

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.

$d = F_E + 1 \rightarrow F_E$ Fehler erkennbar

$d = 2F_K + 1 \rightarrow F_K$ Fehler korrigierbar

$d=2 \rightarrow$ 1 Fehler erkennbar, kein Fehler korrigierbar

$d=3 \rightarrow$ 2 Fehler erkennbar, 1 Fehler korrigierbar

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

00001
00010 \rightarrow 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	\rightarrow	Prüfsumme, ACK, FEC, CRC
Verlorene Pakete	\rightarrow	Timer, Sequenznummer
Falsche Reihenfolge	\rightarrow	Sequenznummer
Duplizierte Pakete	\rightarrow	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 Repeat
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 Bandwidth-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, darf 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 kommunikationstechnische 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.

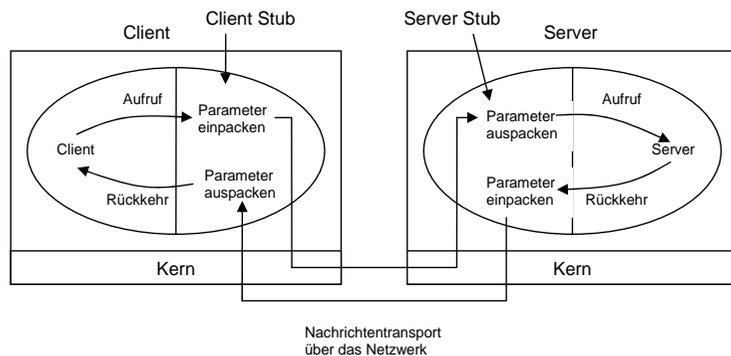
52. Was sind RPC-Orphans?

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 Protocol: 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 auf 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 wieder 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 Mobilten 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.

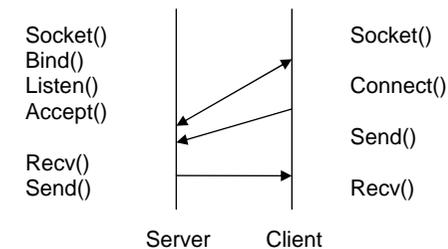
70. Zuverlässiger TCP-Dienst auf einer sicheren LLC-Schicht. Wie kann es trotzdem passieren, dass Pakete an die Transportschicht wiederholt werden?

Aufgrund der unsicheren 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 - Im Appl. Layer - 40 Dezimalzahlen	- nach Zahlen orientiert - bis zu 3 Layer - 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
- CS hat nur Ausbreitungsverzögerungen der Signale
- VS ist eine Variante der Paketvermittlung
- 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 besetzten 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 (Zeitschlitz)
- 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 Preemptive 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 wählt 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 Senderversuch 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 Überwachungsfunktion	- Zentrale Überwachungsfunktion

111. Was versteht man bei HDLC unter Piggybacking?

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

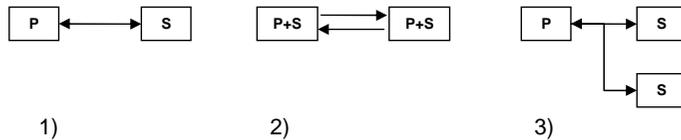
112. Welche Mechanismen können im HDLC zur Flusskontrolle eingesetzt werden?

(High Level Data Link Control)
RNR, RR

113. Erklären Sie Bitstuffing bei HDLC.

Jeder Rahmen beginnt und endet mit einem Flag 01111110. Um Missverständnisse zu vermeiden, stopft der Sender nach jeder aufeinander folgenden fünften 1 eine 0 (außer im Flag), die beim Empfänger wieder entfernt wird.

114. Skizzieren sie die drei Operationsmodi von HDLC. Erläutern.



Unbalanced Configuration: Punkt-zu-Punkt, eine Primary und eine Secondary Station (1), oder eine Primary und mehrere Secondary Stationen (3)
Balanced Configuration: Punkt-zu-Punkt, jede Station ist Primary und Secondary Station (2)

Operationsmodi:

- a) NRM (Normal Response Mode): für Unbalanced Configuration, Secondary Stationen dürfen nur Senden, wenn es die Primary Erlaubt [1, 3]
- b) ARM (Asynchronus R. M.): für Unbalanced Configuration, Secondary Stationen dürfen ohne Erlaubnis senden. [1, 3]
- c) ABM (Asynchronus Balanced Mode): Balanced Configuration. Vollduplex: d.h. alle Stationen sind gleichberechtigt. [2]

115. Was ist LAPB?

LAPB ist ein Subset von HDLC für Punkt-zu-Punkt Verbindungen (vollduplex) zwischen einem Computer und einem Packetswitching Netzwerk (z.B. X.25).

116. Wie wird Signaling in T1 realisiert? Wie kommt es zu 1.544 Mbps? Probleme für Datenübertragung?

Der T1 Träger besteht aus 24 Sprachkanälen, die gemultiplext werden. Jeder der 24 Sprachkanäle fügt 8 Bit in den Ausgangsstrom (7 Bit Nutzdaten, 1 Bit Steuerung). Ein Rahmen besteht also aus $24 \cdot 8$ Bit. Bei jedem Rahmen wird

ein Bit angehängt, um die Rahmensynchronisation zu ermöglichen. Nach Nyquist reichen 800 Samples pro Sekunde für 4 KHz aus.
→ $[(24 \cdot 8) + 1] \cdot 8000 = 1544000$

Für die Signalisierung wird bei jedem 6. bzw. 12. Rahmen ein Bit geklaut, um einen Superframe zu bilden. Bei Daten ist dies problematisch, bei Sprache noch hinnehmbar. Dadurch muss auf jedem Kanal auf das 8.Bit verzichtet werden, was zur Reduzierung der Datenrate auf $7 \cdot 8000 = 56\text{kbs}$ führt statt $8 \cdot 8000 = 64\text{kbs}$.

117. Erklären Sie den Unterschied zwischen Inchannel und Common Channel Signaling.

Inchannel: Steuersignale benutzen den gleichen Kanal wie die Datensignale
Common Channel: Steuersignale haben einen eigenen Kanal

118. Was ist Signalisierung?

Übermittlung von Kontroll- und Managementdaten.

119. Welche Konsequenzen hat diese Signalisierung für eine Datenübertragung?

Konsequenz bei Bitrobbing: Nutzdatenreduzierung. Statt 64 kbps nur 56 kbps

120. Nennen Sie die verschiedenen Signalisierungstechniken.

- Inchannel Inband Signaling: Steuersignale benutzen den gleichen Kanal und denselben Frequenzband wie die Daten.
- Outband Channel Signaling: Steuersignale benutzen den gleichen Kanal wie die Daten. Für die Steuersignale wird aber ein schmales Frequenzband reserviert.
- Common Signaling: Steuersignale haben einen eigenen Kanal

121. Wozu „fast select“ bei X.25?

Keine zusätzliche Call-Setup Phase, N_Connect.Request wird auf das Call Request gepackt.

122. Welche API Aufrufe gibt es bei einem Daytime-Client (UDP)?

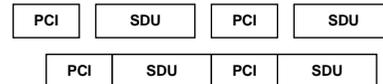
- Server: Socket(), Bind(), Recvfrom(), Sendto()
- Client: Socket(), Bind(), Sendto(), Recvfrom()

123. Wie sind die 2 Mbit/s im E1 Standard aufgeteilt?

32 Kanäle mit jeweils 8 Bit und 8000 Abtastungen.
→ $32 * 8 * 8000 = 2048000$

124. Erläutern Sie die Begriffe Blocking / Deblocking. Nennen Sie ein dabei möglicherweise auftretendes Problem.

Mehrere PCIs und SDUs werden der Reihe nach zusammengeführt.
Nachteil: unbegrenztes Warten



125. Was bedeutet plesiochron Multiplexing?

Da mehrere Quellen eigenständige Timer haben, kann es zur gewissen Drift kommen. Daher wird beim Kanal eine Bitrate benutzt, die höher als die Summe der Inputkanäle ist. (plesiochron = nahezu synchron)

126. Erläutern Sie den Begriff „Statistical Multiplexing“.

Nur die Stationen die senden möchten werden gemultiplext und mit einem Adress-Header bestückt und anschließend gesendet. Somit wird Bandbreite gespart.

127. Was ist ein Dienst? Was ist ein Protokoll? Welcher Zusammenhang besteht zwischen den beiden?

Ein Protokoll beinhaltet Regeln, die die Formate von Paketen und Nachrichten festlegen. Es beinhaltet Festlegungen für die Kommunikation zwischen zwei Schichten der Ebene N. Ein Protokoll ermöglicht einen Dienst.

Ein Dienst ist eine Gruppe von Operationen, die eine Schicht der über ihr liegenden Schicht zur Verfügung stellt. Eine niedrigere Schicht erledigt spezifische Aufgaben, auf die die höhere Schicht aufbauen kann. Dieser Dienst wird an SAP angeboten.

Es ist im Prinzip die Richtung der Kommunikation die sich ändert. Bei einem Dienst handelt es sich um eine Gruppe von Operationen, die eine Schicht der über ihr liegenden Schicht zur Verfügung stellt. Ein Protokoll definiert Regeln die in beiden Richtungen der Kommunikation gelten.

128. Geben Sie drei verschiedene Verfahren an, mit deren Hilfe Framesynchronisation durchgeführt werden kann.

Bitstopfen, Zeichenstopfen, Zeichenzählen, Code Verletzung

129. In wie weit löst das RTS / CTS das Problem des hidden Terminals?

Jede Station die eine RTS bzw. CTS hört verzögert das Senden.

130. Beschreiben Sie mit knappen Worten den Unterschied zwischen einem Computer Netzwerk und einem Verteilten System.

Bei einem Verteilten System weiß der Benutzer nicht, dass er mehrere Prozessoren zur Verfügung hat. Sein Rechner erweckt den Anschein eines virtuellen Einzelprozessors. Bei einem Netz muss der Benutzer selbst mit einer Maschine interagieren. Er muss seine lokalen und entfernten Vorgänge selbst erledigen. In einem Verteilten System wird dies automatisch vom System geregelt, ohne das Wissen des Benutzers.

131. Was ist eine Spezifikation?

Eine Spezifikation ist eine Beschreibung des System-Verhaltens. Es wird beschrieben, wie sich ein System mit seiner Umwelt verhält, es wird aber nicht auf seine Implementierung eingegangen.

132. Erklären Sie den Begriff Expedited Data Transfer.

Beschleunigte Pakete, die im Netz quasi immer Vorfahrt haben.

133. Was verstehen Sie unter FDM?

Frequency Division Multiplexing: Die verfügbare Bandbreite wird bei N Benutzern in N gleich große Teile zerlegt. Interessieren sich weniger als N Benutzer für Kommunikation, so wird Bandbreite vergeudet. Damit sich Frequenzbereiche nicht überschneiden, entstehen zwischen zwei Frequenzbereichen Lücken.

134. Erklären Sie den Unterschied zwischen expected und quaranted QoS.

Quaranted QoS: Vereinbaren eines Mindeststandard, die immer zu Verfügung steht.
Expected QoS: Basiert auf Schätzungen und befindet sich in einer gewissen Toleranzbreite.

135. Wie kann man einen Layer testen?

Mit Conformance Testing.

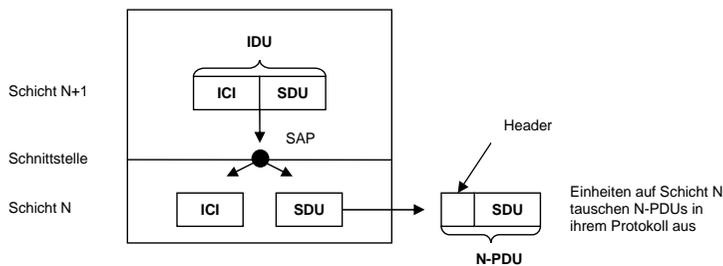
136. Welche Parameter müssen für einen bestätigten Datengrammdienst mindestens angegeben werden?

Quelladresse, Zieladresse und Nutzdaten

137. Welche OSI Schichten werden von X.25 abgedeckt?

Bitübertragungs-, Sicherungs- und Vermittlungsschicht

138. PDU, SDU, ICI im Layer-Diagramm zeichnen.



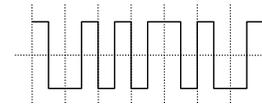
SAP = Service Access Point (Dienstzugriffspunkt)
 IDU = Interface Data Unit (Schnittstellendateneinheit)
 SDU = Service Data Unit (Dienstdateneinheit)
 PDU = Protocol Data Unit (Protokolldateneinheit)
 ICI = Interface Control Information (Schnittstellensteuerdaten)

139. Nennen Sie die sieben Schichten des OSI Referenzmodelles in richtiger Reihenfolge. Darf Schicht N auf Schicht N-2 zugreifen?

7. Verarbeitungsschicht (Application Layer)
6. Darstellungsschicht (Presentation Layer)
5. Sitzungsschicht (Session Layer)
4. Transportschicht (Transport Layer)
3. Vermittlungsschicht (Network Layer)
2. Sicherungsschicht (Data Link Layer)
1. Bitübertragungsschicht (Physical Layer)

Schicht N darf nicht auf Schicht N-2 zurückgreifen.

140. Manchester Code in Bitfolge zurückwandeln.



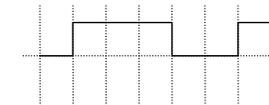
High → Low = 0
 Low → High = 1

→ 0111001

141. Bitfolge in NRZ1 umwandeln.

0111001

0 Null
 1 High



142.

143. Asynchrone und synchrone Kommunikation erklären.

Bei asynchroner, kann die Kommunikation zu jedem Zeitpunkt stattfinden. Der Abstand der eintreffenden Bits kann beliebig lang sein. Bei synchroner Kommunikation wird in jeder Periode ein Symbol erwartet, auch wenn es keine Information trägt.

144. Wireless LANs: Hidden und Exposed Terminal Szenario beschreiben.

A B C D

A sendet an B und C will an B senden.
 C hört nicht das A an B sendet, und es entsteht eine Kollision.

B sendet an A und C will an D senden.
 C hört das B sendet und um eine Kollision zu vermeiden sendet C nicht, obwohl es zu keiner Kollision kommen kann.

145. Erläutern Sie den Begriff „TDMA“. Nennen Sie Vor- und Nachteile dieses Verfahrens.

(Time Division Multiple Access)

Jede Station erhält einen festen Zeitschlitz, indem sie senden darf.
Nachteil: Bandbreite Verschwendung bei nicht sendenden Stationen.
Overhead bei großen Paketen.
Großer Puffer notwendig

146. Was ist der Unterschied zwischen den Einheiten Bitrate und Baudrate?

Bitrate: Sagt aus, wie viel Bits in einer Sekunde übertragen werden.
Baudrate: Die Anzahl der Änderungen in einem Signale pro Sekunde.

147. Was für eine Bandbreite ist bei Manchester Codierung erforderlich, um eine Übertragungsrate von 10 MBit/s zu erreichen.

Doppelte Bandbreite → 20 Mbit/s

148. Was ist 4B3T Codierung?

Codierung, bei der eine Sequenz von 4 Bits durch 3 Pulsniveaus dargestellt wird. In Folge dieser Codierung wird die Baudrate gesenkt.

149. Wofür steht die Bezeichnung M/M/1?

M / M / 1
Ankunftszeit der Kunden im System / Bedienzeit der Kunden im System /
Serveranzahl im System

150. Nennen Sie drei Beispiele für physikalische Bustypologien.

Ring, Bus, Stern

151. Nennen Sie die Glasfaserarten.

Singlemode Faser, Multimode Glasfaser, Multimode Stufenfaser

152. Ursache für Multipath?

Shadowing, Reflexion, Diffraction

153. Nennen Sie drei QoS Parameter.

Fehlerrate, Verzögerung, Durchsatz

154. Was ist Random Early-Drop?

Das ist eine Verbesserung zu Leaky Bucket, der nach einem Risikobereich, die ankommenden Pakete mit einer bestimmten Wahrscheinlichkeit herauswirft.

155. Was ist Conformance Testing?

Mit diesem Testverfahren kann man einen Layer testen. So wird festgestellt, ob die Implementation mit der Spezifikation übereinstimmt.

156. Wofür wird ASN.1 verwendet?

Alle gesendeten Daten gehören zu einem bestimmten Datentyp. ASN legt Regeln für die Definition und Benutzung von Datentypen fest. ASN unterscheidet zwischen Datentypen und Variable von diesem Typ.

157. Wie ist V.34 codiert?

Trellis Code

158. Wie werden die Verbindungen zwischen zwei Rechnern herausgefunden? Mit welchem Protokoll und welchen Optionen?

Mit traceroute.
a> traceroute b → a-c-b ; b-d-e-a
Die Topologie wird somit ausgekundschaftet.

Protokoll ICMP mit dem TTL Feld.

159. Problematik bei 2-Way-Handshake für Verbindungsaufbau?

Pakete von alten Verbindungen könnten fälschlicherweise eine neue Verbindung herstellen.

160. Was sind Abstrakte Syntax und Transfersyntax?

Abstrakte Syntax: Welche Datenstrukturen werden kodiert?
Transfersyntax: Wie werden diese Datenstrukturen übertragen?

161. Nennen Sie drei Merkmale des Radioempfangs.

Mehrweg Empfang, Interferenzen, Doppler Effekt, nichtlineare Dämpfung

162. Was verstehen Sie unter Intersymbol – Interference?

Wie kann diese bei drahtloser Übertragung Zustände kommen.

Überlagerung von Signalen, die beim Empfänger zeitlich verzögert ankommen.
Das Signal vom Sender wird durch Reflexion etc. Mit zeitlicher Verzögerung beim Empfänger ankommen.

163. Wovon hängt die Dämpfung eines Kabels ab?

Länge, Material

164. Erläutern Sie GPS bei Sheduling. Erläutere WFQ. Nenne Unterschiede zwischen diesen beiden.

Generalized Processor Sharing: N Sessions mit Gewichten und einem Server. Der Server bearbeitet gleichzeitig mehrere Prozesse, die verschiedene Gewichte haben.
Weighted Fair Queuing: Verbesserung von GPS. Bearbeitet nach Gewicht.

165. Deadline Monotic Sheduling optimal?

Ja, statisches Sheduling mit statischen Prioritäten.

166. Deferable Server in Rate Monotic Sheduling?

Ist eine periodische Aufgabe mit fester Priorität und bestimmter Rechenzeit, die einer periodischen Aktivität zugeordnet werden kann.

167. Rahmensynchronisation bei Ethernet?

Präambel

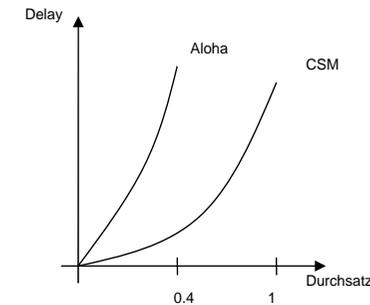
168. Trellis Code?

Codierung um die Wahrscheinlichkeit der Erkennung von Fehlern zu steigern.

169. Mechanismen durch die der Sender den Zustand des Empfängers erfährt (bei verbindungsorientiert)?

RNR, RR, Sliding Window

170. CSMA und Aloha. Durchsatz und Delay Diagramm zeichnen.



171. Guard-Time bei TDMA erklären.

Zwischen zwei Stationen, um eine mögliche Überlappung zu verhindern.

172. LCN bei X.25 mit LOC und HOC?

(Logical Channel Numbers)
HOC = Highest Outgoing Channel
LOC = Lowest Outgoing Channel

173. TEI und SAPI?

Im Falle einer Punkt-zu-MultiPunkt Verbindung müssen mehrere logische Verbindungen (Prozesse) über einen Kanal gemultiplext werden.

SAPI: Um zwischen verschiedenen Layer 3 Prozessen zu unterscheiden
TEI: Um zwischen verschiedenen ISDN Geräten zu unterscheiden, welche dieselben Layer 3 Prozesse benutzen d.h. dieselbe SAPI haben.

174. Welche Vorteile hat Twisted Pair?

Billig, Leichte Wartung, Flexibleres Installieren, Länge

175. Was ist ein SAP?

Ein *Service Access Point* ist die Schnittstelle zwischen zwei Schichten. Diese Dienstzugriffspunkte besitzen eine eindeutige Adresse.

176. Was ist ein idealer Kanal?

Unbegrenzter Durchsatz, keine Verzögerungen, keine Fehler

177. Kanaleigenschaften: Durchsatz, Verzögerung und Zuverlässigkeit erklären.

Durchsatz: Informationsmenge (Bit) die in einer vorgegebenen Zeit (s) über den Kanal übertragen werden kann.

Verzögerung: Die vergangene Zeit, die eine Information benötigt, bis es am Ziel angekommen ist.

Zuverlässigkeit: Welche Art und welche Menge an Fehlern sind während der Übertragung aufgetreten.

178. Erläutern Sie DPLL und die Funktionsweise.

Digital Phase Locked Loop dient dazu, um bei dem Empfänger eine optimale Abtastung des empfangenen Signals durchzuführen. Die DPLL tut das Signal mit einer höheren Rate als die empfangene ab, und kontrolliert, ob die Signalgrenzen innerhalb des erwarteten Intervalls liegen. Falls das nicht der Fall ist, wird der lokale Taktgeber nachgeregelt. So lässt sich jedes Abtastzeitpunkt vom vorherigen Signal bestimmen, um in der Mitte der Periode abzutasten.

179. Wozu dient Bitsynchronisation. Drei Methoden angeben.

Bitsynchronisation dient dazu, um die ankommenden Bits im optimalen Zeitpunkt abzutasten.

- DPLL
- Self Synchronizing Codes
- Training Folge

180. Eigenschaften von Koax?

Gut abgeschirmt. Analoge und digitale Übertragung möglich. Hohe Bandbreite. Ausgezeichnete Rauschbeständigkeit.

181. Eigenschaften von Glasfaser?

Übertragung in Lichtgeschwindigkeit. Sehr zuverlässig (Fehler). Mehrkanal Übertragung möglich.

182. Eigenschaften von Radiowellen?

Rundstrahlend. Merkmale sind Frequenzabhängig. Auf allen Frequenzen sind Radiowellen Störungen ausgesetzt (Elektroanlagen etc.). Sind leicht zu erzeugen, legen große Entfernungen zurück und dringen mühelos in Gebäuden ein.

183. TDM?

Jeder Benutzer erhält für eine bestimmte Zeit die gesamte Bandbreite.