KN – Klausurfragen

1. Hamming Distance erklären. Welche Eigenschaften hat ein Code mit d=2, d=3?

Die Anzahl der Bitpositionen, in denen sich zwei Codewörter unterscheiden.

$d = F_E + 1$ ➔ F_E Fehler erkennbar

$d = 2F_K + 1$ ➔ F_K Fehler korrigierbar

d=2 ➔ 1 Fehler erkennbar, kein Fehler korrigierbar
d=3 ➔ 2 Fehler erkennbar, 1 Fehler korrigierbar

2. Hamming Distance bei einem Codewort mit 4 Bit und 1 Bit Parität?

00001
00010 → Es unterscheiden sich zwei Bits, deshalb ist die Hamming Distance = 2

3. Wie groß muss der minimale Hammingabstand bei einem Codewort sein, mit dem x Fehler erkennen und y Fehler korrigieren möchte?

$d_{min} = x + 1$ um x Fehler zu erkennen
$d_{min} = 2y + 1$ um y Fehler zu korrigieren

4. Eigenschaften von FEC?

Forward Error Correction
+ Keine Verzögerung, da Fehler beim Empfänger korrigiert werden (kein ACK)
+ Leitungen werden dadurch weniger belastet
+ Kein Speicher beim Sender notwendig
- Hoher Overhead
- Komplex
Einsatz: Highspeed Netze und Satellit

5. Eigenschaften ARQ?

Automatic Repeat reQuest
+ kleiner Overhead
+ einfach
- zusätzliche Verzögerung durch Bestätigungen

6. Nennen Sie vier verschiedene Fehlerarten und Methoden, um diese zu erkennen?

Fehlerhafte Pakete	→	Prüfsumme, ACK, FEC, CRC
Verlorene Pakete	→	Timer, Sequenznummer
Falsche Reihenfolge	→	Sequenznummer
Duplizierte Pakete	→	Sequenznummer

7. Mit welchen Fehlerarten muss die Transportschicht umgehen können?

Fehlerhafte, Verlorene, Falsche, Duplizierte Pakete

8. Nennen Sie drei ARQ Protokolle?

Send and Wait
Go back N
Selective Repeat

9. Wozu wird explizit Flusskontrolle bei ARQ benutzt?

Um zu verhindern, dass der Empfänger nicht mit Paketen überschüttet wird, falls er Pakete nicht bearbeiten kann.

10. Arbeitet ARQ nur mit positiven ACKs und Timern zufrieden stellend. Wenn ja, wozu gibt es NACKs.

Timer und NACKs veranlassen den Sender erneut zu senden, falls Pakete fehlerhaft sind. Anstatt den Timer abzuwarten, wäre es besser, wenn der Empfänger einen NACK sendet. Somit kann die Effizienz der Übertragung erhöht werden.

11. Welches ARQ Verfahren ist am effizientesten?

Selective Repeat: Es werden nur fehlerhafte Pakete wiederholt.

12. Wie muss das Generatorpolynom aussehen, um ungerade Anzahl von Fehlern zu erkennen?

x + 1

13. Zugriff bei ALOHA (Wie)?

Der Kanal wird nicht abgehört, um zu erkennen, ob der Kanal belegt ist. Jeder Sender darf senden, wann er will. Jedoch ist eine feste Rahmengröße vorgeschrieben. Falls es zu einer Kollision kommt, wartet jeder Sender eine zufällig gewählte Zeit, und sendet dann erneut. Kollisionen werden hier durch

Bestätigungen des Empfängers erkannt. Nach jeder Übertragung eines Rahmens wird der Kanal auf eine Bestätigung abgehört.

14. Mit Hilfe welcher Mechanismen erkennt ein Sender bzw. Empfänger bei Verwendung eines ARQ Protokolls Fehler?

Timer, Sequenznummer

15. Ein Sender arbeitet mit Go back N, ein Empfänger mit Selective Repeat. Funktioniert die Kommunikation zwischen den beiden? Wenn nicht wie müssten die Rechner (oder einer der Rechner) konfiguriert werden, damit es funktioniert. Wie ist es umgekehrt.

Sender: Go back N → Empfänger: Selective Repat
Es entstehen Duplikate beim Empfänger.
Lösung: Kein Speicher für ankommende Pakete, es wird immer ein Paket verarbeitet.

Sender: Selective Repeat → Empfänger: Go back N
Paket Verlust.
Lösung: es funktioniert nicht.

16. Welches Protokoll ist bei Langstrecken am besten?

ALOHA (slotted)

17. Reicht die Voraussetzung, dass Quittungen immer fehlerfrei übertragen werden, damit Send and Wait korrekt funktioniert (Begründung)?

Nein (Bei längeren Verzögerungen). Wenn der Timer abläuft können Duplikate entstehen, die der Empfänger als solche nicht erkennt.

18. Ist CSMA immer effizienter als ALOHA (Begründung)?

CSMA ist viel besser als Aloha, da Stationen genug Anstand besitzen, von einer Unterbrechung der Übertragung anderer Stationen absehen. Jedoch kann die Überprüfung des Mediums bei langen Strecken Fehler hervorrufen.

19. Warum sollte bei Go back N das Fenster immer mindestens zweimal so groß wie die Leitungskapazität sein?

Damit eine kontinuierliche Übertragung gewährleistet ist, sonst ist der Sender unnötig blockiert.

20. Unter welchen Umständen kann bei einem Sliding-Window-Protokoll auf den Einsatz Retransmission Timern beim Sender verzichtet werden?

- Wenn angenommen wird, dass alle Pakete korrekt beim Empfänger ankommen.
- Wenn der Sendefenster unendlich groß ist.

21. Wozu ist bei Sliding-Window-Protokollen ein Verbindungsaufbau nötig?

Festlegung von Parametern, wie Fenstergröße, Sequenznummer, ...

22. Was verstehen Sie unter dem „Open Loop Approach" zur Fehlerkontrolle? Nennen Sie eine Methode zu Realisierung. Ist Selective Repeat ein solches Verfahren (Begründung).

Fehlerhafte Codewörter werden beim Empfänger korrigiert. Es erfolgt kein ACK an den Sender.

Methode: Hamming Distance

Selective Repeat ist nicht so ein Verfahren. Es ist ein ARQ Verfahren.

23. Nennen Sie Probleme, die bei einem großen Bandwith-Delay-Product bei Go Back N auftreten können.

Bandbreite Verzögerung → langer oder defekter Kanal
→ daher muss der Puffer vom Sender groß sein, um den falschen noch einmal zu senden.

24. Worin unterscheiden sich die Protokolle Alternating-Bit und Send and Wait? Welches Problem wird dadurch gelöst?

Alternating-Bit besitzt eine Sequenznummer. Hierdurch wird die Unterscheidung von neuen und duplizierten Paketen ermöglicht.

25. Open / Closed Loop Ansatz darstellen –erklären (Permits/ACK-Entkopplung).
Welcher Ansatz ist besser für sehr lange Hochgeschwindigkeitsleitungen geeignet.

OL → Fehlerhafte Pakete werden erkannt und korrigiert.
CL → Fehlerhafte Pakete können nur erkannt werden und deshalb werden diese veranlasst nochmals vom Sender zu übertragen.

Permits sind quasi ein Erlaubnis zum weitersenden.

Permits/ACK-Entkopplung: Permits können auch mit ACKs mitverschickt werden. Bei einer Überflutung werden Permits von der ACKs entkoppelt und alleine abgeschickt.

Open Loop ist für sehr lange Hochgeschwindigkeitsleitungen gut geeignet.

26. Selective Repeat / Go back N erläutern.

Selective Repeat:
Es wird nur das fehlende oder fehlerhafte Paket erneut gesendet. Alle nachfolgenden, bereits gesendeten werden beim Empfänger zwischengespeichert.

Go back N:
Ab dem fehlenden oder fehlerhaften Paket werden nochmals alle Pakete gesendet. Nach einem fehlerhaft empfangenen werden alle Pakete verworfen und nicht zwischengespeichert.

27. Warum sollte im Transport Layer nicht immer mit Sequenznummer 0 begonnen werden?

Um nach einem Systemabsturz zu verhindern, das mehrere Rechner mit der gleichen Sequenznummer anfangen.

28. Warum ist es sinnvoll, Permits so früh wie möglich und nicht erst nach Erhalt eines kompletten Fensters zu senden?

Weil die Permits und damit auch die ACKs lange verzögert werden. Wenn die ACKs zu lange verzögert werden, dann kann der Timer beim Sender zuschlagen und damit unnötige erneute Übertragungen einleiten. Also um eine bessere Auslastung zu erzielen.

29. Beschreiben Sie die Funktionsweise des Sliding-Window-Protokolls.

Beim SWP wird dem Sender eine Erlaubnis erteilt, bestimmte Anzahl von Rahmen zu senden. Bevor ein weiteres Permit ankommt, dar der Sender keine weiteren Daten verschicken. Der Empfänger kann durch das Zurückhalten von Permits den Datenfluss regulieren.

30. Was ist der Unterschied zwischen Congestion Control und Flow Control?

Das eine ist für Vorbeugung (Flow Control) und das andere direkte Maßnahme.
Das eine findet zwischen Empfänger und Sender statt (Flow Control) und das andere innerhalb des Netzes.

31. Beschreiben Sie die Funktionsweise des Leaky-Bucket.

Die unregelmäßig kommenden Daten werden in einem Puffer aufgefangen und gleichmäßig weitergeleitet. Wenn der Puffer voll ist, werden die ankommenden Daten verworfen.

32. Wofür braucht man Congestion Control bzw. welches kommunikationstechnisches Problem soll es lösen.

Um die Datenübertragung im Netz zu regulieren. Staus im Netz zu verhindern.

33. Erläutern Sie den Protokollmechanismus der Flusskontrolle.

Wenn der Sender schneller ist als der Empfänger, dann kann der Empfänger nicht alle Pakete bearbeiten und sie gehen verloren. Deshalb teilt der Empfänger dem Sender mit, wann und wie viel er zu senden hat, um alle Pakete sicher zu bearbeiten.

34. Wozu werden eindeutige Sequenznummern bei Verbindungsaufbau auf der Transportebene benutzt? Wie kann man diese erhalten?

Um Pakete von alten Verbindungen auszuschließen. Diese werden mit 3 Way Handshake erhalten.

35. Warum ist es besser absolute Permits zu benutzen anstatt relative?

Bei relativen Permits kann es durch Überlastung des Puffers zu Paketverlust kommen. Aber bei absoluten Permits halt nicht. Erst wenn der User ein Paket aus dem Puffer nimmt, wird ein Permit geschickt.

36. Erläutern Sie „isarithmic flow control“. Welche Probleme können dabei auftreten?

Bei diesem Mechanismus gibt es eine bestimmte Anzahl von Permits, die von Stationen gefangen werden, um zu senden. Nachdem Fangen von Permits werden die direkt zerstört. Beim Austritt eines Paketes muss der Sender ein neues Permit wieder erzeugen.
Probleme:
Gleichverteilung der Permits, Anzahl der Permits im Netz

37. Weshalb gibt es eine Verbotene Zone im Sequenznummernraum von Transportprotokollen?

Damit nach einem Absturz die Stationen keine alten Sequenznummern benutzen, die noch im Umlauf sind.

38. Was ist Bitsynchronisation und welche Verfahren gibt es? Erläutern.

Bitsynchronisation dient dazu, um die ankommenden Bits im optimalen Zeitpunkt abzutasten.
- DPLL
- Self Synchronizing Codes
- Training Folge

39. Was verhindert das Rumirren von vielen Paketen bei Flooding?

Im Header jedes Paketes befindet sich ein Streckenzähler, der nach jedem Streckenabschnitt dekrementiert wird. Erreicht es die Null, so wird das Paket verworfen.

Der Router merkt sich jedes Paket und verwirft sie bei erneutem Empfang.

40. Nennen Sie wünschenswerte Eigenschaften eines Routing-Algorithmus.

- Optimal
- Fair
- Robust
- Stabil
- genau

41. Was ist Source Routing?

Die zu laufende Strecke wird im Header des Paketes angegeben.

42. Welches Problem löst das Split-Horizon-Verfahren?

Count-to-Infinity

43. Was verstehen Sie unter Hot-Potato-Routing?
Was ist Flooding?

HPR: Das ankommende Paket wird zufällig an eine Ausgangsleitung weitergeleitet. Alle Ausgänge werden mit derselben Wahrscheinlichkeit ausgewählt.
Flooding: Das Paket wird an alle Ausgänge weitergegeben.

44. Konvergenz bei Routing Algorithmen?

Routing Algorithmus, der sich seinem Ende nähert.

45. Was ist Routing? Nennen Sie Routing Verfahren?

Wegbeschreibung für einen Paket.
Flooding, Hot Potato, Bellman Ford

46. Erklären Sie das Bellmann Ford (Distance Vector) Verfahren.

Ein dynamischer Routing Algorithmus. Jeder Router führt eine Routing Tabelle, indem alle Router aufgelistet sind. Einträge: bevorzugte Ausgangsleitung zum Ziel, geschätzte Zeit oder Entfernung zum Ziel. Einträge werden alle T ms an die direkten Nachbarn gesendet. Die Einträge werden dann verglichen und verändert, falls Änderungen vorliegen.

47. ISDN. Welche Kanaltypen gibt es? Kurz erklären.

B-Kanal: für Datensignale oder Sprache, 64kBit
D-Kanal: für Steuersignale, 16kBit

48. Welches Rahmensynchronisationsverfahren wird bei ISDN verwendet?

Code Verletzung

49. Was ist CAPI?

(Common ISDN API) Programmierschnittstelle zwischen den ISDN-Geräten und dem Anschluss.

50. Warum beträgt die Übertragungsrate des B-Kanals im amerikanischen ISDN nur 56kBit/s gegenüber 64kBit/s im europäischen ISDN?

Bitrobbing → Der 8.Bit von jedem Frame wird für die Signalisierung benutzt.
Daher folgt: 7 * 8000 = 56kBit/s

51. Was ist RPC?

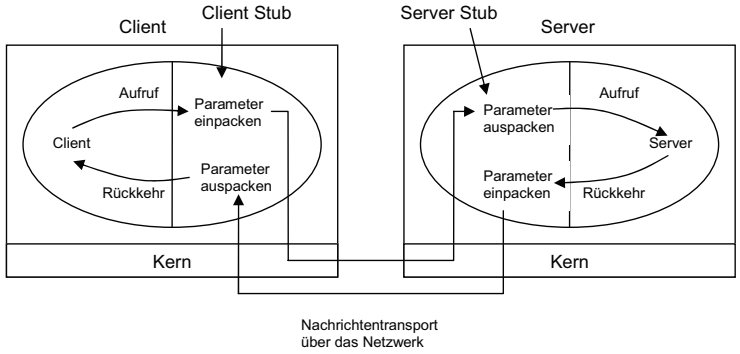
Remote Procedure Call: Ist im Client/Server Modell darstellbar. Es erlaubt einem Programm entfernt (z.B. auf einem Server) eine Procedure aufzurufen. Im Falle eines lokalen Procedure führt die Callee die Operation aus. Im Falle eines RPC ist die Callee eine Stub Procedure. Diese formt aus den gegebenen Parametern eine Message und sendet es an den Server. Im Server existiert auch ein Stub Procedure, die die Message erhält und eine lokale Procedure aufruft. Der Server Stub nimmt das Resultat aus dem Aufruf und sendet es an den Clienten. Der Client sendet das Resultat an den aufrufenden zurück.

52. Was sind RPC-Orphans?
Nennen Sie drei Strategien zu deren Bekämpfung.

Wenn der Client einen Prozess bei einem entfernten Server aufruft und anschließend abstürzt, dann nennt man diesen Server, der keinen Client mehr hat Waise (Orphan).

Extermination: Client legt ein RPC-Logfile an.
Expiration: Ein RPC muss innerhalb einer Zeit T bearbeitet werden. Wenn der Client nach einem Neustart eine Zeit T wartet, können keine Orphans entstehen.
Reincarnation: Zeit wird in Epochen eingeteilt. Nach jedem Neustart beginnt der Client mit seiner neuen Epoche und das meldet er allen Servern. Daten der alten Epoche werden gelöscht.
Gentle Reincarnation: Wenn ein Server eine Nachricht erhält, die eine neue Epoche anzeigt, versucht er den Client zu finden, um anzufragen, was gemacht werden soll. Wenn dieser nicht gefunden wird, werden alle Daten der alten Epoche gelöscht.

53. Beschreiben Sie anhand einer Skizze den grundsätzlichen Ablauf eines RPCs.



54. Was sind die Hauptprobleme von RPC gegenüber lokalen Procedure Calls?

- Adressen
- Server und Client stürzen ab
- Parametrisierung
- Nachricht Verlust

55. Wozu dienen die Portnummern bei TCP und UDP?

Zur Adressierung, um Daten an eine bestimmte Applikation der Anwendungsschicht zu schicken (z.B. Telnet, FTP ...)

56. Was ist IP?

Internet Protocoll: Ist ein verbindungsloses Protokoll, der den Weg der Nachrichten durch das Netz regelt und dabei insbesondere die Integration einer Vielzahl von Teilnetzen zu einem Gesamtnetz unterstützt. Seine Aufgaben:
- Routing
- Fragmentierung / Reassembly
- Error Reporting

57. Erläutern Sie Concatenation / Separation.

Concatenation: Die Pakete (PDU) werden ohne Steuerelemente zusammengefügt.

Separation: Die zusammengefügten PDUs werden beim Peer-Entity wieder auseinander genommen.

58. Soll TCP oder UDP für eine interaktive Sprachübertragung gewählt werden? Begründung.

Für die interaktive Sprachübertragung wird UDP bevorzugt, weil UDP keine Fehlererkennungs- und korrektur Mechanismen hat und daher keine zeitliche Verzögerung mit sich bringt, was für die Übertragung sehr schlecht wäre.

59. Systemarchitektur des WWW und das Konzept des Hypertexts erklären.

WWW basiert au Webseiten mit Text, Bild und Verknüpfung zu anderen Webseiten. Hypertexte sind Textketten in Webseiten mit Verknüpfungen zu anderen Seiten.

60. Was ist IP-Subnetting? Wozu?

Subnetting ist eine Methode nach der man große Netze in mehrere kleine Netze aufteilen kann. Es wird verwendet, um einen Host schneller zu erreichen und den Router zu entlasten. Vereinfachung der Routing durch schnelleres auffinden.

61. Vor- und Nachteile der Segmentierung / Reassembly (Internet)?

+ Paket kommt so bei Netzen mit kleinerer maximaler Paketgröße auch durch.
- zusätzlicher Overhead

62. Welche Hauptaufgabe hat IP im Zielrechner?

- Reassembling
- Error Reporting

63. Beschreiben Sie den Reassembling Deadlock im Internet.

Beim Zusammenführen der Pakete kann der Puffer voll werden und ein Paket vor dem Puffer kann nicht weitergeleitet werden. Aus diesem Grund kommt es zu einem Deadlock.

64. Erklären Sie die folgenden Begriffe in Bezug auf Internetworking: Subnet, Intermediate Systeme, Gateway, Router, Protokollkonverter

Subnet: Netz in einem Netzverbund
Intermediate Systeme: Verbindet zwei Netzwerke miteinander
Gateway: 4. Schicht: Verbindet Netze die verschiedene Adressierungsarten haben (IP ←→ X.25)
Router: 3.Schicht: Dient als Verbindung zwischen LAN Segmenten oder als Gateway zwischen LANs und WANs.
Protokollkonverter: 4.Schicht: Setzt die Vorschriften ohne Inhaltsverlust in ein anderes Protokoll um.

65. Was ist Splitting / Recombining?

Splitting: Ein großes Paket (oder Rahmen) wird in kleine Pakete mit Zusatz von Steuerinformationen aufgeteilt.
Recombining: Beim Empfänger werden die kleinen Pakete nach der Steuerinformation wider zu einem großen Paket zusammengeführt.

66. Nennen Sie grundsätzliche Unterschiede zwischen IP und X.25 Ebene 3.

IP ist verbindungslos und unzuverlässig. X.25 ist verbindungsorientiert und zuverlässig.

67. Warum ist TCP nicht zur Übertragung von Videokonferenzen geeignet?

TCP hat Fehlerkontrolle, womit er die Übertragung verlangsamt. Dies darf bei einer Videokonferenz nicht passieren.

68. IP-Adressen aufschreiben.

Klasse	Bereich	Host Adressbereich
A	0 | 7-Bit Netz | 24-Bit Host	1.0.0.0 – 127.255.255.255
B	10 | 14 Bit Netz | 16 Bit Host	128.0.0.0 – 191.255.255.255
C	110 | 21 Bit Netz | 8 Bit Host	192.0.0.0 – 223.255.255.255
D	1110 | Multicast	224.0.0.0 – 239.255.255.255

69. Erläutern Sie den Mobile-IP Ansatz.

Mobiler Host meldet sich bei einem Fremdagenten an. Der Fremdagent kontaktiert den Heimagenten. Somit bekommt der Heimagent die Adresse des Mobilen Hosts. Wenn ein Paket beim Heimagenten ankommt (für den mobilen Host) wird es gekapselt und im Tunnelverfahren an den Fremdagenten gesendet. Der Fremdagent entpackt das Paket und sendet es an den mobilen Host. Der Heimagent teilt dem Sender die Adresse des Fremdagenten mit, damit Pakete zukünftig direkt zu ihm gesendet werden.

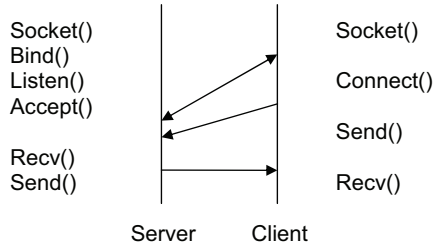
70. Zuverlässiger TCP-Dienst auf einer sicheren LLC-Schicht. Wie kann es trotzdem passieren, dass Pakete an die Transportschicht wiederholt werden?

Aufgrund der unsichern IP.

71. 3-Wege Handshake innerhalb TCP erläutern.

3-Wege Handshake wird für ein zuverlässiges öffnen und schließen von Transportverbindungen über einem Datengramm Vermittlungsdienst verwendet. Sie verlangt vom Initiator zu bestätigen, dass die Verbindungsanforderung gültig ist, bevor die Verbindung benutzt werden kann.

72. Sie sollen ein Client-Server Programm, das TCP verwendet mittels Socket-Schnittstelle realisieren. Diagramm vervollständigen.



73. Unterschied zwischen X.500 Adressen und Internet Adressen? Die Eigenschaften von diesen beiden Adressierungsarten nennen.

X.500	Internet
- File-System orientiert	- nach Zahlen orientiert
- Im Appl. Layer	- bis zu 3 Layer
- 40 Dezimalzahlen	- 12 Dezimalzahlen

74. Was sind die Unterschiede und die Gemeinsamkeiten zwischen Namen und Adressen?

Name sagt aus, wer das ist → ortsunabhängig
Adresse sagt aus, wo es ist → ortsabhängig

Die Gemeinsamkeit besteht darin, dass beide das gleiche Objekt identifizieren

75. Weshalb ist IPv6 schneller als IPv4?

- Das Protokoll wurde vereinfacht, damit Router Pakete schneller abwickeln können.
- Reduzierung des Umfangs der Routing Tabellen

76. Worauf sollten Retransmission Timer der Transportschicht aufgesetzt werden? Retransmission Timer innerhalb der Transportschicht über verbindungsloses Internet berücksichtigen?

Vielfaches von RTT (Ist die Zeit, die ein Paket von Sender bis zum Empfänger und wieder zurück zum Sender benötigt)

77. Aufbau eines Modems?

Scrambler – Codierer – Modulator – Steuerung – Descrambler – Decodierer – Demodulator

78. Was ist ein Nullmodem? Welche Leitungen der V.24 werden mindestens für eine bidirektionale Kommunikation zwischen zwei Endgeräten benötigt und wie müssen diese geschaltet sein?

Nullmodem verbindet zwei Rechner untereinander ohne einen Modem zu benutzen. Folgende Leitungen sind notwendig:

TD	Transmit Data
RD	Receive Data
RTS	Request to Send
CTS	Clear to Send

DTR	Data Terminal Ready
DSR	Data Set Ready
GND	Ground

Transmit Data und Receive Data werden vertauscht angeschlossen.

79. Was ist der Unterscheid zwischen Circuit Switching und Virtual Switching?

- CS ist Leitungsvermittlung	- VS ist eine Variante der Paketvermittlung
- CS hat nur Ausbreitungs-verzögerungen der Signale	- VS hat Store und Forward Delay

80. Erklären Sie Circuit Switching.

CS ist eine Leitungsvermittlung, wo erst eine Verbindung zwischen den Endgeräten aufgebaut wird, bevor Daten übertragen werden. Die Verbindung bleibt während der ganzen Übertragungszeit aufgebaut. Während der Verbindungsaufbau und –abbau kann keine Übertragung erfolgen.

81. Was sind einstufige und mehrstufige Switches?

Einstufig:	Das Senden von Daten erfolgt in einem Schritt
Mehrstufig:	Das Weiterleiten von Daten erfolgt in mehreren Schritten

82. Nennen Sie Vor- und Nachteile der Spread-Spectrum Technologie.

Vorteile:	Antiinterferenzen
	Gesicherte Übertragung
Nachteile:	Höhere Systemkomplexität
	Größere Bandbreite

83. Es gibt zwei unterschiedliche Methoden der Frequenz-Hopping SS. Nennen Sie diese.

Fast FHSS:	mehr als ein Hop / Bit
Slow FHSS:	weniger als ein Hop / Bit

84. Wie funktioniert Space Division Switching? Nennen Sie zwei Arten von Time Division Switching und deren Prinzip.

SDS: Für jede Verbindung muss ein physikalischer Weg durch das Netzwerk geschaltet werden.

TDS:
1) Bus: Ein Bus versorgt mehrere Anzahl von Verbindungen, indem er Daten von den Schnittstellen der Eingangsleitungen nimmt und sie zu den Ausgangsleitungen weiterleitet.
2) Memory: Switching erfolgt durch das Schreiben der Daten in einen Puffer und das Anlegen der Daten an die jeweiligen Ausgänge.

85. Was verstehen Sie unter einem nicht-blockierendem Switch?

Wenn von einem freien Eingang zu einem nicht besetztem Ausgang eine Verbindung aufgebaut werden kann.

86. Wie werden bei Aloha Kollisionen erkannt?

Hier werden Kollisionen nur vermutet, nicht erkannt. Wenn der Sender nach einer bestimmten Zeit kein ACK erhält, geht er davon aus, dass eine Kollision stattgefunden hat.

87. Beschreiben Sie die Funktionsweise eines Verkabelungszentrums beim Token-Ring.

Im VZ befindet sich ein Bypass-Relais für jede Station, die über die jeweilige Station versorgt wird. Fällt eine Station aus, so schließt das zugehörige Relais und die Station wird dadurch abgeklemmt.

88. Welches Fairness Problem tritt bei dem Aloha Backoff Verfahren auf?

Da das Backoff Fenster bei wiederholter Kollision verdoppelt wird, werden Stationen die hintereinander einer Kollision ausgesetzt sind, benachteiligt, indem sie lange warten müssen.

89. Zugriffsverfahren Aloha erläutern.

Jeder darf senden, wann er Daten zu versenden hat. Wenn es zu einer Kollision kommt (kein ACK vom Empfänger), dann wartet die Station eine zufällige Zeit und sendet anschließend erneut.

90. Beschreiben Sie das COMB Zugriffsverfahren (Binäres Countdown). Nennen Sie einige Nachteile.

Alle Stationen die senden möchten erzeugen eine Bitsequence (ihre Adresse). Diese werden Bit für Bit von links nach rechts verglichen. Die eins gewinnt. Letztendlich bleibt eine Station übrig, die senden darf.
Nachteil: Key Management, Umschaltung zwischen Senden und Empfangen kritisch

91. Benennung von drei möglichen Verbesserungen für Aloha.

- slotted Aloha (Zeitschlitze)
- CSMA (Träger abhören)
- CSMA/CD (Träger abhören und Kollisionen erkennen)

92. Prioritätenkontrolle beim Token-Ring?

Rahmen mit höherer Priorität werden zuerst gesendet.

93. Warum liefert slotted Aloha eine höhere Effizienz als Aloha?

Da Stationen nur zu bestimmten Zeiten anfangen dürfen, um zu senden, werden bereits sendende Stationen seltener gestört.

94. Erläutern Sie das Zugriffsverfahren EY-NPMA.

Elimination Yield – Non Preemtive Priority Multiple Access
Zugriffsverfahren mit 3 Phasen:
1. Phase: Zeit wird in Prioritätsslots unterteilt. Stationen die höhere Prioritäten haben dürfen vorher senden.
2. Phase: Jede Station wähl eine zufällige Sendezeitlänge aus dem Survival Intervall aus. Stationen mit der längsten Sendezeit erreichen die 3. Phase.
3. Phase: Station darf nach CSMA senden.

95. Was ist der Unterschied zwischen non-persistent und p-persistent CSMA?

Bei non-persistent CSMA wird sofort gesendet, wenn der Kanal frei ist. Bei p-persistent CSMA wird mit einer Wahrscheinlichkeit p auf einem getaktetem Kanal gesendet.

96. Ist CSMA/CS immer besser als CSMA? Begründen Sie Ihre Antwort.

Bei längeren Strecken und kleinen Paketen ist CSMA genauso gut wie CSMA/CD.

97. CSMA und CSMA/CS erläutern.

CSMA: Hört den Träger ab, wenn dieser frei ist wird gesendet, wenn nicht wird eine zufällige Zeit abgewartet und erneut eine Sendeversuch vorgenommen.
CSMA/CD: Das gleiche wie CSMA, aber mit der folgenden Verbesserung: Wird eine Kollision erkannt, so stoppt der Sender das Senden. Somit wird Zeit und Bandbreite gewonnen.

98. Unterschied zwischen COMB und CSMA/CS?

COMB ist ein Verfahren um Kollisionen zu verhindern. CSMA/CS ist ein Verfahren der während einer Kollision Hilfe leistet.

99. Nennen Sie die drei Operationsmodi in einem Token-Ring.

Single Packet:	Free Token nach Erhalt des letzten Bits der gesendeten Pakete.
Single Token:	Free Token nach Erhalt des letzten Bits des busy Tokens.
Multiple Token:	Free Token gleich nach Erhalt des letzten Bits der gesendeten Daten.

100. Für welchen Zweck verwendet man eine so genannte Bridge und welche Nachteile hat sie? Welchen Vorteil hat sie speziell bei Ethernet?

LANs werden mit Hilfe von Bridges miteinander verbunden.

Nachteil:	Store-Forward Verzögerung. Bei Umwandlung für verschiedene Systeme (Ethernet / Token-Ring) kommt es zu Problemen.
Vorteil-Ethernet:	Segmentierung von großen LANs. → Verbesserung der Zuverlässigkeit, Verfügbarkeit und Dienstfähigkeit.

101. Welche möglichen Veränderungen an Ethernet erlauben eine Vervielfachung der Übertragung (2)?

- CSMA/CR
- CSMA/CA

102. Zugriffsverfahren bei Ethernet?

CSMA/CS

103. Beschreiben Sie kurz, wie das beim Ethernet verwendete Backoff Verfahren funktioniert.

Zeit wird in Schlitze unterteilt. Kollidierte Stationen warten eine Zeit = 2^{i-1} * Schlitzzeit (i: Anzahl der Kollisionen) ab. Ab 10 Kollisionen wird die Schlitzzeit eingefroren, ab 16 wird die Übertragung abgebrochen.

104. Zusätzliche MAC Protokollmechanismen nennen. Wie kann man bei Ethernet Kollisionen verhindern?

- CSMA/CR (Bitmustermethode)
- COMB (Binärer Countdown)

105. Ethernetpakete besitzen eine mindestens eine Größe von 64 Bytes. Warum?

Um die Unterscheidung von Müll und gültigen Rahmen zu erleichtern.

106. Beschreiben Sie kurz wie die Kollisionserkennung im Ethernet funktioniert.

CSMA/CS erklären ...

107. Wie werden beim Ethernet die Pakete vom Bus entfernt?

Abschlusswiderstände sorgen dafür, dass alle Pakete neutralisiert werden.

108. Was verstehen Sie unter „Jabber-Control“ beim Ethernet?

Ein fehlerhafter Sender sendet zufällige Daten, die Kollisionen verursachen. Diese Daten werden isoliert.

109. Ist Ethernet synchron oder asynchron?

Bezüglich des Zugriffsverfahrens ist Ethernet asynchron.
Synchron in Bezug auf Rahmensynchronisation (Präambel).

110. Unterschiede zwischen Token-Ring und Token-Bus erklären?

Token-Bus	Token-Ring
- Reines Broadcast	- Punkt-zu-Punkt Verbindung
- logischer Ring	- echter Ring
- Dezentrale Überwachungs-funktion	- Zentrale Überwachungsfunktion

111. Was versteht man bei HDLC unter Piggypacking?

Nicht zu jedem Paket wird gleich ein ACK gesendet, sondern im Huckepack mit eigene Nutzdaten mitverschickt.

112. Welche Mechanismen können im HDLC zur Flusskontrolle eingesetzt werden?

(High Level Data Link Control)
RNR, RR