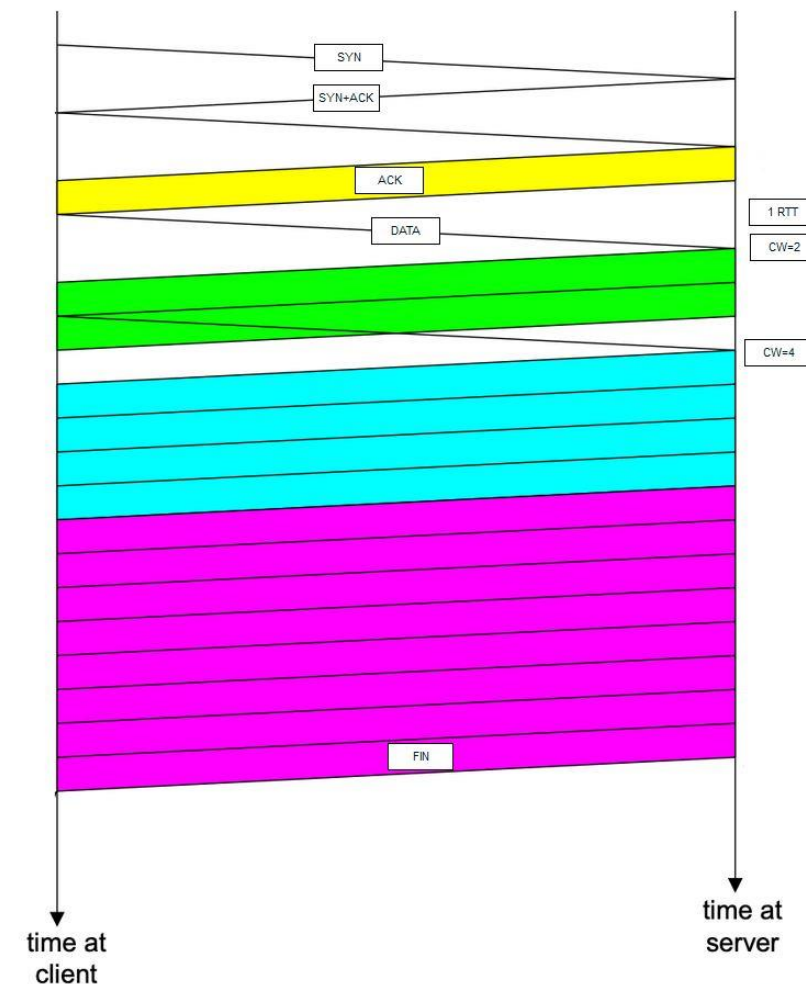
28. Frage: (3P) Erläutern Sie die Funktionsweise der Flusskontrolle in TCP.

Antwort:

- Puffer beim Empfänger: IP fügt neue empfangene Daten ein, Anwendung liest Daten aus, der jeweils freie Pufferplatz wird der Senderseite mitgeteilt(1)
- Puffer beim Sender: Anwendung schreibt neue Daten, IP entfernt soviel Daten, wie es der Puffer der Empfangsseite zulässt(1)
- Anwendung auf Sendeseite blockiert, wenn der Puffer voll ist, dadurch reguliert die Empfängeranwendung die Senderanwendung(1)

29. Frage: (2P) Ordnen Sie im folgenden Diagramm die wichtigsten Elemente des TCP-Ablaufs zu.

Antwort: ACHTUNG: ACK und DATA müssen vertauscht werden!



30. Frage: (P) Berechnen Sie die Zeit zum Kopieren eines Objektes vom Client zum Server mit TCP (inkl. Verbindungsauf- und abbau, keine explizite Anfrage benötigt, keine Paketverluste).

[S: MSS in Byte, O: Objektgröße in Byte, R: Bitrate, OWD: one-way delay]

O = 10000 Byte

S = 500 Byte

R = 1MBit/s

OWD = 1s

Begründen Sie den Rechenweg.

Antwort:

Aufbau 1 RTT (1)

Objekt: Slow Start (1) erkannt,

MSS (1) <-- richtige Fenstergröße

1. Fenster W=1, 1xRTT

2. Fenster W=2, 1xRTT

3. Fenster W=4, 1xRTT

4. Fenster W=8, 1xRTT

5. Fenster W=5, 1xRTT

Abbau 1.5 RTT (1)

Summe 7.5 RTT = 15s (1)

31. Frage: (2P) Welche Aussagen zu TCP im modernen Internet sind korrekt?

Antwort:

a) Die RTT steigt über die Jahre stetig an

b) Selective Acknowledgements helfen TCP über Weitverkehrsnetze

c) Der drahtlose letzte Hop hat einen grossen Einfluss

d) 5G macht TCP überflüssig

Die richtigen Antworten sind:

Der drahtlose letzte Hop hat einen grossen Einfluss,

Selective Acknowledgements helfen TCP über Weitverkehrsnetze

Socket

32. Frage(2P) In welcher Reihenfolge müssen die folgenden Socket-Funktionen ausgeführt werden, um einen Server-Socket einzurichten, der eine eingehende Verbindung annehmen kann?

Antwort:

1) socket

2) bind

3) listen

4) accept

33. Frage: (2P) Markieren Sie **alle** Socket-Funktionen die (sofern keine andere Konfiguration vorgenommen wurde) blockieren, d.h., die Ausführung des Programms unterbrechen bis ein von außen veranlasstes Ereignis eintritt.

Antwort:

Falsch	Close
Wahr	recv
Wahr	connect
Falsch	socket
Falsch	bind
Falsch	listen
Wahr	accept
Wahr	send

34. Frage: (1P) Welche der folgenden Aussagen über Portnummern ist richtig?

Antwort: a

- a) Portnummern unterschiedlicher Transportprotokolle (z.B. TCP, UDP) sind voneinander unabhängig.
- b) Eine Portnummer darf je Adresse nur von einem Transportprotokoll (z.B. TCP, UDP) belegt werden.

35. Frage: (5P) Gegeben sei die folgende Funktion:

```
void read_four_ints(int sock) {
    char buf[16];
    uint32_t firstInt, secondInt, thirdInt, fourthInt;
    recv(sock, &buf, 16, 0);
    memcpy(&firstInt, &buf, 4);
    memcpy(&secondInt, &(buf[4]), 4);
    memcpy(&thirdInt, &(buf[8]), 4);
    memcpy(&fourthInt, &(buf[12]), 4);
    printf("Read integers: %u %u %u %u", firstInt, secondInt, thirdInt,
    fourthInt);
}
```

Es gelten die folgenden Annahmen:

Der Code kompiliert korrekt.

Die Funktion `read_four_ints` wird mit einem gültigen Socket-Identifizier als Argument `sock` aufgerufen.

Das Socket `sock` ist korrekt mit einem beliebigen anderen Host verbunden und bleibt dies für die Dauer des Aufrufes von `read_four_ints`.

Das Socket `sock` ist korrekt als ein STREAM Socket konfiguriert.

Auf den verbundenen Socket auf dem anderen Host ist eine gültige Nachricht mit 4 *unsigned long* Zahlen geschrieben worden.

Der Datentyp `unsigned long` ist auf allen beteiligten Rechnern exakt 4 Bytes lang.

Dennoch enthält der Code zwei subtile Fehler.

Benennen Sie die zwei Fehler in diesem Code und skizzieren Sie kurz (Stichworte genügen!) wie diese Fehler behoben werden können.

Antwort:

Fehler im Code:

1. Verlass auf vollständig empfangene Nachricht (16 bytes).

Der Rückgabewert von `recv` wird nicht berücksichtigt.

Lösungsansatz: Schleife mit wiederholtem Aufruf von `recv` bis alle 16 Bytes empfangen sind.

Punkte: (1) für Problembeschreibung; (1) für Berücksichtigung von Rückgabewert von `recv`: (1) für Verwendung einer Lese-Schleife

2. Verlass auf gleiche Byte Order der Hosts bzw. fehlende Konvertierung aus Network Byte Order.

Lösungsansatz: Alle Ints mit `ntohl` konvertieren.

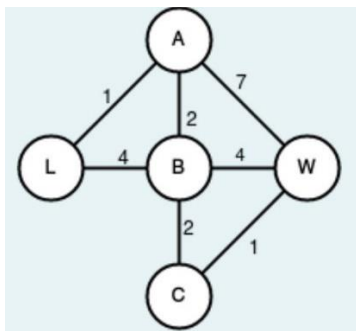
Routing & Switching

36. Frage: (3P) Beurteilen Sie die folgenden Aussagen über **Switching**.

Antwort:

Wahr	Switching agiert auf Layer 2 des OSI Modells
Falsch	Die Forwarding Tabelle ist statisch und muss manuell bearbeitet werden
Falsch	Mehrere Hosts können durch einen einzelnen Eintrag in der Forwarding Tabelle gruppiert werden
Wahr	Pakete können nicht immer direkt weitergeleitet werden, auch wenn der Ausgangsport frei ist
Falsch	Switching verwendet IP Adressen
Wahr	Switching verbindet mehrere Hosts miteinander

37. Frage: (12P) Die folgende Abbildung zeigt ein Netzwerk mit fünf Knoten.



Führen Sie aus Sicht von Knoten **L** das Dijkstra-Verfahren für die Minimierung des Graphen durch. Füllen Sie für die Distanz **D** und Vorgänger **p** die folgende Tabelle aus. Achten Sie darauf, alle Zellen auszufüllen.

Hinweise:

Nutzen Sie 'inf' für die unendliche Distanz und '-' (einfacher Strich/Minus) für einen leeren Eintrag, schreiben Sie Namen der Knoten in Großbuchstaben. Sortieren Sie die Einträge innerhalb von N' aufsteigend nach dem Alphabet und achten Sie darauf, dass Knoten **L** bereits eingetragen ist. Verwenden Sie außerdem folgende Notation:

N': Trennung durch Komma (',') und kein Leerzeichen. Beispiel: X,Y,Z

D(*),p(*): Trennung durch Komma (',') und kein Leerzeichen (siehe Tabellenkopf). Beispiele: 8,X oder inf,-

Antwort:

L	N	D(A),p(A)	D(B),p(B)	D(C),p(C)	D(W),p(W)
	L	1,L	4,L	inf,-	inf,-
	L,A	1,L	3,A	inf,-	inf,-
	L,A,B,	1,L	3,A	5,B	7,B
	L,A,B,C,	1,L	3,A	5,B	6,C
	L,A,B,C,W	1,L	3,A	5,B	6,C

Verfolgen Sie in folgender Tabelle den Ablauf des Forward-Search-Algorithmus für den Knoten **W**. Achten Sie darauf, alle Zellen auszufüllen.

Hinweise:

Nutzen Sie 'inf' für die unendliche Distanz und '-' (einfacher Strich/Minus) für einen leeren Eintrag/Wert, schreiben Sie Namen der Knoten in Großbuchstaben. Sortieren Sie die Einträge innerhalb der Zellen aufsteigend nach der Distanz (siehe Beispiel unten). Verwenden Sie außerdem folgende Notation:

Liste: Umklammerung eines Eintrags, Trennung durch Komma (',') und kein Leerzeichen. Beispiele: (T,2,-),(Y,5,U),(X,8,Z) oder –

W	Bestätigte Liste	Vorläufige Liste
	(W,0,-)	(C,1C),(B,4,B),(A,7,A)
	(W,0,-),(C,1,C)	(B,3,C),(A,7,A)
	(W,0,-),(C,1C),(B,3,C)	(A,5,C),(L,7,C)
	(W,0,-),(C,1C),(B,3,C),(A,5,C)	(L,6,C)
	(W,0,-),(C,1C),(B,3,C),(A,5,C),(L,6,C)	-

38. Frage: (1P) Welches der folgenden Verfahren eignet sich nicht für Intra-Domain-Routing?

Antwort: g

- a) Link-State-Routing
- b) Forward-Search-Algorithmus
- c) Bellman-Ford-Verfahren
- d) Open Shortest Path First
- e) Dijkstra-Verfahren
- f) Distanzvektor-Routing
- g) Border Gateway Protocol**

IP

39. Frage: (1P) Welche für einen Host erlaubte IP befindet sich im Netz 192.168.1.0 mit der Netzmaske 255.255.255.0?

Antwort: b

- a) 192.168.1.255
- b) 192.168.1.5**
- c) keine der oben genannten
- d) 192.168.2.5

40. Frage: (1P) Welche Aussage über CIDR (Classless Inter-Domain Routing) ist richtig?

Antwort: d

- a) CIDR ermöglicht verschiedenen Nutzern innerhalb eines lokalen Netzes den Zugang zum Internet.
- b) CIDR erhöht die Anzahl der bits pro IP-Adresse auf 128, so dass mehr Adressen zur Verfügung stehen
- c) CIDR verteilt innerhalb eines lokalen Netzes automatisch IP-Adressen.
- d) CIDR ermöglicht Netzwerke-Teile von IP-Adressen mit beliebig vielen Bits, so dass die festen Klassen A, B und C nicht mehr nötig sind.**

41. Frage: (2P) Bei IP ist die Adressefür den Loopback reserviert und die Adresse.....für den Broadcast.

Antwort: Bei IP ist die Adresse 127.0.0.1 für den Loopback reserviert und die Adresse 255.255.255.255 für den Broadcast.