Chapter 1 – Transmission Principles

1) Was versteht man unter paralleler Übertragungstechnik? Wo wird diese Technik eingesetzt? Wie erfolgt die Taktsynchronisation?

ein Datenwort (8-bit, 16-bit, ...) werden gleichzeitig auf mehreren parallelen Datenleitungen (Bus) übertragen

Bus-System:
- data-bus: für Übertragung von Datenwörtern
- address-bus: Übertragung von Speicheradressen (addressing memory location)
- control-bus: zur Signalisierung der Übertragungsrichtung (read/write), clock (clk), interrupt, ...

eingesetzt bei Datenübertragugen über kurze Distanzen (Computersysteme); würde für weite Strecken zu teuer sein

Taktsynchronisation erfolgt über Kontrollbus mit geeignetem Clock Signal

2) Was versteht man unter serieller Übertragungstechnik? Wo wird diese Technik eingesetzt? Warum verwendet man keine separate Leitung für die Übertragung der Taktinformation? Was versteht man unter Bitsynchronisation und wie erfolgt diese prinzipiell?

Bits werden auf einer Datenleitung nacheinander übertragen; jedes Bit wird in einem konstanten Zeitintervall (bit-cell) gesendet
Empfänger muss mit dem Sender synchronisiert sein, um die Bits zum richtigen Augenblick abzutasten; eine seperate clock-line ist zu teuer
=> Bit-Synchronisation:
Signaländerungen werden vom Empfänger zur Taktrückgewinnung genutzt (clock recovery); Empfänger kann nun einen Takt generieren, mit dem die Bits abgetastet werden (wegen schwächer werdender Signalstärke , Bandbreitenbeschränkumg oder delay distortion am besten in der Bitmitte)
es gibt 2 Arten der Bitsynchronisation: asynchron, synchron

serielle Übertragungstechnik wird zwischen Computersystemen (auf langen Wegen, im WAN-Bereich) eingesetzt (parallel wäre hier zu teuer)

3) Wie erfolgt die Bitsynchronisation bei asynchroner Übertragung? Für welche Zeit-Dauer ist die Bitsynchronisation gewährleistet? Welcher Trick wird bei der Taktrückgewinnungsschaltung angewendet (Stichwort Oversampling)? Welchen fundamentalen Nachteil hat dieses Verfahren?

Sender und Empfänger haben voneinander unabhängige Taktgeneratoren, die aufeinander abgestimmt werden müssen; die Bitsynchronisation erfolgt nur über die Länge eines Datenwortes; Datenwörter können unabhängig gesendet werden und werden unabhängig voneinander synchronisiert
die Technik der Start/Stopp-Bits wird verwendet:
- Start-Bit: Änderung von 1 auf 0; synchronisiert das folgende 8-Bit-Wort mittels Oversampling (Überabtastung)
- Stopp-Bit: ein oder zwei Bits (binär 1); stellt sicher, dass das nächste Start-Bit erkannt wird

das Intervall zwischen den Datenwörtern ist variabel; Synchronisierung nur während der Übertragung der Datenwörter
ineffizient, weil für 8 Bits zusätzlich 3 Bits zur Synchronisation benötigt werden

4) Wie erfolgt die Bitsynchronisation bei synchroner Übertragung? Für welche Zeit-Dauer ist die Bitsynchronisation gewährleistet? Welcher Trick wird bei der Taktrückgewinnungsschaltung angewendet (Stichwort PLL)? Durch welche Maßnahmen erreicht man genügend Signalflanken?

Bit-Synchronisation dauert zumindest so lange, wie die Übertragung eines Datenblocks; aus dem übertragenen Signal kann auf Grund der Flankenwechsel im Signal auf das Clock-Signal rückgeschlossen werden
PLL … Phase Locked Loop: wird verwendet, um receiver clock einzufrieren, wenn keine Signaländerungen erfolgen
es werden nur zu Beginn eines Datenblocks zusätzliche Synchronisations-Bits benötigt; Sender und Empfänger bleiben immer im selben Takt (synchron in Phase und Frequenz)

trotzdem werden „hin und wieder“ (bei langen Folgen von 0en oder 1en) Signalflanken benötigt, was durch den simplen NRZ-Code nicht gewährleistet werden kann; stattdessen: Manchester-Code, NRZI, RZ, AMI, HDB3

5) Geben Sie die Codierungsvorschrift für den Manchester-Code an. Vergleichen Sie die Eigenschaften dieses Codes bezüglich Bandbreite, Gleichanteil (DC = direct current) mit dem NRZ-Code. In welchen Netzwerken werden diese Codierung verwendet (LAN oder WAN)?

- Bit wird in zwei Hälften geteilt
- erstes Halb-Bit ist Komplement des Datenbits; zweites Halb-Bit ist identisch mit dem Datenbit
- Bits werden in der Mitte abgetastet, also dort wo sich jetzt die Flanke befindet
- Wechsel der Signallevels tritt in der Mitte jedes Bits auf
  Wechsel von 1 nach 0 beschreibt logisch 0
  Wechsel von 0 nach 1 beschreibt logisch 1
  => jedes Bit wird nun mit 2 Signalhälften dargestellt -> doppelt so viele Signaländerungen wie beim NRZ-Code

benötigt doppelt so viel Bandbreite wie NRZ; hat keinen oder einen konstanten Gleichanteil (direct current - dc)

Manchester-Code wird gewöhnlich in LANs verwendet

6) Geben Sie die Codierungsvorschrift für den HDB3-Code an. Vergleichen Sie die Eigenschaften dieses Codes bezüglich Bandbreite, Gleichanteil (DC = direct current) mit dem NRZ-Code. In welchen Netzwerken werden diese Codierung verwendet (LAN oder WAN)?

- logische 1en werden durch einen Impuls mit alternierender Polarität dargestellt; eine logisch 0 durch ein gleich 0 bleibendes Signal
- bei einer Folge von drei 0en, wird die vierte 0 vom Code automatisch mit einem 1-Signal codiert (Bitstuffing); Empfänger versteht damit, dass es sich um eine längere Folge von 0en handelt

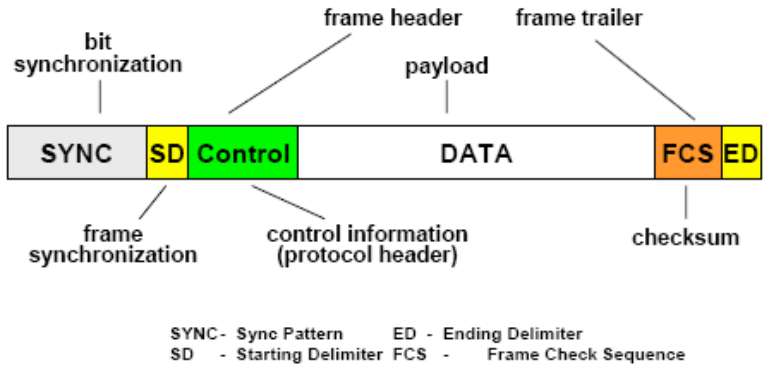
- benötigt genauso viel Bandbreite wie NRZ
- hat keinen oder einen konstanten Gleichanteil (direct current - dc)
- wird gewöhnlich in WANs verwendet

7) Warum werden Übertragungsrahmen (Frames) zur Übertragung von Informationen eingesetzt? Wie schaut der prinzipielle Aufbau eines Übertragungsrahmens aus? Wozu werden die einzelnen Felderverwendet?

Aufteilung in Datenblöcke ist nötig …

- … um im Fehlerfall nicht die gesamten Daten erneut übertragen zu müssen, sondern kleinere Portionen (Frames)
- … um Fehler überhaupt zu erkennen
- … damit die Übertragungsstrecke von mehreren Teilnehmern benutzt werden kann und nicht durch die Datenübertragung eines einzelnen blockiert wird
- … um die Flexibilität eines großen Netzwerkes wie dem Internet gewährleisten zu können, wo die Datenblöcke nicht unbedingt auf dem selben Weg zum Ziel gelangen

Aufbau eines Übertragungsrahmens:



SYNC … spezielles Bit-Muster (typischerweise 010101...-Pattern); wird zur Bit-Synchronisation nach einer Idle-Periode verwendet; kann in Idle-Zeit als Füll-Pattern genutzt werden, um die receiver clock synchronisiert zu halten

Control … für die Implementierung von Protokoll-Prozeduren (z.B.: frame type, protocol type: Data, Connect, Disconnect, Reset, IP, AppleTalk etc.; Sequence Numbers für die Identifikation der Frame-Sequenz; Adress-Information der Quelle und des Ziels; Frame-Länge etc)

SD, ED … Start/End-Delimiter; spezielle Bit-Muster, die den Beginn und das Ende eines Blockes markieren; Bit-Muster darf nicht innerhalb des Frames vorkommen

DATA … zu übertragende Daten

FCS … Frame Check Sequence; eine Prüfsumme

8) Was versteht man unter Rahmensynchronisation (Framesynchronization)? Wieso ist diese erforderlich (Zwei Szenarien: Leitung vor Aussenden eines Rahmens im Idle-Zustand; Leitung in Übertragungspausen mit SYNC Zeichen im synchronen Zustand gehalten)?

Rahmensynchronisation: Anfang und Ende eines Blockes müssen erkannt werden

Datensätze werden blockweise übertragen; um Beginn und Ende eines Blockes zu erkennen und von SYNC-Signalen zu unterscheiden, benötigt man Rahmensynchronisation

(wird nach einer Idle-Phase ein Rahmen gesendet, ist SYNC notwendig, um die Synchronisation durchzuführen; in Übertragungspausen wird SYNC als Fill Pattern verwendet, um die Synchronisation aufrechtzuerhalten

9) Was versteht man unter Datentransparenz und wie wird diese erreicht? Erklären Sie das an Hand der bitorientierten (bit-oriented) Methode.

Datentransparenz: Techniken, die das Auftreten von Bit-Mustern, die z.B. für SD und ED verwendet werden, innerhalb der Rahmen vermeiden

Methoden: byte stuffing, bit stuffing, code violations, byte count technique, idle line before SD and ED

bitorientierte Methode: SD und ED = 01111110 (so genanntes Flag); jedes andere Bit-Muster wird als Beginn des Rahmens interpretiert
Flag darf nicht im Rahmen auftreten -> nach fünf 1en fügt der Sender eine 0 ein; Empfänger entfernt 0 nach fünf 1en

10) Wie wird Datentransparenz bei der zeichenorientierten (character-oriented) Methode erreicht?

es werden Control Characters verwendet (ASCII, EBCDIC):
- SOH (Start of Header)
- STX (Start of Text)
- ETX (End of Text)

Control Characters werden nur als solche erkannt, wenn ihnen das DLE (Data Link Escape) vorangestellt ist; muss im Datenblock auch ein DLE gesendet werden, wird dieses verdoppelt und kann danach wieder entfernt werden

11) Wie erfolgt Rahmensicherung (frame protection) und Fehlererkennung (error detection), wenn man Feedback Error Control Technik verwendet? Welche bekannte Verfahren zur Prüfsummenbildung gibt es?

es wird so viel redundante Information in einen Block gepackt, dass der Empfänger Fehler erkennen, jedoch nicht selbst korrigieren kann = Error Detection (error detecting codes -> Frame Check Sequence - FCS); danach kann der Rahmen erneut angefordert werden
Sender generiert Checksumme (FCS), die am Ende des Rahmens angehängt wird (frame protection)

Empfänger bildet seine eigende Checksumme und vergleicht diese mit der Mitgesendeten (error detection); Rahmen wird dann neu gesendet

Möglichkeiten zur Prüfsummenbildung (FCS):

(i) mittels Paritätsbit: ein zusätzliches Bit wird am Ende eingefügt, so dass die Summer aller 0en bzw. 1en entweder gerade oder ungerade ist
Nachteil: bei einer geraden Anzahl an Fehlern gleichen sich diese wieder aus

(ii) Summierung aller Datenwörter modulo 2

(iii) Cyclic Redundancy Check (CRC)

12) Welchen Ansatz verfolgt Forward Error Control? Wann wird diese Technik eingesetzt?

es wird so viel redundante Information in die Blöcke gepackt, dass der Empfänger Fehler korrigieren kann -> error correcting codes (Wichtig: Hamming Distance)

benötigt wird Forward Error Control in „extremen" Situationen/auf stark fehlerbehafteten Übertragungswegen (hohe Bitfehler-Rate); z.B. extrem lange Strecken (Weltall)

13) Wie kann man sich bei der physikalischen Signal-Übertragung mithilfe des Ansatzes der Fourier-Reihe die Effekte Attenuation (Abschwächung) und Limited Bandwidth (Grenzfrequenz) erklären?

Durch die Fourier-Reihe lässt sich jedes periodische Signal mit Periode T durch Summen von Sinus- und Kosinusschwingungen (und evt. Gleichanteil) darstellen.

Ein Rechteck-Impuls besteht aus einer (unendlichen) Summe von Sinus- und Kosinusschwingungen steigender Frequenzen. Anteile bis zur Grenzfrequenz fc werden ungeschwächt übertragen, alles darüber wird mehr und mehr abgeschwächt. Daher „verschwinden" die hochfrequenten Anteile und aus dem Rechteck wird ein abgerundetes „Trapez".
Die Abschwächung wird durch den ohmschen Widerstand der Leitung verursacht.

14) Wie kann man sich bei der physikalischen Signal-Übertragung mithilfe des Ansatzes der Fourier-Reihe den Effekt Delay Distortion (Verzerrung) bei der physikalischen Übertragung erklären?

Unterschiedliche Frequenzen (Komponenten) des Fourier-Spektrums haben unterschiedliche Laufzeiten. Daher verzerrt sich ein Rechteck-Impuls.

15) Welche Auswirkungen haben die physikalischen Aspekte (Attenuation, Delay Distortion, Noise) für die Bitsynchronisation und für die maximal erreichbare Bitrate eines Übertragungssystems?

Bitsynchronisation funktioniert nur bei einer „sauberen" Flanke und möglichst unverzögerter Übertragung. Durch Attenuation, Delay Distortion und Noise wird die Signalqualität verschlechtert. Wenn auch noch die Bitrate gesteigert wird, wird die Bit-Synchronisation sogar in der Mitte der Bits immer komplizierter. Ab einer bestimmten Obrgrenze ist keine Synchronisation mehr möglich.

16) Was besagt das Theorem von Nyquist?
beschäftigt sich damit, wie viele Bits über eine ideale (rauschfreie) Leitung transportiert werden können

$R = 2*B*\log_2(V)$
R … maximale Bitrate in Bit/s, B … Bandbreite in Hz, V … Anzahl der Signallevel

Das Theorem besagt, dass ein beliebiges (gefiltertes, Tiefpass) Signal der Bandbreite B durch eine Abtastrate von 2B vollständig wiederhergestellt werden kann. Wobei eine Abtastrate von mehr als 2B höchstens (nutzlose) Anteile höherer (bereits gefilterter) Frequenzen entdecken würde. Die Formel gilt für V diskrete Stufen.

17) Was besagt das Theorem von Shannon?

beschäftigt sich damit, wie viele Bits über eine verrauschte Leitung gesendet werden können

max R = B*log2(1+S/N)
R … maximale Bitrate in Bit/s, B … Bandbreite in Hz, S … Signalstärke, N … Rauschstärke

GSM und UMTS z.B. arbeiten knapp unter dem Shannon-Limit.

18) Was versteht man unter Baseband Transmission?

Die gesamte Bandbreite wird benutzt, um einen Datenstrom zu übertragen.
Signale werden als rechteckige Impulse übertragen; physikalischer Zustand der Leitung, Sendeleistung, Sensibilität des Empfängers und S/N-Rate limitieren die erreichbare Bitrate
Das Signal wird kodiert, um Bit-Synchronisation sicherzustellen, um einen Gleichanteil zu vermeiden und um die elektromagnetische Strahlung gering zu halten.

19) Was versteht man unter Narrowband Transmission? Was ist ein Modem?

Bandbreite wird absichtlich begrenzt -> es können keine rechteckigen Impulse übertragen werden; diese müssen vorher adaptiert werden; Adaption erfolgt durch Modulation (z.B. Modem für die Übertragung über Telefonleitung)

Modem (Modulator/Demodulator): adaptiert digitale (rechteckige) Signale auf eine analoge Trägerschwingung; verschiedene Modulationstechniken (Amplitudenmodulation, Frequenzmodulation, Phasenmodulation, ...)

20) Was versteht man unter Broadband Transmission (zwei Sichtweisen: Aus Sicht der analogen Nachrichtentechnik, aus Sicht der digitalen Übertragungssysteme)?

In der Nachrichtentechnik: Die verfügbare Bandbreite der seriellen Leitung wird in mehrere Teile mit kleiner Bandbreite aufgeteilt (verfügbare Bandbreite wird in mehrere „Kanäle“ unterteilt), um gleichzeitig mehrere serielle Verbindungen zu ermöglichen.
In analogen Systemen kann man das realisieren, indem man jedem Kanal seinen eigenen Träger gibt, auf den dann die Information aufmoduliert wird (z.B. Kabelfernsehen).

In digitalen Systemen bedeutet Broadband meist einfach nur High-Speed-Übertragung.

Chapter 2 – Protocol Principles

21) Welche Services kann die Kommunikationsschicht prinzipiell der Applikationsschicht zur Verfügung stellen (3 Schichtenmodell)? Charakterisieren Sie diese kurz.

Communication Software stellt der Application Software einen Service zu Verfügung; Service kann connection-less oder connection-oriented sein

Connection-Less (CL): ist der einfachste Dienst, Communication SW nutzt nur Basis-Elemente (Frame Synchronization, Frame Protection, Error Detection), um Datenblöcke zu übermitteln; Übertragungsfehler -> Empfänger verwirft Datenblöcke; geringe Implementations-Anforderungen an die Communication SW; aber error recovery (korrigieren von Fehlern) muss von der Applikation gemacht werden

Connection-Oriented (CO): eine Verbindung wird zum Empfänger aufgebaut und bis zum Abbau aufrechterhalten; nach dem Aufbau werden die Daten übertragen, wobei jedes Paket bestätigt und durch Fehlerkorrektur- oder auch Fehlererkennungscodes auf Fehler geprüft wird; ist ein Paket/Frame fehlerhaft (oder es „fehlt“) wird es erneut übertragen oder durch den Fehlercode gleich beim Empfänger wiederhergestellt; anspruchsvollere Communication SW wird benötigt

22) Was ist die Grundidee von ARQ? Nur bei welcher Service-Art ist diese Technik durchführbar?

ARQ … Automatic Repeat Request

bezeichnet Techniken, bei denen eine zuverlässige Datenübertragung durch das wiederholte Senden von beschädigten oder verlorenen Frames/Paketen garantiert wird; Empfänger muss den Erhalt von Frames/Paketen bestätigen (Feedback Error Control); jeder übertragene Dataframe wird bis zum Erhalt des

Acknowledgement (der Bestätigung) in einem Retransmission-Buffer gespeichert; wenn Acknowledgement nicht erhalten -> Dataframe nach einem Timeout erneut senden

ARQ ist nur bei verbindungsorientierten Services verfügbar

23) Welche Betriebsmittel benötigt man zur Realisierung einer ARQ-Methode?

Für ARQ benötigen die Teilnehmer zusätzlich für jeden Frame
- einen Timer
- eine Liste, in welcher nicht bestätigte Pakete verwaltet werden (Retransmission-Buffer)
- Sequenznummen in den Frames; es müssen Duplikate erkannt werden und/oder die Pakete/Frames umgeordnet werden

24) Was ist die Grundidee von Idle-RQ? Welches Protokoll der TCP/IP-Suite verwendet diese Technik?

Idle-RQ: Simple ARQ-Implementation

Grundidee: Sender und Empfänger besitzen jeweils einen Timer. Nach Ablauf des Timers beim Sender nimmt der Sender an, dass der Frame verloren gegangen ist und sendet diesen erneut und wartet auf eine Bestätigung des Empfängers (Stop-&-Wait-Protokoll: Vorrichtung wartet auf Acknowledgement (ACK), bevor der nächste Dataframe gesendet wird). Der Empfänger sendet nur dann eine Bestätigung, wenn er einen unbeschädigten neuen Frame erhalten hat.
Nachteil: schlechte Nutzung der verfügbaren Bandbreite
Vorteil: einfach, Flusskontrolle, kein Frame geht verloren

Basis-Methode kann durch NACK verbessert werden (NACK führt zur Neuübertragung des Frames)

TCP/IP-Suite-Protokoll, das Idle-RQ verwendet: TFTP (Trivial File Transfer Protocol) verwendet

25) Wie erfolgt bei Idle-RQ die Fehlerbereinigung (Error Recovery) im Fehlerfall (zwei Szenarios: I-Frame gestört, ACK- Frame gestört)?

I-Frame gestört: Empfänger bekommt keinen I-Frame -> Empfänger sendet kein ACK -> Sender bekommt kein ACK, wartet Timeout ab und sendet dann I-Frame erneut
Empfänger kann auch NACK senden, das zur Neuübertragung führt; NACK wird für die Verbesserung der Bandbreitenausnutzung verwendet, da so der Timer nicht erst ablaufen muss

ACK-Frame gestört: Empfänger des I-Frames sendet ACK an Sender, dieser kommt aber nicht an -> Sender wartet Timeout ab und sendet I-Frame erneut -> Empfänger erkennt Frame als Duplikat und sendet ACK erneut

26) Was ist die Grundidee von Continous-RQ? Welche in der Vorlesung behandelten Protokolle verwenden diese Technik?

um Full Duplex Lines effizienter auszunutzen wird nicht auf ACKs von bereits gesendeten Frames gewartet; Full Duplex Protocol; bis zum Erhalten der ACKs werden die Dataframes in einer Retransmission-List gebuffert; jedes einkommende ACK entfernt den dazugehörigen Dataframe von der Liste; Empfänger speichert Dataframes in einer Receive-List (um Duplikate zu erkennen und die Sequenz zu sortieren – Pakete können in beliebiger Reihenfolge ankommen)

Protokolle, die diese Technik verwenden: z.B. TCP

27) Was ist die Grundidee von Continous-RQ in der Variante „Selective Acknowledgment“?

Bei Selective Acknowledgement muss jedes Paket explizit bestätigt werden. Wird das Paket nicht vor ablaufen des (zugehörigen) Timers bestätigt, so wird es erneut übertragen und ein Eintrag an das Ende der Retransmission-List gestellt. Der Empfänger muss die Reihenfolge wiederherstellen.
Bei Übertragungsfehlern verhält sich Continous-RQ mit Selective Acknowledgement wie Idle-RQ.
Wird ein I-Frame zerstört, läuft der Timer am Sender für das I-Frame aus und es wird erneut gesendet bzw. der Empfänger sendet ein NACK.

Wird das ACK gestört, läuft der Timer am Sender für das zugehörige I-Frame aus und das I-Frame wird erneut gesendet. Der Empfänger erkennt das Duplikat (es wird verworfen) und sendet erneut ein ACK.

jeder Dataframe wird explizit bestätigt; wenn ACK nicht ankommt wird der dazugehörige Dataframe erneut gesendet und am Ende der Retransmission-List gespeichert

28) Wie erfolgt bei Continous-RQ in der Variante „Selective Acknowledgment" die Fehlerbereinigung (Error Recovery) im Fehlerfall (zwei Szenarios: I-Frame gestört, ACK-Frame gestört)? Ist ein Umordnen dabei erforderlich? Ist die Erkennung von Duplikaten erforderlich? Wozu wird der Timer benötigt? Welche Bedeutung hat ein ACK (single oder multiple)?

I-Frame gestört: der I-Frame kommt nicht beim Empfänger an -> es wird vom Empfänger kein ACK gesendet; Timeout beim Sender für den unbestätigten Dataframe -> dieser wird am Ende erneut gesendet; Empfänger muss dann die Dataframes neu ordnen

ACK-Frame gestört: ACK für Dataframe kommt nicht an -> Timeout für den unbestätigten Dataframe -> Dataframe wird am Ende erneut gesendet und durch ACK bestätigt; doppelter Dataframe wird vom Empfänger erkannt und verworfen

Wird ein Paket (Frame) nicht vor Ablauf des zugehörigen Timers bestätigt, so wird es erneut gesendet. Dabei kann die Reihenfolge „durcheinander" kommen und der Empfänger muss die Pakete ordnen und somit eine Liste führen und Duplikate erkennen.
Der Timer wird für die erneute Übertragung der Dataframes benötigt. Jeder Dataframe startet einen eigenen Timer, der erst beendet wird, wenn der ACK-Frame ankommt.
Gibt es keinen Timer, so kann der Verlust eines Pakets vom Sender nicht festgestellt werden.

Bedeutung von ACK: Single (ein ACK bestätigt einen Dataframe)

29) Was ist die Grundidee von Continous-RQ in der Variante „Go-BackN"?

Der Empfänger nimmt zu einem Zeitpunkt immer nur genau das Paket an, das er gerade erwartet. Der Empfänger bestätigt mit einem ACK(n) alle Pakete bis inklusive n.

Im Falle eines Fehlers werden alle Dataframes seit n von einem NACK erneut angefordert.
Alle dem n folgenden Dataframes bis auf den, mit der korrekten Sequenznummer, werden vom Empfänger verworfen.

- ➔ es ist keine Umordnung erforderlich
- ➔ Software des Empfängers kann einfacher gehalten werden

ein einzelner ACK könnte mehrere Dataframes bestätigen (Multiple Acknowledgement) -> ACK-Anzahl kann gering gehalten werden

Jeder übertragene Dataframe startet einen individuellen Timer.

- ➔ wird zurückgesetzt wenn ACK ankommt
- ➔ bei Timeout wird Dataframe erneut gesendet

Szenario:
Empfänger erwartet Paket 1
es kommen an: 3, 2, 1, 4
3 wird verworfen, weil 1 erwartet wird, ebenso 2; 1 wird angenommen -> ACK(1); 4 wird wieder verworfen, weil 2 erwartet wird
Sender wartet vergeblich auf ACK(2) -> Timeout und sendet alle Pakete ab 2 erneut

30) Wie erfolgt bei Continous-RQ in der Variante „Go-BackN" die Fehlerbereinigung (Error Recovery) im Fehlerfall (zwei Szenarios: I-Frame gestört, ACK-Frame gestört)? Ist ein Umordnen dabei erforderlich? Ist die Erkennung von Duplikaten erforderlich? Wozu wird der Timer benötigt? Welche Bedeutung hat ein ACK (single oder multiple)?

I-Frame gestört: Bei dieser Variante des RQ kann ein ACK mehrere Frames bestätigen und im Falle einer fehlerhaften Übertragung eines Frames werden alle Frames bis zum letzten ACK nochmals übertragen; ein Umordnen ist daher nicht erfoderlich.

(I-Frame n gestört: alle nach n folgenden Dataframes werden nicht angenommen; NACK wird gesendet -> alle Dataframes seit n werden neu angefordert; danach jeder Dataframe durch ACK bestätigt)

ACK-Frame gestört: wenn das ACK für das nächste I-Frame ankommt wird auch das vorherige I-Frame (dessen ACK verloren ist) bestätigt (Multiple-ACK); war es der letzte ACK, der gestört wurde, so läuft der Timer für das zugehörige I-Frame ab und das I-Frame wird erneut übertragen; Empfänger erkennt das Duplikat und sendet erneut ein ACK

(ACK(n+1) gestört: macht nichts, denn ACK(n+2) bestätigt alle Dataframes bis (n+2))
Multiple-ACK

31) Was ist die Grundidee von Continous-RQ in der Variante „Positive Acknowledgement“?

Dataframes werden durch ACK bestätigt, solange sie in der richtigen Reihenfolge ankommen; Multiple-ACK möglich; wenn Dataframes nicht mehr in der richtigen Reihenfolge sind, wird die Bestätigung gestoppt; es werden aber alle folgenden Dataframes gespeichert
jeder übertragene Dataframe startet einen individuellen Timer; dieser wird zurückgesetzt wenn ACK ankommt; bei Timeout wird der Dataframe erneut gesendet
Dataframes, die der Empfänger bereits gespeichert hat, können mit Multiple-ACKs bestätigt werden, wenn der fehlende Dataframe ankommt

Wenn also eine Lücke entsteht (Paket gestört), wird erst wieder bestätigt, wenn diese Lücke gestopft ist.

32) Wie erfolgt bei Continous-RQ in der Variante „Positive Acknowledgement“ die Fehlerbereinigung (Error Recovery) im Fehlerfall (zwei Szenarios: I-Frame gestört, ACK-Frame gestört)? Ist ein Umordnen dabei erforderlich? Ist die Erkennung von Duplikaten erforderlich? Welche Bedeutung hat ein ACK (single oder multiple)?

I-Frame gestört: I-Frame kommt nicht an -> keine Bestätigung; auch folgende Dataframes werden nicht bestätigt, aber gespeichert
Timer des unbestätigten Dataframes läuft ab -> fehlender Dataframe wird am Ende erneut gesendet und dann werden durch Multiple-ACK alle Dataframes bestätigt

ACK-Frame gestört:
1) der Dataframe, der nicht bestätigt wurde, wird von einem ACK für ein späteres Paket bestätigt
2) keine weiteren Pakete mehr -> Timer des Senders läuft ab -> erneute Übertragung des Paketes; Empfänger sendet ACK und verwirft Duplikat

Umordnung erforderlich; Erkennung von Duplikaten erforderlich
Multiple-ACK

33) Was ist die Grundidee von Continous-RQ in der Variante „Selective Reject“?

Empfänger speichert alle empfangenen Pakete; Pakete werden aber nur so lange bestätigt, so lange sie in der richtigen Reihenfolge ankommen; Multiple-ACK möglich
im Falle eines Fehlers wird nur der fehlende Dataframe explizit vom Empfänger durch SREJ(n) neu angefordert
Wenn nach dem verlorenen Paket keine Pakete mehr ankommen, erkennt der Empfänger keinen Fehler. Beim Sender läuft allerdings der Timer ab und er sendet das entsprechende Paket erneut.

34) Wie erfolgt bei Continous-RQ in der Variante „Selective Reject“ die Fehlerbereinigung (Error Recovery) im Fehlerfall (zwei Szenarios: I-Frame gestört, ACK-Frame gestört)? Ist ein Umordnen dabei erforderlich? Ist die Erkennung von Duplikaten erforderlich? Welche Verbesserung gegenüber Go-BackN ergibt sich bei der Anwendung dieser Methode?

I-Frame gestört: I-Frame kommt nicht an -> wird nicht bestätigt; I-Frame wird mit SREJ(N) erneut angefordert -> I-Frame wird erneut gesendet und danach werden alle I-Frames bestätigt (Multiple-ACK)

ACK-Frame gestört:
1) ACK kommt nicht an -> durch den nächsten ACK werden alle Dataframes bestätigt (Multiple-ACK)
2) War das Paket, dessen ACK gestört war, das letzte zu sendende Paket, dann läuft beim Sender der Timer ab und das Paket wird erneut gesendet und dann vom Empfänger bestätigt.

Umordnung der Dataframes und Erkennung von Duplikaten ist nötig

Vorteil gegenüber Go-BackN: es müssen nur wirklich verlorene oder gestörte Dataframes erneut übertragen werden

35) Wie werden die für ARQ-Techniken notwendigen Identifier realisiert? Wie wird deren Handhabung mittels Registervariablen realisiert bzw. wie arbeiten die entsprechenden Elemente zusammen?

Identifier der Dataframes sind ansteigende Zahlen: Sequenz-Nummern

Registervariablen sind nötig: V(S), V(R); müssen beim Verbindungs-Setup initialisiert werden (auf 0 gesetzt werden)

V(S): zeigt die Sequenznummer des I-Frames, der als nächstes gesendet wird
V(R): zeigt die Sequenznummer des nächsten erwarteten I-Frames der empfangen werden soll

wird ein Paket gesendet, so wird V(S) um eins erhöht; wird ein Paket empfangen, so wird V(R) um eins erhöht

36) Was versteht man unter piggy-backed Acknowledgement?

ACKs sind in einem Dataframe des Empfängers enthalten; wenn der Empfänger keinen Dataframe zu senden hat -> ACK wird gesendet

37) Was versteht man unter Sendefenster? Wozu wird es benötigt?

die Anzahl W der Dataframes, die für die Retransmission gespeichert sind, muss limitiert sein: W = Sendefenster
wird benötigt, da ohne Limitierung der Zahl der unbestätigten Dataframes Continuous-RQ unendlich viele Identifier und Bufferspeicher benötigen würde
Die Fenstergröße entspricht der Anzahl der Pakete, die ohne ACK gesendet werden können. Wurden alle Pakete innerhalb des Windows gesendet und noch kein ACK dazu empfangen, so wartet der Sender auf ACKs des Empfängers.

38) Wie wirkt sich ein Sendefenster auf Windowing aus? Was versteht man dabei unter „das Window öffnet bzw. schließt sich“? Was versteht man dabei unter „usable“ Window?

Je größer das Fenster ist, desto mehr Speicherplatz wird benötigt (für die Listen, die für den Fehlerfall und Duplikate geführt werden).

Ein Window schließt sich, wenn alle Pakete im Window gesendet wurden. Ein Window öffnet sich, wenn es weiterbewegt wird (wenn also ACKs angekommen sind) und so neue Pakete gesendet werden können.

Usable Window: die Dataframes im aktuellen Window, die noch nicht gesendet wurden

39) Wie wirkt sich ein Sendefenster auf die Anzahl der benötigten Identifier aus? Wie lassen sich dadurch Sequencenumbers durch nummerieren?

Nummerierung der Dataframes kann wegen Window durch Modulo-Operation erfolgen -> weniger Identifier nötig

40) Was versteht man unter „Serialization Delay“? Was versteht man unter „Propagation Delay“? Wieso hat ein Bit auf einer Übertragungsstrecke eine Länge?

Serialization Delay: die Zeit, die benötigt wird, um alle Bits eines Frames „auf die Leitung zu legen“

Propagation Delay: die Zeit, die das Signal (die Bits auf der Leitung) benötigt, um vollständig beim Empfänger anzukommen

Auf Grund der endlichen Ausbreitungsgeschwindigkeit eines Signals bekommt ein Bit eine „Länge“. Länge in m = 1/(Bitrate pro sek) * (Geschwindigkeit in m/s)

41) Was versteht man unter „Delay-Bandwidh“ Produkt?

Das Delay-Bandwidth-Produkt ((Bits pro sek)*RTT – round trip time) gibt an, wie viele Bits in der RTT-Zeit übertragen werden können. Damit kann die Window-Size optimiert werden (das Sendefenster muss groß genug sein, so dass der Sender den Kanal voll ausnutzen kann).

42) Warum sollte das Sendefenster zumindestens die Größe des „Delay-Bandwidh“ Produktes aufweisen?

Ziel ist eine ideale Auslastung der Verbindung. Wenn die Frames eines Windows ca. die Delay-Zeit brauchen, um beim Empfänger anzukommen, so kann der Empfänger mit dem Versenden der ersten ACKs (für die bereits empfangenen Frames) beginnen, während der Sender noch Pakete sendet. So wird Zeit und Kapazität gespart bzw. besser ausgenützt.
Ist das Sendefenster zu klein, muss die Übertragung immer wieder gestoppt werden, bis das ACK da ist.

43) Was versteht man unter Flußkontrolle (Flow Control)? Wie kann sie realisiert werden?

wenn Dataframes schneller ankommen, als sie der Empfänger verarbeiten kann -> Empfänger hat nicht mehr genug Bufferspeicher und muss gute Dataframes verwerfen -> müssen neu übertragen werden -> werden wegen zu wenig Buffer wieder verworfen
Empfänger sollte Übertragungsrate der Dataframes kontrollieren (Flow Control); Flow-Control-Messages, die dem Sender Bufferoverflows mitteilen; Sender stoppt und wartet bis Empfänger wieder Dataframes verarbeiten kann
Flow-Control basiert auf Flow-Control-Frames und Windowing
im Falle eines Staus: Empfänger signalisiert Stopp -> Sender unterbricht; Empfänger signalisiert Go, wenn Datenfluss weitergehen kann

44) Warum reicht Windowing für Flow Control alleine nicht aus?

Nach einem Timeout werden unbestätigte Frames erneut übertragen. Nach einer bestimmten Anzahl an nicht erfolgreichen Übertragungen, wird die Verbindung als unterbrochen angesehen.

45) Was versteht man unter „adaptive Windowing“?

Um den Datenfluss zu kontrollieren, wird die Window-Size variiert. Der Startwert der Fenstergröße wird beim Verbindungsaufbau ausgehandelt und während der Übertragung dynamisch an den optimalen Wert angepasst, so dass der Empfänger nicht überlastet und die Leitung ideal genutzt wird.
Beispiel: TCP

Chapter 3 – TDM Techniques

46) Was versteht man unter Multiplexen im Allgemeinen und unter Time Division Multiplexen im Speziellen?

Multiplexen: mehrere Sender/Empfänger tauschen Daten über eine physikalische Leitung aus

Time Division Multiplexen: es wird jedem Kanal eine bestimmte Zeitperiode lang die Leitung zugeteilt

47) Wie geht man bei synchronem TDM vor? Welche Bandbreite auf der Trunk-Leitung benötigt man? Benötigt man Adressierung? Wäre Flow Control wünschenswert? Was passiert in Übertragungspausen eines Channels? Kann die Bandbreite von einem anderen Channel genützt werden?

In einem periodisch generierten Frame befindet sich eine gleich bleibende Anzahl an Zeitschlitzen mit gleicher Länge. Die Zeitschlitze können durch ihre Position im Frame identifiziert werden. Es wird also keine Adressierung benötigt.
Somit besitzt jeder Eingangskanal einen eigenen Zeitschlitz. Hat ein Sender nichts zu senden, so bleibt die Trunk ungenutzt – steht als auch keinem anderen Kanal zur Verfügung (Bandbreitenverschwendung).

Flow-Control ist nicht notwendig, da jedem Teilnehmer fixe Zeitschlitze zugeordnet sind.

Trunk-Speed = (Anzahl der Zeitschlitze) * (User Access Rate)

48) Wie geht man bei asynchronem (statistischen) TDM vor? Wie ist die Bandbreite auf der Trunk-Leitung ausgelegt? Benötigt man Adressierung? Wäre Flow Control wünschenswert? Was passiert in Übertragungspausen eines Channels? Kann die Bandbreite von einem anderen Channel genützt werden?

Geräte kommunizieren in statistischer Art und Weise: nicht alle Geräte haben Daten, die zur gleichen Zeit übertragen werden müssen; die Bandbreite wird nicht fix aufgeteilt, sondern dem Datenverkehr angepasst
wenn Geräte gleichzeitig übertragen: nur ein Kanal kann Trunk Line besetzen; Daten müssen im Multiplexer gebuffert werden, bis Trunk wieder verfügbar ist
man benötigt Adressierung, um jeden Zeitschlitz identifizieren zu können
Mechanismus, der verhindert, dass die Trunk nicht nur von einem einzigen Kanal benutzt wird, muss implementiert werden

Die Bandbreite der Trunk-Line wird nach dem durchschnittlichen Datenumsatz ausgelegt.

Hat ein Kanal nichts zu senden, kann die Leitung von einem anderen benützt werden. Möchte ein Sender mehr senden, als er momentan an Zeitschlitzen hat, dann kann ihm entweder mehr Kapazität (Zeitschlitze) zugeteilt werden, oder er wird angehalten zu warten/langsamer zu senden (Flow-Control).

49) Zählen Sie die Vor- und Nachteile des synchronen TDM auf?

Vorteile:
- minimale Verzögerungen
- Protokoll-Transparent
- für das Endsystem erscheint die Leitung wie eine normale Point-to-Point-Verbindung

Nachteile:
- hohe Bitrate wird benötigt (teuer)
- in Übertragungspausen bleibt die Leitung ungenützt

50) Zählen Sie die Vor- und Nachteile des asynchronen TDM auf?

Vorteile:
- variable Aufteilung der Bandbreite
- bessere Ausnützung der Trunkline
- Trunkline kann langsamer ausgelegt sein

Nachteile:
- Datenquellen kommunizieren zu verschiedenen Zeiten (statistische Verteilung)
- Daten müssen evtl. im Multiplexer zwischengespeichert werden, bevor die Leitung frei wird -> längere, variable Verzögerung
- Adressierung notwendig
- nicht Protokoll-Transparent

51) Was besagt das Nyquist Theorem? Wie wird es bei der Digitalisierung von analoger Sprache angewendet? Wofür steht PCM? Welche Bitrate wird für PCM Sprachkanal benötigt?

Nyquist Theorem (Frage 16):
beschäftigt sich damit, wie viele Bits über eine ideale (rauschfreie) Leitung transportiert werden können

$R = 2*B*\log_2(V)$
R … maximale Bitrate in Bit/s, B … Bandbreite in Hz, V … Anzahl der Signallevel

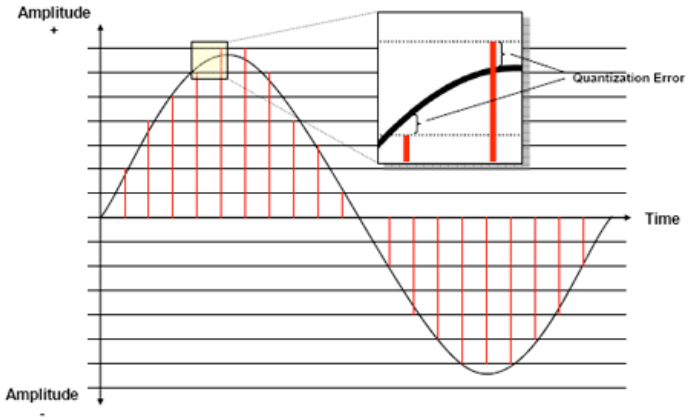
Das Theorem besagt, dass ein beliebiges (gefiltertes, Tiefpass) Signal der Bandbreite B durch eine Abtastrate von 2B vollständig wiederhergestellt werden kann. Wobei eine Abtastrate von mehr als 2B höchstens (nutzlose) Anteile höherer (bereits gefilterter) Frequenzen entdecken würde. Die Formel gilt für V diskrete Stufen.

jedes analoge Signal mit maximaler Frequenz f_B kann mit der Abtastfrequenz fs abgetastet (gesampelt) und rekonstruiert werden, wenn gilt: fs = 2*f_B.

analoge Sprache kann mit Verwendung von Pulse-Code-Manipulation (PCM) digitalisiert werden; es wird ein digitaler 64-kbit/s-Kanal benötigt
Stimme wird alle 125 usec gesamplet (8000x pro sek.)
jedes Sample wird in 8 Bit kodiert
(Abtastrate = 8000 Samples/sek., 8 Bits/Sample -> ergibt 64 000 Bit/sek.)

52) Was ist der Quantisierungsfehler? Warum verwendet man eine logarithmische Kurve und nicht eine lineare Kurve zur Quanitisierung? Wie sieht ein PCM Sample aus?

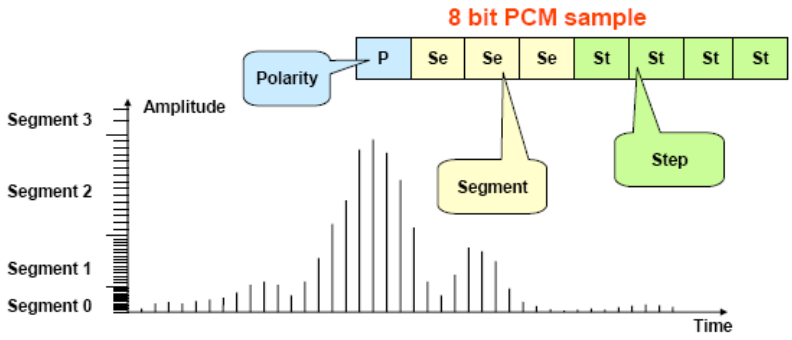
Quantisierungsfehler entstehen bei der analog-digital-Umsetzung von Signalen. Während analoge Signale dem Wertebereich der reellen Zahlen genügen, werden in der digitalen Darstellung Dezimalbrüche mit endlicher Genauigkeit verwendet. Daher muss bei der Umsetzung/Umwandlung gerundet werden. Der entstehende Rundungsfehler ist der Quantisierungsfehler.



gleichförmige (lineare) Quantisierung: gleich große Intervalle

Quantisierungsfehler machen sich bei kleinen Signalwerten stärker bemerkbar (Quantisierungsrauschen)
kleine Unterschiede werden bei leisen Signalen stärker wahrgenommen als bei lauten
=> um die Signalqualität zu verbessern, werden niedrigere Amplituden mit Hilfe der logarithmischen Quantisierung besser aufgelöst (feinere Sampling-Stufen bei niedrigen Amplituden Levels) -> bessere Signalqualität für leisere Sprachteile

PCM-Sample:



Das analoge Signal wird mit einer bestimmten Frequenz in zeitgleichen Abständen abgetastet. Es entsteht ein pulsamplitudenmoduliertes Signal (PAM) mit zunächst beliebig vielen Amplitudenwerten. Das PAM-Signal wird nun mit einem AD-Wandler quantisiert; dazu werden die Amplitudenwerte in eine begrenzte Zahl

von Quantisierungsstufen (=Samplingtiefe) eingeteilt. Aus jedem quantisierten Abtastwert wird ein Codewort berechnet, das die Amplitudeninformation beinhaltet. Aus der zeitlichen Folge der Codeworte, wird ein Digitalsignal erzeugt. Die Anzahl der möglichen Quantisierungsstufen n ergibt sich aus der Anzahl z der Bits, die ein Codewort hat.

Bei der Rückumwandlung deckt sich das Signal nicht mehr mit dem Ausgangssignal, da es in endlich viele Quantisierungsstufen eingeteilt wurde.

53) Welcher Trick wird bei ADPCM angewendet? Was erreicht man damit?

ADPCM … Adaptive Differential Pulse Code Manipulation

es wird nur der Unterschied von einem Sample-Pulse zum nächsten übertragen; weniger Bits werden zum Kodieren des Unterschieds benötigt

54) Wozu dienen synchrone TDM Multiplexer-Hierachien? Welche zeitlichen Anforderungen muss ein Rahmen prinzipiell erfüllen?

Nur eine hierarchische digitale Multiplexing-Infrastruktur, die standardisiert ist, kann Millionen von (Low-Speed) Kunden in der Stadt/dem Land/der Welt verbinden.

Man unterscheidet zwei Hauptarchitekturen: PDH und SDH.

PDH: synchrone Übertragung: Zeitdifferenzen werden mit Bitstuffing ausgeglichen; wird für Niedriggeschwindigkeitsleitungen benutzt; kann für höhere Geschwindigkeiten nicht benutzt werden, da der Overhead dabei drastisch ansteigt.

SDH: übergeht Nachteile von PDH (steigender Overhead, verschiedene Multiplexing-Strukturen, Wechsel von Kanälen erfordert demultiplexen)

55) Was ist PDH? Wo liegen die Limitierungen? Wodurch sind diese prinzipiell bedingt? Ist Add/Drop Multiplexing eines Sprachkanals ohne Durchlaufen der gesamten Hierarchie möglich?

PDH: plesiochronous digital hierarchy

plesio = beinahe synchron
synchrone Übertragungs-Zeitdifferenzen werden mit Bit-Stuffing ausgeglichen

Limitierungen: kann für höhere Geschwindigkeiten nicht benutzt werden, weil der Overhead mit hohen Bitraten dramatisch ansteigt
Add/Drop-Multiplexing ist wegen der unterschiedlichen Länge (je nachdem, wie viele Bits gestufft wurden) nicht möglich

56) Was ist SDH? Wie erfolgt die Taktung? Ist Add/Drop Multiplexing eines Sprachkanals ohne Durchlaufen der gesamten Hierarchie möglich?

SDH … synchronous digital hierarchy
übergeht Nachteile von PDH (steigender Overhead, verschiedene Multiplexing-Strukturen, Wechsel von Kanälen erfordert demultiplexen)
weiters forderte man ein echtes synchrones Netzwerk; Add/Drop-Multiplexing ist möglich

Chapter 4 – Network Principles

57) Auf welchem TDM Verfahren beruht die Leitungsvermittlung (circuit switching)? Welche Eigenschaften erbt damit Circuit Switching von diesem TDM Verfahren? Wodurch wird ein Zeitmultiplexer (TDM Switch) netzwerkfähig?

Die Leitungsvermittlung beruht auf synchronem TDM. Damit erbt Circuit-Switching folgende Eigenschaften: minimale Verzögerung; hohe Bitrate auf den Trunk-Lines; ungenutzte Timeslots, wenn nichts übertragen wird; Protokoll-Transparenz.

Netzwerkfähig durch: eine Circuit-Switching-Table (welche Leitung mit welcher „verbinden“): statisch (durch Admin festgelegt, unflexibel); dynamisch (Einträge werden durch ein Management-Protokoll festgelegt; Soft-Permanent-Circuit-Switching); on demand -> bei Verbindungsaufbau wird eine Route gesucht

58) Was wird dabei in einer in der Circuit-Switching Tabelle festgehalten? Was ist ein Transit-Switch? Warum ist es günstig TDM auch am Access Port anzuwenden?

In einer CS-Tabelle ist festgehalten, welcher Timeslot von welcher Leitung zu welchem Timeslot auf welcher Leitung verbunden werden soll. Beispiel: Leitung 1 (Timeslot 3) zu Leitung 2 (Timeslot 5).
Ein Transit-Switch ist ein Switch, der einkommende Trunk-Leitungen auf eine Trunk-Leitung mappt (die Timeslots werden gemappt) – ein Switch, der nicht direkt mit den Endgeräten verbunden ist.
TDM am Access-Port ist deshalb günstig, weil so mehrere verschiedene virtuelle Verbindungen auf einem Kabel übertragen werden können. Das Mapping kann wie bei Trunk-Leitungen erfolgen.

59) Was versteht man unter einem „permanent circuit service“? Wie bezeichnet ein Service Provider dieses Service? Was wird durch „soft permanent circuit service“ daran verbessert?

permanent circuit service = eine permanente Verbindung (permanente Einträge in den CS-Tabellen); basiert auf redundanten, synchronen TDM-Netzwerken; Provider nennen dies „digital leased line“

soft permanent circuit service:
dynamische (fail safe) Switching-Tabelle: Einträge werden automatisch vom TDM-Netzwerk-Management-Protokoll geändert, um zu einem redundanten Pfad umzuschalten, falls eine Trunk-Line nicht funktioniert

60) Was versteht man unter einem „switched circuit service“? Wozu benötigt man dabei Signalisierung? Welche bekannte Netzwerktechnologie beruht auf dieser Technik?

Dabei wird durch ein Signal-Protokoll ein Pfad im Circuit-Switched-Network gesucht**,** bevor Daten übertragen werden können. Die dynamischen Einträge in den Switching-Tabellen werden bei Bedarf generiert.
Die Signalisierung ist notwendig, um die Verbindung zwischen zwei Switches aufzubauen oder abzubauen.
Beispiel: ISDN Signaling System 7 (SS7)

61) Was ist ISDN BRI? Wie viele Nutzkanäle gibt es dabei? Wozu dient der D-Kanal? Wieso benötigt man am D-Channel eine Access-Control (Zugriffs-Kontrolle)?

BRI … Basic Rate Interface (wurde für den normalen Konsumenten entworfen)
2 Nutzkanäle (B – bearer) mit je 64 kbit/s für digitalisierte Sprache oder Daten; 1 Datenkanal (D – data) mit 16 kbit/s Signaling-Zwecke.
Access-Control am D-Kanal wird benötigt, weil mehrere Geräte um die Bandbreite konkurrieren (Fax, Telefon, PC, …)

62) Was ist ISDN PRI? Wie viele Nutzkanäle gibt es dabei? Wozu dient der D-Kanal? Wieso benötigt man am D-Channel keine Access-Control?

PRI … Primary Rate Interface (wurde für Business-Kunden entworfen)

30 Nutzkanäle mit je 64 kbit/s; 1 D-Kanal mit 64 kbit/s

Access-Control ist nicht notwendig, weil niemand um die Bandbreite konkurriert (nur Point-to-Point-Verbindungen).

63) Auf welchem TDM Verfahren beruht die Paketvermittlung (packet switching)? Welche Eigenschaften erbt damit Packet Switching von diesem TDM Verfahren?

beruht auf asynchronem TDM (die Timeslots werden nicht fix, sondern dynamisch (statistisch) aufgeteilt)

Eigenschaften, die Packet-Switching von asynchronem TDM erbt:
- es wird keine Bandbreite für Idle-Pattern vergeudet
- nicht Protokoll-Transparent
- Adressierung notwendig
- Verzögerung ist variabel und gegebenenfalls höher als bei synchronem TDM

- weniger Bandbreite auf der Trunk nötig
- keine Any-to-Any-Topologie notwendig

64) Beschreiben Sie das Grundprinzip des Packet Switching. Wozu benötigt man Adressinformation? Wie erfolgt das Forwarding prinzipiell? Wozu dienen redundante Wege?

Pakete werden auf Grund der Adressinformation (in den Headern der Pakete gespeichert) und einem passenden Eintrag in einer Tabelle weitergeleitet und gelangen so zum Empfänger. In den Tabellen wird im Grunde nur gespeichert, wie ein Paket von Adresse A nach Adresse B kommt. Die Adressinformation wird benötigt, um zu entscheiden (der Router/Switch tut dies), an welche Leitung das Paket weitergegeben werden soll (Forwarding).
Fowarding: Ein Paket mit der Sourceadresse A und der Zieladresse B kommt am Interface 4 des Routers/Switches an. Nun steht in der Tabelle des Geräts z.B.: bei Zieladresse B gib das Paket an Interface 6 weiter (abschicken/weitersenden).
Redundante Wege ermöglichen es zum einen, die Last gleichmäßig zwischen zwei Wegen aufzuteilen und zum anderen ermöglichen Sie den weiteren Netzverkehr, für den Fall, dass eine Leitung ausfällt.

65) Warum sollten die Adressen bei Packet-Switching strukturiert sein und die Adressierung der physikalischen Struktur eines Netzwerkes folgen?

Da nur so die Router (Geräte, die das Forwarding von Paketen übernehmen) eindeutig entscheiden können, wie ein Paket weitergeleitet werden soll.
Wären die Adressen mehrdeutig oder würden sie nicht mit der Topologie übereinstimmen, so würden Pakete im schlimmsten Fall gar nicht beim Empfänger ankommen.

66) Was sind Routingtabellen? Was wird in einer Routingtabelle festgehalten? Wie werden sie erstellt?

In Routingtabellen wird gespeichert, wie ein Paket mit der Zieladresse X an ihr Ziel kommt. In einer Routingtabelle wird daher pro Zeile mindestens folgendes gespeichert: Zieladresse und Interface (oder line) an das das Paket weitergehen soll.

statisches Routing: Routing-Tabellen sind vorkonfiguriert, werden vom Netzwerk-Administrator erstellt; Nachteil: ber Änderungen in der Topologie reagiert der Router nicht automatisch

dynamisches Routing: Routing-Tabellen werden vom Routing-Protokoll erstellt

67) Welche Services lassen sich bei Packet-Switching prinzipiell unterscheiden? Wozu werden dabei die Routingtabellen verwendet? Wann und wozu benötigt man Switchingtabellen beim Packet-Switching?

connection-oriented service (CO): Routing-Tabellen werden genutzt, um Einträge für Switching-Tabellen zu generieren; nach der Herstellung der Verbindung werden die Switching-Tabellen genutzt, um die Weiterleitung der Datenpakete zu kontrollieren

connection-less service (CL): Routing-Tabellen werden genutzt, um die Weiterleitung von jedem Paket zu kontrollieren

68) Geben Sie die Basiseigenschaften bzw. auch Vor- und Nachteile von Packet-Switching bei Connectionless Service an. Welche bekannte Netzwerktechnologie beruht auf dieser Technik?

Pakete können gesendet werden, ohne dass vorher eine logische Verbindung zwischen den Endsystemen hergestellt wird; Pakete haben keine Sequenznummer; kein Flow-Control; Pakete können von Packet-Switches verworfen werden (bei Netzwerk-Stau, Übertragungsfehlern); jedes Paket wird einzeln geroutet/geswitcht, daher ist nur ein geringer Overhead notwendig (weniger Info im Header eines Pakets); jedes Paket beinhaltet die komplette Adressinformation (Ziel- und Quelladresse); variable Verzögerung; Lieferung von Paketen wird vom Netzwerk nicht garantiert

IP beruht auf dieser Technik

69) Wieso benötigt man bei Connectionless Service einen Kill-Mechanismus? Wodurch wird er bei IP implementiert?

falls Routingtabellen falsch/beschädigt sind, kann es vorkommen, dass Pakete im „Kreis“ geschickt werden => Kill-Mechanismus
Bei IP wird das durch einen „Eintrag“ im Header eines jeden Pakets erreicht. Dieser „Eintrag“ heißt TTL (Time To Live) und war einst für Zeit in Sekunden gedacht und wird heute als Hop-Count (Wie viele Router darf das Paket passieren?) verwendet. Ist die TTL gleich 0, so wird das Paket vom Router zerstört.

70) Was passiert wenn eine Trunk-Leitung bzw. ein Packet-Switch bei Packet-Switching im Connectionless Service ausfällt (Annahme redundante Leitung und dynamisches Routingprotokoll)?

Zuerst können die Pakete, die die ausgefallene Trunk-Leitung passieren hätten müssen, nicht zugestellt werden. Dies geht solange nicht, bis das dynamische Routing-Protokoll einen alternativen Weg gefunden hat. Normalerweise generiert ein Router, der ein Paket nicht zustellen kann, eine ICMP-Meldung.

71) Wie erfolgt beispielhaft der Verbindungsaufbau bei Packet-Switching im Connectionoriented Service? Wozu dient der „Local Connection Identifier“? Welche Rolle spielen dabei Routingtabellen und Switchingtabellen?

Es werden zwei PCs A und B angenommen. A will eine Verbindung zu B aufbauen. A schickt ein Call-Setup-Packet an B. Die Router zwischen den beiden Endgeräten suchen für das erste Setup-Packet einen Weg von A nach B und bauen dabei Switching-Tabellen (für die Nutzdatenpakete) auf. Danach schickt B eine positive Antwort (bei einer negativen Antwort wird die Verbindung beendet und die Switching-Tabellen werden zerstört) an A. Das zweite Setup-Packet läuft den Weg des ersten „rückwärts“. Danach müssen A und dann B noch ein ACK für die Verbindung schicken und es können Daten übertragen werden.
Der Identifier identifiziert die Verbindung nur zwischen zwei Devices eindeutig, hat also nur lokale Bedeutung.
Die Routing-Tabellen werden für das erste Setup-Packet gebraucht (muss zu B gelangen) und nach dem ersten Setup-Packet sind auch die Switching-Tabellen erzeugt.

72) Was passiert, wenn eine Trunk-Leitung bzw. ein Packet-Switch nach erfolgtem Verbindungsaufbau bei Packet-Switching im Connectionoriented Service ausfällt (Annahme redundante Leitung und dynamisches Routingprotokoll)?

Die Virtual-Circuits werden geschlossen und müssen von den Endsystemen mit Call-Setup-Packets neu aufgebaut werden.
Wenn es zumindest einen redundanten Pfad gibt, können die Packet-Switches über diesen einen neuen Virtual-Circuit herstellen.

73) Geben Sie die Basiseigenschaften von Packet-Switching bzw. auch Vor- und Nachteile von Packet-Switching bei Connectionoriented Service an.

Basiseigenschaften: asynchrones, statistisches TDM in einem Netzwerk
Das Netzwerk besteht aus Endgeräten, Switches, Trunks zwischen Switches und Access-Lines zwischen Switch und Endgerät.
Die Endgeräte zerstückeln die Daten in Pakete und senden sie ab. Die Switches leiten sie entsprechend der Zieladresse weiter.
Packet-Switching hat allgemein den Vorteil, dass der Zwischenweg, den Pakete nehmen, dem Sender und dem Empfänger nicht bekannt sein muss (Abstraktion).
Vorteile (Connection-Oriented): Ressourcen können reserviert werden; Quality of Service (QoS) kann angeboten werden; die Endsysteme glauben, eine Punkt-zu-Punkt-Verbindung zu nutzen. Außerdem weiß der Sender, dass der Empfänger die Pakete bereitwillig annimmt; Flow-Control ist sehr gut möglich (keine Overflows); Verbindung kann abgelehnt werden, wenn QoS nicht garantiert werden kann

Nachteile (Connection-Oriented): Verbindungsaufbau benötigt Zeit; System ist komplexer -> intelligentere Geräte notwendig

74) Warum nennt man Packet-Switching im Connectionoriented Service auch Virtual Circuit Technik? Wodurch ist die Anzahl der virtual circuits begrenzt? Was ist in diesem Zusammenhang SVC und PVC Betrieb? Welche bekannten Netzwerktechnologien beruhen auf dieser Technik?

CO-Services werden deshalb auch Virtual-Circuit-Technik genannt, weil der Verbindungsaufbau mit dem Suchen einer Verbindung bei Circuit-Switching (oder beim Telefonieren) vergleichbar ist, nur dass Tabellen erstellt und keine Leitungen durchverbunden werden.
Die Anzahl der VCs ist durch den Speicher der Router und durch die Anzahl der möglichen Logical-Identifier begrenzt.

SVC: VC muss durch Setup aufgebaut werden
PVC: Provider richtet permanente Verbindung ein

Beispiele: ATM, X.25, Frame Relay

75) Was ist die Grundidee des OSI Referenzmodells (Stichwort Layers, Services, Protocols)? Worauf bezieht sich das „open"? Hilft das OSI Referenzmodell bei der Erstellung von rechner-internen Standards?

Die Kommunikation zwischen Systemen kann eine komplizierte Aufgabe sein, somit trennt man sie in mehrere Sub-Tasks, sogenannte Layers. Jeder Layer implementiert nur einen Teil des gesamten Kommunikationssystems.
Eine Schicht kann der oberen Services anbieten und die Services der unteren nutzen. So ist es auch möglich (klar definierte Schnittstellen vorausgesetzt), eine Schicht zu ändern, ohne die Anderen zu beeinflussen. Daher das „open": Es bezieht sich auf „offene" Systeme zur Kommunikation (unabhängig von dem, der es implementiert).
Für Rechner-interne-Standards hilft es nicht, da das OSI-Modell nur die Kommunikation zwischen zwei Systemen regelt, nicht aber die Kommunikation im System selbst.

76) Was ist - im Zusammenhang mit OSI - Encapsulation / Decapsulation und welcher Vorteil und Nachteil ist damit verbunden? Was ist ein OSI Intermediate System?

Encapsulation: Daten einer oberen Schicht werden als Rohdaten für die untere Schicht angesehen und noch einmal in einen Schicht-spezifischen Header/Trailer verpackt.

Decapsulation: Die untere Schicht entfernt die Schicht-spezifischen Daten (Header/Trailer) und gibt die „ausgepackten" Daten nach oben weiter.

Vorteil: Für jede Schicht sieht es so aus, als würde sie mit der Schicht auf dem anderen Rechner direkt kommunizieren.
Nachteil: viel zusätzlicher Overhead (viele Header/Trailer)

OSI-Intermediate-System: alle Geräte, die Pakete verarbeiten und dann weiterleiten (store and forward); Packet-Switches; alle Geräte, die nur auf Schicht 1-3 arbeiten

77) Geben Sie für folgende Komponenten deren Lage bezüglich OSI Layer an: Repeater, SDH-Switch, Bridge, Ethernet-Switch, IP-Router, X.25-Switch, Frame-Relay-Switch, ATM-Switch. Warum ist es für X.25-Switch, Frame-Relay-Switch und ATM-Switch so schwierig deren Lage bezüglich OSI Layer an zugegeben (Stichwort: Betrachtungsweise vor und nach dem Aufbau eines virtual circuits)?

Repeater: Layer 1; SDH-Switch: Layer 1; Bridge: Layer 2; Ethernet-Switch: Layer 2; IP-Router: Layer 3; X.25-Switch: Layer 3; Frame-Relay-Switch: Layer 2; ATM-Switch: Layer 2

Die Lage für X.25-Switch, Frame-Relay-Switch und ATM-Switch ist schwierig anzugeben, weil diese Protokolle bevor eine Verbindung steht auf Level 3 arbeiten und danach auf Level 2.

Chapter 5 – Local Area Networks (LANs) and Legacy Ethernet

78) Was sind die grundlegenden Charakteristiken von LANs?

Ausdehnung eines LANs kann derzeit bis zu ein paar km betragen. Geräte in einem LAN greifen alle auf ein Medium (Kabel) zu. Alle Geräte sind gleichberechtigt (kein Master/Slave) und können beliebig miteinander kommunizieren.
Die Datenrate beträgt bis zu 10 Gbit/s. Es sind verschiedene Topologien zulässig: Bus-, Stern- oder Ringtopologie. Bei Multipoint-Lines sind besondere Zugriffsmechanismen und Adressen notwendig.

Access Control ist nötig (Media Access Control - MAC); Adressing ist nötig; Messages, die eine Station sendet, erreichen alle anderen Stationen im LAN; Layer 1 und Layer 2 des OSI-Modells sind ausreichend, um die Kommunikations-Aspekte von LAN zu erfüllen

79) Welche OSI Schichten sind für eine Kommunikation innerhalb eines LANs notwendig? Warum ist bei LANs eine Aufteilung der OSI-Schicht 2 in zwei Subschichten LLC und MAC notwendig?

Die Schichten 1 und 2 sind ausreichend für eine Kommunikation innerhalb eines LANs.
OSI-Layer 2 wurde eigentlich für Point-to-Point-Verbindungen entwickelt, was bei LAN nicht der Fall ist (LAN: Multipoint-Line, Shared Media). Deshalb wurde der Layer 2 in LLC (Logical Link Control) und MAC (Media Access Control) geteilt.

MAC regelt den Zugriff auf das geteilte Medium und war bei OSI nicht vorgesehen.
- Adressierung der Systeme
- Prüfsumme

LLC erledigt die Data-Link-Aufgaben nach OSI.
- Adressierung des Service-Access-Points (IP, IPX oder NetBEUI etc.)
- Typ des Services (Connectionless oder Connection-oriented)

80) Welche prinzipielle Aufgaben erfüllt LLC-Layer (Services, Funktion von DSAP/SSAP- und Control-Feld)?

Diese Schicht kann als ein Multiplexer von Kommunikationsprotokollen interpretiert werden. Es umfasst die Adressierung der Service-Access-Points (SAP) der Endsysteme, nicht die Adressierung der Endsysteme. Im LLC-Layer wird auch die Art des Dienstes festgelegt; LLC spezifiziert vier Dienstmethoden:
- Klasse 1: verbindungsloser Datagrammdienst
- Klasse 2: verbindungsorientierter Datagrammdienst
- Klasse 3: Klasse 1 plus Acknowledgement
- Klasse 4: Klasse 2 plus Acknowledgement

DSAP (Destination Service Access Point) und SSAP (Source Service Access Point) dienen der Identifizierung der höheren Protokollprozesse der Ziel- und Absendersysteme.
Das Controlfeld (8 oder 16 Bit) enthält Steuerinformationen für Hilfsfunktionen wie z.B. Datenflusssteuerung.

81) Welche prinzipiellen Aufgaben erfüllt MAC-Layer?

Diese Teilschicht wird zur Steuerung des Medienzugriffs (CSMA/CD) benutzt und signalisiert spezielle Zustände des physikalischen Mediums, wie „Medium belegt“, „Medium frei“ oder „Kollision auf dem Medium“.
Der MAC-Layer übernimmt auch die Adressierung der Endsysteme:
Jede Station ist durch die eindeutige MAC-Adresse ansprechbar. MAC-Layer ist verantwortlich dafür, ob ein Paket an die höheren Schichten weitergeleitet wird oder nicht, falls MAC-Adresse = Zieladresse.

82) Wie sind MAC-Adressen aufgebaut? Wie erfolgt die Broadcastadressierung? Was ist eine Multicast-Adresse? Was ist die BIA? Was sind „IEEE globally administered Addresses“? Können BIA Adressen überschrieben werden?

MAC-Adresse:
6 Byte (48 Bit)
I/G (Individual/Group) Bit: 0 … individual address, 1 … group address
U/L (Universal/Local) Bit: 0 … universal verwaltet, 1 … lokal verwaltet

alle 48 Bit auf 1 gesetzt = Broadcast-Adresse

Eine Multicast-Adresse ist eine MAC-Adresse, bei der das erste Bit 1 ist. Eine Multicast-Adresse ist ein Broadcast für eine Gruppe (group broadcast).

„IEEE globally administered Adresses“ sind von IEEE administrierte Adressen. IEEE gibt Herstellern von Netzwerkkomponenten einen Code, der dann Teil der BIA (Burn-In Address) einer Netzwerkkomponente ist. Diese MAC-Adresse ist dem Produkt fest zugewiesen. BIAs können z.B. durch LAAs (Locally Administered Address) überschrieben werden.

83) Wann empfängt ein Ethernet-Controller einen Rahmen (Stichwort Ziel-MAC-Adresse) und gibt diesen an höhere Layer weiter? Was bedeutet das für die Performance des entsprechenden Systems (Stichwort Interrupt)?

Jeder Rahmen wird durch den Ethernet-Controller (wegen LAN-Verhalten) empfangen. Nur wenn die Ziel-MAC-Adresse und die Station-MAC-Adresse übereinstimmen, leitet der Controller den Frame zu den höheren Schichten weiter.
Der Controller interrupted normalerweise die CPU der Station, wenn der Rahmen für die höheren Schichten bestimmt ist; wenn nicht, wird er still verworfen.

84) Charakterisieren Sie kurz die ursprünglichen Aspekte (Topologie, Ankopplung, Reichweite, Kollisionserkennung, Coding, Baseband oder Broadband Transmission) des IEEE 802.3 LANs (das sind Ethernets auf Basis 10Base5 bzw.10Base2).

Topologie: Bus
Ankopplung: bei 10Base5 mit Vampirtransceivern, bei 10Base2 mit Coax-T-Steckern
Reichweite: bei 10Base5 500m, bei 10Base2 185m
Kollisionserkennung: CSMA/CD; konkrete Erkennung: DC-Anteil > -40mA -> Kollision
Coding: Manchester mit -40mA DC-Anteil
Baseband vs. Broadband: 10Base5 und 10Base2 mit Baseband, 10Broad36 als Einziges mit Broadband

85) Was bedeutet CSMA/CD und wie funktioniert dieses Verfahren? Was bedeutet dabei „Truncated Exponential Backoff“? Auf welche Anzahl sind die Wiederholungsversuche maximal limitiert? Ist Ethernet ein deterministisches Medium?

CSMA/CD = Carrier Sense Multiple Access / Collision Detection

Das Verfahren nimmt bewusst Kollisionen von Datenpaketen in Kauf. Jede Arbeitsstation in einem Netzwerk kann versuchen, zu jeder Zeit Daten zu versenden („wahlfreier Zugriff“). CD wird durch gleichzeitiges Mitlesen der gesendeten Information und dessen Vergleich realisiert. Bei einer Kollision auf dem Übertragungsmedium werden Signale ausgelöscht bzw. verstärkt. Stellt dies nun eine der beiden sendenden Stationen fest, bricht sie den Sendevorgang ab und generiert ein Störsignal (JAM-Signal), das anderen Stationen die Kollision mitteilt. Nach dem Störsignal befindet sich das Übertragungsmedium im Ruhezustand.

Exponential Backoff liefert die maximale Auslastung der Bandbreite:
- nach einer Kollision; setze: Standardverzögerung = Slot-Time
- totale Verzögerung = Standardverzögerung * Zufallszahl
- 0 <= Zufallszahl < 2^k (k = min(Anzahl der Übertragungsversuche, 10))

Truncated Exponential Backoff: k <= 10

Nach der Kollision versuchen die Stationen zufällig nach einer oder zwei (2^1) Slot-Times von je 51,2 µs erneut ihre Sendung zu übertragen. Beim nächsten Versuch wird wieder per Zufall ein neuer Starttermin ausgewählt, dieses Mal allerdings aus vier Möglichkeiten: 0, 1, 2 oder 3 Slot-Times, also 2^2.
Bei einer erneuten Kollision sind es dann 2^3 = 8 Möglichkeiten, dann 16, 32, 64, 128, 256, 512 und schließlich 1024. Auch bei der 11.-15. Kollision bleibt es bei maximal 1024 Möglichkeiten.
Nach 16 erfolglosen Übertragungsversuchen mit Kollision wird abgebrochen.
Ethernet ist kein deterministisches Netzwerk.

86) Was ist das Collision-Window bzw. die Slot-Time bei Ethernet? Welche Auswirkungen hat dieses auf die minimale Rahmenlänge? Warum ist die maximale Rahmenlänge ebenfalls limitiert? Was bedeutet das für die maximale Ausdehnung eines 10MBit Ethernets? Was bedeutet das für die maximale Ausdehnung eines 100MBit bzw. 1000Mbit Ethernets?

Die maximale Zeit, die benötigt wird, um eine Kollision („collision window“ bzw. „slot time“) zu erkennen, ist ca. gleich der zweifachen Signallaufzeit zwischen den zwei weit Entferntesten Stationen im Netzwerk.
Man hat zuerst eine maximale Ausdehnung festgelegt (Slot-Time = [maximale Signallaufzeit (zwischen den zwei Entferntesten Stationen)]*2), dann eine minimale Rahmenlänge so definiert, dass die Worst-Case-Kollisionserkennung noch garantiert ist.

minimale Rahmenlänge in Byte = (Slot-Time * Übertragungsrate)/8
maximale Rahmenlänge ist limitiert (Fairness), damit jeder Teilnehmer die Möglichkeit zur Übertragung hat

Ausdehnung:
10-Mbits/s-Ethernet: 2000-3000m
100-Mbit/s-Ethernet: ca. 200m
1000-Mbit/s-Ethernet: ca. 10-20m oder 200m

87) Welche prinzipielle Funktionen sind im Ethernet Controller, in der PLS und in der PMA/MAU (Transceiver) realisiert? Was war AUI? Warum musste für High Speed Ethernet die Funktionen von PLS und AUI durch Reconciliation, MII/GMII und PCS ersetzt werden?

Ethernet-Controller: OSI-Layer-2: MAC (CSMA/CD und Adressierung) und LLC
PLS: OSI-Layer-1, erledigt das Encoding und Decoding in Manchester-Code
Physical-Signaling dient dem Austausch der Daten zwischen zwei MAC-Schichten; signalisiert spezielle Zustände des physikalischen Mediums; die Funktionalität ist in der Medium Access Unit (MAU) implementiert

PMA = MAU: Physical Medium Attachment

AUI … Attachment Unit Interface
Schnittstelle zur physikalischen Trennung von Transceiver und Ethernet-Controller; AUI ist mit PMA und enthält MAU-Transceiver und Clock-Recivery-Logic für die empfangenen Datenströme

88) Was ist ein Repeater? Welcher neue Segment-Type tritt bei der Verbindung von remote Repeatern auf? Werden Kollisionen durch einen Repeater an andere Segmente weitergeleitet?

Ein Repeater ist ein Signalverstärker (regeneriert Signale), um Ausdehnungsbeschränkungen auf Grund von Signalabschwächungen aufzuheben; er arbeitet auf OSI-Layer 1 (Protokoll-Transparent).
Ein Remote-Repeater verbindet zwei räumlich getrennte Netzsegmente über ein so genanntes Link-Segment. Link-Segment = zwei Repeater, die per Glasfaserkabel verbunden sind, um größere Distanzen zu überbrücken.
Repeater trennen die Kollisionsdomänen nicht, somit werden Kollisionen weitergeleitet.

89) Wieso musste sich Ethernet zu 10BaseT weiterentwickeln (Stichwort structured cabling)? Wie hat sich die Topologie von 10BaseT Netzwerken verändert? Warum spricht man von „CSMA/CD in a box“? Warum ist „Hub“ ein ungenauer Ausdruck?

Die ursprüngliche Ethernet-Topologie war eine reine Bus-Topologie. Es wurde ein internationaler Standard zur strukturierten Verkabelung von Gebäuden definiert, der eine Sterntopologie, die zu einem (oder mehreren) zentralen Punkt über Twisted-Pair geführt wird, vorsah. Diese Anforderungen passen exzellent zu Token-Ring, daher musste Ethernet angepasst werden, um Zukunftstauglich zu bleiben.

Repeater mit mehr als zwei Segmenten und verschiedenen Medien werden Multiportrepeater genannt. Sind Endsysteme und Multiportrepeater in einer Stern-ähnlichen Topologie zusammengeschalten, wird der Repeater „Hub“ genannt.
Dies ist der Hauptverwendungszeck für 10BaseT in heutigen Ethernet-Netzwerken. Der Hub simuliert den Bus – „CSMA/CD in a box“.
Es ist nur Halfduplex-Betrieb möglich; nur eine Station kann das Netzwerk zu einem gegebenen Zeitpunkt nutzen, alle anderen müssen warten.

90) Welche Rahmenformate für Ethernet gibt es? Zählen Sie diese auf. Was sind die wesentlichen Unterschiede?

IEEE 802.3, IEEE 802.3 with SNAP, Ethernet Version 2 (Ethernet II)

Unterschiede: Ethernet II hat keinen LLC-Sublayer, Length-Feld wird für Protokoll-Typ verwendet; IEEE 802.3 with SNAP wird verwendet, um Ethernet II über IEEE 802.3 zu transportieren

LLC, Ethernet II, SNAP, Ethernet 802.3 sind vom Frameaufbau ziemlich ähnlich

91) Unterstützt Ethernet Version2 auch Connection-oriented Service auf Layer 2? Unterstützt Ethernet 802.3 plus 802.2 auch Connection-oriented Service auf Layer 2? Welchen Grund gibt es für das SNAP Verfahren?

Ethernet II unterstützt keine connection-oriented Services auf Layer 2.
IEEE 802.3 plus 802.2 unterstützt connection-oriented Services auf Layer 2 durch den LLC-Sublayer.

LLC-SAP-Felder (8 Bit) können keine Ethernet-Version-2-Protocol-Type (16 Bit) enthalten, deshalb wird eine Anpassungsschicht eingeführt.
SNAP (Subnetworl Access Protocol) ist ein Protokoll, das die Übertragung von Ethernet-Version-2-Daten über IEEE-LANs ermöglicht.

Chapter 6 – Packet Switching on LANs

92) Warum entwickelte man Transparent Bridging für Ethernet LANs (Packet-Switching auf Layer 2)?

Da auf einer Leitung mehrere Systeme senden können, kommt es zu Kollisionen. Um eine Erkennung von Kollisionen in einem definierten Zeitraum zu ermöglichen, musste die Länge der Leitung beschränkt werden. Da aber selten Pakete an alle geschickt werden und da man öfters Netze größerer Ausdehnung benötigte (ohne die aktuellen Architekturen zu verändern, z.B. neue Software) entwickelte man Transparent-Bridging. Damit kann eine Leitung unterteilt werden und so das Netz größere Ausdehnung bekommen.
Außerdem wird die Performance besser, weil sich nicht mehr alle die Bandbreite teilen müssen, sondern nur noch alle Hosts in einem Segment.

93) Auf welchem Layer des OSI Modells, mit welchen Adressen arbeitet Bridging? Was ist in Bridging-Tabellen enthalten? Muss eine Bridge jeden Rahmen empfangen? Auf welchem Layer des OSI Modells, mit welchen Adressen arbeitet IP Routing? Was ist in IP Routing-Tabellen enthalten? Muss ein IP-Router jeden Rahmen empfangen? Ist der IP-Router aus Endgerätesicht sichtbar?

Bridging arbeitet auf OSI-Layer 2 mit MAC-Adressen, um zu entscheiden, ob ein Frame weitergeleitet werden muss oder nicht. In der Bridging-Tabelle sind die MAC-Adressen aller Stationen registriert, die durch das zugehörige Interface erreichbar sind. Eine Bridge muss wegen Transparenz jeden Rahmen des LANs empfangen.
IP-Routing arbeitet auf Layer 3 mit IP-Adressen. In IP-Routing-Tabellen steht der nächste Hop, also der nächste Router. Ein IP-Router empfängt nur Pakete, die an seine MAC-Adresse(n) gehen. IP-Router sind aus Endgerätesicht sichtbar.

94) Wie wird die Bridging-Tabellen Falle vom dynamischen „Plug and Play“ aufgebaut? Welche Adressen einer Ethernet Rahmens werden dafür verwendet? Wieso benötigt man einen Alterungsmechanismus? Was passiert, wenn man vor Ausaltern das LAN Segment wechselt?

Bridges lernen aus der Source-MAC-Adresse der Pakete, die sie empfangen, an welchem ihrer Ports welcher Host steht.
Alterungsmechanismus benötigt man, weil Hosts in andere Segmente (z.B.: Host A wechselt von Segment 1 nach 2) wechseln können. Die Bridge glaubt immer noch, Host A ist in Segment 1 und leitet Pakete dorthin weiter. Dann altert der Eintrag aus und die Bridge lernt neu, wo sich Host A befindet.
Wenn eine bereits registrierte MAC-Adresse nicht innerhalb einer bestimmten Zeitspanne als Quell-Adresse eines Frames gesehen wird, wird der Bridging-Tabellen-Eintrag gelöscht.

95) Wie arbeitet eine Transparent Bridge prinzipiell? Ist die Bridge aus Endgerätesicht sichtbar? Aufgrund welcher Adressen eines Ethernet Rahmens werden die Entscheidungen Forwarding, Filtering bzw. Flooding getroffen? Was bedeutet Forwarding, Filtering und Flooding konkret?

Die Transparent-Bridge verwendet Layer 2. Sie hat drei Funktionen und die Ziel-Adresse des Rahmens wird für die folgenden Entscheidungen verwendet: Filtering, Forwarding und Flooding.

Filtering: der Rahmen wird abgelehnt, falls sich das Ziel im gleichen LAN-Segment befindet

Forwarding: ein Duplikat des Rahmens wird an das LAN-Segment weitergegeben, in dem sich das Ziel befindet

Flooding: das Ziel ist für die Bridge noch unbekannt, und der Rahmen wird an alle Interfaces weitergegeben

Transparent Bridge ist für Endsysteme unsichtbar

96) Was ist Ethernet-Switching (Ethernet-Switch) im Vergleich zu Transparent Bridging (Bridge)? Womit kann eine Ethernet Switching Tabelle verglichen werden: Routing-Tabelle von Packet-Switching im Conectionless Service oder Switching-Tabelle von Packet-Switching im Connectionoriented Service?

Ein Ethernet-Switch ist im Prinzip eine Multiport-Bridge, also ein Bridge mit mehr als zwei Ports.

Ethernet-Switching bedeutet schnelles Transparent-Bridging in Hardware implementiert. Beim Ethernet-Switching wird nur von der Layer-2-Adresse (MAC) gebrauch gemacht. Der Switch muss dabei Switching-Tabellen pflegen, um die verschiedenen Adressen den verschiedenen Netzen zuzuordnen, und in Folge die Pakete dorthin weiterleiten zu können.

Eine Ethernet-Switching-Tabelle kann mit einer Routing-Tabelle im Connectionless-Service verglichen werden. Die Entscheidung, wohin das Paket weitergeleitet wird, wird individuell getroffen; es gibt kein explizites Connection-Setup, es gibt keine Local-Connection-Identifier.

97) Was passiert mit Ethernet Broadcasts und Multicasts?

Rahmen mit Broadcast/Multicast-Adressen werden immer zu allen anderen Ports weitergeleitet.

98) Warum sollte man Transparent Bridging nicht über WAN Links einsetzen?

Häufige Broadcasts auf Netzen und eine langsame WAN-Verbindung kann einen Bufferoverflow bzw. eine Blockade in der Bridge verursachen.

99) Was ist zum Thema Collision Domain und Broadcast Domain bei Transparent Bridging festzustellen?

Bridges teilen LANs in mehrere Collision-Domains; eine Kollision auf einem LAN-Segment wird auf anderen LAN-Segmenten nicht gesehen. Jedoch ist das ganze Netzwerk immer noch eine Broadcast-Domain. Broadcast-Rahmen werden immer noch auf das ganze LAN versendet.
Bridges sind transparent für Endsysteme: Eine Bridge teilt eine Collision-Domain; Kollisionen können sich nicht über Bridges fortpflanzen. Eine Broadcast-Domain ist also der Bereich, in dem ein Broadcast einer Station von anderen empfangen werden kann. Durch eine Transparent-Bridge lassen sich zwei LANs zusammenhängen; sie erscheinen den Endgeräten dadurch als ein großes, logisches LAN. Die zwei ursprünglichen LANs bleiben jedes eine Collision-Domain für sich, aber beide sind nun eine einzige Broadcast-Domain, was mitunter Probleme mit sich bringt.

100) Welche Probleme gibt es bei der Basistechnik Transparent Bridging bei redundanten Wegen zwischen LAN Segmenten? Wie werden diese Probleme prinzipiell gelöst?

Es gibt das Problem, dass Rahmen im Kreis geschickt werden können, z.B. bei Broadcasts. Um dies zu vermeiden, werden redundante Links deaktiviert (durch das Spanning-Tree-Protokoll).

101) Was ist die Grundidee des Spanning Tree Protocols? Warum verwendet man den Ausdruck Tree? Woran erkennen Sie, dass ein Ethernet-Switch STP unterstützt?

Spanning Tree Protocol (STP) schaut, dass es zwischen zwei Stationen immer nur genau einen Weg gibt; wird von einem speziellen Bridge-Protokoll, das zwischen den Bridges zur Kommunikation verwendet wird, implementiert; Fehler eines aktiven Pfades führt zur Aktivierung eines redundanten Pfades
Der Ausdruck Tree wird verwendet, weil nach Anwendung des STP eine Baum-Struktur entsteht.
Man erkennt durch die Bezeichnung IEEE 802.1D, dass ein Ethernet-Switch STP unterstützt.

102) Wie sind die prinzipiellen Abläufe beim Spanning Tree Protocol?

Nach dem Hochfahren des Netzwerks werden alle Ports in den Blocking-State gesetzt. Jede Bridge versucht nun, Root-Bridge (RB) des Spanning-Tree zu werden, indem sie Configuration-BPDUs sendet. Mit

diesen teilt sie mit, welche Bridge als RB gesehen wird, welche Path-Costs zu dieser RB bestehen und ihre eigene Bridge und Port-ID.
Die Bridge mit der niedrigsten Bridge-ID wird RB und setzt alle Ports auf Forwarding. Nachdem eine RB gewählt wurde, wird das Senden von BPDUs ausschließlich durch die RB ausgelöst. Jede Bridge setzt den Port, der den kürzesten Weg zur RB hat, auf Forwarding.
Außerdem werden Designated-Bridges gewählt (die mit dem kleinsten RPC gewinnt), die dann als Einzige ein Segment bedienen darf: „designated" Port auf Forwarding. Alle anderen Bridges, die dranhängen bleiben auf Blocking.

103) Welche Basisparameter werden beim Spanning Tree Protocol verwendet? Wie ist deren Default Handhabung? Was kann ein Netzwerkadministrator durch Konfiguration der einzelnen Parameter erzielen?

Bridge Identifier (Bridge ID): Kombination aus MAC-Adresse und einer Prioritätsnummer (typischerweise wird die niedrigste MAC-Adresse aller Ports dafür verwendet); Prioritätsnummer kann vom Administrator konfiguriert werden; niedrigste Bridge-ID hat höchste Priorität
Default-Prioritätsnummer: 32768; Bridge mit der niedrigsten MAC-Adresse hat höchste Priorität

Port Cost (C): Kosten, um lokales Interface zu erreichen; Kosten sind verkehrt proportional zur Übertragungsrate
Default-Cost: 1000/(Übertragungsrate in Mbit/s); kann vom Administrator geändert werden

Port Identifier (Port ID): Kombination aus Portnummer und Prioritätsnummer
Default-Port-Priority: 128; kann vom Administrator konfiguriert werden

104) Welche vier Basiswerte werden in einer BPDU vorrangig verwendet?

Root-ID … wer ist oder scheint die Root-Bridge zu sein (R-ID); 2 Bytes für Priorität, 6 Bytes für MAC-Adresse

Root Path Cost … wie weit ist die Root-Bridge von mir entfernt (RPC)

Bridge-ID … ID der Bridge, die diese BPDU überträgt (O-ID); wie Root-Identifier strukturiert

Port-ID … Port, über den diese BPDU übertragen wurde (P-ID); 1 Byte Priorität (Default: 128), 1 Byte Portnummer

105) Was ist die Root-Bridge und wie wird die Root Bridge gefunden?

Empfängt eine Bridge einen Configuration-BPDU mit niedrigerer Root-Bridge-ID als die eigene Bridge-ID, hört sie auf Configuration-BPDUs auf diesem Port zu versenden. Der empfangene und abgeänderte Configuration-BPDU wird auf allen anderen Ports weitergeleitet.
Empfängt eine Bridge eine Configuration-BPDU mit höherer Root-Bridge-ID als der eigenen Bridge-ID, fährt die Bridge fort damit, Configuration-BPDUs mit ihrer eigenen Bridge-ID als Root-Bridge-ID auf allen Ports auszusenden. Die anderen Bridges sollten damit aufhören (das Senden der Configuration-BPDUs wird exklusiv von der RB ausgelöst).

die Konfigurations-BPDUs sagen:
- welche Bridge aktuell als Root-Bridge (RB) gesehen wird
- welche Pfadkosten zu dieser RB existieren (Root Path Cost)
- die eigene Bridge-ID und Port-ID

106) Was ist das Root-Port und wie wird das Root-Port gefunden?

Der Root-Port ist jener Port von einer Bridge, der die niedrigste Root-Path-Cost hat. Die Root-Path-Cost ist die Summer aller Path-Costs von dieser Bridge zur RB, die inkludiert die Port-Costs aller dazwischenliegenden Bridges. Die Kalkulationsmethode ist die Root-Path-Cost, die mit dem BPDU erhalten wurde plus der Port-Cost des lokalen Ports, der diese BPDU empfangen hat. Dieser Port wird dann der Root-Port; im Falle von gleichen Kosten entscheidet die Port-ID (niedriger ist besser).

107) Was ist die Designated Bridge und wie wird sie gefunden?

Für jedes LAN-Segment wird eine Designated-Bridge (DB) ausgewählt.
Die Bridge mit der niedrigsten Root-Path-Cost auf ihren Root-Ports wird die DB (im Falle eines Gleichstands gewinnt die Bridge mit der niedrigsten Bridge-ID).

108) Welche Ports einer Bridge werden nach Ablauf des Einschwingvorganges in den Forwarding State versetzt? Was passiert auf Ports im Blocked State? Werden auf Blocked Ports BPDUs empfangen?

Jede Designated-Bridge erklärt ihre Ports zu Designated-Ports und setzt sie zusammen mit dem Root-Port in den Forwarding-State.
Das Endsystem kann Ethernet-Frames auf Blocked-Ports weder empfangen noch weiterleiten, jedoch können immer noch BPDU-Frames empfangen, durch die Bridge manipuliert, und weitergesandt werden.

109) Was passiert wenn die Root-Bridge ausfällt? Wie kann dieses erkannt werden?

Die RB generiert (triggering) normalerweise alle 1-10 Sekunden eine Configuration-BPDU, die über die Root-Ports von jeder anderen Bridge empfangen wird und über die Deignated-Ports weitergeleitet wird.
Bridges, die nicht designated sind, hören noch immer auf solche Messages an ihren geblockten Ports. Wenn das Triggering ausaltert sind zwei Szenarien möglich:

1) Ein Ausfall der Root-Bridge, bei dem eine neue RB gesucht wird und sich in Folge der Spanning-Tree ändern wird.

110) Was passiert wenn die Designated Bridge ausfällt? Wie kann dieses erkannt werden?

siehe 109

2) Ein Ausfall einer Designated-Bridge, bei dem (sofern vorhanden) eine andere Bridge des LAN-Segments für diese einspringen wird.

111) Zählen Sie zwei Vor- und zwei Nachteile des Bridgings im Vergleich zum IP Routing auf?

Vorteile des Bridgings:

- ist nur von MAC-Adressen abhängig
- für Endsysteme unsichtbar
- schneller, weil in Hardware implementiert
- Transparent, keine Einstellungen auf Clients notwendig

Nachteile des Bridging:

- muss jeden Rahmen behandeln
- Anzahl der Tabellen-Einträge = Anzahl aller Geräte im ganzen Netzwerk
- kein Flow-Control
- kein LAN/WAN-Coupling wegen hohem Traffic (Broadcast-Domain)
- alles bleibt eine Broadcast-Domain

112) Zählen Sie zwei Vor- und zwei Nachteile des IP Routings im Vergleich zum Bridging auf?

Vorteile von Routing:

- behandelt nur Rahmen, die an ihn adressiert sind
- Anzahl der Tabellen-Einträge = Anzahl der Subnetze
- Flow-Control ist möglich (Router wird von Endsystemen gesehen)
- Router kennt für jeden Rahmen den besten Weg
- teilt Broadcast-Domains

Nachteile von Routing:

- benötigt strukturierte Adressen (muss konfiguriert werden)
- Endsystem muss seinen Default-Router kennen
- langsamer, weil gewöhnlich in Software implementiert und weil Adress-Auflösung (address resolution, ARP) nötig ist

113) Bleibt bei einem Ethernet-Netzwerk basierend auf Repeater-Technologie die Collision-Domain zwischen zwei Ethernet Segmenten erhalten oder wird sie unterteilt? Begründen Sie Ihre Antwort.

Ein Repeater ist prinzipiell nur ein Signalverstärker, der es ermöglicht, den Umfang eines Netzes zu vergrößern. Das Netzwerk wird von solch einem Verstärker aber nicht beeinflusst, d.h. sowohl Kollisionsdomänen als auch Broadcast-Domäne bleiben erhalten.

114) Bleibt bei einem Ethernet-Netzwerk basierend auf Bridging/Switching-Technologie die Broadcast-Domain zwischen zwei Ethernet Segmenten erhalten oder wird sie unterteilt? Begründen Sie Ihre Antwort. Wie sieht das bezüglich Collision-Domain aus?

Die Broadcast-Domain bleibt erhalten, da Bridges/Switches Broadcast und Multicast-Messages immer an alle Ports weitergeben.
Die Collision-Domain hingegen wird an der Stelle der Bridge/des Switch geteilt.

115) Was sind die Gemeinsamkeiten bzw. was sind die Unterschiede zwischen Transparent Bridging und Ethernet Switching?

Ein Switch ist im Prinzip eine Multiport-Bridge. Beim Bridging versucht man, mehrere Netzwerksegmente zu bekommen, um kleinere Collision-Domains zu erhalten.
Verwendet man hingegen Switches und hängt jeden einzelnen Client direkt an den Switch, so entstehen lauter kleine Collsion-Domains (Client- und Switch-Port), wo keine Kollision mehr auftreten kann, da es nur zwei Geräte darin gibt, die miteinander im Full-Duplex-Modus kommunizieren können.

116) Was versteht man unter full-duplex Ethernet? Welche Ethernet-Segment-Typen bzw. Ehernet-Technologien können im full-duplex Modus arbeiten?

Unter Full-Duplex versteht man, dass man Senden und Empfangen gleichzeitig kann. Geräte, die an Switches hängen, können z.B. im Full-Duplex-Modus senden/empfangen.
(Nur Point-to-Point-Verbindungen können im Full-Duplex-Modus arbeiten, Shared-Media nicht.)

117) Wieso ist auf einem full-duplex Ethernet Link das Collision Window nicht mehr eine limitierende Größe? Welche Konsequenz lässt sich daraus ableiten (Stichwort: Ethernet als WAN-Technologie)?

Collision-Window ist bei Collision-Detection wie CSMA/CD nötig, wo Leitungen vor dem Senden abgehört werden werden müssen (Shared-Media).
Beim Full-Duplex-Traffic stehen Leitungen für beide Richtungen auf Point-to-Point-Verbindungen zur Verfügung, somit kann auf ein Collision-Windows gänzlich verzichtet werden.
Über Glasfaserkabel lässt sich eine Distanz von bis zu 70km erreichen (WAN).

118) Warum ist Flow Control zwischen einem L2-Ethernet-Switch und einem Ethernet Endsystem wünschenswert bei L2 geswitchten Netzwerken? Wie wird diese Flow Control realisiert?

Die Geschwindigkeits-Anforderungen an Switches sind bei Full-Duplex sehr hoch; auch leistungsstarke Switches können einen Buffer-Overflow nicht verhindern. Ein L4-Flow-Control zwischen Endsystemen wäre nicht effizient genug. Somit wurde ein MAC-basiertes L2-Flow-Control spezifiziert (wird mit MAC-control-protocol und MAC-pause-command realisiert).

119) Was wird bei Autonegotiation prinzipiell ausgehandelt? Bei welchen Ethernet-Technologien ist Autonegotiation anwendbar?

Signal-Rate (10, 100 oder 1000 Mbit/s), Half-Duplex (=CSMA/CD) or Full-Duplex; ist möglich bei 100BaseT und 1000BaseT, also nur mit Kupferkabeln
(er werden also Informationen über das Potential/die Kapazität ausgehandelt)

120) Wieso musste für High Speed Ethernet die Codierungsarten von Manchester auf 4B/5B bzw. 8B/10B geändert werden und die PLS/AUI Funktion durch Reconcilation/MII-GMII/PCS ersetzt werden? Wie geht man bei diesen Codes vor? Welche Bitrate (Signalrate) ergibt sich daraus tatsächlich am Medium?

weil die Effizienz von Manchester (50%) für die hohen Bitraten zu gering ist; 4B/5B hat eine Effizienz von 80%; es wird jeder 4-Bit-Codegruppe eine 5-Bit-Codegruppe zugeordnet bzw. jeder 8-Bit-Codegruppe eine 10-Bit-Codegruppe zugeordnet; tatsächliche Bitrate 125 Mbit
das alte Physical Layer Signaling Interface (PLS), repräsentiert durch AUI, war für die neuen Coding-Technologien nicht geeignet; AUI wurde durch MII (Media Independet Interface) für Fast-Ethernet und durch GMII für Gigabit-Ethernet ersetzt
MII ist ein Interface zwischen MAC-Layer und dem physikalischen Layer; versteckt Coding-Angelegenheiten vor dem MAC-Layer

121) Wieso muss man bei Gigabit Ethernet die Methoden Carrier-Extension oder Frame-Bursts anwenden, wenn man Gigabit Ethernet mit einem Repeater betreibt? Charakterisieren Sie diese beiden Methoden kurz. Ist das auch bei der 10Gbit Ethernet-Technologie notwendig (Begründung)?

CSMA/CD: die Station muss die doppelte Zeit der Signal-Propagation abhören, um Kollisionen zu entdecken; Kollisions-Fenster von 512 Bits bei 1 Gbit/s limitiert die Netzausbreitung auf maximal 20 Meter
=> man verwendet Carrier-Extension oder Frame-Bursting, um die Netzausdehnung zu erhöhen

Carrier-Extension: zusätzliche Bytes werden dem Ethernet Frame vom Physical Layer hinzugefügt (und wieder entfernt); der Frame befindet sich länger auf dem Medium

Frame-Bursting: die Station kann mehrere Frames zusammenketten und diese auf einmal übertragen

Mit beiden Methoden wird die minimale Frame-Länge von 521 auf 4096 Bits erhöht.
Dies ist bei 10-Gbit-Ethernets nicht notwendig, da 10-Gbit-Ethernet keine Operationen mehr mit CSMA/CD erlaubt.

122) Was ist die Basis-Idee von VLAN? Welche prinzipiellen Mittel benötigt man (Aufzählung)?

Die Grundidee hinter VLANs (Virtual LANs) ist eine logische Aufteilung eines physikalischen LANs in mehrere Arbeitsgruppen-LANs, die nur untereinander kommunizieren können und nichts von der Existenz der anderen – auf denselben Sytemen und Medien betriebenen LANs – erfahren. Dies hat seine Hintergründe darin, dass die Daten von einer Arbeitsgruppe von den anderen ferngehalten werden sollen (Sicherheit), dass Broadcasts nur die eigene Arbeitsgruppe betreffen und dass die Netzwerke dadurch sehr flexibel werden.

prinzipielle Mittel:
- VLAN-Tagging für VLAN über mehrere Switches hinweg
- seperates STP
- seperate Bridging/Switching-Tables
- seperates Broadcast-Handling
- Methoden zur Zuordnung zu einem VLAN (Port-, MAC-, Protocol-Based)

123) Welche Methoden gibt es, um ein Endsystem einem VLAN zuzuordnen (kurze Erklärung)?

port-based:
- fixe Zuordnung z.B. Port 4 -> VLAN x

MAC-based:
- MAC A -> VLAN x

protocol-based:
- IP-traffic, port 1 -> VLAN x
- NetBEUI-traffic, port 1 -> VLAN y
- eine Station könnte Mitglied verschiedener VLANs sein

124) Wieso benötigt man VLAN Tagging auf Trunkleitungen? Wo befindet sich der VLAN Tag in einem Ethernet Rahmen? Wozu dient das UP–Feld und wozu kann das ein Ethernet-Switch verwenden?

VLAN-taugliche Switches können über Trunked-Ports (IEEE 802.1 Q) miteinander verbunden werden (Uplink). Empfängt ein Switch von einem Trunked-Port einen Frame, in dem er einen VLAN-Tag erkennt, so wird der Frame an den entsprechenden Port weitergeleitet. Falls sich an diesem Port ein Endgerät befindet,

wird zuvor das Tag entfernt. Logischerweise wird beim Weiterleiten eines Frames von einem Endgerät über einen Trunked-Port das Tag hinzugefügt. Damit können auf derart verbundenen Switches gleiche VLANs benutzt werden. In größeren Cisco-Netzwerken kommt das VTP-Protokoll zum Verteilen von VLANs zum Einsatz.
Das VLAN-Tag befindet sich im Ethernet-Rahmen an vierter Stelle, nach der Preamble, DA und SA und beinhaltet TPID (Tag Protocol Identifier) und TCI (Tag Control Information); wobei das TCI wiederum in UP (User Priority), CFI (Canonical Format Identifier) und VID (VLAN-Identifier) unterteilt ist.
Das UP-Feld (3 Bit) dient zum Verwalten von Prioritäten - 7 hat die höchste, 0 die niedrigste Priorität. Frames mit höherer Priorität werden vom Switch vorrangig behandelt.

125) Was versteht man unter Fast- oder Gigabit-Ethernet Channeling? Warum wird es benötigt?

Full-Duplex-Trunks mit hohen Kapazitäten könnten durch STP nicht genützt werden, weil sie geblockt werden. Channeling fasst redundante Trunks zusammen und täuscht STP eine logische Verbindung vor. Dadurch können die zu Verfügung stehenden Komponenten genutzt werden.

Chapter 8 – IP Technology

126) Charakterisieren Sie kurz IP (OSI Layer, Network Type (Packet oder Circuit Switching) / Service Type (CO oder CL), beteiligte Komponenten (IP Host, Router), Forwarding Prinzip, Grundeigenschaften).

IP … Internet-Protocol; Endsystem wird IP-Host genannt; auf OSI-Layer 3; Network-Type: Packet-Switching; Service-Type: Connectionless (Datagramme werden gesendet, ohne dass vorher Verbindung aufgebaut wird); Router kümmern sich nur um Zustellung der Pakete, übernehmen aber keine Garantie für die Zustellung (best effort delivery: Datagramme können wegen Übertragungsfehlern oder Netzwerkverstopfung verworfen werden), diese muss auf höherer Ebene vom Host übernommen werden (z.B. auch Schicht 4 – TCP)

127) Charakterisieren Sie kurz TCP (OSI Layer, Protokoll Type (CO oder CL), beteiligte Komponenten (IP Host, Router), Grundeigenschaften).

TCP … Transmission Control Protocol; auf OSI-Layer 4; Connection-Oriented; Sequencing; Windowing; Error-Recovery durch erneute Übertragung; Flow-Control; TCP ist im Prinzip eine Point-to-Point-Verbindung (Aufbau TCP-Verbindung nach Drei-Wege-Handshake); TCP ist in den höheren Schichten des IP-Hosts implementiert; sorgt für gewisse Sicherheit, weil kontrolliert wird, ob die Daten nach Menge, Reihenfolge und Prüfsummen korrekt übertragen wurden

128) Wozu wird bei IP TTL benötigt? Wie wird es gehandhabt? Was passiert im Zusammenhang mit ICMP?

TTL … Time To Live
limitiert die Lebenszeit eines Datagrams -> verhindert, dass es ewig zirkuliert, falls Routing-Fehler auftritt
Quelle setzt Startwert fest (32 bis 64 sind gewöhnliche Werte); jeder Router dekrementiert TTL (TTL = hop count); TTL erreicht 0 -> Datagram wird verworfen; ICMP generiert Fehlermeldung, wenn TTL = 0

ICMP … Internet Control Message Protocol
erzeugt Fehlermeldungen, um Infos über Fehler und Paketverluste im Netzwerk zu liefern; IP-Station (Router oder Ziel), die Übertragungsprobleme bemerkt, erzeugt ICMP-Message; ICMP-Message adressiert an Sender des originalen IP-Pakets

129) Wozu wird bei IP Fragmentierung benötigt? Wie wird diese gehandhabt (Wer fragmentiert, welche Felder im Header werden verwendet; wo wird wieder zusammengesetzt?

Jedes Netz hat eine maximale Paketgröße (MTU = Maximum Transfer Unit); IP muss also zu große Pakete in mehrere Frames aufteilen; jedes Fragment erhält einen vollständigen IP-Header mit Identifikationsnummer (Identification und Flags werden im Header verwendet), um sie wieder zusammenzusetzen
bei der Ziel-Station wird wieder zusammengesetzt, da Fragmente verschiedene Wege nehmen können

verwendete Felder: Identification; Offset; More Fragments Flag; Don’t Fragment Flag

130) Wie kann die maximale MTU zwischen zwei Netzen in Zusammenarbeit mit ICMP herausgefunden werden?

MTU … Maximum Transfer Unit
Die Station sendet das größtmögliche Paket mit gesetztem DF-(Don't Fragment)-Bit. Das Paket muss daher unfragmentiert übertragen werden. Wenn das Paket aber ein Netz mit kleinerer MTU durchläuft, wird das Paket verworfen, da es nicht fragmentiert werden darf und eine ICMP-Error-Message wird der Ursprungsstation gesendet (Paket zu groß und DF-Bit gesetzt).
Der Sender kann somit das Paket so lange verkleinern, bis er keine ICMP-Error-Message mehr erhält.

131) Wozu diente das TOS Feld ursprünglich? Welche Möglichkeiten hatte man prinzipiell?

TOS … Type of Service
Teilte die Priorität und die bevorzugten Netzwerk-Charakteristiken (niedrige Kosten, hohe Sicherheit, wenig Verzögerung) des Pakets mit.

zeigt Priorität eines Datagrams und der bevorzugten Netzwerk-Charakteristiken an

132) Was ist die heutige Idee von TOS Feld (Stichwort: DSCP)? Wofür ist heute bedeutsam?

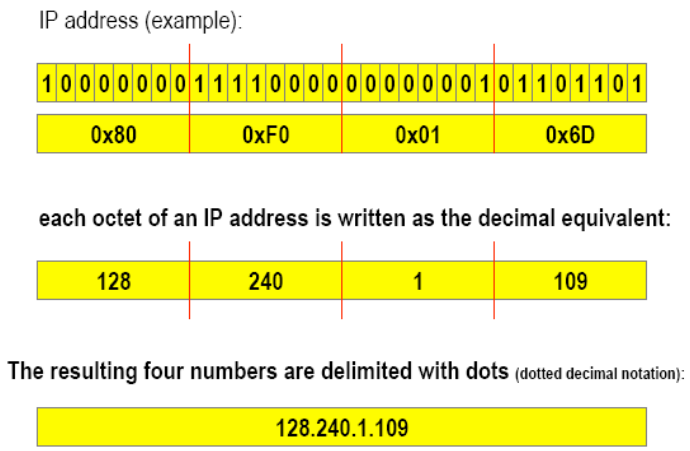
TOS steht für Type of Service und wurde zu DSCP (Differentiated Service CodePoint). Es bezeichnet jetzt die Verkehrsklasse eines Flusses (flows). Unter einem flow versteht man dabei eine Sitzung zwischen zwei IP-Hosts.
DSCP ist wichtig für QoS; mit Hilfe von DSCP kann ein QoS angefordert werden. IP verwendet die Best-Effort-Strategie und ist daher nicht bestens für interaktive Real-Time-Traffic geeignet (Video, Sprache, ...). Mt Hilfe von DSCP kann ein IP-Datagramm einer bestimmten Traffic-Klasse und innerhalb dieser Klasse einer bestimmten Behandlungsstufe zugeordnet werden (Limited-Delay usw.).

133) Was konnte man mit den IP Optionen bewerkstelligen? Warum sind diese heute deaktiviert?

Sicherheits- und spezielle Routing-Einstellungen (jeder passierte Router trägt seine IP-Adresse ein, um die Route aufzuzeichnen oder das Paket muss die durch IP-Adressen vorgegebenen Router passieren) festlegen; heute wegen Sicherheitslücken durch Firewalls blockiert

135) Was kennzeichnet eine IP Adresse? Aus welchen Teilen ist sie prinzipiell aufgebaut? Wie wird sie dargestellt?

32 Bit lang; Darstellung: dotted decimal; IP-Adresse ist eindeutig; Basis-Struktur: net-id, host-id; IP-Adressen sind in verschiedene Klassen mit unterschiedlich langer net-id und host-id unterteilt



136) Welche Adressklassen gibt es? Welche Adress-Bereiche werden von welcher Klasse verwendet? Was ist die First-Octet-Rule?

Klassen A-E
A (Bereich: 1-127 Bit), B (128-191), C (192-223; Unicast), D (224-239; Multicast), E (240-255; Experimental)
Klasse definiert Anzahl der Adress-Bits, die für net-id verwendet werden

Klasse A: 7-Bit-net-id, 24-Bit-host-id; 126 Netze, 16 777 214 Hosts
Klasse B: 14-Bit-net-id, 16-Bit-host-id; 16 384 Netze, 65 534 Hosts
Klasse C: 21-Bit-net-id, 8-Bit-host-id; 2 097 512 Netze, 254 Hosts
Klasse D: 28-Bit-Multicast-Gruppenmitglied

First-Octet-Rule:
Am ersten Byte kann man ablesen, zu welcher Klasse eine Adresse gehört.

Klasse A: 0 1-127
Klasse B: 10 128-191
Klasse C: 110 192-223
Klasse D: 1110 224-239
Klasse E: 1111 240-255

137) Was ist ein IP Limited Broadcast? Wie wird diese Adresse dargestellt? Was passiert dabei auf LANs bezüglich L2 Adressierung?

Als Ziel wird die IP-Adresse 255.255.255.255 angegeben. Dieses Ziel liegt immer im eigenen Netz und wird direkt in einen Ethernet-Broadcast umgesetzt. Ein Limited-Broadcast wird von einem Router nicht weitergeleitet.

138) Was ist ein IP Directed Broadcast? Wie wird diese Adresse dargestellt? Was passiert dabei auf LANs bezüglich L2 Adressierung? Warum und wo wird er heute unterbunden?

Ziel sind Teilnehmer eines bestimmten Netzes; Adresse wird durch Kombination aus Zielnetz und Setzen aller Hostbits auf 1 angegeben; wird erst im Zielnetz in einen Ethernet-Broadcast+Limited-Broadcast umgesetzt; wegen Denial-of-Service-Attacken wird er heute unterbunden

139) Was versteht man unter Subnetting? Wie wird das dargestellt bzw. konfiguriert?

Netz wird für die interne Verwendung in mehrere Teilnetze aufgeteilt; nach außen trotzdem noch ein Netz (Subnetting)
ein paar Bits der host-id können als subnet-id genutzt werden; subnet-id erweitert net-id Bedeutung: subnet-id bits werden nur lokal innerhalb des Subnets interpretiert; net-id bits werden weiterhin überall gesehen
Netzmaske ist genauso lang wie die IP-Adresse; alle Bits den Netzwerkteils sind auf 1 und alle Bits des Geräteteils auf 0 gesetzt (dotted decimal notation)

140) Warum kann man unter Anlehnung von RFC 950 bei Classful Routing das Subnet Zero und Subnet Broadcast nicht verwenden?

Subnet-Zero und Subnet-Broadcast sind mehrdeutig
Problem:
bedeutet 10.0.0.0 net-ID von Netz 10 oder Subnetz 10.0?
bedeutet 10.255.255.255 directed broadcast für das ganze Netz 10 oder für das Subnetz 10.255?

141) Was muss im IP Host bezüglich IP Adressierung im Minimum konfiguriert werden, um IP Kommunikation lokal und global zu ermöglichen? Welche Sichtweise (lokal oder global) haben die IP Hosts dadurch?

- IP-Adresse (eindeutig)
- IP-Host benötigt Subnet-Mask; wird ein Netz in mehrere Teilnetze aufgeteilt, muss jeder Host innerhalb eines Netzes die gleiche Subnetmask haben, um mit den anderen Hosts im Netz zu kommunizieren; hat er eine unterschiedliche, glaubt er, er wäre in einem anderen Netz und fragt den Router
- Standard-Gateway

Hosts haben nur eine lokale Sichtweise des Netzwerkes

142) Was versteht man unter direct und indirect delivery? Wie ist die Aufgabenverteilung zwischen IP Hosts und IP Routern?

direct delivery: wenn sich Sender und Empfänger im gleichen physischen Netzwerk befinden (net-id of source = net-id of destination); Host macht alles selber, Router wird nicht gebraucht

indirect delivery: wenn net-id of source != net-id of destination; Host schaut, ob seine Subnetzmaske und die des Ziels gleich sind; wenn nicht schickt er das Paket mit der Ziel-IP des Ziel-Hosts an die MAC-Adresse des Routers, der sich um die Weiterleitung kümmert

143) Was muss in IP Routern konfiguriert werden, um IP Kommunikation zu ermöglichen? Welche Sichtweise (lokal oder global) haben die IP Router dadurch?

manuell konfiguriert werden müssen:
- IP-Adressen und Subnetmasken der Interfaces
- Default-Router

IP-Router kennt von Anfang an seine direkten Nachbarn (Next-Hop-Router), über die er dann in der Lage ist, das ganze Netzwerk zu lernen; Router haben eine globale Sichtweise

144) Wie ist eine IP Routing-Tabelle prinzipiell aufgebaut? Was sind diese Einträge prinzipiell aus Sicht des Packet-Switchings?

sind „Adress-Tabellen“
Aufbau: net-id/mask, next hop, metric (Entfernung in hops), Port, Zeitstempel (age)
aus Sicht des Packet-Switchings: Wegweiser

145) Welche drei Grund-Paradigmen gibt es beim IP Routing (Aufzählung und kurze Erklärung)?

i. Destination-Based-Routing: Quelladresse spielt für die Auswahl des Pfades keine Rolle
ii. Hop-by-Hop-Routing: IP-Datagramme folgen demjenigen Pfad, der durch den aktuellen Status der Routing-Tabelle angezeigt wird
iii. Least-Cost-Routing: nur der beste Pfad wird zum Weiterleiten von Datagrammen berücksichtigt

146) Wann und wozu wird das ARP Protokoll benötigt? Wie geht man prinzipiell vor? Welche Reichweite hat ARP (lokal, global oder beides)?

ARP … Address Resolution Protocol
eine IP-Adresse identifiziert den logischen Zugang zu einem IP-Netzwerk; die Station kann ohne weiterer Adressierung erreicht werden, wenn das physikalische Netzwerk nur aus Point-to-Point-Verbindungen besteht
auf einem Shared-Media-LAN werden MAC-Adressen benutzt, um Pakete zu einer bestimmten Station zu liefern -> ein Mapping zwischen IP-Adresse und MAC-Adresse wird benötigt
das Mapping zwischen MAC- und Protokoll-Adresse in einem LAN kann statisch (Tabellen-Einträge) oder dynamisch (ARP-Protokoll und ARP-Cache)

Vorgang:
Station A will zu Station B senden und kennt die MAC-Adresse nicht (beide sind im selben LAN); A sendet einen ARP-Request in Form eines MAC-Broadcast; ARP-Request beinhaltet IP-Adresse von B; Station B sieht den ARP-Request mit seiner IP-Adresse und sendet einen ARP-Response als MAC-Frame; B gibt das neu gelernte Mapping (Quell-MAC und IP-Adresse von A) in seinen ARP-Cache
ARP-Response beinhaltet MAC-Adresse von Station B; A speichert MAC- und IP-Adress-Mapping für Station B in seinem ARP-Cache; für nachfolgende Pakete von A nach B oder B nach A werden die MAC-Adressen aus dem ARP-Cache verwendet
Einträge im ARP-Cache werden gelöscht, wenn sie eine bestimmte Zeit lang nicht verwendet werden

ARP hat nur lokale Reichweite

Sicherheitsproblem (ARP-Spoofing); Gratuitous ARP: System schickt Paket ins Netz und fragt sich selbst ab (primär um doppelte Adressen zu erkennen; möglicherweise auch um den ARP-Cache der anderen Hosts mit seiner Adresse zu beglücken)

147) Wozu dient der ARP Cache? Wann wird er refresht? Gibt es dabei eine Möglichkeit der Authentifizierung?

speichert zu lokalen IP-Adressen die jeweilige MAC-Adresse
Refresh: passiv: wenn der Host (zufällig) brauchbare Pakete bekommt (z.B. einen ARP-Request), verwendet er sie, um MAC-Adressen zu lernen
keine Authentifizierung

148) Welche Informationen können IP Geräte aus dem Empfang eines ARP Requests gewinnen? Welches Gerät reagiert? Werden alle Geräte eines LANs oder nur die IP Geräte aufgeweckt?

sie gewinnen neuen ARP-Cache-Eintrag; nur angesprochenes Gerät reagiert, aber alle werden aufgeweckt; wird nicht durch Router weitergeleitet

149) Welche Informationen können IP Geräte aus dem Empfang eines ARP Replys gewinnen? Welche Geräte bekommen den ARP Reply? Was passiert mit dem ARP Cache?

Informationen: die MAC-Adresse zur IP-Adresse eines Hosts
der Host, der über ARP-Request angefragt hat, bekommt den ARP-Reply
Anfrage-Host und Empfänger-Host refreshen ihren Cache (neuer Eintrag wird gemacht)

150) Was ist ein gratuitous ARP? Wofür wird er verwendet?

dient zur Erkennung, ob eine IP-Adresse evtl. doppelt vorliegt; ein Host sendet dafür einen Broadcast mit seiner eigenen Adresse aus und erwartet keine Antwort, falls die eigene IP-Adresse einmalig ist
alle anderen Stationen, die dieser Broadcast erreicht, können diesen nützen, um ihre Cache-Einträge aufzufrischen

152) Wozu dient das ICMP Protokoll? Was ist das generelle Grundprinzip, wenn man von Echo Request, Echo Reply absieht?

ICMP … Internet Control Message Protocol
erzeugt Fehlermeldungen, um Infos über Fehler und Paketverluste im Netzwerk zu liefern;

IP-Stationen (Router oder Ziel), die Übertragungsprobleme bemerkt, erzeugt ICMP-Message; diese wird an den Absender des IP-Pakets gesendet
falls auch die ICMP-Message nicht übertragen werden kann, werden keine weiteren Messages mehr gesendet, um eine „ICMP-Lawine“ zu verhindern

153) Was ist ein Ping? Mit welchen Mitteln wird er realisiert?

Ping sendet ein ICMP-Echo-Request-Paket an die Zieladresse des zu überprüfenden Hosts. Der Empfänger muss, sofern er das Protokoll unterstützt, laut Protokollspezifikation eine Antwort zurücksenden: ICMP Echo-Reply. Ist der Zielrechner nicht erreichbar, antwortet der zuständige Router: Network unreachable (Netzwerk nicht erreichbar) oder Host unreachable (Gegenstelle nicht erreichbar).
Aus einer fehlenden Antwort kann man allerdings nicht eindeutig darauf schließen, dass die Gegenstelle nicht erreichbar ist. Manche Hosts sind nämlich so konfiguriert, dass sie ICMP-Pakete ignorieren und verwerfen.

154) Wie werden ICMP Messages transportiert? Was passiert, wenn eine ICMP Message einen Fehler verursacht?

werden über IP transportiert
es wird kein neues ICMP-Paket erstellt (Lawineneffekt)

155) Was kann ICMP Message „Destination Unreachable“ in der Basisvariante (also ohne RFC1112) alles signalisieren (Aufzählung und kurze Erklärung)?

- Network unrechable: no path to network known or network down; generated by intermediate or far-end router
- Host unreachable: host-id can’t be resolved or host not responding; generated by far-end router
- Protocol unreachable: protocol specified in IP header not available; generated by end system

- Port unreachable: port (service) specified in layer 4 not available; generated by end system
- Fragmentation needed and do not fragment bit set: DF bit=1 but the packet is to obig for the network (MTU); generated by router
- Source route failed: Path in IP Options couldn't be followed; generated by intermediate or far-end router

156) Was kann ICMP Message „Source Quench" signalisieren? Warum ist das vor allem theoretischer Natur? Welches Protocol (TCP oder UDP) muss aber darauf unbedingt hören und was wird dabei bewirkt?

theoretische Flusskontroll-Möglichkeit von IP; teilt dem Sender mit, seinen Traffic zu Router oder Host zu reduzieren; wird z.B. generiert, wenn nicht genug Buffer (Host oder Router) zu Verfügung steht
von theoretischer Natur weil es keine Sicherheiten gibt; weil man dem Endsystem nicht trauen kann

157) Was ist Traceroute? Mit welchen Mittel wird das realisiert? Lassen sich damit alle Wege eines Netzes aufzeichnen?

listet die genaue Route, die ein Paket im Netzwerk nehmen wird, auf
UDP-Segment und Manipulation des TTL-Feldes des zugehörigen IP-Headers wird verwendet; zuerst TTL auf 1 gesetzt, dann auf 2, …, wenn UDP am Ziel ankommt, wird ICMP-Port-Unreachable-Message generiert; von der Quelladresse kann der Pfad rekonstruiert werden
nur der beste Weg zum Zielhost; parallele Wege werden natürlich nicht erkannt; auch Switches und sonstige Layer-2-Elemente werden nicht erkannt

158) Was kann ICMP Message „Redirect" signalisieren? Wann kommt das sinnvoll zum Einsatz? Wieso ist ICMP Redirect aber unter Umständen gefährlich?

kennt ein Router einen besseren (schneller, kürzer) Pfad zu einem Ziel, so wird der Sender über eine ICMP-Redirect-Message darüber informiert; der Router sendet aber auf jeden Fall auf dem alten ineffizienten Pfad weiter, d.h. wird die Redirect-Message vom Sender ignoriert, so wird das Datenpaket zweimal über das Netz verschickt

bei Redirect-Attacken werden Pakete auf ungewollte Pfade geführt

159) Was definiert der Basis-RFC zum Thema PPP prinzipiell und was kann man damit machen?

drei Hauptkomponenten:
- HDLC-Framing und Encapsulation (RFC 1662): Bitstuffing für synchrone serielle Leitungen; modifiziertes Bytestuffing für asynchrone serielle Leitungen
- Link Control Protocol (LCP, RFC 1661): Aufbauen und Schließen der PPP-Verbindung; testet die Verbindung auf QoS-Features; Aushandeln der Parameter; konfiguriert die PPP-Verbindung
- Familie der Network Control Protocols (NCP, div. RFCs): konfiguriert und hält Network Layer Protocols instand; NCPs existieren für IP, OSI, DECnet, AppleTalk, Novell; NCPs werden nach dem Verbindungsaufbau durch LCP gestartet

PPP ist „das" standardisierte Übertragungsprotokoll verschiedenster Protokolle über serielle Leitungen; connection-less
z.B. Verbindungsaufbau über Wählleitungen (zumeist über Modem oder ISDN); ermöglicht Übertragung verschiedenster Netzwerkprotokolle (z.B. IP, IPX, AppleTalk, …)

Seltener wird PPP für statische Verbindungen verwendet, beispielsweise um Authentifizierungs-Mechanismen (PAP, CHAP) zu nutzen.

160) Was versteht man unter einer PPP Verbindung? Wird hier Error Recovery durchgeführt? Welches Protokoll kommt zum Aufbau einer PPP Verbindung zum Einsatz? Welche Phasen unterscheidet man?

PPP … Point to Point Protocol
kein Error-Recovery; LCP zum Aufbau

vier Phasen:
1. Verbindungsaufbau und Konfigurationsaustausch (LCP)

2. optionale Prozeduren, die in Phase 1 ausgemacht wurden (z.B. CHAP)
3. Netzwerk-Layer-Konfigurations-Verhandlung (erledigt von zugehörigen NCPs)
4. Verbindungsabschluss

161) Welche Parameter lassen sich bspw. durch LCP-PPP aushandeln?

Authentication; Maximum Receive Unit; Quality Protocol; Compression

162) Was ist das IPCP bei PPP? Was kann man damit machen? Zu welcher PPP Familie gehört es?

Das Internet Protocol Control Protocol (IPCP) dient zur automatischen Konfiguration von Computern, die sich typischerweise über eine Einwählverbindung wie Analog-Modem oder ISDN mit einem Netz verbinden. Bei der Konfiguration durch IPCP werden unter anderem die IP-Adresse, der Default-Gateway und die DNS-Server der einwählenden Arbeitsstation mitgeteilt. Ferner könnte beispielsweise auch der Komprimierungsalgorithmus durch IPCP definiert werden. Demzufolge funktioniert IPCP ähnlich wie DHCP in Ethernet-Netzwerken, jedoch für Einwählverbindungen (Punkt-zu-Punkt-Verbindungen).

IPCP gilt aufgrund seiner Funktion als NCP (Network Control Protocol) für das Internet Protocol (IP) über PPP.

163) Wie kann man Authentication mit PPP-CHAP durchführen (kurze Erklärung)? Warum verwendet man dabei Zufallszahlen?

Drei-Wege-Handshake-Verfahren:
Station, die Handshake startet, prüft Authentication des Anderen

1. zufälliger Wert (Challenge) an Station B übertragen, die sich authentifizieren muss
2. B bildet aus der Zufallszahl und dem Passwort einen Hashwert und überträgt zurück zu A; aus übertragenem Hashwert lässt sich das Passwort nicht wieder errechnen
3. Station A errechnet ebenfalls Hashwert aus der Zufallszahl der ID und bei ihm hinterlegten Passwort; Übereinstimmung -> Authentifizierung

164) Wozu wird bei einem ADSL-Anschluss das Protokoll PPP prinzipiell benötigt? Wieso werden Protokolle wie PPPoE oder PPTP noch zusätzlich gebraucht?

für Accounting und für die automatische Konfiguration des Endgeräts; um Authentifizierungs-Mechanismen (PAP, CHAP) nutzen zu können
PPPoE, PPTP, PPPoA wird benötigt, weil PPP nicht direkt auf einer Leitung läuft, sondern über ATM-Backbones (PPPoA) oder Ethernet-Segmente (PPPoE).

Chapter 9 – Introduction to IP Routing

165) Was ist ein Default Gateway und wann muss die IP-Adresse des Default Gateways in einem IP Host konfiguriert sein?

Als Default-Gateway wird eine Netzwerkadresse bezeichnet, an die Clients ihre Pakete senden, wenn die Zieladresse außerhalb des eigenen Netzwerks ist und keine anderen Hinweise (Routing-Informationen), wie das Zielnetzwerk erreicht werden kann, vorliegen.

166) Was sind die prinzipiellen Eigenschaften des „Static Routings“ (Stichwort: Management von Statischen Routen, Anpassung bei Topologieänderungen, CPU-Bedarf, Bandbreitenbedarf)?

- Routing-Tabellen sind vom Netzwerkadministrator vorkonfiguriert
- zeitintensives Setup und aufwändig zu ändern bei komplexen Netzwerken
- Topologie-Änderungen werden nicht automatisch behandelt
- kein zusätzlicher CPU-Bedarf
- kein Overhead-Traffic

167) Wann können statische Routen prinzipiell verwendet werden (Stichwort: Wegeredundanz)? Wann müssen statische Routen verwendet werden (Stichwort: Network Technologies)?

Statische Routen können bei Mangel an jeglichen Netzwerk-Redundanzen verwendet werden, z.B. bei Stub- oder Hub-and-Spoke-Netzwerken. Manchmal wird es auch aus Sicherheitsgründen eingesetzt oder weil es der einzige Weg in bestimmten Technologien ist.
Der Vorteil dieser Methode ist, das absolut kein Overhead vorhanden ist; der Nachteil ist allerdings das fehlende Reaktionsvermögen auf Topologie-Änderungen oder Ausfälle.
Statische Routen müssen verwendet werden, wenn die Netzwerktechnologie kein (oder nur schlecht) dynamisches Routing erlaubt (Dial on Demand Networks, z.B. X.25, ISDN, Frame Relay, ATM). Manchmal wird es auch auch Sicherheitsgründen verwendet.

168) Was passiert, wenn ein Router ein Datagram mit einer unbekannten Zieladresse empfängt und dem Router keine Default Route bekannt ist?

Das Datagram wird verworfen und eine ICMP-Message wird gesendet.

169) Was passiert, wenn ein Router ein Datagram mit einer unbekannten Zieladresse empfängt und dem Router eine Default Route bekannt ist?

das Datagram wird zu einer Default-Route (default network) gesendet -> ein anderer Router könnte mehr Netzwerke kennen

170) Was ist eine Default Route? Wo wird sie konfiguriert (am Router oder am IP Host)?

vorkonfigurierte Route, an die ein Paket mit unbekannter Zieladresse Default-mäßig gesendet wird; anderer Router hat vielleicht mehr Informationen; am Router konfiguriert

171) Warum ist die Technik der Default Route beim Anschluss eines IP-Netzwerkes an das Internet so wichtig? Welches Routing Paradigma spielt hier eine Rolle?

ohne Default-Route müsste jeder Router immer alles „wissen“ alle Ziele, die dem Router unbekannt sind, werden zu der Default-Route (Default-Network) gesendet; ein anderer Router könnte mehr Netzwerke kennen
Hop-by-Hop-Paradigma, weil der Router nur den Next-Hop kennen muss

172) Was sind die prinzipiellen Eigenschaften des „Dynamic Routings“ (Stichwort: Management von Routen, Anpassung bei Topologieänderungen, CPU-Bedarf, Bandbreitenbedarf)?

- Routing-Tabellen werden mit Informationen von anderen Routern dynamisch mit Hilfe von Routing-Protokollen aktualisiert
- bei Topologie-Änderungen werden die Routing-Tabellen automatisch angeglichen
- höherer CPU-Bedarf
- höherer Bandbreitenbedarf

173) Was ist die prinzipielle Aufgabe eines Routing-Protokolles? Welche Rolle spielt dabei die Metrik? Basieren die Metrik auf statischen oder dynamisch veränderbaren Parametern?

Routing-Protokoll erkennt aktuelle Netzwerk-Topologie; ermittelt besten Pfad zu jedem erreichbaren Netzwerk; behält Information über den besten Pfad in der Routing-Tabelle
Metrik-Information ist für die Entscheidung des besten Pfades nötig; in den meisten Fällen basiert die Metrik auf statisch vorkonfigurierten Werten

174) Was versteht man unter Konvergenz im Zusammenhang mit dynamischen Routing? In welchen typischen Bereich ist die Konvergenzzeit im worst case für RIP und OSPF angesiedelt (Minuten, Sekunden, Millisekunden)?

Die Zeit, die gebraucht wird, um Topologie-Änderungen auch in den einzelnen Routing-Tabellen wieder auszugleichen (RIP: Minuten; OSPF: Sekunden).

175) Charakterisieren Sie kurz die Distance Vector Methode. Bewirkt diese Methode am Router eine limitierte Sichtweise (Begründung)?

die Routing-Tabelle wird periodisch zu allen Nachbar-Routern gesendet (IP-Limited-Broadcast); eingehende Updates werden nach Änderungen durchsucht; die eigene Routing-Tabelle wird daraufhin angeglichen; diese Änderungen werden beim nächsten periodischen Update weitergegeben
=> limitierte Sicht der Topologie: die Sicht des Routers basiert nur auf seiner Routing-Tabelle -> genaue Sicht, wie man lokale Nachbarn erreicht; aber Topologie hinter den Nachbarn ist versteckt

176) Charakterisieren Sie kurz die Link State Methode. Bewirkt diese Methode am Router eine limitierte Sichtweise (Begründung)?

Bei Link-State-Protokollen haben die Router eine globale Sicht der Netzwerktopologie, also exakte Kenntnis über alle Router, Verbindungen und deren Kosten (Metrik) eines Netzwerks. Diese Informationen werden in einer Topologie-Datenbank („Roadmap“) gespeichert, man spricht dabei auch vom Straßenkarten-Prinzip (Roadmap-Principle).
Der SPF (Shortest Path First, Dijkstra)-Algorithmus wird angewandt, um die günstigste Verbindung zu jedem Zielnetzwerk zu finden; dieser wird dann in der Routingtabelle gespeichert. Veränderungen der Topologie (link up or down, link state) werden von Routern, die für die Überwachung dieser Verbindungen zuständig sind, erkannt und ins restliche Netzwerk weitergegeben.

177) Was wird bei RIP prinzipiell periodisch ausgesendet (Annahme kein Split Horizon)? Warum werden periodische Updates benötigt auch wenn es gar keine Änderungen in der Netzwerktopologie gibt? Wann altern Routen in der Routingtabelle bei RIP aus?

Routingtabelle wird alle 30 Sekunden an alle angeschlossenen Netze geschickt -> Routing-Update; nicht mehr am Netz befindliche Interfaces werden so erkannt und altern nach 180 Sekunden aus

178) Was sind „Good News“ im Zusammenhang mit RIP? Was sind „Bad News“ im Zusammenhang mit RIP? Wann werden „Bad News“ nicht ignoriert?

Nachrichten von einem metrisch besseren Pfad werden als „Good News“ bezeichnet und von jeder Quelle angenommen („trusted news“) und in der Routing-Tabelle verwendet.
„Bad News“ sind Meldungen über einen Pfad zu einem Netzwerk, der schlechter ist, als der, den man derzeit selbst kennt. Die Routing-Tabelle muss nur dann mit der neuen Information aktualisiert werden, falls der Sender des Routing-Updates der nächste Hop-Router für dieses Netzwerk ist.

179) Welches prinzipielle Problem gibt es bei RIP (Stichwort: Count-to-Infinity)? Was ist ein Routing-Loop und warum ist dieser so unangenehm?

Bei Count-to-Infinity passiert folgendes: Ein Netz, das direkt an einen Router angebunden ist, fällt aus. Nach 180 Sekunden altert der Eintrag des Routers aus und er weiß nicht mehr, wie und mit welcher Metrik er das Netz erreicht.
Nun erhält er aber ein Routing-Update von einem benachbarten Router, welcher vom Ausfall noch nichts mitbekommen hat und somit also einen Pfad zum ausgefallenen Netzwerk vorweisen kann.
Der Router empfängt dieses Update, das einen besseren Weg als seinen nicht mehr vorhandenen anbietet und trägt den Nachbarn als Next-Hop ein und übernimmt dessen Metrik.
War unser ursprünglicher Router allerdings der einzige Zugang in das ausgefallene Netz, zeigt der Nachbar eigentlich wieder auf ihn selbst als Next-Hop. Sendet er also nun selbst ein Routing-Update, übernimmt der Nachbar die schlechtere Metrik, die er dem Router beim nächsten Update wieder mitteilt usw.
Da jeder beteiligte Router dabei den Hop-Count erhöht, zählen sie so ins Unendliche (eigentlich nur bis 16, weil das ist das RIP-Limit); IP-Pakete werden inzwischen im Kreis geschickt.
Ein Routing-Loop ist unangenehm, weil es lange dauert, bis die Routing-Tabellen wieder konsistent sind. So lange werden IP-Pakete im Kreis geschickt.
(Folie 46 ff)

180) Was bewirkt der Max-Hop-Count im Zusammenhang mit dem Count-to-Infinity Problem? Kann dadurch ein temporärer Routing-Loop verhindert werden?

Maximum Hop Count: maximale Distanz zwischen zwei Subnetzen ist auf 16 beschränkt; Distanz-Wert von 16 in Routing-Tabelle bedeutet, dass das zugehörige Netzwerk nicht erreichbar ist
Routing-Loops können allerdings nicht verhindert werden

181) Was ist Split Horizon im Zusammenhang mit RIP? Was ist Poisen Reverse im Zusammenhang mit RIP? Kann durch diese Methoden ein temporärer Routing-Loop immer verhindert werden?

Split-Horizon wurde entwickelt, um der langsamen Konvergenz und den Routing-Loops entgegenzuwirken; Maximum-Hop-Count alleine kann nämlich Schleifen nicht verhindern.
Split-Horizon hält Router davon ab, Informationen über die Erreichbarkeit eines Netzwerkes in die Richtung, aus der die Information ursprünglich kam, weiterzuleiten. Eine Ausnahme dieser Regel ist, wenn der Router einen besseren Pfad kennt. Es imitiert also eine menschliche Verhaltensweise: “Don’t tell me what I’ve told you!”

Poison-Reverse ist eine alternative Methode gegen Routing-Loops und langsame Konvergenz. Der Router sendet Unerreichbarkeits-Nachrichten („Poison“) via Routing-Updates in die Richtung, aus der die Information über dieses Netzwerk ursprünglich kam. Sobald der Eintrag also ausaltert, wird er sofort mit 16 überschrieben.

182) Was ist Hold Down im Zusammenhang mit RIP? Kann dadurch ein temporärer Routing-Loop immer verhindert werden?

Hold-Down ergänzt Split-Horizon in komplexen Netzwerkumgebungen, in denen es allein oft nicht ausreicht. Wenn z.B. Router einen Ring bilden, hilft Split-Horizon nichts, wenn Updates im Kreis weitergegeben werden.
Die Grundidee hinter Hold-Down ist, dass Netzwerkfehler-Nachrichten eine bestimmte Zeit benötigen, um sich wie eine Welle über das Netzwerk auszubreiten.
Mit Hold-Down erhalten alle Router die Chance, diese Nachricht zu empfangen, indem er nach dem Empfang solch einer Fehlernachricht für einen bestimmten Zeitraum (typischerweise 240 Sekunden) keine weiteren Informationen über dieses Netzwerk mehr annimmt. Der Nachteil dieser Methode ist allerdings die langsame Konvergenzzeit.

183) Ist das Grundprinzip von RIPv2 identisch mit RIPv1? Welche drei wichtigen zusätzlichen Features weist RIPv2 im Vergleich zu RIPv1 auf (Stichworte: Classless Routing, Adressierung von RIP Updates am LAN (Ethernet) und IP Layer, Sicherheit)?

prinzipiell gleiches Grundprinzip, aber mit Verbesserungen:
RIPv2 verwendet die ungenutzten Felder im RIPv1-Message-Format

die drei wichtigsten zusätzlichen Features:

1. Classless-Routing: RIPv2 unterstützt Classless-Routing, kann also (beliebige, nicht nur Class A, B, …) Subnetzmasken weitergeben.
2. Adressierung von RIP-Updates am LAN (Ethernet): RIPv2 verwendet Class-D-Multicast-Adressen statt Broadcasts wie RIPv1, um Routing-Updates weiterzugeben. Deswegen müssen auch nur mehr die Router, die Mitglied der Multicast-Gruppe sind, die Pakete bearbeiten.
3. Sicherheit: RIPv2 unterstützt Authentifizierungsmechanismen: Routing-Updates werden nur von „trusted“ Routern angenommen.

184) Welche prinzipielle Eigenschaft eines Routing Protocols bewirkt Classful Routing? Kann VLSM Technik verwendet werden? Werden IP Subnetze an der Klassengrenze zusammengefasst, wenn diese in Updates in Richtung anderen IP Netze gemeldet werden?

Routing-Potokolle wie RIP oder IGRP können keine Subnetz-Informationen in ihren Routing-Updates behandeln. Das hat mehrere Konsequenzen; wenn eine gegebene Class-A-, B-, oder C-Adresse gesubnetted ist, muss die Subnetzmaske im Ganzen Gebiet gleich sein – es kann keine Variable-Length-Subnet-Mask (VLSM) genutzt werden.
Wenn ein Routing-Update an ein Interface mit einer Netzwerknummer verschieden von der des Subnetted-Network gesendet wird, wird nur die übergeordnete Klasse A, B oder C mitgeteilt.
Route-Summarization wird an den Klassengrenzen ausgeführt werden, daher muss eine Subnetted-Area kontinuierlich sein. Dieses Verhalten wird als Classful-Routing bezeichnet.

185) Welche prinzipielle Eigenschaft eines Routing Protocols bewirkt Classless Routing? Kann VLSM Technik verwendet werden? Werden IP Subnetze an der Klassengrenze zusammengefasst, wenn diese in Updates in Richtung anderen IP Netze gemeldet werden?

Classless-Routing-Protokolle wie RIPv2, OSPF oder eIGRP können Subnetzinformationen in Routing-Updates behandeln. Dies hat mehrere Vorteile; VLSM kann genutzt werden, d.h. das Subnetting einer

gegebenen Adresse kann entsprechend der voraussichtlichen Anzahl an Hosts durchgeführt werden und so der Adressraum effizienter genutzt werden (Subsubnetting).
Route-Summarization kann an jeder Adressgrenze durchgeführt werden und nicht nur an Klassengrenzen.

186) Was ist die VLSM-Technik? Wann kann diese eingesetzt werden (bei Classful oder Classless Routing)? Was ist der positive Aspekt bezüglich Ausnützung eines zugewiesenen IP Adress-Bereiches?

Bezeichnet die Möglichkeit, unterschiedlich lange Subnetzmasken für die gleiche Netzwerknummer in verschiedenen Subnetzen angeben zu können. VLSM hilft damit, den verfügbaren Adressraum besser auzulasten.

kann bei Classless-Routing eingesetzt werden

187) Was ist Supernetting? Wo kann es verwendet werden (bei Classful oder bei Classless Routing)? Welchen positiven Effekt hat das auf das Internet Routing?

Supernetting: mehrere Netzwerke werden nach außen zu einem zusammengefasst; die Subnetzmaske ist kleiner als die eigentliche Subnetzmaske einer gegebenen Klasse

kann bei Classless-Routing verwendet werden

positiver Effekt: die Routing-Tabellen werden kleiner; statt aller einzelnen Netze müssen die Router nur mehr das eine Supernet kennen

188) Warum sollte auch bei Classless Routing, die IP Adressierung der physikalischen Topologie folgen (Stichwort: Anzahl der Einträge in den Routing Tabellen der Internet Core Router, CIDR)?

Um die Anzahl der Einträge in der Routingtabelle klein zu halten, sollte die Adressierung der Netze die Routenzusammenfassung möglichst effizient nutzen – vor allem in großen Netzen wie dem Internet.
Die Adressierung sollte der physikalischen Topologie folgen, weil sonst u.U. die Pakete lange Wege zurücklegen müssen.

189) Wozu dienen die privaten IP Adress-Bereiche? Welche Rolle spielt NAT in diesem Zusammenhang?

Drei Adressblöcke wurden für die Adressierung von privaten Netzwerken reserviert:
10.0.0.0 – 10.255.255.255 (10/8 Prefix)
172.16.0.0 – 172.31.255.255 (172.16/12 Prefix)
192.168.0.0 – 192.168.255.255 (192.168/16 Prefix)

Wenn ein Host mit einer privaten IP-Adresse ins Internet verbinden will, so geht das erst einmal nicht, weil private IP-Adressen nicht eindeutig sind und auch nicht geroutet werden können.
Lösung: Die Übersetzung von privaten in global einzigartige Adressen erfolgt über NAT.

Chapter 10 – OSPF Fundamentals

190) Was ist kurz und prägnant die Grundidee von OSPF (Stichworte: Topology Database, Shortest Path)? Wie kommt ein OSPF Router zu seiner Routingtabelle? Was ist der fundamentale Unterschied zu RIP?

Die Grundidee ist, dass jeder Router die gesamte Netzwerktopologie inklusive Subnetze und anderer Router kennt.

Die Routing-Tabelle wird mittels eines Algorithmus errechnet.

Es gibt kein Warten auf die Gerüchte anderer Router mehr, was Grund für viele Probleme unter RIP war, da andere Router sich auch auf Gerüchte verließen.

191) Wie funktioniert der Dijkstra Algorithmus bei OSPF prinzipiell?

Jeder Router führt eine Topology-Database, eine Art Straßenkarte für das Netzwerk (RIP hat nur Signposts). Diese Datenbank basiert auf einem Graphen, in dem jeder Knoten für einen Router und jede Kante für ein Subnetz steht. Den Kanten werden Wegkosten zugeordnet. Der Dijkstra-Algorithmus sorgt dafür, dass es zu jedem Knoten im Netzwerk nur noch einen Weg gibt.
Der Router benutzt diesen Graphen, um den kürzesten Weg zu allen Subnetzen zu berechnen.

Prinzip:
1. Auswahl der Wurzel
2. Nachbarn der Wurzel werden hinzugefügt
3. Auswahl von V mit den geringsten Kosten
4. Nachbarn werden hinzugefügt
5. für diese Nachbarn werden die Kosten mit Hilfe von V als Vorgänger berechnet
6. weiter mit 3

192) Wofür stehen Link States bei OSPF? Wie kommen sie zustande? Schildern Sie kurz die Kommunikationsabläufe beim Kennenlernen zweier benachbarter OSPF Router bis zum Ereignis Link State ok. Welches LSA wird am Ende dieses Prozesses generiert?

Bis jetzt wurde immer eine a priori vorhandene, konsistente Datenbank in jedem Router angenommen. In Wirklichkeit sind der Grundstein zur Erstellung und dem Erhalt dieser Datenbank die sogenannten „Link States".
Ein Link-State steht für lokale Nachbarschaft zwischen zwei Routern. Der Link-State wird von diesen zwei Routern erzeugt, andere Router werden über diesen Link-State über einen Broadcast-Mechanismus in Kenntnis gesetzt.
Link-States werden kontinuierlich durch „Hello"-Messages überprüft. Jede Link-State-Veränderung wird allen anderen Routern der OSPF-Domain kundgemacht. Dazu werden Link-State-Advertisements (LSAs) – ein weiterer Broadcast-Mechanismus – benutzt.
LSAs sind viel kleiner als Routingtabellen, da sie nur die eigentlichen Veränderungen enthalten, weshalb Distance-Vector-Protokolle auch langsamer sind.
Die ganze Topologiekarte beruht auf LSAs.

Während der Initialisierung sendet ein Router „Hello"-Messages an alle seine direkt erreichbaren Nachbarn, um seine Nachbarschaft kennen zu lernen. Dies kann in Broadcast-Netzwerken und bei Point-to-Point-Verbindungen durch Verwendung der IP-Multicast-Adresse 224.0.0.5 (all OSPF-Routers) geschehen. In nicht-Brodcast-Netzwerken müssen die Nachbarschaftsrouter eigens konfiguriert werden (z.B. X.25). Dieser Router empfängt ebenfalls „Hello"-Messages von anderen Routern.
Zwei einander bekannte Router senden sich gegenseitig Database-Description-Messages, um ihre Topologiedatenbanken bekannt zu machen. Der empfangende Router überprüft diese auf unbekannte oder alte Einträge, welche dann über Link-State-Requests und Link-State-Update-Messages nachgefragt und aktualisiert werden, was die Topologiedatenbanken synchronisiert.
Der Empfang jeder Message wird dabei durch ein LSA-ACK bestätigt. Nach der erfolgreichen Synchronisation erklären beide Router ihre Nachbarschaft über Router-LSAs (using link state update messages), verteilt über das ganze Netzwerk.
Jeder Router kontrolliert regelmäßig seinen Link-State zu den Nachbarn über „Hello"-Messages.

Welches LSA wird am Ende dieses Prozesses generiert? Router-LSA.

193) Was ist ein LSA prinzipiell? Wann wird ein LSA ausgesendet? Wer ist für das Aussenden eines LSA verantwortlich? Was bewirkt ein LSA bei anderen OSPF Routern?

LSA … Link State Advertisement

Ein LSA ist eine Nachricht von einem Router, die allen anderen Routern mitteilt, dass dieser Router direkt mit einem anderen Router (wird dann ein Router-LSA) oder Netzwerk (wird ein Netzwerk-LSA; nur von Designated-Routern) verbunden ist.
Wann wird ein LSA ausgesendet? Wenn sich an den Links etwas ändert sofort und außerdem alle 30 Minuten für alle Links.

194) Wie erfolgt die Verteilung eines LSA's über die gesamte OSPF Domain? Wie kann man das anschaulich beschreiben? Welche Bedeutung hat dabei die LSA Sequence-Number?

OSPF-Messages werden über IP transportiert; sie haben IP-Protokollnummer 89.

LSAs müssen sicher an alle Router in der Area (Domain) verteilt werden; die Konsistenz der Topologie-Datenbanken verlässt sich darauf. Ein LSA wird daher geflooded und an alle Nachbarn weitergesandt.

Jedes LS-Update wird explizit bestätigt. Wenn eine solche Bestätigung ausständig bleibt, wird das LS-Update erneut gesendet (Timeout).
Wenn das LS-ACK nach mehreren Versuchen nicht ankommt, wird die Nachbarschaftsbeziehung aufgelöst. Diese Methode sichert ein verlässliches Weiterleiten von LSAs.
LSAs werden immer von Hop zu Hop übertragen, dabei bestätigt der Router zuerst den Empfang und schickt es erst dann weiter. Die LSAs tragen eine Sequenznummer, damit dieselbe LSA nicht immer im Kreis wandert und um sie einzigartig und somit wieder erkennbar für die Bestätigung zu machen.

195) Welche OSPF Messages gibt es (Aufzählung)? Wie werden diese transportiert? Warum benötigt man ein LS Acknowledgement? Wie erfolgt die Adressierung von OSPF Messages auf LANs?

OSPF-Messages:
- hello
- database description
- LS request
- LS update
- Router LSA
- Network LSA
- LS ACK

über IP transportiert; ACK benötigt, weil IP die Übertragung nicht garantiert; Adressierung der OSPF-Messages auf LANs erfolgt mit Dedicated-IP-Multicast-Adressen (224.0.0.5 und 224.0.0.6).

196) Welches Problem tritt bei OSPF in einer Broadcast Umgebung (LANs) auf? Wie wird es prinzipiell gelöst? Hat das auf das Weiterleiten von IP Datagrammen einen Einfluss?

Das Basiskonzept von Link-State beruht auf Point-to-Point-Verbindungen. Dieses Konzept passt am besten für Point-to-Point-Netzwerke wie Serial-Lines. Das verursacht jedoch ein Problem mit Shared-Media-Multiaccess-Networks, z.B. in LANs.
Hello, Database-Description und LSA-Updates zwischen all diesen Routern kann hohen Netzwerk-Traffic und CPU-Belastung verursachen. Wenn mehrere Router ein Multiaccess-Netzwerk teilen, skaliert Any-to-Any sehr schlecht. Die Information über sämtliche möglichen Nachbarschaftsbeziehungen erscheint redundant.
Das Konzept des Virtual-Node (oder Virtual-Router) wurde eingeführt, um das Problem zu lösen. Nur der Virtual-Node muss N-1 Point-to-Point-Verbindungen aufrechterhalten; Any-to-Any ist nicht notwendig. In OSPF wird dieser Virtual-Node Designated-Router (DR) genannt.
Im Falle eines Fehlers des DR würde dies einen „single point of failure“ darstellen, daher wird ein zusätzlicher Backup-Designated-Router (BR) benutzt.
Hat nur Einfluss darauf, wie Routing-Informationen übertragen werden, nicht auf das Routing an sich.

197) Welche Funktion hat der Designated Router in einer Broadcast Umgebung? Wozu dient der Backup Router? Mit welchen LSA-Typ wird eine Broadcast Umgebung bekannt gegeben und wer gibt es bekannt?

Der Designated-Router (DR) versorgt alle anderen Router dieses Segments mit Nachbarschaftsverbindungen über virtuelle Punkt-zu-Punkt-Verbindungen. Der DR ist für das Senden von Network-LSAs verantwortlich. Ein Network-LSA beschreibt, welche Router Mitglieder des zugehörigen Broadcast-Netzwerkes sind.
Der Backup-Router (BR) ist die Ausfallssicherung für den DR, er übernimmt dessen Aufgabe, falls dieser ausfällt.

Chapter 11 – Internet Transport Layer

198) Was sind die grundlegenden Eigenschaften von TCP (OSI Layer, Connectionless oder Connectionoriented Protokoll Service, nur auf IP Hosts oder auf IP Hosts und IP Routern präsent, Error Recovery vorhanden ja oder nein, Flow Control vorhanden ja oder nein)?

Es ist ein zuverlässiges, verbindungsorientiertes Transportprotokoll. Es ist in Schicht 4 des OSI-Referenzmodells angesiedelt. Auf Grund seiner vielen angenehmen Eigenschaften - Datenverluste werden erkannt und automatisch behoben, Datenübertragung ist in beiden Richtungen möglich, Netzwerküberlastung wird verhindert (Flow-Control) und viele mehr - ist TCP ein weit verbreitetes Protokoll zur Datenübertragung. TCP ist nur auf IP-Hosts präsent.

199) Welche Klassifizierung gemäß Kapitel „Protocol Principles" kann man für TCP treffen? Welche Spielart des Error Recovery wird dabei realisiert? Welche Spielart der Flow Control wird dabei realisiert?

Full-Duplex-Protokoll; Piggy-Packed-ACKs; Error-Recovery: Sequenznummer und Positive-Acknowledgement; Flow-Control durch Adaptive-Windowing

200) Wozu dienen TCP Ports? Wer ist Client und wer ist Server aus Sicht einer TCP Verbindung?

TCP stellt seine Services an höhere Schichten durch Ports zur Verfügung. Jedem kommunizierenden Prozess wird eine Portnummer zugeordnet.
Wenn aber ein Rechner mehrere Dienste über denselben Port in Anspruch nehmen will, müssen diese simultanen Verbindungen zusätzlich gekennzeichnet werden. Das geschieht über Socketnummern (zusammengesetzt aus der IP-Adresse und dem jeweiligen Port).
Die TCP-Software funktioniert also wie ein Multiplexer und Demultiplexer für TCP-Verbindungen.
0-1023 sind die Well-Known-Ports, also vordefinierte Ports, die für bestimmte Services reserviert sind (z.B. Port 80: HTTP) und ab 1024 kommen die registrierten Ports.
Client ist derjenige, der das Service, das durch den Server zu Verfügung gestellt wird, verwendet. Der Client stellt die Verbindung her, der Server lauscht und wartet.

201) Wie erfolgt die Handhabung der TCP Portnummer auf der Client Seite einer TCP Verbindung?

Client-Application wählt einen freien Port (zwischen 1024 und 65 535); Client einer TCP-Verbindung ist der, der die Verbindung anfordert; Server der, der auf eine Anforderung wartet (muss nicht zwingend wirklich ein Server sein)

202) Was sind well-known TCP Port Nummern? Was kennzeichnen sie?

sind für häufige Applikationen und Services wie Telnet, WWW, FTP usw. reserviert; gehen von 0 bis 1023; werden von der IANA (Internet Assigned Numbers Authority) kontrolliert; Server-Applikationen lauschen auf ihren Well-Known-Ports nach eingehenden Verbindungen

203) Wozu benötigt man die Socket Nummern?

Sockets sind die Kombination aus IP-Adresse und Port-Nummer. Mit dem Socket spricht man sozusagen einen bestimmten Port auf einem bestimmten Server an

204) Wie erfolgt der TCP Verbindungsaufbau im Detail?

mit dem Three-Way-Handshake-Verfahren; Client (Initiator) schickt eine SYN-Message mit seiner (zufälligen) SEQ-Nummer an den Server (Listener); anschließend schickt der Server ein SYN mit seiner (zufälligen) SEQ-Nummer und ein ACK mit der SEQ-Nummer + 1 vom Client als Bestätigung zurück an den Client; dieser bestätigt wiederum mit einer ACK-Message mit der SEQ-Nummer + 1 vom Server; nach dieser Aktion ist die Verbindung aufgebaut und die Gesprächspartner sind synchronisiert

205) Wie erfolgt der TCP Verbindungsabbau im Detail?

Der Verbindungsabbau erfolgt ähnlich dem Three-Way-Handshake.
Beim Verbindungsabbau müssen beide Seiten ein FIN-Flag an die Gegenseite schicken, das durch ein ACK von der Gegenseite wahrgenommen wird.
Der Austausch von FIN- und ACK-Flags versichert, dass beide Parteien alle Oktette erhalten haben.

206) Warum müssen beim TCP Verbindungsaufbau die Startwerte der Sequence Numbers synchronisiert werden? Warum wählte man diesen Ansatz?

Die Wahl der Start-Sequenznummer erfolgt zufällig, da noch Segmente von älteren Sessions herumschwirren können. Durch den Zufallswert wird TCP immun dagegen. Diese Zufallszahl muss aber auch mit dem Receiver synchronisiert werden („Three-Way-Handshake“).

207) Was kennzeichnet die Sequence Number exakt im Bezug auf den TCP Oktett Strom? Was kennzeichnet die Acknowledgement Number exakt im Bezug auf den TCP Oktett Strom? Wie ist die Handhabung der Sequence Numbers zweier unmittelbar hintereinander folgender TCP Segmente (Blöcke)?

Sequenznummer: 32 Bit; kennzeichnet die Position des ersten Nutzdatenbytes dieses TCP-Segments
ACK-Nummer: 32 Bit; bestätigt alle vorhergehenden Oktette und zeigt die Nummer des Oktetts, das als nächstes vom Empfänger erwartet wird

Handhabung der Sequenznummern:
-> Segment A (3 Byte): Seq = 902 (3 Bytes Nutzdaten: #902, #903, #904)
<- ACK 905
-> Segment B (5 Byte): Seq = 902 + 3 = 905 (#905, ..., #909)

208) Wie erfolgt das Error Recovery ursprünglich bei TCP? Welche Änderung hat sich beim aktuellen TCP ergeben und warum?

Ursprünglich: Paket geht verloren -> Empfänger sendet kein ACK; Sender wartet auf Timeout; Retransmission

Aktuell: Paket geht verloren; Empfänger sendet Duplicate-ACKs für das verlorene Paket; nach 3 Duplicate-ACKs sofortige Retransmission

Warum: weniger unnütze Wartezeit; bessere Ausnützung der Bandbreite

209) Wieso muss das Timeout für Error Recovery bei TCP adaptiv ausgelegt werden? Über welchen Bereich erstreckt sich die TCP Checksum? Sind in der TCP Checksum auch Teile des IP Headers enthalten?

Timeout hat Einfluss auf die Performance eines Systems; zu lange -> lange Wartezeit; zu kurz -> möglicherweise viele Pakete noch einmal senden
TCP-Checksum erstreckt sich über TCP-Header, TCP-Data und 12 Byte Pseudo-IP-Header; dieser enthält: Source- und Destination-IP-Address, IP-Protocol-Type, IP-Total-Length
dies dient dazu, den ganzen Socket zu schützen, auch jene Bereiche, die mit TCP nicht erfasst werden (Socket = IP-Adresse + TCP-Port)

210) Wie wird das adaptive Windowing für TCP Flow Control exakt realisiert (Stichworte: Zusammenspiel Window Feld, Acknowledgement Number Feld im empfangenen TCP Segment, Auswirkungen auf das Sliding Window bezüglich linke und rechte Kante des Fensters im laufenden Sequence Number Raum)?

Der Sender darf nur so viele Bytes offen - also unbestätigt - haben, wie der Empfänger ihm im Window-Feld mitgeteilt hat.
Wenn ein ACK (z.B. für 4 Bytes) eintrifft, verschiebt sich die linke Kante um 4 nach recht. Wenn das Window-Feld gleich bleibt, verschiebt sich die rechte Kante auch um 4, es können also 4 weitere Bytes gesendet werden.
Wenn das Window-Feld gleichzeitig um 4 kleiner wird, verschiebt sich die rechte Kante nicht (+4 wegen ACK, -4 wegen kleinerer Window-Size = 0), es darf also nichts mehr gesendet werden.

211) Welche Grundannahme gibt es beim TCP „Slow Start and Congestion Avoidance Algorithm“ bezüglich Verlust von TCP Segmenten?

TCP-Segmente gehen vor allem durch Überlastung verloren und nicht durch Bitfehler auf den Leitungen, da die Übertragung sehr robust ist (optische und digitale Übertragung).

212) Was ist die Grundidee des „Slow Start and Congestion Avoidance Algorithm“ bei TCP?

Man versucht, sich an die maximale Kapazität des Netzes heranzutasten - Balance zwischen möglichst hohem Durchsatz und niedrigem Packet-Loss.
Mit dem Congestion-Window wird dazu ein zusätzliches Fenster eingeführt. Das Congestion-Window startet mit der Größe 1 und wird mit jedem ACK vergrößert. Wenn es sich nun staut, wird wieder langsamer gesendet.

213) Wie lässt sich beim TCP „Slow Start and Congestion Avoidance Algorithm“ ein leichter Stau (Congestion) von einem schweren Stau unterscheiden (Stichworte: Timeout versus Duplicate Ack)?

geht ein Paket verloren, die die unmittelbar danach kommen, gehen aber durch, so schickt der Empfänger Duplicate-ACKs -> leichter Stau
gehen ab einem gewissen Punkt alle Pakete verloren, so schickt der Empfänger auch keine Duplicate-ACKs; der Sender merkt nun durch den Timeout, dass etwas schief gegangen ist -> schwerer Stau

214) Schildern Sie was prinzipiell beim TCP „Slow Start and Congestion Avoidance Algorithm“ passiert (Stichworte: congestion window cwnd, round trip time RTT, slow start threshold ssthresh, exponential versus linear)?

- sstresh = 65535 (maximal möglicher Wert)
- cwnd = 1 Segment

- solange cwnd < sstresh, wird cwnd jede RTT (= mit jedem empfangenen ACK) verdoppelt
- wenn aber cwnd > sstresh, so folgt nur mehr ein linearer Anstieg von cwnd (Congestion-Avoidance)

bei Fehlern:
1) wenn Duplicate-ACKs auftreten:
   a) ssth = cwnd/2
   b) cwnd = ssth
2) wenn ein Timeout auftritt
   a) ssth = cwnd/2
   b) cwnd = 1 Segment

215) Welche Performanceaspekte stellen sich durch den TCP „Slow Start and Congestion Avoidance Algorithm“ für zwei Rechner, die über eine TCP Verbindung kommunizieren, prinzipiell ein?

bzgl. der Übertragungsrate: ein Wave-Effekt; sie pendelt zwischen maximaler Übertragungskapazität und der Hälfte davon

216) Was sind die grundlegenden Eigenschaften von UDP (OSI Layer, Connectionless oder Connectionoriented Protokoll Service, nur auf IP Hosts oder auf IP Hosts und IP Routern präsent, Error Recovery vorhanden ja oder nein, Flow Control vorhanden ja oder nein)?

OSI-Layer 4; Connectionless; verwendet die selben Ports wie TCP; UDP ist bei weitem nicht so komplex wie TCP; kein Flow-Control; UDP stellt Prüfsumme für die Daten zur Verfügung

217) In welchen drei charakteristischen Situationen wird UDP eingesetzt?

- wenn der Overhead des Herstellens einer TCP-Verbindung nicht erwünscht ist; z.B. für sehr kurze Anfragen (DNS, ...)
- wo die Implementation so klein wie möglich sein muss (TCP ist komplex, UDP einfach)
- wo die Neuübertragung von verlorengegangenen Datenpakten nicht erforderlich ist (z.B. VoIP)

Chapter 12 - Application Protocols for Administration

218) Was ist die Grundidee des BootP Protokolls? Wie ist der Transportmechanismus (UDP oder TCP)? Welche Datenbank muss der BootP Server haben? Wie werden BootP Messages adressiert (ohne Einsatz eines BootP Relay Agents)?

BootP wurde entwickelt, um Clients Betriebssystem-Code und Konfigurations-Parameter von einem zentralen Server laden zu lassen.
Transportmechanismus: UDP

Datenbank: Eine Tabelle, die MAC-Adressen IP-Adressen und ggf. weitere Parameter zuordnet.
Adressierung: IP-Limited-Broadcast (Source-Address: 0.0.0.0, Destination-Address: 255.255.255.255)

219) Welche Konfigurationsparameter lassen sich im BootP Basis Header in der Antwort transportieren (Aufzählung)? Wozu dienen sie bzw. welche Abläufe folgen nach BootP?

Konfigurationsparameter in der Antwort (Transaction-ID etc. sind keine Konfigurationsparameter):
YOUR IP: IP-Adresse des Clients
SERVER-IP: IP-Adresse des Servers, der das Boot-Image zur Verfügung stellt
SERVER HOST NAME: Hostname dieses Servers
BOOTFILENAME: beinhaltet den Pfad und Filenamen des Bootfiles
ROUTER IP: IP-Adresse des BootP-Relay-Agent

nach BootP kann der Host über das Netzwerk booten

220) Wozu benötigt man ein BootP Relay Agent? Was passiert in diesem Fall? Wo spiegelt sich das im BootP Basis Header wieder?

Ein Relay-Agent ist ein kleines Programm, das als Relay für DHCP/BOOTP-Nachrichten zwischen Clients und Servern in verschiedenen Subnetzen dient.
Broadcasts funktionieren nicht über Subnetzgrenzen (bzw. Router) hinweg. Wenn der BootP-Server in einem anderen Subnetz steht als ein Client, benötigt man einen Relay-Agent, um die BootP-Broadcasts dorthin weiterzuleiten.
Der Relay-Agent setzt ROUTER IP ADRESS auf seine IP-Adresse und leitet das Paket an den BootP-Server weiter. Der BootP-Server antwortet an diese ROUTER IP ADRESS.

221) Wodurch besteht ein Zusammenhang zwischen DHCP und BootP? Welche Basis DHCP Messages gibt es (Aufzählung)?

DHCP ist eine Erweiterung von BootP. DHCP verwendet das „VENDOR SPECIFIC AREA“-Feld von BootP für weitere Konfigurationsparameter.
DHCP-Messages:
- DHCPDISCOVER
- DHCPOFFER
- DHCPREQUEST
- DHCPACK
- DHCPNACK
- DHCPRELEASE
- etc.

222) Was kann man mit DHCP alles bewerkstelligen? Welche Arten der Address Allocation gibt es bei DHCP (kurze Erklärung)?

Mit DHCP kann man folgende Parameter dynamisch vom Server an den Client übergeben lassen:
- alle BootP-Parameter
- IP-Adresse
- Subnetzmaske
- DNS-Server
- NetBios-Name-Server
- default TTL
- MTU
- List of Default Gateways
- Ethernet Encapsulation

Es gibt drei Arten von Address-Allocation:
a) Dynamic: der Client erhält eine Adresse aus einem Adresspool für eine limitierte Zeitspanne
b) Autmatic: es wird eine permanente IP an den Host übergeben
c) Manual: IP-Adresse wird manuell am Client festgelegt und nur diverse andere Parameter werden vom DHCP-Server geholt

223) Schildern Sie kurz die Abfolge des Protokolls, damit ein DHCP Client zu einer dynamischen IP Adresse kommt?

1) DHCPDISCOVER: Broadcast, um den DHCP-Server zu finden
2) DHCPOFFER: DHCP-Server bietet eine IP-Adresse an
3) DHCPREQUEST: Parameteranforderung durch Client
4) DHCPACK: Server gibt die IP-Adresse mit den Parametern und eine Bestätigung

224) Woran erkennt ein DHCP Client, wie lange er eine dynamische Adresse verwenden kann? Was passiert, um die Adresse zu erneuern (Spiel mit Timern T1, T2)?

am Feld LEASELENGTH im DHCPACK-Paket; zusätzlich werden die Zeiten T1 und T2 übergeben; nach 0,5 der LEASELENGTH (T1) wird versucht, die LEASE-Time für die IP-Adresse zu verlängern; klappt dies nicht, versucht sich der Client bei 0,85 der LEASELENGTH (T2) eine neue (ggf. andere) IP-Adresse zu holen

225) Wozu dient das TFTP Protokoll? Welche Grundeigenschaften hat es? Wie ist der Transportmechanismus (UDP oder TCP)? Welche Klassifizierung gemäß Kapitel „Protocol Principles“ kann man für TFTP treffen?

Das Trivial File Transfer Protocol wurde für ressourcenarme Systeme entwickelt. Es arbeitet mit UDP und ist hauptsächlich für disklose Systeme gedacht.
Es ist Connection-oriented und verwendet das Idle-RQ-Prinzip und Sequenznummern.

226) Was macht DNS prinzipiell? Wie ist der Transportmechanismus für DNS Messages (UDP oder TCP)? Warum benötigt man symbolische Namen?

DNS ist das Domain Name Service. Es löst alphanumerische Namen in IP-Adressen auf. DNS-Anfragen werden normalerweise auf Port 53 UDP beantwortet (falls die Antwort sehr umfangreich ausfällt (größer 512 Bytes), wird diese auf Port 53 TCP übermittelt). Zonentransfers werden stets auf Port 53 TCP durchgeführt.
Symbolische Namen werden verwendet, weil man sich diese leichter merken kann.

227) Wie ist der Aufbau des DNS Directories (Verzeichnis, „Telefonbuch“) gelöst? Warum macht man das so? Wie kann man da mit einem Filesystem vergleichen?

DNS teilt Hosts in Bäume = Verzeichnishierarchie ein; jeder komplette Subtree (+ Untereinträge) der Hierarchie = Domain; kompletter Name eines Node (Domain, Host) = Domain-Name; dieser Domain-Name-Tree spiegelt nicht die physische Netzwerkstruktur wider
Warum: Um die enorme Anzahl an Einträgen effizient verwalten zu können und um die Verwaltung der einzelnen Domains delegieren zu können.
Heutige Dateisysteme sind auch nach Bäumen organisiert.

228) Wie erfolgt die Bildung eines symbolischen Namens im Bezug auf den DNS Tree? Welche Bedingungen gibt es für die Bildung eines Label? Was versteht man unter einer Domain? Was versteht man unter einem Domain Name? Wie ist der DNS Baum tatsächlich realisiert?

Der symbolische Name wird gebildet, indem man von der Wurzel (.) ausgeht und alle folgenden Labels mit . verknüpft.
Ein Label darf nur „A-Z“ und „0-9“ mit maximal 63 Zeichen enthalten. Ein Domain-Name ist der symbolische Name eines bestimmten Nodes (z.B. orf.at). Eine Domain ist ein kompletter Subbaum, also alles unter einem bestimmten Domain-Name (z.B. *.orf.at).
Der DNS-Baum ist tatsächlich auf viele verschiedene Server verteilt – er ist eine Distributed-Database.

229) Wozu dient die In-Addr.Arpa Domain? Was kann man damit machen?

Mit der In-Addr.Arpa-Domain kann man Reverse-Lookups durchführen, also zu einer gegebenen IP-Adresse den dazugehörigen Hostnamen herausfinden.

230) Welche Parameter lassen sich prinzipiell über DNS erfragen (Aufzählung der vier wichtigsten Ressource Records plus ihrer Bedeutung)?

A: Host-Adresse

NS: autoritativer Name-Server
MX: Mailserver, der für diesen Domain-Name zuständig ist
PTR: um zu einer IP-Adresse den Domain-Name zu finden
CNAME: authorisierter Name für einen Alias
SOA: Authoritätsursprung

231) Was ist die Grundidee, um den DNS Namensbaum auf DNS Server aufzuteilen? Wie sind DNS Server untereinander prinzipiell verkettet? Wann erfolgt diese Verkettung? Wozu benötigt man die Root Hints?

Die Grundidee ist, dass jeder DNS-Server (immer repliziert, um bessere Ausfallsicherheit zu gewährleisten) für eine eigene Zone verantwortlich ist. Es darf keine Überschneidungen geben, da es sonst zu inkonsistenz kommen kann.
DNS-Server sind von oben nach unten verkettet. Will man einen Domain-Name auflösen, muss man sich von oben nach unten durchhangeln, bis man schließlich den zuständigen Nameserver gefunden hat.

Root-Hints: Wo fängt man an mit der Auflösung? Bei einem Root-Server. Und wie bekommt man den, wenn man keinen kennt? Genau, gar nicht. Deswegen benötigt man (mindestens einen) voreingestellten Root-Server.

232) Was steht prinzipiell im Masterfile (Zone Files) eines DNS Servers? Sind Antworten daraus „Authoritative“?

die Zuordnung der Symbole zu den IP-Adressen; die Antworten daraus sind authoritativ; außerdem: welche Bereiche einer Domain wohin delegiert wurden

233) Wie geht DNS mit Caching von DNS Namen um? Wie lange bleibt ein Eintrag im DNS Cache gültig? Sind Antworten daraus „Authoritative“? Wo findet man DNS Caches (am Server, am Client oder auf beiden)?

Wie: Erfragt ein Host die IP-Adresse zu einem Domain-Name, speichert er sie, um zukünftige Fragen nach dem selben Domain-Name selbst beantworten zu können.
Wie lange gültig: Bei jedem DNS-Query wird ein TTL-Wert mitgeliefert, so lange bleibt ein Eintrag gültig.
DNS-Caches findet man auf Clients und auf Servern.

234) Was ist der Unterschied zwischen primary und secondary master Name Server bzw. wozu benötig man sie? Wie kommunizieren diese (TCP oder UDP) und was passiert dabei (Stichwort Zone Transfer)?

der Primary-Master-Name-Server hat das Original der Zone-File, hier kann es der Admin ggf. ändern; der Secondary holt sich das Zone-File per TCP, was dann Zone-Transfer genannt wird

235) Was versteht man unter rekursiven und iterativer DNS Abfrage? Was ist ein reverse/inverse DNS Lookup?

Rekursiv: man fragt einen DNS nach einem Domain-Name, dieser kümmert sich um alles (der Job wird delegiert; er fragt z.B. andere DNS-Server) und gibt die IP-Adresse (oder was auch immer man haben möchte)
Iterativ: man fragt einen DNS nach einem Domain-Name und wenn dieser nicht zuständig ist, gibt er nur eine Liste von Nameservern, die man statt dessen selbst fragen soll, zurück; die Root-Server antworten nur iterativ

Foward-Lookup: Umsetzung von Domainnamen in IP-Adressen
Reverse-Lookup: Auflösung von IP-Adressen in Namen

236) Schildern Sie kurz die prinzipiellen Abläufe einer DNS Abfrage unter der Annahme, dass der Default Name Server eines PCs nicht für das Symbols zuständig ist und keinen Eintrag im Cache dafür hat? Gehen Sie davon aus, dass dreimal die SOA nach unten im DNS übergeben wurde?

Aufzulösen: a.www.orf.at.

1) frage einen Root-Server nach „a.www.orf.at.“; dieser gibt eine Liste von zuständigen Nameservern für „at.“ zurück

2) frage einen dieser Nameserver nach „a.www.orf.at.“; dieser gibt eine Liste von zuständigen Nameservern für „orf.at.“ zurück
3) frage einen dieser Nameserver nach „a.www.orf.at.“; dieser gibt eine Liste von zuständigen Nameservern für „www.orf.at.“ zurück
4) frage einen dieser Nameserver nach „a.www.orf.at.“; dieser sagt, dass es diesen Domain-Namen nicht gibt

Beispiel Namensauflösung
Im Beispiel wird www.example.net in drei Schritten mit Hilfe des Resolver-Tools dig iterativ „per Hand“ aufgelöst. Ausgangspunkt ist der Root-Server A.root-servers.net. Dessen Adresse (198.41.0.4) ist in Nameservern und Resolvern fest einkonfiguriert. Der Rootserver enthält für die Domain net eine Delegation (NS-Record) zum Server A.GTLD-SERVERS.net. Dieser wiederum verweist für die Domain example.net auf den Server a.iana-servers.net, der schließlich den gesuchten Eintrag www.example.net enthält. Die Ausgabe ist auf das Wesentliche gekürzt.

```
$ dig +norecurse @198.41.0.4 www.example.net
   net.                172800  IN      NS      A.GTLD-SERVERS.net.
   A.GTLD-SERVERS.net.  172800  IN      A       192.5.6.30

$ dig +norecurse @192.5.6.30 www.example.net
   example.net.        172800  IN      NS      a.iana-servers.net.
   a.iana-servers.net. 172800  IN      A       192.0.34.43

$ dig +norecurse @192.0.34.43 www.example.net
   www.example.net.    172800  IN      A       192.0.34.166
```