

Ausgearbeiteter Fragenkatalog SS 2007 Datenkommunikation

Schöfegger Stefan

26. August 2007

1 Transmission Principles (Version 1.1)

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

Es wird ein komplettes Datenwort gleichzeitig transportiert, für jedes Bit steht eine eigene Leitung zur Verfügung. Die Synchronisation erfolgt durch eigene Kontrolleleitungen am Kontrollbus (CLK, Read, Write Leitungen). Die Technik wird bei Datenübertragung über kurze Distanzen (Computersysteme) eingesetzt und würde für weitere Strecken zu viel Geld kosten.

1.2 Was versteht man unter serieller Übertragungstechnik? Wo wird diese Technik eingesetzt? Warum verwendet man keine separate Leitung für die Übertragung der Taktinformation?

Bei serieller Übertragung werden die Bitmuster auf einer Leitung nacheinander übertragen. Dazu muss der Empfänger mit dem Sender synchronisiert sein, um die Bits genau zum richtigen Augenblick abtasten zu können. Aus Kostengründen wird keine separate Leitung für den Takt verwendet, sondern andere Techniken verwendet (Bitsynchronisation). Eingesetzt wird die serielle Übertragung auf langen Wegen, wo eine hohe Anzahl von parallelen Leitungen zu teuer wird.

1.3 Was versteht man prinzipiell unter Bitsynchronisation bei serieller Übertragung? Welche 2 prinzipielle Methoden unterscheidet man (Aufzählung)?

Die Clock Synchronisation des Empfängerlocks für serielle Übertragung nennt man Bit Synchronisation. Aus dem Daten wird der erforderliche Clock zurückgewonnen. Mögliche Methoden: synchrone und asynchrone Übertragung.

1.4 Wie erreicht man Bitsynchronisation bei asynchroner Übertragung prinzipiell? Für welche Zeit-Dauer ist die Bitsynchronisation gewährleistet (bzw. was bedeutet asynchron in diesem Zusammenhang)? Welchen fundamentalen Nachteil hat dieses Verfahren?

Zu jedem Datenwort werden Start und Stopbit hinzugefügt, die Synchronisation ist nur für jeweils 1 Datenwort gültig. Zwischen den einzelnen Datenwörtern kann eine beliebige Zeitspanne liegen. (->asynchron). Durch das Einfügen von Start und Stopbits kommt es zu einem sehr grossen Overhead von 2-3 Bits pro 8 Datenbit was die Durchsatzrate stark verkleinert.

1.5 Was versteht man unter Oversampling im Zusammenhang mit der asynchroner Übertragung?

Überabtastung, abtasten eines Signals mit einem vielfachen der eigentlichen Frequenz

1.6 Wie erreicht man Bitsynchronisation bei synchroner Übertragung prinzipiell? Für welche Zeit-Dauer ist die Bitsynchronisation gewährleistet (was bedeutet synchron in diesem Zusammenhang)? Durch welche drei prinzipielle Maßnahmen erreicht man genügend Signalfanken (Aufzählung)?

Die Synchronisation wird durch Sync-Bits am Beginn des Datenblocks hergestellt und durch Signalfanken im Datenstrom aufrecht erhalten. Die Gültigkeit bezieht sich auf einen ganzen Datenblock. Sender und Empfänger sind synchron mit der Frequenz und der Phase. ManchesterCode, NRZI, HDB3

1.7 Wozu verwendet man eine PLL / VCO Schaltung bei synchroner Übertragung?

PLL: Phase Locked Loop, speicherung des Takts wenn zu wenig Signalwechsel vorliegen. VCO: Voltage controlled oscillator: Stellt die Abtastfrequenz zum abtasten des Signals zur Verfügung.

1.8 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)?

Beim Manchester-Code werden die Bits in der Hälfte geteilt. Die erste Hälfte ist das Komplement (0 wird 1 und umgekehrt) des Datenbits, die zweite Hälfte das Original-Bit. Abgetastet werden die Signalfanken in der Mitte der ursprünglichen Bits aus denen der Bitwert gewonnen wird. Eine Positive Flanke bedeutet log.1 (High), negative Flanke log.0 (Low). Da nun jedes Bit mit 2 Signalhälften dargestellt wird, ergeben sich doppelt so viele Signaländerungen als beim NRZ-Code und daher ist die erforderliche Bandbreite für den Manchester-Code doppelt so hoch im Vergleich zum NRZ-Code! Der Gleichanteil ist jedoch durch die regelmäßig wechselnden Signalzustände zwischen zwei Pegeln null oder konstant. Der Manchester-Code wird in Ethernet LANs verwendet.

1.9 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)?

Hierbei wird eine log. 1 durch einen alternierenden Impuls dargestellt (Flanke), eine 0 erzeugt keinen Puls. Kommt es zu einer Folge von mehr als drei Nullen hintereinander, wird vom Code automatisch die vierte Null mit einem 1-Signal codiert (so genanntes Bitstuffing). Kein oder Konstanter Gleichanteil durch A- und V Bits; Bandbreitenanforderung wie bei NRZ. Verwendung u.a. bei: ISDN, WANs in Europa

1.10 Was ist ein Scrambler bzw. wozu dient er in Zusammenhang mit synchroner Übertragung?

Ein Scrambler "verschlüsselt" die Daten um eine lange Folge von Nullen im Datenstrom zu verhindern.

1.11 Wie schaut der generische Aufbau eines Übertragungsrahmens (Frame) aus? Wozu werden die einzelnen Felder prinzipiell verwendet (jeweils ein Stichwort pro Feld; Achtung hier keine ausführliche Beschreibung des Control Fields)?

Bit Synchronisation - wird für die Bit Synchronisation von Sender und Empfänger verwendet. Starting Delimiter - Spezielle Bitfolgen um den Beginn eines Frames anzuzeigen. Control Information - Spezielle Protokollinformationen werden übertragen. Data - Nutzdaten die übertragen werden sollen. Checksum - Notwendig zur Fehlererkennung und eventuell Fehlerkorrektur. Ending Delimiter - Markiert das Ende der Frames.

1.12 Wozu dient das Control Field eines Übertragungsrahmens? Welche Elemente lassen sich darin transportieren (Aufzählung)?

Das Controllfeld implementiert spezielle Protokollinformationen. Frame-Type, Protocol-Type (Data, ACK, Conect; IP, IPX, Appletalk, ...) Sequenze Number für die identifizierung der einzelnen Frames Adressinformationen Framelänge

1.13 Was versteht man unter Rahmensynchronisation (Framesynchronisation)? Wieso ist diese bei synchroner Übertragung erforderlich trotz erfolgter Bitsynchronisation erforderlich?

Die Bitsynchronisation ist nur für die Erkennung der einzelnen Bits auf der Leitung zuständig. Rahmensynchronisation: Um Anfang und Ende eines Blockes zu erkennen müssen bekannte Delimiter am Anfang und am Ende stehen. Notwenig ist das um die Daten von der Sync-Sequenz unterscheiden zu können.

1.14 Was versteht man unter Datentransparenz? Durch welcher Methoden lässt sich diese prinzipiell erreichen (Aufzählung)

Die Applikation des Senders muss nicht dafür sorgen dass Starting- und Enddelimiter nicht im Datenstrom auftauchen. Es könnte dann der Beginn und das Ende eines Frames nicht mehr korrekt erkannt werden. Bitstuffing, Bitstuffing, Code Violation, Byte Count Technique, Idle Line

1.15 Wie erreicht man Datentransparenz bei der bitorientierten (bit-oriented) Methode (Stichwort plus kurze Beschreibung)?

SD und ED werden durch spezielle Zeichenfolgen dargestellt, diese Folgen dürfen nicht innerhalb eines Frames auftauchen. Um dies zu verhindern werden nach nach 5 1er automatisch eine 0 eingefügt die der Empfänger wieder automatisch löscht.

1.16 Wie erreicht man Datentransparenz bei der zeichenorientierten (character-oriented) (Stichwort plus kurze Beschreibung)?

Control Daten werden nur als solche interpretiert wenn zuvor ein Data Link Escape (DLE) kam. Sollte die Zeichenfolge des DLE's in den Daten auftauchen wird diese automatisch verdoppelt.

1.17 Welchen Ansatz verfolgt Forward Error Control bezüglich Rahmensicherung (frame protection), Fehlererkennung (error detection) und Fehlerbereinigung (error recovery)? Wann wird diese Technik eingesetzt?

Redundante Daten werden dem Rahmen vom Sender eingefügt um Fehler erkennen und selbst bereinigen zu können. Wird verwendet bei langen Verzögerungszeiten (Weltall).

1.18 Welchen Ansatz verfolgt Forward Error Control bezüglich Rahmensicherung (frame protection), Fehlererkennung (error detection) und Fehlerbereinigung (error recovery)? Welche bekannte Verfahren der Prüfsummenbildung gibt es (Aufzählung)?

Redundante Daten werden dem Frame vom Sender eingefügt um Fehler erkennen zu können. Wiederholung der Übertragung um korrekte Daten zu bekommen. Parity Bit, CRC, Summe der Datenbyte modulo 2

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

Jedes Periodische Signal kann als eine Summe von Sinus Signalen dargestellt werden. Attenuation: Alle Frequenzen werden durch das Transportmedium gleich stark abgeschwächt. Limited Bandwidth: Frequenz bestimmt durch die physikalischen Eigenschaften des Transportmediums, Filter. Hohe Frequenzen des Signals werden geblockt.

1.20 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.

1.21 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 unverzögerten Übertragung. Bei immer höheren Bitraten werden beide Bedingungen immer schlechter erfüllt, sodass ab einer best. Obergrenze keine Synchronisation mehr möglich ist.

1.22 Was besagt das Theorem von Nyquist?

wie viele Bits können über eine ideale störungsfreie Leitung übertragen werden. $R_{max} = 2 * B * \log_2 V$
 R =max. Bitrate (bit/sec), B = Bandwidth, V = Number of Signal Levels

1.23 Was besagt das Theorem von Shannon?

wie viele Bits können über eine störungsbehaftete Leitung übertragen werden. $\max R = B * \log_2 (1+S/N)$.
 S = Signal Power, N = Noise Power

1.24 Was versteht man unter Baseband Transmission?

Die Gesamte Bandbreite wird benutzt um ein Signal auf einer Leitung zu übertragen. Signale werden als Rechteckimpulse übertragen. Physikalische Eigenschaften des Transportmediums, Leistung des Senders, Empfindlichkeit der Empfänger und S/N Ratio sind die limitierenden Eigenschaften für die erreichbare Bitrate.

1.25 Was versteht man unter Narrowband Transmission? Was ist ein Modem?

Bandbreite wird absichtlich beschränkt, Datenübertragung muss genau auf diese Frequenz abgestimmt werden. ANpassung erfolgt über Modulation. Modem: Modulator / Demodulator übersetzt die digitalen Signale um sie über ein Netzwerk verschicken zu können.

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

die 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. Beispiel: Kabelfernsehen.

In digitalen Systemen meint man meist einfach high-speed-Übertragung.

2 Protocol Principles (Version 1.2)

2.1 Was versteht man unter „ConnectionlessService im Zusammenhang mit Leitungsprotokollen? Welche Eigenschaften hat dieses Service der Kommunikationsschicht für die darüberliegende Applikationsschicht (3 Schichtenmodell)?

Daten werden ohne eine softwaremässig aufgebaute Verbindung verschickt, ohne Kenntnis darüber ob der Empfänger die Daten empfangen kann. (Best Effort Service). VT: Einfache Implementierung der Kommunikationssoftware, Übertragungsfehler müssen von der Applikation erkannt und ausgebessert werden (Fehlende Pakete)

2.2 Was versteht man unter „Connection-orientedService im Zusammenhang mit Leitungsprotokollen? Welche Eigenschaften hat dieses Service der Kommunikationsschicht für die darüberliegende Applikationsschicht (3 Schichtenmodell)?

Ein Kommunikationskanal wird vor der Verbindung aufgebaut. Übertragungsfehler werden von der Kommunikations SW erkannt und behoben (feedback error controll). Spezielle Frames sind für den Verbindungsaufbau und Abbau notwendig. Die Komminikationssoftware ist aufwändig da ARQ (Automatic Repeat Request) implementiert sein muss.

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

ARQ steht für 'Automatic Repeat-reQuest' und bezeichnet Techniken bei denen eine zuverlässige Datenübertragung, durch das wiederholte Senden von beschädigten oder verlorenen Frames/Paketen, garantiert wird. Um dies zu erreichen muss der Empfänger den Erhalt von Frames/Paketen bestätigen (Feedback Error Control). Bleibt eine Bestätigung aus wird der Frame (das Paket) erneut gesendet. ARQ ist nur bei verbindungsorientierten Services möglich.

2.4 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, Sequenznummern in den Frames. Es müssen Duplikate erkannt werden und/oder die Pakete/Frames umgeordnet werden.

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

Der Sender schickt das nächste Frame erst wenn der Empfänger das vorhergehende Paket bestätigt hat, dadurch entsteht eine schlechte Ausnutzung der Bandbreite. Bestätigt der Empfänger nicht innerhalb einer bestimmten Timeout-Zeit so wird das Packet erneut gesendet. TFTP (Trivial File Transfer Protocol)

2.6 Wie erfolgt bei Idle-RQ die Fehlerbereinigung (Error Recovery)? Behandeln Sie kurz 2 Szenarios: I-Frame gestört, ACK-Frame gestört.

Nach dem Versenden von Daten wird ein Timer gestartet, läuft dieser ab werden die Daten erneut gesendet. I-Frame: Während der Timeout-Zeit kommt keine Bestätigung, Daten werden erneut gesendet.

Sender hat auch die Möglichkeit ein NACK zu versenden. ACK: Wie bei I-Frame, Empfänger muss Duplikate erkennen und verwerfen. Er sendet trotzdem ein ACK um dem Sender den Empfang zu signalisieren.

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

Es werden je nach Window Size gleich mehrere Pakete fortlaufend gesendet, ohne sofort auf ein ACK zu warten. Für jedes Paket wird ein Timer gestartet und zusätzlich eine Liste von noch nicht bestätigten Paketen geführt. Der Empfänger muss die Pakete eventuell neu ordnen (Paket-Nummer), da nun die Pakete in beliebiger Reihenfolge ankommen können. Der Mechanismus für beschädigte/verlorene Pakete ist der selbe wie bei Idle-RQ (Die Liste muss allerdings bei Bestätigung eines Pakets (oder mehrerer Pakete) entsprechend aktualisiert werden!) Beispiel: TCP

2.8 Was ist die Grundidee von Continous-RQ in der Variante „Selective Acknowledgement“? Ist ein Umordnen dabei erforderlich? Ist die Erkennung von Duplikaten erforderlich? Welche Bedeutung hat ein ACK (single oder multiple)?

Jedes Paket muss einzeln bestätigt werden. Wird von einem Paket keine Bestätigung beim Sender erhalten (innerhalb einer Timeout Zeit) so wird dieses eine Paket erneut versendet, dadurch ist beim Empfänger eine Umordnung notwendig. Wird ein vom Empfänger gesendetes ACK gestört so kommt es ebenfalls zu einer Neuversendung des Pakets, der Empfänger muss dieses Duplikat erkennen, mit einem ACK bestätigen allerdings verwerfen.

2.9 Wie erfolgt bei Continous-RQ Variante „Selective Acknowledgement die Fehlerbereinigung (Error Recovery)? Behandeln Sie kurz 2 Szenarios: I-Frame gestört, ACK-Frame gestört. Wann wird der Timer benötigt?

I-Frame: es kommt ein ACK vom nächsten Paket zurück, damit ist klar dass ein Paket verloren gegangen ist. -> erneut senden ACK: das ACK vom nächsten Paket wird erhalten, deshalb wird das erste Paket nochmals gesendet. Der Empfänger muss das Duplikat erkennen aber mit ACK bestätigen. Timer wird nur für das letzte gesendete Paket benötigt.

2.10 Was ist die Grundidee von Continous-RQ in der Variante „Go-BackN“? Ist ein Umordnen dabei erforderlich? Ist die Erkennung von Duplikaten erforderlich? Welche Bedeutung hat ein ACK (single oder multiple)?

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. Ein Umordnen ist nicht erforderlich da nur Pakete in der richtigen Reihenfolge angenommen werden. Ebenso werden Duplikate automatisch verworfen. Ein ACK kann mehrere Pakete bestätigen -> multiple ACK

2.11 Wie erfolgt bei Continous-RQ Variante „Go-BackN“ die Fehlerbereinigung (Error Recovery)? Behandeln Sie kurz 2 Szenarios: I-Frame gestört, ACK-Frame gestört. Wann wird der Timer benötigt? Welches bekannte Protokoll der basiert auf dieser Variante?

Mit jeder Übertragung eines I-Frames wird ein Timer gestartet, welcher zurückgesetzt wird sobald ein ACK des zugehörigen I-Frames oder eines nachfolgenden I-Frames eingetroffen ist. Trifft kein ACK vor Ablauf des zugehörigen Timers ein, wird der Frame nochmals gesendet. I-Frame fehlerhaft: 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 erforderlich. ACK-Frame zerstört: wenn das ACK für das nächste ankommt wird auch das vorherige (dessen ACK verloren ist) bestätigt (multiple ACK); war es das letzte ACK so läuft der Timer für das zugehörige I-Frame ab und das I-Frame wird erneut übertragen. Der Empfänger bemerkt das Duplikat und sendet erneut ein ACK.

2.12 Was ist die Grundidee von Continuous-RQ in der Variante „Positive Acknowledgement“? Ist ein Umordnen dabei erforderlich? Ist die Erkennung von Duplikaten erforderlich? Welche Bedeutung hat ein ACK (single oder multiple)?

ACKs werden gesendet solange Pakete in der richtigen Reihenfolge ankommen; multiple ACK möglich; wird ein I-Frame gestört, werden keine ACKs mehr gesendet, jedoch werden alle nachfolgenden I-Frames die noch gesendet worden sind, trotzdem gespeichert; wieder hat jedes Paket einen Timer, wenn dieser abläuft wird das zugeh. I-Frame erneut gesendet und anschließend durch ein ACK bzw. falls schon nachfolgende I-Frames empfangen wurden durch ein Multiple ACK bestätigt. Wenn also eine Lücke entsteht (Paket kaputt), wird erst bestätigt, wenn diese Lücke gestopft ist.

2.13 Wie erfolgt bei Continuous-RQ in der Variante „Positive Acknowledgement“ die Fehlerbereinigung (Error Recovery)? Behandeln Sie kurz 2 Szenarios: I-Frame gestört, ACK-Frame gestört. Wann wird der Timer benötigt? Welches Protokoll der TCP/IP Suite basiert auf dieser Variante?

I-Frame zerstört: Paket wird nicht bestätigt; Timer des Senders läuft ab -> erneute Übertragung; Ein ACK gilt für N Pakete; ACK-Frame zerstört: Es gibt keine Timer für ACKs! Zwei Möglichkeiten: 1) Empfänger schickt später sowieso ein ACK für ein späteres Paket. Dieses ACK bestätigt auch alle älteren Pakete -> kein Problem. 2) Keine weiteren Pakete: Timer des Senders läuft ab -> erneute Übertragung. Empfänger verwirft das (doppelte) Paket, sendet aber noch ein ACK dafür. Ein umordnen ist im Empfänger notwendig. TCP

2.14 Wie werden die für ARQ-Techniken notwendigen Identifier realisiert? Was sind $N(S)$, $N(R)$, $V(S)$, und $V(R)$ in diesem Zusammenhang? Wie arbeiten diese Elemente prinzipiell zusammen ?

Jedes Paket (Frame) bekommt eine Identifier-Number (die Pakete werden einfach durchnummeriert;). Empfänger und Sender benötigen nun auch jew. 2 Register. Ein Register (VS) speichert die ID-Number des nächsten Pakets das gesendet werden soll. Das andere (VR) speichert die nächste ID-Number für das nächste erwartete Paket (empfangen). Wird ein Paket gesendet so wird das VS um eins erhöht (für empfangen analog). $N(S)$ = Sequenze Number des I-Frames vom Sender $N(R)$ = Sequenze Number des ACK/NACK vom Empfänger

2.15 Was versteht man unter „piggy-backed Acknowledgement“? Aufgrund welcher Elemente im Protokoll Header lässt sich eine Unterstützung von „piggy-backed Acknowledgement“ ablesen?

Schiebefensterprotokolle (Sliding Windows Protocols) sehen die Bestätigung von empfangenen Rahmen (Frames) vor. Um wertvolle Bandbreite zu sparen kann der Empfänger die Bestätigung (Acknowledgement) seinem nächsten Rahmen (Frame) aufschnallen“ (zB.: in Form einer Nummer oder eines Flags) anstatt einen eigenen Rahmen hierfür zu senden. Diese Vorgehensweise nennt man piggy-backed Acknowledgement.

2.16 Warum benötigt man Windowing? Wie wird es realisiert (Stichwort Sendefenster)? Wieviele Identifier würde man ohne Windowing benötigen?

Da Speicher begrenzt ist werden bei Continuous-RQ auch die Anzahl der ohne ACK zu sendenden Pakete begrenzt (durch die Window-Size). Dabei entspricht die Window-Size (oder nur Window) 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.

2.17 Warum spricht man vom „sliding Window“? Was versteht man dabei unter „das Window öffnet bzw. schließt sich“? Was versteht man unter „usable“Window?

Je größer das Fenster ist desto mehr Speicherplatz wird benötigt (für die Listen die für den Fehlerfall und Duplikate geführt werden). Außerdem werden weniger ID-Nummern benötigt (die Nummerierung kann durch modulo Operationen erfolgen). Das Sendefenster verschiebt sich mit der Zeit über die Daten die geschickt werden sollen. Ein Window schließt sich wenn alle Pakete im Window gesendet wurden. Ein Window öffnet sich wenn es weiterbewegt wird (ACK angekommen) und so neue Pakete gesendet werden können. Das useable Window wird durch die Pakete im aktuellen Window (Fenster), die noch nicht gesendet wurden, gebildet.

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

Je größer das Fenster ist desto mehr Speicherplatz wird benötigt (für die Listen die für den Fehlerfall und Duplikate geführt werden). Außerdem werden weniger ID-Nummern benötigt (die Nummerierung kann durch modulo Operationen erfolgen).

2.19 Was versteht man unter „Serialization Delay“? Wie wirkt sich die Bitrate (die Bandbreite) einer Leitung (eines Kommunikationskanals) darauf aus?

Serialization Delay ist die Zeit die benötigt wird um eine bestimmte Anzahl von Bytes auf die Leitung zu legen“. Je mehr Bandbreite desto kürzer die Verzögerung.

2.20 Was versteht man unter „Propagation Delay“?

Verzögerungszeit der Daten bei der Übertragung. Entscheidender Faktor ist die Übertragungsgeschwindigkeit der Leitung.

2.21 Wieso hat ein Bit auf einer Übertragungsstrecke eine Länge? Lassen sich Bits auf einer Übertragungsleitung quasi „speichern“?

die Länge = Kehrwert der Geschwindigkeit * Geschwindigkeit der Übertragungsstrecke. Nein, weil die Ladungen schnell abfließen.

2.22 Was versteht man unter „Delay-Bandwidth”Produkt? Warum sollte das Sendefenster zumindestens die Größe des „Delay-Bandwidth”Produktes aufweisen?

$W = RTT * BW$ Die Windosize sollte mindestens so gross sein wie das Delay-Bandwidth Produkt um die Leitung optimal ausnutzen zu können.

2.23 Welche Parameter beeinflussen den Wert für den Retransmission Timer bei Leitungsprotokollen? Kann dieser Wert statisch sein? Warum ist das bei manchen Netzwerkprotokollen nicht möglich?

Für die Retransmission Time ist die Propagation Delay und die Serialization Delay wichtig und wird meist dynamisch geregelt. Da Pakete unterschiedliche Wege durch ein Netzwerk nehmen können (Routing) ist die Weglänge nicht vorhersehbar.

2.24 Was benötigt man Flusskontrolle (Flow Control)? Wie kann sie prinzipiell realisiert werden?

Problem: Der Empfänger könnte vom Sender mit Paketen/Frames überschwemmt/überfordert werden, es müssten Pakete verworfen werden die später erneut gesendet werden müssen. Lösung: Flow-Control. Erreichbar ist dies durch spezielle Pakete des Empfängers die dem Sender stoppen. (Feedback-basierte Flusskontrolle) oder durch Flusskontrolle basierend auf der Übertragungsrate (hier wird durch einen im Protokoll inkludierten Mechanismus die max. Übertragungsrate reguliert).

2.25 Warum reicht Windowing alleine für Flow Control nicht aus?

Nach dem Timeout unbestätigter Frames werden diese nochmals gesendet. Nach einer definierten Anzahl von erfolglosen Sendeversuchen wird die Verbindung als unterbrochen betrachtet und getrennt.

2.26 Was versteht man unter „adaptive Windowing”? Bei welchem Protokoll der TCP/IP Suite wird diese Technik eingesetzt?

Um den Datenfluss zu kontrollieren wird die Window-Size variiert. Dabei wird der Wert zwischen Sender und Empfänger ausgehandelt und während der Übertragung dynamisch geändert, so dass der Empfänger nicht überlastet wird und die Leitung ideal genutzt wird. Beispiel: TCP

3 TDM Techniques (Version 1.2)

3.1 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 : teilt jedem Kanal eine bestimmte Zeitperiode lang die Leitung zu.

3.2 Wie geht man bei synchronem TDM prinzipiell vor?

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. Jeder Eingangskanal wird 1 Timeslot zugeteilt.

3.3 Synchrones TDM: Welche Bandbreite auf der Trunk-Leitung benötigt man? Benötigt man Adressierung? Was passiert in Übertragungspausen eines Channels; kann die Bandbreite von einem anderen Channel genutzt werden? Wird Flow Control benötigt?

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.

3.4 Was sind die Basiseigenschaften von synchronem TDM? Welche Vorteile, welche Nachteile weist synchrones TDM auf?

nur kurze Verzögerungszeit durch Packen und Entpacken der Daten für Trunk Line. Protocol Transparent, jedes Protokoll kann verwendet werden. Für die Endsysteme erscheinen die Leitung wie eine PTP Leitung. Bitrate auf Trunk Line muss für die Summe der einzelnen Übertragungsraten ausgelegt sein. Hat 1 Sender keine Daten zu senden, so wird Bandbreite verschwendet.

3.5 Wie geht man bei asynchronem (statistischen) prinzipiell TDM vor?

Datenleitungen werden nach aktuellem Bedarf auf die Trunk Line geschaltet -> statistisches Verhalten weil nicht alle Datenleitungen das selbe Datenaufkommen haben.

3.6 Asynchrones TDM: Wie ist die Bandbreite auf der Trunk-Leitung ausgelegt? Benötigt man Adressierung? Was passiert in Übertragungspausen eines Channels; kann die Bandbreite von einem anderen Channel genutzt werden? Warum ist Flow Control wünschenswert? Was sind die Konsequenzen wenn keine Flow Control verwendet wird?

Die Bandbreite ist für das durchschnittliche Datenaufkommen ausgelegt. Da keine festen Zeitschlitze den Datenleitungen zugeordnet sind muss eine Kennung für die Daten eingebaut werden -> Adressierung. In Übertragungspausen wird der Kanal nicht auf die TrunkLine geschaltet und die Bandbreite kann von anderen Kanälen verwendet werden. Um einen Bufferüberlauf zu verhindern sollte eine Flow-Controll realisiert werden, da ansonsten Daten verworfen werden müssen.

3.7 Was sind die Basiseigenschaften von asynchronem TDM? Welche Vorteile, welche Nachteile weist asynchrones TDM auf?

Vorteile: variable Aufteilung der Bandbreite, bessere Ausnutzung der Trunkline, Trunkleitung kann langsamer ausgelegt sein. Nachteile: Datenquellen kommunizieren zu verschiedenen Zeiten (statistische Verteilung), Daten müssen evtl. im Multiplexer zwischengespeichert werden bevor die Leitung wieder frei wird -> längere, variable Verzögerung; Adressierung notwendig, nicht Protokoll-transparent, Flow Control notwendig

3.8 Wie wird das Nyquist Theorem bei der Digitalisierung von analoger Sprache angewendet? Wofür steht PCM? Welche Bitrate wird für PCM Sprachkanal benötigt?

Jedes Bandbreite beschränkte Signal kann hinreichend mit einer Abtastfrequenz von 2-fachen rekonstruiert werden. Sprache ist bandbreitenbeschränkt -> Nyquist Theorem Analoge Sprache wird mit PCM (Puls Code Modulation) auf einem 64 kBit-Kanal digitalisiert.

3.9 Was ist der Quantisierungsfehler? Warum verwendet man eine logarithmische Kurve und nicht eine lineare Kurve zur Quantisierung? 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/Umwandelung 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 Deshalb: Um die Signalqualität zu verbessern werden niedrigere Amplituden mit Hilfe der logarithmischen Quantization besser aufgelöst. ->bessere Signalqualität für leisere Sprachteile. 1 Bit Polarity, 3 Bit Segment, 4 Bit Step

3.10 Wie wird mit ADPCM bei der Codierung digitaler Sprache gemacht? Was erreicht man damit bezüglich benötigter Bitrate?

ADPCM ist eine Puls-Code-Modulation mit Vorhersagefunktion. Bei der Verarbeitung des Signals wird versucht, den weiteren Signalverlauf innerhalb des nächsten Abschnitts vorherzusagen. Für die Quantisierung des Signals im nächsten Zeitschritt wird so nur die Differenz zwischen vorhergesagtem und realem Signal verwendet.

3.11 Was ist ein Waveform Coder? Was ist ein Vocoder?

Waveform: Der verlauf des Sprachsignals wird abgehackt, kodiert und übertragen. (PCM, ADPCM=Vocoder: Sprache wird analysiert und mit einem Codebuch verglichen. Die Sprachausgabe erfolgt mit einem synthesizer.

3.12 Wozu dienen synchrone TDM Multiplexer-Hierarchien? Welche zeitliche Anforderungen muss ein Rahmen einer beliebigen TDM Hierarchy prinzipiell erfüllen?

Nur eine standardisierte Hierarchie kann Millionen von Benutzer auf der Welt verbinden. Man unterscheidet 2 Hauptarchitekturen: PDH, SDH

Da die Rahmenrate in jeder Stufe der Hierarchie 8000 Rahmen/s betragen muss, darf ein Rahmen nur 125µs groß sein.

3.13 Was ist PDH prinzipiell? Wie erfolgt die Taktung? Wo liegen die Limitierungen? Ist Add/Drop Multiplexing eines Sprachkanals ohne Durchlaufen der gesamten Hierarchie möglich?

PDH (plesiosynchronous digital hierarchy): Plesio bedeutet nahezu. Jeder PDH Multiplexer gibt seinen eigenen Takt vor. Synchroner Übertragungszeitdifferenzen werden mit Bitstuffing ausgeglichen. Limitierung: Kann für höhere Geschwindigkeiten nicht benutzt werden, da der Overhead dabei schnell ansteigt. Dieser Overhead ist abhängig von den Bitraten der Übertragung. Er wird bedingt durch das notwendige Bitstuffing. Add/Drop Multiplexing ist wegen der unterschiedlichen Länge (je nachdem wieviele Bits gestuft wurden) nicht möglich.

3.14 Was ist SDH prinzipiell? Wie erfolgt die Taktung? Was sind die Vorteile? Ist Add/Drop Multiplexing eines Sprachkanals ohne Durchlaufen der gesamten Hierarchie möglich?

SDH (synchronous digital hierarchy): Macht die Nachteile von PDH weg. (Nämlich: Steigender Overhead, verschiedene Multiplexing-Strukturen, Wechsel von Kanälen erfordert demultiplexen). Weiteres forderte man ein echtes synchrones Netzwerk. VT: Nachteil für alle der selbe, weltweiter Standard. Add/Drop möglich

4 Network Principles (Version 1.2)

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

Die Leitungsvermittlung beruht auf synchronem TDM. (kurze Verzögerung, hohe Bitrate auf Trunk Line, Idle Pattern, Netzwerkfähig weil mapping informations in circuit switching tabllen gespeichert werden)

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

In ein einer CS-Tabelle ist festgehalten welcher Timeslot von welcher Leitung zu welchem Timeslot auf welcher Leitung verbunden werden soll. Ein Transit-Switch ist ein Switch der einkommende Trunk-Leitung auf eine Trunk-Leitung mappt (er mappt natürlich die Timeslots). TDM am Access Port ist deshalb günstig weil so mehrere verschiedene virtuelle Verbindngen auf einem Kabel übertragen werden können. Das Mapping kann wie bei Trunk-Leitungen erfolgen.

4.3 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); Provider nennen dies "digital leased line". Wie permanent circuit service nur das im Fehlerfall automatisch auf einen redundanten Pfad umgeschalten wird.

4.4 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 und dabei Einträge in den CS-Tabellen hinzugefügt. Die Signalisierung ist notwendig um die Verbindung zw. zwei switches aufzubauen oder abzubauen. Beispiel: ISDN

4.5 Was ist ISDN BRI? Wie viele Nutzkanäle gibt es dabei? Wozu dient der D-Channel? Welche zwei prinzipiellen physikalischen Konfigurationen gibt es bei ISDN-BRI (Aufzählung)? Wieviele ISDN TEs lassen sich anschließen? Wieso benötigt man am D-Channel eine Access-Control (Zugriffs-Kontrolle)?

ISDN: Integrated Service Digital Network BRD: Basic Rate Interface

2 Linkkanäle mit 64kbit / sec, D Kanal dient zur Signalisierung von Verbindungsaufbau. physikalische Konfiguration: PTP, Multipoint (MP mit bis zu 8 Teilnehmer und teilen sich einen D Kanal)

4.6 Bezüglich die Access-Control am D-Channel bei ISDN BRI: Welche Rolle spielen die D- und E-Bits? Wer setzt sich bei gleichzeitigem Zugriff von 2 ISDN-TEs schlussendlich durch? Wodurch ist das bedingt?

TE benutzt D Bits m NT ansprechen zu können.

E-Bits: NT benutzt Echo Bits um TE's antworten. Gleichzeitiger zugriff: TE mit den meisten 0 setzt sich durch da 0 einen Signalwechsel erzeugt und eine 1 nicht.

4.7 Bezüglich die Access-Control am D-Channel bei ISDN BRI: Wieso benötigt man am D-Channel Bitstuffing für lange Folgen von Einsen? Wie erreicht man Fairness beim Zugriff auf dem D-Channel (bzw. wie erreicht man, dass ein TE nach erfolgreicher Okkupation des D-Channels diesen nicht gleich wieder okkupiert)?

P4-14 Nach 8 Einsen muss eine Null eingefügt wreden da ansonsten andere Teilnehmer den D Bus verwenden würden obwohl dieser noch nicht frei ist. TE muss D Kanal freigeben nachden er eine Mesage geschickt hat. TE wartet dann auf 9 1er bevor er erneut versucht zu senden, so haben andere TE die Möglichkeit den D Kanal zu benutzen-

4.8 Was ist ISDN PRI? Wie viele Nutzkanäle gibt es dabei? Wozu dient der D-Channel? Wieviele ISDN TEs lassen sich anschließen? Wieso benötigt man am D-Channel keine Access-Control? Welches PDH Framing steckt dahinter? Welchen Timeslot verwendet der D-Channel?

Integrated Devices Digital Natwork. PRI = Promary Rate Interface. 30 TE können sich anschliessen, jeweils 64kbit, 1 D Kanal mit 64kbit. D Kanal nenützt Timeslot 16, der Rest (ausser 0) kann für die B Kanäle verwendet werden. Access-Control ist NICHT notwendig da niemand um die Bandbreite konkurriert (nur Point-to-Point Verbindung). Am ende der Leitung sitzt z.B. eine einzige große Telefonzentrale.

4.9 Auf welchem TDM Verfahren beruht die Paketvermittlung (Packet Switching)? Welche prinzipiellen Eigenschaften erbt damit Packet Switching von diesem TDM Verfahren?

Es beruht auf asynchronem TDM. Info: asynchrones TDM teilt die Timeslots (im Gegensatz zu synchronem) nicht fix auf sondern dynamisch (statistisch) nach Bedarf auf. Eigenschaften, die packet switching von Async. TMD erbt:

- Es wird keine Bandbreite für Idle-Pattern vergeudet.
- Es ist nicht Protokoll-Transparent.
- Zusätzliche Informationen (Adressen) um die Pakete richtig weiterzuleiten (routen) werden benötigt.
- Das Delay ist variabel und ggf. höher als bei Sync. TDM.
- Man braucht weniger Bandbreite auf der Trunk-Leitung, weil man voraussetzt, dass nicht alle immer (viel) Traffic verursachen.
- Keine any-to-any-Topologie notwendig.

4.10 Beschreiben Sie ist das Grundprinzip des Packet Switching beim Weiterleiten (Forwarding) von Paketen? Was macht das Endsystem prinzipiell, was macht der Packet Switch prinzipiell?

Endsystem verpackt die Daten in kleinen Pakete, versieht sie sie mit Adressinfos und stellt sie dem Switch zu. Pakete werden aufgrund 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.

4.11 Welche zwei prinzipielle Arten von Adressen gibt es beim Packet Switching? Welche Adress-Art wird von Switching tabellen, welche Art wird von Routingtabellen in Anspruch genommen, um das Forwarden eines Paktes zu realisieren?

- virtual Call service for switching
- Datagram servie for routing

4.12 Welche zwei prinzipiellen Arten von Services gibt es beim Packet Switching? Wie unterscheidet sich die Verwendung der Routingtabellen bei diesen zwei Services? Nur bei welchem Service gibt es Switchingtabellen?

connection oriented, connection less. Bei CO wird die Routing-tabel benutzt um die switching Table zu erzeugen. Nur zum Verbindungsaufbau notwendig, danach werden switching-tables verwendet. Bei CL werden routing-tables zum Weiterleiten verwendet.

4.13 Wann spricht man von einem „routable“Protokoll? Was ist hingegen ein Routingprotokoll?

routable: Protokoll das einzigartige strukturierte Adressen benutzt. Routingprotokoll: Protokoll mit dem Switches kommunizieren um z.b Netzwerktopologie ausmachen zu können.

4.14 Was sind Routingtabellen eines WAN Packet-Switching Systems prinzipiell bzw. was wird ein einer Routingtabelle festgehalten? Wie lassen sich Routintabellen prinzipiell erstellt? Wozu dient ein Routingprotokoll in diesem Zusammenhang?

In Routingtabellen wird gespeichert wie ein Paket an ihr Ziel kommt. In einer Routingtabelle wird daher mindestens gespeichert: Zieladresse, Interface (oder line) an das das Paket dann weitergeleitet werden soll. Die Routingtabelle wird entweder statisch oder dynamisch (durch ein Routingprotokoll) erstellt.

4.15 Was sind Switchingtabellen eines WAN Packet-Switching Systems prinzipiell bzw. was wird ein einer Switchingtabelle festgehalten? Wann werden diese Einträge erstellt.?

Switchingtabellen werden bei CO Services beim Vebindungsaufbau aufgebaut und geben an welchen Weg die Pakete von A nach B zu nehmen haben.

4.16 Was spielt sich prinzipiell bei Packet-Switching im Falle des Connectionless Services (Datagram Service) ab?. Welche bekannte Netzwerktechnologie beruht auf dieser Technik?

Pakete werden versandt ohne vorher eine logische Verbindung aufzubauen, jedes Paket wird unabhängig von anderen versandt, Weiterleitung beruht auf den aktuellen Stand der Routingtable, best effort service. Weiterleitung hängt von den verfügbaren Ressourcen ab, es können keine Ressourcen im vorhinein reserviert werden. IP, IPX, AppleTalk

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

Fällt eine Trunk Line aus unterbricht der Transport in diese Richtung so lange bis das Routingprotokoll einen neuen Pfad bestimmt hat oder falls eine redundante Leitung vereinbart wurde.

4.18 Geben Sie die wesentlichsten Vor- und Nachteile von Packet-Switching in der Spielart Datagram Service an.

- + small Protocol Overhead, schnellste Datenverbreitung zwischen Endsystemen da keine Verbindung aufgebaut werden muss.
- . Datenzustellung ist nicht garantiert, muss von den Endsystemen sichergestellt werden., Flow Control ist nicht möglich.

4.19 Wieso benötigt man bei Connectionless Service von Packet-Switching einen Kill-Mechanismus? Wodurch wird er bei IP implementiert?

Inkonsistente oder nicht geänderte Routingtable können dazu führen dass die Pakete im Kreis geschickt werden.-> Ressourcenverbrauch. Um die Endlosschleife unterbrechen zu können ist der KILL Mechanismus notwendig. IP: Time To Live, Maximum Hop Count

4.20 Was spielt sich prinzipiell bei Packet-Switching im Falle des Connection-oriented Services (Virtual Call Service) ab?. Welche bekannte Netzwerktechnologien beruhen auf dieser Technik?

Spezielle Kontrollpakete bauen eine virtuelle Verbindung zwischen 2 Endsystemen auf, diese Verbindung wird in SwitchingTabellen gespeichert. Danach können die Daten übertragen werden, nach Ende der Übertragung wird die Verbindung wieder abgebaut. Alle Pakete verwenden lokale Identifier die die Verbindung kennzeichnen.

4.21 Was kennzeichnet ein „Local Connection Identifier“ bei Packet-Switching im Falle des Connection-oriented Services (Virtual Call Service)? Wo wird dieser im Packet Switch abgelegt? Ändern Pakete in der Datentransferphase die Adress-Information, wenn sie durch einen Packet Switch weitergeleitet werden?

LCI: Entspricht einer Kennung einer aufgebauten Verbindung zwischen 2 Teilen eines Netzwerks und werden in den Switching Tabellen abgelegt. Diese Kennung ändert sich bei jedem Packet Switch.

4.22 Was passiert wenn eine Trunk-Leitung bzw. ein Packet-Switch nach erfolgten Verbindungsaufbau bei Packet-Switching im Connection-oriented Service ausfällt (Annahme redundante Leitung und dynamisches Routingprotokoll)?

Die virtuelle Verbindung wird getrennt und muss neu aufgebaut werden. Gibt es einen alternativen Weg kann das paket-Sewitch eine neue virtuelle Verbindung aufbauen.

4.23 Geben Sie die wesentlichsten Vor- und Nachteile von Packet-Switching im in der Spielart Virtual Call Service an.

- + Ressourcen vom Paket Switch kann beim Verbindungsaufbau reserviert werden, somit ist QOS möglich. Die Endsystembereitschaft kann im vorhinein überprüft werden. Endsystem hat eindeutige Verbindung, Netzwerkinterne Fehlererkennung möglich, FlowControll und error Recovery ebenso möglich.
- Verbindungsaufbau kostet Zeit, kompliziertere Protokolle für Endsysteme und Paket-Switches.

4.24 Warum nennt man Packet-Switching im Connection-oriented Service auch Virtual Circuit Technik? Was ist in diesem Zusammenhang SVC und PVC Betrieb?

- Virtual Circuit: es wird eine direkte Verbindung aufgebaut die jedes mal anders sein kann und nie direkt zum Ziel führt..
- SVC: Switches Virtual Circuit: Verbindung wird jedes mal neu aufgebaut und nach der Übertragung abgebaut.
- PVC: Permanent Virtual Circiut: Dauerhaft Verbindung, Datenübertragung jederzeit möglich, Verbindungs auf- und abbau entfällt, trotzdem eine store and foreard Technologie mit variablen Delays.

4.25 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 Idee des OSI Modells ist die Gliederung der Aufgaben für die Datenkommunikation in Schichten. Wodurch eine Abstraktion von einer Schicht auf die andere möglich ist. Daher kann eine Schicht der oberen Services anbieten und die 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 offeneSSysteme zur Kommunikation (unabhängig von dem der es Implementiert). Für rechner-interne Standards hilft es nicht, da das OSI Modell nur die Kommunikation zw. 2 Systemen regelt nicht aber die Komm. im System selbst.

4.26 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 nocheinmal in einen schichtspeziellen Header/Trailer verpackt.

Decapsulation: Die untere Schicht entfernt die schichtspeziellen Daten (Header/Trailer) und gibt diese äusgepackten”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); paket switches; alle Geräte die nur auf Schicht 1 bis 3 arbeiten.

4.27 Geben Sie für folgende Komponenten deren Lage bezüglich OSI Layer an: Repeater, SDH-Switch, Bridge, Ethernet-Switch, IP-Router, ISDN-Switch.. Warum ist es für den ISDN-Switch so schwierig seine Lage bezüglich OSI Layer anzugeben (Stichwort: Betrachtungsweise vor und nach dem Aufbau eines circuits)?

Repeater Layer 1 (kurz: L und dann die Nummer; also L1); SDH-Switch: L1; Bridge: L2; E-Switch: L2; IP-Router: L3; X.25-Switch: L3; Frame-Relay-Switch: L2; ATM-Switch: L2; Weil diese Protokolle bevor eine Verbindung steht auf L3 arbeiten, danach auf L2.

4.28 Geben Sie für folgende Komponenten deren Lage bezüglich OSI Layer an:, 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 anzugeben (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 Layer2
- ATM-Switch Layer 2

Weil diese Protokolle bevor eine Verbindung steht auf L3 arbeiten, danach auf L2.

5 LAN Principles and Legacy Ethernet (Version 1.1)

5.1 Was sind die wesentlichen Charakteristiken von LANs (Aufzählung)?

- Multipoint Line
- Broadcast behavior
- Layer 1 und Layer2 des OSI Modells
- All Stations share the same Media, equal rights

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

Layer 1 und 2 sind nötig für die Kommunikation. Da Layer 2 ursprünglich nur für eine P2P Verbindung entworfen war, muss jetzt aufgeteilt werden wegen multipoint und shared Media in

LLC Logical Link Control

MAC Media Access Control

5.3 Welche prinzipiellen Aufgaben erfüllt der LLC-Layer? Welche Services sind möglich (Control-Feld) und welche Funktion haben DSAP/SSAP?

LLC erledigt die Data-Link Aufgaben nach OSI

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 4 Dienstmethoden: verbindungsloser -, verbindungsorientierter Datagrammdienst, 1. + acknowledgement, 2. + acknowledgement.

DSAP (Destination Service Access Point) SSAP (Source Service Access Point) dient der Kennzeichnung der höheren Protokollprozesse der Ziel- und Absendersysteme. Controlfeld (8 oder 16 Bit) mit Steuerinformationen für Hilfsfunktionen wie zB Datenflusssteuerung.

5.4 Welche prinzipielle Aufgaben erfüllt der MAC-Layer (Aufzählung)?

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 verantwortlich dafür ob ein Paket an die höheren Schichten weitergeleitet wird oder nicht.

5.5 Wie sind MAC-Adressen aufgebaut? Welchen LAN Layer sind sie zuzurechnen? Was ist die BIA? Was sind „IEEE globally administered Addresses“? Können BIA Adressen überschrieben werden?

48 Bit Lang. Bit1: I/G(Individual Group) bit, Bit2: U/L(Universal/Local) bit, Bit3-23 Organizational Unique Identifier, Bit 24-47 Individual Address Part.

BIA: Burned in Address, anderer Name für MAC Adresse

IEEE globally administered address, Byte 0 bis 2 enthält eine Kennung des Herstellers, den Rest verwaltet der Hersteller selbst. BIA Adressen können nicht überschrieben werden

5.6 Wie erfolgt die Broadcastadressierung bei LANs? Was ist eine Multicast-Adresse? Welche Vorteile hat L2 Multicast gegenüber L2 Broadcast? Was muss am Endsystem für Unterstützung von Multicast geamcht werden?

Broadcast: alle Bits der MAC-Adresse vom Empfänger auf 1

Multicast: Der Empfänger kann eine bestimmte Multicastadresse zugewiesen werden auf die er hören soll.

VT: Es werden nur jene Rechner aufgeweckt die in der Multicast-Gruppe sind und nicht alle angeschlossenen wie bei Broadcast. Die richtige Multicastadresse muss am Rechner konfiguriert werden.

5.7 Wann genau empfängt ein Ethernet-Controller einer LAN-Station einen Rahmen (Stichwort Ziel-MAC-Adresse) und gibt diesen an höhere Layer weiter? Gehen Sie auf dabei auf alle Adressierungsmöglichkeiten ein. Was bedeutet das für die Performance des entsprechenden Systems (Stichwort Interrupt)?

Die NIC empfängt alle Daten die sich auf dem Medium befinden. Layer 2 entscheidet ob die Daten an die nächste Schicht weitergeleitet werden sollen, oder ob die Daten verworfen werden sollen. Bei Broadcast werden die Daten jedenfalls weitergeleitet, bei Multicast nur wen die Gruppenzugehörigkeit stimmt und bei normalen Daten muss die Ziel-Adresse mit der eigenen MAC Adresse überein stimmen. Bei jeder Übergabe von Daten an den Layer 3 erhält der Rechner von der NIC einen Interrupt.

5.8 Für welche Topologie wurden 10Base5 und 10Base2 ausgelegt? Wie erfolgt die Ankopplung dabei? Welche Leitungs- Codierung wird verwendet? Welche Reichweite hatten ergeben sich daraus ohne Einsatz von Repeatern? Welche Betriebsarten sind möglich bezüglich Half- und Full-Duplex? Welche Segment-Type hat 10Base5/10Base2?

10Base5 und 10Base2 basieren auf Koaxkabel, Ankopplung erfolgt passiv und unterbrechnungsfrei über Vampirtransceivern oder T-Stecker, Coding: Manchester mit -40mA DC-Anteil, Reichweite 500 / 200m.

5.9 Was bedeutet CSMA/CD und wie funktioniert dieses Verfahren prinzipiell? Wie erfolgt die Kollisonserkennung und die Konfliktbereinigung?

Carrier Sense Multiple Access / Collision Detection.

Kollisionen werden am DC Level auf dem Medium erkannt. Bei 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 Kollision mitteilt. Jeder Teilnehmer startet einen zufälligen Timeout nachdem erneut versucht wird zu Übertragen. Nach jedem Fehler wird der Bereich der Zufallszeit erhöht. Nach 16 Versuchen wird die Übertragung unterbrochen und der Fehler an die höhere Schicht weitergeleitet.

5.10 Wie funktioniert prinzipiell „Truncated Exponential Backoff“ bei CSMA/CD? Auf welche Anzahl sind die Wiederholungsversuche maximal limitiert? Ist Ethernet ein deterministisches Medium?

Binary Exponential Backoff ist ein Stauauflösungsmechanismus.

Algorithmus der den Timeout nach Auftreten eines Fehlers bestimmt, tritt ein Fehler öfters auf verlängert sich der Timeout durch den Algorithmus automatisch. max. 16 Versuche werden unternommen. Nicht deterministisch durch die Ausbreitungsgeschwindigkeit dann es zu unvorhersehbaren Kollisionen kommen.

5.11 Was ist das Collision-Window bzw. die Slot-Time bei Ethernet? Was möchte man damit sicherstellen? Welche Auswirkungen hat die Festlegung der Slot-Time von 51,2 μ s auf die minimale Rahmenlänge eines Ethernets? Welche maximale Reichweitenergeben sich daraus für 10Mbit/s 100Mbit/s Gigabit/s Ethernets?

Die grösste Zeit die man abwarten muss um eine zuverlässige Fehlererkennung zu erhalten. (2 mal die Signallaufzeit) heißt Collision Window oder Slot-Time. Festlegung auf 51,2 μ s bei 10Mbit/s. Minimale Rahmenlänge 64 byte, maximale Rahmenlänge (wegen fairness) 1518 Byte. Reichweiten: 10 MBit/s: 3000m, 100MBit/s: 200m, 1000MBit/s: 20m.

5.12 Warum ist die maximale Rahmenlänge bei Ethernet ebenfalls limitiert? Was passiert, wenn sich eine LAN Station bei Ethernet nicht daran hält? Welche Aufgabe hat die Jabber Control eines Transceivers?

Max Rahmenlänge ist limitiert(Fairness) damit jeder Teilnehmer die Möglichkeit zur Übertragung hat. Jabber Control soll genau das kontrollieren und bricht die Übertragung automatisch bei der maximalen Länge ab.

5.13 Welche prinzipielle Funktionen sind im Ethernet Controller einer LAN Station untergebracht? Was macht PLS? Was ist in der PMA (Transceiver) realisiert? Was erlaubt das AUI Interface?

Ethernet Controller bestehen aus LLC und MAC die parallel arbeiten.

PLS: OSI Layer 1, Bitübertragungsschicht. Erledigt das Encoding und Decoding in Manchester-Code. Das Physical Signalling 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(Der physikalische Medienzugang übernimmt die funktionale Schnittstelle zum Übertragungsmedium. Die PMA-Schnittstelle erbringt eine Reihe von Übertragungs- und Steuerfunktionen, das Reset, Transmit, Receive, Carrier Sense, Link Integrität, Jabber, Align und Clock Recovery.)=MAU(Die MAU, bekannt als Transceiver, enthält die Elektronik zum Senden und Empfangen der codierten physikalischen Signale, die in das Kabel eingespeist bzw. von ihm ausgefiltert werden.): Physical Medium Attachment AUI = ?Attachment Unit Interface?.AUI dient der Verbindung der Physical Layer Signalling (PLS) und Medium-Anschlusseinheit (MAU) und besteht aus dem Kabel, den Steckverbindungen und den notwendigen Leistungstreibern.

5.14 Warum mussten bei High Speed Ethernets (100BaseT, 1000BaseT) die Funktionen von PLS und AUI durch Reconciliation, MII/GMII und PCS ersetzt werden?

da auf AUI nicht so hohe Frequenz übertragen werden können, Manchester braucht doppelte Bandbreite also 2000MBit. Geschwindigkeit ist zu hoch, Schirmung ist schwer daher andere Technik.

5.15 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?

Einfacher Verstärker um die Reichweite eines Ethernet Segments zu vergrössern. Kollisionen werden vom Repeater erkannt und ein Jam Signal erzeugt. Das neue Segment wird Link-Segment genannt.

5.16 Wieso lassen sich Ethernet Netzwerke mittels Repeatern nicht beliebig vergrößern?

wegen der Collision Window bzw. slot Time von $51,2\mu s$.

5.17 Warum hat sich Ethernet zu 10BaseT weiterentwickeln ? Wie erfolgt die Ankopplung dabei? Benötigt man eine aktive Komponente? Welche Betriebsarten sind möglich bezüglich Half- und Full-Duplex? Welche Segment-Type hat 10BaseT?

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 (od mehr) zentralen Punkt über TwistedPair geführt wird vorsah. Diese Anforderungen passen exzellent zu Token Ring, daher musste Ethernet angepasst werden um Zukunftstauglich zu bleiben.

5.18 Wie hat sich durch 10BaseT die Topologie von Ethernet LANs verändert? Warum spricht man von „CSMA/CD in a box“? Warum ist aber „Hub“ein ungenauer Ausdruck?

Repeater mit mehr als zwei Segmenten und verschiedenen Medien werden Multiportrepeater genannt, sind Endsysteme und Multiportrepeater in einer sternähnlichen Topologie Zusammengeschaltet wird der Repeater "Hub"genannt. Dies ist der Hauptverwendungszweck für 10BaseT in heutigen EthernetNetzwerken. 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. Der Ausdruck „Hub“wird auch für zentrale Ethernet-Switches verwendet

5.19 Welche Rahmenformate gibt es bei Ethernet (Aufzählung)? Was sind die wesentlichen Unterschiede? Welche ist heute das gebräuchlichste Format?

IEEE 802.3, IEEE 802.3 with SNAP, Ethernet II

Unterschied: Ethernet II hat keinen LLC Sublayer, Length Feld wird für Protocol-Type (>1518) verwendet. IEEE 802.3 with SNAP wird verwendet, um Ethernet II über IEEE 802.3 zu transportieren.

LLC, Ethernet II, SNAP, Ethernet 802.3, Ethernet II und Ethernet 802.3 sind vom Frameaufbau ziemlich ähnlich, bzw. SNAP und LLC sind auch wieder ähnlich vom Frameaufbau.

5.20 Unterstützt das Rahmenformat Ethernet Version2 auch ein Connection-oriented Service auf Layer 2 (Begründung)? Welchen Grund gibt es für das Ethernet Rahmenformat SNAP? Wie ist es prinzipiell aufgebaut?

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(8bit) können keine Ethernet V2 protocol type(16bit) enthalten deshalb wird eine Anpassungsschicht eingeführt. SNAP(Subnetwork Access Protocol) ist ein Protokoll das die Übertragung von Ethernet V2 Daten über IEEE LANs ermöglicht

6 Packet Switching on LAN (TB / STP / RSTP) (Version 1.1)

6.1 Welche Gründe führten zur Entwicklung von Transparent Bridging für Ethernet LANs (Packet-Switching auf Layer 2)?

- LAN war zwar für shared Media Access, aber nicht mit so vielen Teilnehmer entwickelt worden. Bei vielen Teilnehmern kommt es zu einer hohen Wahrscheinlichkeit von Kollisionen auf dem Netz.
- für bessere Ausnutzung des Netzwerks
- Kollisionen reduzieren
- aus Sicherheitsgründen
- um auf entfernte Netzwerke zugreifen zu können

6.2 Wie arbeitet Transparent Bridging prinzipiell? Mit welcher Methode aus dem Network Principles Kapitel lässt es sich vergleichen? Auf welchem Layer des OSI Modells, mit welchen Adressen arbeitet Bridging?

Bridging ist für die Endsysteme unsichtbar. Bridging arbeitet auf OSI Layer 2 mit MAC Adressen. In der Bridging-Tabelle sind die MAC Adressen der Stationen enthalten, die durch das zugehörige Interface erreichbar ist. Eine Bridge muss alle Rahmen empfangen und bearbeiten Vergleich mit Packet switching.

6.3 Welche Einträge weist eine Ethernet Bridgingtabelle auf? Wie kommen diese Einträge im Falle der dynamischen „Plug and Play“Technik zustande? Welche Adresse eines Ethernet Rahmens wird dafür verwendet? Wieso benötigt man einen Alterungsmechanismus? Was passiert, wenn man vor Ausaltern das LAN Segment wechselt?

in der Bridgingtabelle wird festgehalten auf welchem Port sich eine bestimmte Adresse MAC befindet. Ein Offlinegehen eines Rechners kann nur dadurch erkannt werden dass über eine längere Zeit keine Daten mehr empfangen werden, daher ist ein Alterungsmachanismus notwendig. Pakete werden beim wechseln falsch weitergeleitet. Sendet der Recher auf dem neuen Segment, so wird die Bridgingtabelle aktualisiert.

6.4 Was bedeutet Forwarding, Filtering und Flooding bei Transparent Bridging konkret? Anhand welcher Adresse eines Ethernet Rahmens wird die Entscheidungen Forwarding, Filtering bzw. Flooding getroffen?

Forwarding: Kopie des Rahmens wird weitergeleitetan den Port auf dem die Adresse hängt.

Filtering: Rahmen wird verworfen wenn die Zieladresse auf dem selben Port wie die Sendeadresse hängt.

Flooding: während der Lernphase werden die Pakete an allen Ports weitergeleitet wenn für die Adresse noch kein Eintrag in der Tabelle existiert.

6.5 Ist eine Ethernet Bridge aus Endgerätesicht sichtbar? Muss eine Ethernet Bridge jeden Rahmen eines LAN Segmentes empfangen (Begründung)?

Ethernetbridge ist für die Endsysteme unsichtbar. Es wird jeder Rahmen empfangen und dann entschieden ob er weitergeleitet werden muss.

6.6 Wie geht eine Ethernet Bridge beim Empfang von Broadcast oder Multicast Rahmen vor? Warum sollte man Transparent Bridging nicht über WAN Links einsetzen?

Ethernet Broadcasts und Multicasts werden an alle ports weitergeleitet. Häufige Broadcasts auf Netzen und ein langsamer Wan Link zwischen zwei Half Bridges können zu einem ständigen Bufferoverflow bzw. einer ständigen Blockade führen.

6.7 Was ist Ethernet-Switching (Ethernet-Switch) im Vergleich zu Transparent Bridging (Ethernet Bridge)? Womit kann eine Ethernet Switching Tabelle verglichen werden: Routingtabelle von Packet-Switching im Connectionless Service oder Switchingtabelle von Packet-Switching im Connection-oriented Service?

Ein Ethernet-Switch ist im Prinzip ein Multiport Bridge. Also eine 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 Switchingtabellen pflegen um die verschiedenen Adressen den verschiedenen Netzen zuzuordnen, und in Folge die Pakete dorthin weiterleiten zu können.

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

6.8 Auf welchem Layer des OSI Modells, mit welchen Adressen arbeitet IP Routing? Was ist in IP Routingtabellen enthalten? Muss ein IP-Router jeden Rahmen empfangen? Ist der IP-Router aus Endgerätesicht sichtbar?

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 ist aus Endgerätesicht sichtbar.

6.9 Was ist zum Thema Collision Domain und Broadcast Domain bei Transparent Bridging festzustellen? Wie ist das im Vergleich zu einem Ethernet LAN mit Repeatern?

Eine Bridge teilt eine Collision Domain, collisions können sich nicht über Bridges fortpflanzen. 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. Repeater sind nur Signalverstärker, Broadcast als auch Kollisions werden weitergeleitet.

6.10 Welche Probleme gibt es beim Transparent Bridging / Ethernet Switching bei redundanten Wegen zwischen LAN Segmenten? Wodurch werden diese Probleme prinzipiell verursacht und wie werden diese Probleme prinzipiell gelöst?

Pakete mit unbekannter Adresse können im Kreis geschickt werden, Broadcasts werden vervielfältigt (Broadcast Storm), das Netzwerk wird schnell überlastet. Als Abhilfe gibt es spanning Tree Protokolle die redundante Leitungen deaktivieren.

6.11 Was ist ein Broadcast-Storm bei Transparent Bridging / Ethernet Switching? Welche 2 Arten gibt es?

Ein Endsystem löst einen Broadcast auf einem Netzwerk mit redundanten Leitungen aus. Der Switch gibt den Broadcast an jeden Port weiter, der 2. Switch erhält 2 Broadcasts. Dieser wird wieder zurück an den 1. Switch gesendet es kommt zu einer Endlosschleife an Broadcasts, Broadcaststorm. 2 Arten: Broadcast von Endsystem, Paket an eine unbekannte Zieladresse.

6.12 Wann kann ein Broadcast-Storm bei Transparent Bridging / Ethernet Switching auftreten? Welche Topologien sind anfällig, welche Verkehrstypen lösen diesen Effekt aus?

Ein Broadcast Storm kann bei redundanten Leitungen auftreten durch einen Broadcast oder durch ein Paket an eine unbekannte Zieladresse. Anfällig sind alle Segmente die an einen Switch angeschlossen sind.

6.13 Was ist die Grundidee des Spanning Tree Protocols? Warum verwendet man dafür den Ausdruck Tree? Woran erkennen Sie, dass eine Ethernet Bridge / ein Ethernet-Switch STP unterstützt?

Die Grundidee von STP ist, daß es zu jedem Endsystem nur einen Weg gibt und zusätzliche Pfade abgeschaltet werden. Der Ausdruck Tree wird verwendet, da nach Anwendung des STP eine Baumstruktur entsteht. Bei Geräten die STP unterstützen ist IEEE802.1D aufgedruckt.

6.14 Wie sind die prinzipiellen Abläufe beim Spanning Tree Protocol (Aufzählung des Summary)?

- 1 Bestimmen / wählen der RootBridge
- 2 Bestimmen der Root Ports
- 3 bestimmen einer bestimmten Bridge für jedes LAN Segment das über mehr als eine Bridge angesprochen werden kann.
- 4 Ausgewählte Ports auf weiterleiten schalten, alle anderen auf blockieren schalten
- 5 Erstellen einer einzelnen Verbindung von der Root Bridge zu allen LAN Segmenten.

6.15 Welche Basisparameter werden beim Spanning Tree Protocol verwendet? Was kann ein Netzwerkadministrator durch Konfiguration der einzelnen Parameter erzielen?

Bridge Identifier (Bridge ID): Eine Kombination aus Priority Number und MACAdresse. Typischerweise wird die niedrigste MACAdresse von allen Ports dafür verwendet. Die Priority Number kann durch den Netzwerkadministrator konfiguriert werden. Port Cost (C): Die Kosten um ein lokales Interface zu benutzen. Sie sind umgekehrt proportional zur Übertragungsrate, kann vom Administrator auf einen anderen Wert gesetzt werden. Port Identifier (Port ID): Eine Kombination aus Port MACAdresse und einer Priority Number, die kann vom Administrator geändert werden.

6.16 Was ist die Root-Bridge und was ist das Root-Port beim Transparent Bridging im Zusammenhang mit STP?

Die Bridge mit der niedrigsten ID wird zu Root-Bridge ernannt, von dieser aus werden die Verbindungen im Netzwerk hergestellt. Root Port ist jener Port mit den geringsten Kosten zur Root-Bridge.

6.17 Was ist die Designated Bridge beim Transparent Bridging im Zusammenhang mit STP? Nur in welchen Fall wird sie prinzipiell benötigt?

Hat ein Segment redundante Wege dann wird eine Bridge bestimmt die dieses Segment mit dem restlichen Netzwerk verbindet, sie wird zur Designated Bridge.

6.18 Welche Rolle bezüglich Forwarding und Blocking haben die Root Ports, Designated Ports und alle anderen Ports?

Root Ports und Designated Ports werden in forward state geschaltet, alle anderen Ports werden geblockt.

6.19 Was passiert wenn die Root Bridge beim Transparent Bridging im Zusammenhang mit STP ausfällt? Warum können das andere Bridges entdecken?

Die Root Bridge generiert (triggering) normalerweise alle 1-10 Sekunden eine Configuration BPDU, die über die Root Ports von jeder anderen Bridge empfangen wird und über die Designated Ports weitergeleitet wird. Bridges die nicht Designated sind hören noch immer auf solche Messages an ihren geblockten Ports. Wenn das Triggering ausfällt sind zwei Szenarien möglich: Ein Ausfall der Root Bridge bei dem eine neue RB gesucht wird und sich in Folge der Spanning Tree ändern wird oder ein Ausfall der Designated Bridge.

6.20 Was passiert wenn die Designated Bridge beim Transparent Bridging im Zusammenhang mit STP ausfällt? Wie können das andere Bridges entdecken?

An den Designated Ports wird der Heartbeat weitergeleitet so dass die geblockten Ports über redundanten Bridge mitbekommen, empfangen die geblockten Ports keinen Heartbeat hat die Designated Bridge einen Fehler. Geblockte Ports können aktiviert werden und verbinden die Segmente wieder.

6.21 Was sind die prinzipiellen Nachteile des Spanning Trees beim Transparent Bridging / Ethernet Switching? In welchem Bereich bewegt sich die Konvergenzzeit des STP Protokolls?

- Aktive Pfade werden immer von der Root-Bridge aus gerechnet, Netzwerkströme können aber andere Wege nehmen
- Redundante Wege können nicht zum Ausbalancieren verwendet werden, die werden abgeschaltet
- Maximale Konvergenzzeit ist 50s.

6.22 Zählen Sie drei Vor- und drei Nachteile des Transparent Bridgings / Ethernet Switchings im Vergleich zum IP Routing auf?

- + Schneller, weil es in der Hardware implementiert ist, daher keine address resolution notwendig.
- + Basiert nur auf den MAC-Adressen, die man nicht extra konfigurieren muss.
- + Transparent, keine Einstellungen auf Clients notwendig.
- - Muss jeden Rahmen bearbeiten.

- - Anzahl der Einträge in der Bridge-Tabelle ist die Anzahl von allen Stationen im gesamten Netzwerk.
- - Kein Load-Balancing.

6.23 Wodurch ergibt sich prinzipiell die rasche Konvergenz-Zeit bei Einsatz des Rapid Spanning Tree Protokolls (RSTP)? In welchen Bereich bewegt sich diese?

Bei Netzwerkänderungen können sich Bridges selbstständig in den forward state versetzen wenn sie sich am Root Port der neuen Bridge befinden. Bridges senden selbständig hello messages alle 2 Sekunden. Wird auf einem Root Port keine Hello Message empfangen wird versucht einen anderen Weg zu finden, Die Konvergenzzeit liegt bei einigen Sekunden.

6.24 Welche neuen Port-Rollen es gibt beim Rapid Spanning Tree Protokoll (RSTP)? In welchen Topologien werden sie wirksam?

- Edge Ports: Ports die direkt mit dem Endsystem verbunden sind können keinen BridgingLoop erzeugen und schalten automatisch in den Forward-State
- Link Type: full duplex -> p2p, half duplex -> shared Media

6.25 Was wird beim Proposal/Aggreement Exchange beim Rapid Spanning Tree Protokoll (RSTP) ausgehandelt? Nur für welche Konstellationen gilt das (Edge Ports, Shared Ports oder Point-to-Point Ports)? Nur für welche Konstellationen gibt es den raschen Übergang (Transition) in den Forwarding State (Edge Ports, Shared Ports oder Point-to-Point Ports)?

Bei sich aktivierendem Link versucht die Bridge designated Bridge für dieses Segment zu werden. Die neue Bridge akzeptiert dies wenn die Anfrage über einen Root-Port kam. Nach dem OK setzt die erste Bridge sich in den Forward State. Gilt für Shared-Ports und P2P Ports. Einen raschen Übergang gibt es nur für Edge Ports.

7 Ethernet Evolution, VLAN and High Speed Ethernet (Version 1.1)

7.1 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 bereitet nur das Signal auf (Signalverstärker), das Netzwerk wird dadurch nicht beeinflusst, die CollisionDomain bleibt erhalten.

7.2 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?

Bei Bridging/Switching Technologie bleibt die Broadcast Domain erhalten die sie Protokoll-Transparent sind (sie müssen jedes Paket bearbeiten). Die Collision Domain wird hingegen geteilt da sie eine Store and Forward Technologie sind-

7.3 Vergleichen Sie Transparent Bridging mit Ethernet Switching. Was ist gleich? Wo gibt es Unterschiede?

Ein Switch ist eine Multiport Bridge. Eine Bridge erzeugt kleinere CD. Bei einem Switch hängt auf jedem Port nur 1 Host, daher besteht die CD aus nur 2 Partnern die Full Duplex miteinander sprechen.

7.4 Was versteht man unter full-duplex Ethernet? Ist CSMA/CD auf einem solchem Link aktiv? Welche prinzipiellen Ethernet-Segment-Typen bzw. Ethernet-Technologien können im full-duplex Modus arbeiten?

Beide Partner können gemeinsam gleichzeitig über verschiedene Drähte miteinander sprechen ohne dass es zu Kollisionen kommen kann. CSMA/CD wird deshalb nicht gebraucht, ist also deaktiviert. Nur Point To Point Verbindungen können Full Duplex miteinander sprechen, Shared Media nicht.

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

Da es zu keinen Kollisionen kommen kann können schnelleren Taktraten auf längeren Leitungen verwendet werden.

7.6 Kann man full-duplex Ethernet bei Verwendung von Repeater-Technologie einsetzen (Begründung)? Gehen Sie auf den Begriff „CSMA/CD in a box ein. Können in einem Ethernet-LAN Repeater unterschiedlicher Technologie (10 Mbit/s, 100 Mbit/s, 1Gigabit/s) gemischt verwendet werden?

Repeater ist nur Signalaufbereitung bei Shared Media, d.h. keine Point To Point Verbindung und kein Full Duplex. Keine Mischung möglich da keine Store and Forward Technologie.

7.7 Welche Bedingungen müssen gegeben sein, dass man ein Ethernet LAN vollständig kollisionsfrei betreiben kann (Aufzählung)? Können in einem solchen kollisionsfreien Ethernet-LAN unterschiedlicher Technologie (10 Mbit/s, 100 Mbit/s, 1Gigabit/s) gemischt verwendet werden (Begründung)?

Jeder Host ist über eine Point to Point Verbindung am Multiport-Switch angeschlossen. Bridges verwenden Store and Forward Technologie und können deshalb verschiedene Netzwerktechnologien verbinden.

7.8 Ist STP (Spanning-Tree Protokoll) bzw. RSTP bei einem vermaschten (redundanten), kollisionsfreien L2 geschichteten Ethernet LAN Netzwerk notwendig (Begründung)? Wie bezeichnet man die Verbindung zweier L2 Ethernet-Switches? Wie spiegelt die STP-Port-Rolle den Support des ursprüngliche shared-Media Verhaltens zwischen 2 Ethernet-Switches wider?

Bei einem solchen redundanten System kann es zu einem Broadcast strom kommen und daher ist STP notwendig. Verbindung zwischen 2 Switches heisst Trunk Line.

7.9 Warum ist Flow Control zwischen einem L2-Ethernet-Switch und einem Ethernet Endsystem wünschenswert bei L2 geschichteten LAN Netzwerken? Wie wird diese Flow Control realisiert?

Flow Control ist notwendig um Bufferüberläufe und somit Datenverlust vorzubeugen, realisiert ist dies durch eine MAC Based Flow Control (Pause Commandos)

7.10 Wozu dient der „Pause“Frame bei Ethernet? Welche neue Ethernet Rahmen taucht in diesem Zusammenhang auf? Wie funktioniert das „Pause“Verfahren (kurze Beschreibung)?

Bei jedem Pause Kommando wird der Partner veranlasst kurz zu warten und keine Pakete zu versenden (Ausnahme MAC-Controll-Frames). Das Pause Kommando ist zu wiederholen für längere Pausen. Neues Frame ist Mac-Controll-Frame.

7.11 Worum hat man Autonegotiation bei Ethernet eingeführt? Was wird bei Autonegotiation prinzipiell ausgehandelt? Nur bei welchen Ethernet-Technologien ist Autonegotiation anwendbar?

Es wird Geschwindigkeit, Full-Half-Duplex, Signal Rate ausgehandelt. Es ist nur möglich bei 1000BaseT, 100BaseT, 10BaseT, also bei Kuperkabel

7.12 Ethernet Autonegotiation: Welche Parameter können bei 10BaseT, 100BaseT, 1000BaseT ausgehandelt werden (Aufzählung)? Welche Parameter können bei 1000BaseX ausgehandelt werden?

- 10BaseT: Link Puls
- 100BaseT: Full-Half Duplex, 10/100 MBit/s
- 1000BaseT: Access Mode, Flow Cotrol Mode, Data Rate

- 1000BaseX: Access Mode, Flow Control Mode

7.13 Wozu dient der NLP bei 10BaseT-Ethernet? Wozu dient ein FLP beim 100BaseT Ethernet?

Net Link Puls zum Erkennen der Verbindung

Fast Link Pulse: miteinander verbundene Systeme sollten ihre Eigenschaften / Features austauschen um bestmöglich zusammenzuarbeiten.

7.14 Wieso musste für High Speed Ethernet die Codierungsarten von Manchester auf 4B/5B bzw. 8B/10B geändert werden und die PLS/AUI Funktion durch Reconciliation/MII-GMII/PCS ersetzt werden?

Um die Effizienz zu steigern (von 50% zu 80%) (hohe Bitraten). Das alte Physical Layer Signaling Interface (PLS), repräsentiert durch AUI, war für die neuen Coding-Technologien nicht geeignet; AUI wurde durch MII (Media Independent 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

7.15 Wie geht man beim 4B/5B (100BaseX) bzw. 8B/10B (1000BaseX) prinzipiell vor? Welche Bitrate (Signalrate) ergibt sich daraus tatsächlich am Medium?

Je 4 Bit an Daten werden in einem 5Bit Datenstrom umgewandelt. AUs den 5Bit Wörtern werden nur jede Kombinationen verwendet die hinreichend viele Taktwechsel besitzen, aus einer Bitfolge von 0000 wird dann eine Bitfolge mit mehreren Taktwechsel. Durch das zusätzliche Bit entsteht eine 25% höhere benötigte Datenrate. Für eine 100MBit Übertragung muss die Leitung 125MBit Datenrate aufweisen. Selbiges für 8B/10B.

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

Um die Collision Time einhalten zu können. Die max. Leitungslänge kann so von 20m auf 100m gesteigert werden. Bei 10Gbit nicht notwendig da es sich nicht um ein Shared Media handelt (kein CSMA/CD)

7.17 Wie funktioniert die Methoden Carrier-Extension bei Gigabit-Ethernet (kurze Beschreibung)?

Zusätzliche Bits werden vom Sender eingefügt und vom Empfänger wieder entfernt um die Framelänge zu erhöhen. Der Frame befindet sich dadurch länger auf dem Medium.

7.18 Wie funktioniert die Methoden Frame-Burst bei Gigabit-Ethernet (kurze Beschreibung)?

Es werden mehrere Frames zusammengesetzt (also auf mehr Daten gewartet)

7.19 Was ist die Basis-Idee von VLAN?

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 Systemen 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.

7.20 Welche prinzipiellen Mittel benötigt ein Ethernet-Switch zur Realisierung von VLANs in einer L2 geschichteten Ethernet LAN (Aufzählung)?

VLAN-Tagging, separates STP, separate Bridge/switching Table, Methode zum Zuordnen in einem VLAN

7.21 Welche Methoden gibt es, um ein Endsystem einem VLAN zuzuordnen (Aufzählung)? Welche ist die häufigste Methode?

Port-Based (häufigste), MAC-Based, Protocol-Based

7.22 Welche Arten der Spanning-Tree Unterstützung gibt es bei VLAN Technik (Aufzählung)?

Eigenes Spanning Tree für jedes VLAN, IEEE 802.1w spezifiziert auch ein RSTP für alle VLANs gemeinsam.

7.23 Was ist ein VLAN-Tag? Wo befindet sich der VLAN Tag in einem Ethernet Rahmen? Wird der Ethernet-Rahmen dadurch länger?

Ein VLAN-Tag kennzeichnet eine Zuordnung in einem VLAN. Er wird im 802.1Q Feld gespeichert, der Rahmen wird dadurch um 4 Byte länger. Minimale und Maximale Framlänge erhöhen sich ebenfalls um diese 4 Byte.

7.24 Wozu dient die UP Information im 802.1Q Feld? Wozu kann das ein Ethernet-Switch verwenden?

Mit der UserPriority kann man den Switch anweisen diese Daten schneller zu verarbeiten / weiterzuleiten. Für die verschiedenen Prioritäten existieren verschiedene Stacks.

7.25 Wieso benötigt man VLAN Tagging auf Trunkleitungen? Wie heißt die entsprechende Methode, die den VLAN Tag im Ethernet Rahmen kennzeichnet? Wieso benötigt man i.a. keinen VLAN-Tag am Access-Port zu einem Endsystem?

Die Trunkline ist die Verbindung zwischen 2 Switches. Tagging wird erst durch den Switch zugeordnet (z.B über Port-Based). Am entfernten Switch muss das verwendete VLAN bekannt gemacht werden (z.B für Broadcast). Access-Port ist über eine Point-To-Point Verbindung angeschlossen, daher kein VLAN nötig.

7.26 Wann benötigt man 802.1Q auch auf einen Access-Port zu einem Endsystem? Was kann man damit erreichen?

Access-Port mit Multi-Home-Funktion benötigt auch VLAN. Die Zuordnung zu mehreren VLANs ist dadurch möglich.

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

Redundante TrunkLines würden von STP abgeschaltet werden. Channeling fasst sie zu einer virtuellen Leitung zusammen und erlaubt die grössere Bandbreite sinnvoll zu nutzen.

7.28 Können Endsysteme, die an ein L2 geschwitchtes Ethernet LAN angeschlossen sind aber in unterschiedlichen VLANs liegen, direkt miteinander kommunizieren (Begründung)? Welche Rolle spielt dabei ein Router, der über 802.1Q zu beiden VLANs Zugang hat?

Switches erlauben keine Übertragung zwischen 2 verschiedenen VLANs, dies würde gegen die Grundidee der VLANs widersprechen. Ein 802.1Q Router kann den Zugriff von einem VLAN in ein anderes erlauben wenn er dafür konfiguriert ist.

8 IP Technology (Version 1.1)

8.1 Charakterisieren Sie kurz IP (OSI Layer, Network Type (Packet- oder Circuit-Switching) / Service Type (CO oder CL), Grundeigenschaften, Rolle der beteiligte Komponenten (IP Host, Router) bezüglich Forwarding).

IP steht für Internet Protocol

- Paket switching Technologie
- benutzt strukturierte Technologien auf Layer 3
- Connectionless / best effort Service
- geteilte Verantwortung zwischen Netzwerk und Endsystem. Netzwerk übernimmt die Zustellung der Pakete anhand der Adressen, Endsystem ist verantwortlich für die Kontrolle der Korrektheit der Daten.

8.2 Wie ist die Aufgabenteilung zwischen IP und TCP? Wo findet man IP, wo findet man TCP im Protokoll Stack (am IP Host oder am IP Router oder auf beiden)?

IP ist zuständig für den Versand / Empfang der Daten als Connection-Less Service (Best effort Service), arbeitet auf Layer 3. TCP steht für Transmission Control Protocol und stellt einen Connection Oriented Service zur Verfügung. TCP arbeitet auf Layer 4 aber nur auf dem Host.

8.3 Welche Aufgaben erfüllt der IP Header prinzipiell? Zählen Sie zumindest fünf wichtige Funktionen auf.

- Version: Version des IP Protokolls
- Len: Länge des IP Headers in 32Bit Worten
- Total Length: Gesamtlänge des Datenpackets in Oktets (Byte)
- Protocol: Gibt das aufzurufende Protokoll an
- TTL: Time to Life
- Adressen: Source-Adresse, Destination-Adress.

8.4 Wozu wird bei IP TTL benötigt (Begründung)? Wie wird es gehandhabt? Was passiert dabei im Zusammenhang mit ICMP?

TTL ist ein Hop Count. Um im Kreis zirkulierende Pakete erkennen zu können wird TTL benötigt. Bei jedem Router wird der TTL um eins reduziert, bis bei 0 das Paket verworfen wird. Über ICMP erfolgt eine Meldung an den Host dass ein Paket nicht zugestellt werden konnte um Routingfehler erkennen zu können.

8.5 Wozu wird bei IP Fragmentierung benötigt? Wie wird diese gehandhabt (Wer fragmentiert, welche Felder im Header werden dafür verwendet bzw. wie ist deren Zusammenspiel; wo wird wieder zusammengesetzt und warum?)

Jedes Netz hat eine (MTU Maximum Transfer Unit) maximale Paketgröße, IP muss jetzt zu große Pakete in mehrere Frames aufteilen. Jedes zerteilte Fragment erhält einen vollständigen IP Header mit Identifikationsnummer (Identification und Flags werden im Header verwendet), um sie wieder zusammen zu setzen. Die Daten werden beim Empfänger wieder zusammengesetzt da jedes Paket einen anderen Weg gehen kann. DF-Bit ist das don't fragment bit, MF das more fragment Bit. (es kommen noch mehrere Fragmente)

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

Maximum Transmit Unit) Station sendet das größt mögliche Paket mit DF (Don't Fragment) bit set. 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.

8.7 Wozu diente das ToS Feld im IP Header ursprünglich? Welche Möglichkeiten hatte man prinzipiell?

Type of Service. Teilte die Priorität und bevorzugten Netzwerkcharakteristiken (niedrige Kosten, hohe Sicherheit, wenig Verzögerung, hohe Verfügbarkeit) des Paketes mit. Können für die Pfadauswahl benutzt werden wenn es mehrere Pfade, mit unterschiedlichen Charakteristiken, zum Ziel gibt (Dazu benötigt der Router aber eine Routingtabelle pro Charakteristik). TOS Bits können von Routern ignoriert werden, aber sie führen nie dazu das ein Paket verworfen wird nur weil das gewünschte Service nicht bereitgestellt werden kann.

8.8 Was ist die heutige Idee von ToS Feld im IP Header (Stichwort: DSCP)? Wofür ist das 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, ...). Mit Hilfe von DSCP kann ein IP-Datagramm einer bestimmten Traffic-Klasse und innerhalb dieser Klasse einer bestimmten Behandlungsstufe zugeordnet werden (Limited-Delay usw.).

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

Sicherheits und spezielle Routing Einstellungen festlegen. Record Route: Jeder passierte Router trägt seine IP adresse ein, um die Route aufzuzeichnen. Loose Source Route: das Paket muss die vorgegebenen Router passieren anhand der gegebenen Sequenz in der Liste, andere dazwischenliegende Router können passiert werden. Strict Source Route: Selbes wie Loose Source Route jedoch dürfen kein Router passiert werden die nicht in der Liste stehen). Heute ist der IP-Header wegen Sicherheitslücken, durch Firewalls blockiert.

8.10 Was kennzeichnet eine IP Adresse prinzipiell? Ist die IP Adresse eine strukturierte Adresse? Aus welchen Teilen ist sie prinzipiell aufgebaut? Wie wird sie dargestellt?

32 bit lang, Darstellung: dotted decimal / net-length. Bsp: 101.54.21.41/8. Eine IP-Adresse ist eindeutig, kein Knoten im Internet hat die gleiche wie ein anderer. Struktur: Net-id+Host-id. IP-Adressen sind in versch. Klassen unterteilt, mit untersch. langer Net- Host-id. Darstellung aus 4 mal 8Bit getrennt mit einem Punkt zwischen den Oktetts.

8.11 Wenn Sie einen IP Router mit fünf Netzwerk Interfaces haben, wie viele IP Adressen weist der Router auf? Wieso benötigt ein IP Router überhaupt eine IP Adresse? Zählen Sie die beiden wichtigsten Gründe auf (Denken Sie dabei an Routing und Sichtweise des IP Hosts)?

Pro Netzwerkinterface hat der IP-Router auch eine IP-Adresse. Als Teilnehmer im Netzwerk braucht er einen Zugang zu diesem, die er mit der IP-Adresse bekommt. Die Teilnehmer können den Router dann über diese IP-Adresse ansprechen. Der Router muss expliziet angesprochen werden von den Hosts.

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

Am ersten Oktet kann man ablesen zu welcher Klasse eine Adresse gehört.

- A : Bereich 1-127 NetID: 7, HostID: 24
- B : Bereich 128-191 NetID: 14 HostID: 16
- C : Bereich 192-223 NetID: 21 HostID 8
- D : Bereich 224-239 (unicast)
- E : Bereich 240-255 (experimentell)

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

Ein Teilnehmer sendet einen Broadcast mit 255.255.255.255 aus, daher er will nur die Teilnehmer in seinem Netzwerk, im Netzwerk mit der gleichen Host-ID ansprechen. In Lan's wird auf L2 der Broadcast an alle Netzwerkteilnehmer weitergeleitet.

8.14 Was ist ein IP Directed Broadcast? Wie wird diese Adresse dargestellt? Wie wird dieser Broadcast über ein IP Netzwerk transportiert und was passiert, wenn dieser am Zielnetz ankommt? Warum und wo wird er heute unterbunden?

Ein Teilnehmer löst einen Broadcast in einem anderen Sub-Netz aus indem er am Anfang die NetID setzt. z.b 10.255.255.255. Empfänger der Router für dieses subnet den Broadcast modifiziert er die Adresse zu einem Limited Broadcast und schickt ihn in das betreffende Subnet. Heute wird er unterbunden wegen Denial Of Service Attacks im Betriebssystem und in den Firewalls.

8.15 Was versteht man unter Subnetting und warum wurde es ursprünglich eingeführt? Wie wird das dargestellt bzw. konfiguriert?

Netz wird für die interne Verwendung in mehrere Teilnetzte aufgeteilt, nach außen trotzdem noch ein Netz. (Mechanismus dazu heißt Subnetting) Ein Teil der host-id wird verwendet um net-id Teil zu erweitern. Netzmaske ist genau so lang wie die IP-Adresse, alle Bits des Netzwerkteils sind auf 1 und alle Bits des Geräteteils auf 0 gesetzt. (dotted decimal notation).

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

Subnet Zero und Subnet Broadcast ist nicht eindeutig zuordenbar. 10.255.255.255 kann ein Broadcast zu dem Netz 10. sein oder zu dem Netz 10.255. Selbiges gilt für Subnet Zero.

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

IP-Adresse (eindeutig), Subnetmask und Standard Gateway. Die Hosts haben nur eine lokale Sicht des Netzwerkes.

8.18 Was versteht man unter „direct“ und „indirect delivery“? Woran erkennt ein IP Host wie er vorgehen muss? Wie erfährt ein IP Host die Existenz eines lokalen Routers?

Direct ist wenn Sender und Empfänger sich im gleichen physischen Netzwerk befinden. (net-id of Source = net-id of Destination). Host macht alles selber, Router wird nicht gebraucht. Indirect wenn es nicht so ist. Der Host schaut, ob seine Subnetzmaske und die des Ziels gleich ist, wenn nicht, schickt er das Paket mit der Ziel-IP des Ziel-Hosts an die MAC-Adresse der Router, der sich um die Weiterleitung kümmert. Der Default Gateway muss am Host konfiguriert werden.

8.19 Was muss in IP Routern im Minimum konfiguriert werden, um lokale IP Kommunikation zu ermöglichen (d.h. zwischen den IP Netzen eines Routers)? Was muss in IP Routern weiters konfiguriert werden, um globale IP Kommunikation zu ermöglichen (d.h. über mehrere IP Router hinweg)? Welche Sichtweise haben die IP Router dadurch (lokal oder global)?

Manuell konfiguriert werden müssen die IP Adressen und Subnetmasken der Interfaces und der 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.

8.20 Wie ist eine IP Routing-Tabelle prinzipiell aufgebaut? Was stellen diese Einträge aus Sicht des Packet-Switchings prinzipiell dar? Was findet man zusätzlich in einer IP Routing-Tabelle, wenn man dynamisches Routing verwendet?

IP Routing Table enthält Infos über welchen Port ein bestimmtes Netzwerk erreicht werden kann. Einträge stellen den besten Pfad zum jeweiligen Netzwerk dar. Zusätzlich Kosten der Ports, Alter der Verbindung.

8.21 Welche drei Grund-Paradigmen gibt es beim IP Routing (Aufzählung und Erklärung der Bedeutung bzw. Auswirkung)?

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

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

ARP ist Adress Resolution Protocol.

ARP ist zuständig um eine Zuordnung zwischen MAC Adresse und IP Adresse eines IP-Netzwerks zu schaffen. Will ein Teilnehmer Daten an einen Host schicken dessen MAC-Adresse er noch nicht kennt schickt er einen ARP-Request mit dessen IP-Adresse los. Der Teilnehmer empfängt den ARP-Request und antwortet mit einem ARP-Response in dessen er seine MAC-Adresse packt. Beide Systeme speichern die zugehörigen Adressen in einem ARP-Cache. Reichweite von ARP nur lokal, wird vom IP-Router nicht weitergeleitet.

8.23 Welche Informationen können IP Geräte aus dem Empfang eines ARP Requests gewinnen? Welche Geräte auf einem LAN reagieren? Werden alle Geräte eines LANs oder nur die IP Geräte mit einem CPU Interrupt der Netzwerkkarte aufgeweckt?

Der ARP-Request wird mit einem Layer 2 Broadcast ausgesandt. Alle Teilnehmer am Netz müssen diesen Broadcast verarbeiten, aber nur der Teilnehmer mit der entsprechenden IP-Adresse reagiert mit einem ARP-Response. Geräte bekommen neue Einträge für den ARP-Cache.

8.24 Welche Informationen können IP Geräte aus dem Empfang eines ARP Repls gewinnen? Welche Geräte bekommen den ARP Reply? Werden alle Geräte eines LANs oder nur die IP Geräte mit einem CPU Interrupt der Netzwerkkarte aufgeweckt?

Die Antwort geht nur an den Frageseller, alle anderen Hosts am Netz werden nicht aufgeweckt.

8.25 Was ist ein gratuitous ARP? Wofür wird er verwendet?

Der Sender schickt einen ARP-Request mit seiner eigenen IP-Adresse als Ziel aus. Sinn ist dass allen Teilnehmern seine MAC-Adresse und IP-Adresse bekannt gemacht werden, und Hosts mit der selben IP-Adresse zu ermitteln. Der Host erwartet sich keinen ARP-Response da es seine IP-Adresse nicht noch mal geben sollte.

8.26 Wozu dient der ARP Cache? Wann wird er refresh (zwei Möglichkeiten)? Gibt es eine Möglichkeit den ARP Reply zu authentifizieren?

ARP-Cache ist eine Speicher für die Zuordnung von MAC und IP-Adressen der Teilnehmer im Netzwerk. Um nicht bei jedem Paket das verschickt werden sollte einen ARP-Request schicken zu müssen werden ARP-Einträge für eine bestimmte Zeit gespeichert. Refresh wird er mit einem ARP-Request eines Teilnehmers oder über einen gratuitous ARP.

8.27 Wozu dient das ICMP Protokoll (Aufzählung der sechs wichtigsten Funktionen)?

ICMP ist Internet Control Message Protocol dient dazu Fehlermeldungen abzusetzen um die Zuverlässigkeit der Datenzustellung zu verbessern. Eine IP-Station, die einen Übertragungsfehler registriert, generiert eine ICMP message. Diese wird an den Absender des IP-Pakets gesendet. Falls auch das ICMP message nicht übertragen werden kann, werden keine weiteren messages mehr gesendet um eine ?ICMP-Lawine? zu verhindern.

- Echo Reply
- Echo Request
- Destination unreachable
- Time exceeded
- Network unreachable
- Protocol unreachable: wird vom Host generiert wenn der das Protocol nicht unterstützt.
- Fragmentation needed, but Don't-Fragmentation-Bit gesetzt.

8.28 Was ist das generelle Grundprinzip von ICMP (abgesehen von ICMP Echo Request und Echo Reply)? Wie werden ICMP Messages transportiert? Was passiert, wenn eine ICMP Message selbst einen Fehler verursacht?

Mit ICMP können Fehler von einem Router oder vom Host signalisiert werden. ICMP-Messages werden als Datagramme über das Netz transportiert.. Verursacht ein ICMP-Paket einen Fehler wird kein neues ICMP-Paket erzeugt um Lawinen zu verhindern.

8.29 Was ist ein Ping? Mit welchen Mitteln wird er realisiert? Welche Informationen kann man bei üblichen Implementierungen daraus gewinnen?

Ein Ping ist eine Anfrage an einen Host ob dieser erreichbar und aktiv ist mittels eines Ping-Requests. Als Information bekommt man ob ein Ziel erreichbar ist und wie schnell dieses erreichbar ist. (Ping-Zeit). Der Ping Response kann vom Administrator deaktiviert worden sein.

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

- Network, no path to network known, generated from Router
- Host, host-id can't be solved, host not responding, from Router
- Protocol, protocol specified in ip header not available, from end-system
- Port, unreachable(port specified in layer 4 not available, from End-system
- Fragmentation needed, Paket to big, but don't fragment bit set, from Router
- Source, route failed(path in ip options could not be followed, from Router

8.31 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?

Flusskontrolle. Teilt dem Sender mit seinen Traffic zum Router oder Host zu reduzieren. Source Quench-Messages werden generiert um Bufferüberläufe zu verhindern. TCP muss auf Source Quench reagieren, aber man kann sich nicht darauf verlassen dass ein Empfänger überhaupt Source-Quench Messages generiert.

8.32 Was ist ein Traceroute? Mit welchem Mittel wird das realisiert? Lassen sich damit alle Wege eines Netzes aufzeichnen (Begründung)?

Listet den Pfad zum einem Ziel auf. Verwendet UDP Segment, TTL wird zu Beginn auf 1 gesetzt. Beim nächsten Hop wird eine ICMP-Message generiert, die der Sender empfängt. Daraufhin wird TTL jeweils um 1 erhöht und so der gesamte Weg aufgezeichnet. Parallele Wege werden nicht erkannt.

8.33 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 / schnelleren Pfad, so wird der Host über eine ICMP Redirect Message darüber informiert. Der Router sendet aber auf jeden Fall auf dem alten ineffizienten Pfad weiter, die ICMP Message ist nur zur Information für spätere Datenpakete. Bei Redirect Attacken werden Pakete auf ungewollte Pfade geführt.

8.34 Wozu dient das PPP Protokoll prinzipiell? In welchen zwei Szenarien wird es verwendet?

Die serielle Verbindung von Routern unterschiedlicher Hersteller war nicht von Anfang an möglich, PPP wurde als Standard eingeführt um dieses Problem zu umgehen. PPP ist PointToPoint Protocol

- PPP verbindet Netz über eine serielle Leitung mit Routern unterschiedlicher Hersteller.
- Huete von grösserer Bedeutung: PPP sorgt für eine Verbindung zu einem IP-Netz (Modem, ISDN, ADSL, ...)

8.35 Aus welchen Komponenten besteht die PPP prinzipiell (Aufzählung und kurze Erklärung)?

- HDLC: Framing and Encapsulation. Bitstuffing for synchronous serial Line, Connectionless
- LCP: LinkControl Protocol: Auf- und Abbauf von Verbindungen, Testen des Links, Konfiguration der PPP Connection.
- family of Network Control Protocol: Konfiguriert Netzwerk Layer Protocol.

8.36 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 dabei?

Eine PPP Verbindung wird in 4 Stufen aufgebaut:

- Verbindung herstellen und Konfiguration aushandeln.
- Optionaler Schritt für weitere Konfiguration (CHAP, PAP)
- Netzwerk Layer Protocol Konfigurieren
- Verbindung trennen

8.37 Welche Parameter lassen sich durch LCP (PPP Phase1) aushandeln? Welche zusätzlichen Dinge können in PPP Phase 2 zum Einsatz kommen?

Phase 1:

- die Verpackung / Einrahmung der Daten
- welche Paketgrößen zulässig sind
- erkennen von Konfigurationsfehlern
- um zusätzliche Optionen für die Verbindung auszuhandeln.

Phase 2:

- Authentication (chap)
- compression
- multilink

8.38 Wozu dient IPCP bei PPP? Zu welcher PPP Familie gehört es? Mit welcher am LAN üblichen Methode lässt sich IPCP vergleichen?

Internet Protocol Control Protocol dient zur automatischen Konfiguration von Computern, die sich (typ über Analog-Modem od. ISDN) mit einem Netz verbinden. Bei Konfiguration durch IPCP werden IP-Adresse, Default-Gateway und DNS-Server der einwählenden Station mitgeteilt. Funktioniert IPCP ähnlich wie DHCP in Ethernet-Netzwerken, jedoch Punkt-zu-Punkt-Verbindungen. IPCP gilt aufgrund seiner Funktion als NCP (Network Control Protocol) für das Internet Protocol (IP) über PPP

8.39 Was versteht man unter RAS Technik? Wo kommt sie üblicherweise zum Einsatz?

RAS ist Root Access Server.

Zuständig für die Bearbeitung von Anfragen von Systemem die eine Verbindung zum Netz aufbauen wollen. RAS kommt zum Einsatz bei der Einwahl in ein Firmennetz oder bei der Einwahl in das Internet über einen Internet Service Provider.

8.40 Welche Phasen gibt es bei der RAS Technik (Aufzählung in richtiger zeitlicher Reihenfolge)? Was wird dabei alles überprüft und zugewiesen? Was kann optional gemacht werden?

- Verbindungsaufbau über ein Netz (ISDN) zum Access Server.
- PPP Link, Verbindung wird aufgebaut mit LCP und notwendige Parameter bestimmt und abgefragt, wie z.B Prüfung der Authentifikation.

- PPP NCP weist IP-Adresse, GW, DNS dem anfragendem System zu.
- Endsystem ist Teil des Netzwerks.

8.41 Wozu wird bei einem ADSL-Anschluss das Protokoll PPP benötigt? Welche Rolle spielen Protokolle wie PPPoE oder PPTP in diesem Zusammenhang bzw. warum werden sie überhaupt benötigt??

Bei ADSL wird PPP benötigt um sich über einen ISP ins Internet einzuwählen. PPPoE / PPTP sind Protokolle die nur bis zum ADSL Modem gehen, aus Gründen von Marketing entwickelt, nach ADSLPS erfolgt dann PPPoA das die Verbindung über ATM Netz zum ISP aufbaut.

9 Chapter 9 / 10 IP Routing Overview, OSPF Routing (Version 1.1)

9.1 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. Muss konfiguriert werden wenn Pakete in Netz mit anderer NetzID geschickt werden wollen.

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

die Routing Tabellen sind vom Administrator vorkonfiguriert. Nachteile:

- Zeitintensives set up und aufwändig zu ändern bei komplexen Netzwerken
- reagiert nicht auf Topologieänderungen
- kein zusätzlicher CPU bedarf
- kein overhead Traffic durch Routingprotokolle

9.3 Wann können statische Routen prinzipiell verwendet werden (Stichwort: Wegeredundanz)? Wann müssen statische Routen verwendet werden (Stichwort: Spezielle Netzwerk-Technologien)?

- wenn keine Wegeredundanz gegeben ist.
- aus Sicherheitsgründen.
- wenn bestimmte Technologien kein Routingprotokolle erlauben (X25, ISDN, ATM, Frame-Relay)

9.4 Was ist eine Default Route? Wo wird sie konfiguriert (am IP Router oder am IP Host)? Warum ist die Technik der Default Route beim Anschluss eines IP-Netzwerkes an das Internet so wichtig? Welches Routing Paradigma spielt hier eine Rolle?

Die Default Route wird am Router konfiguriert. Der Router schickt Pakete mit ihm unbekannter Zieladresse über die Default Route zum nächsten Router weiter. Ein Router zum Internet müsste ansonsten jeden Knoten im Netz kennen (riesen grosse Routingtabellen haben). Hop by Hop Route, Datenpaket nimmt den Pfad der gerade in der Routingtabelle aktiv ist.

9.5 Was passiert, wenn ein Router ein Datagramm mit einer unbekanntem Zieladresse empfängt und dem Router keine Default Route bekannt ist? Was passiert, wenn dem Router eine Default Route bekannt ist?

Der Router generiert eine ICMP Message und verwirft das Paket. Ist eine Default Route bekannt, so wird das Paket dorthin weitergeleitet.

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

- Routing Tabellen werden über Routing Protokolle dynamisch konfiguriert mit info von anderen Routern.
- bei Topologieänderungen werden die Routingtabellen automatisch angepasst.
- höherer CPU Bedarf als bei statischem Routing
- höherer Bandbreitenbedarf als bei statischem Routing

9.7 Was sind die prinzipielle Aufgaben eines Routing-Protokolles (Aufzählung)? Welche Rolle spielt dabei die Metrik? Basieren die Metrik auf statischen oder dynamisch veränderbaren Parametern? Welche zwei prinzipiellen Fehlerfälle in einem Netzwerk werden von einem Routing-Protokoll behandelt (Aufzählung)?

- Analyse der momentanen Netzwerktopologie
- Bestimmung des besten / kürzesten Pfads zu jedem erreichbaren Netzwerk
- Speicherung des besten Pfads in Routingtabellen

Metrik-Information ist nötig, um den besten Pfad zu berechnen. Die Metrik basiert meistens auf statisch vorkonfigurierten Werten.

9.8 Was versteht man unter Konvergenz im Zusammenhang mit dynamischen Routing? In welchen Bereich ist die Konvergenzzeit im „worst case“ für RIP und OSPF angesiedelt (Minuten, Sekunden, Millisekunden)? Was kann passieren, wenn noch nicht alle Router konvergiert sind? Was ist ein Routing-Loop und warum ist dieser so unangenehm?

Konvergenzzeit ist jene Zeit die das Netzwerk braucht um sich nach einer Änderung der Netzwerkstruktur auf diese neu einzustellen. (durch z.B Ausfall eines Routers). Konvergenzzeit bei RIP mehrere Minuten, bei OSPF einige Sekunden. Sind noch nicht alle Router konvergiert so können Pakete im Kreis geschickt werden bis sie (durch TTL) verworfen werden. Routing Loops verursachen eine hohe Netzwerkauslastung ohne dass Daten das Ziel erreichen.

9.9 Charakterisieren Sie kurz die Distance Vector Methode. Wird alle Information einer empfangenen Routing-Message (Routing Update) von einem Router weitergegeben (Begründung)? Bewirkt diese Methode am Router eine limitierte Sichtweise (Begründung)? Zählen Sie drei bekannte Routing-Protokolle, die auf Distance Vector Technik basieren, auf.

Bei Distance Vector Protokollen wird die Routingtabelle periodisch an alle unmittelbaren Nachbarn weitergesandt (IP Limited Broadcast), nach dem Einschalten enthält diese nur die Informationen über die lokal angeschlossenen Netzwerke. Einkommende Updates werden auf Veränderungen überprüft, wie neue Netzwerke, Änderungen der Metrik bereits bekannter Netze, etc. Die eigene Routingtabelle wird daraufhin entsprechend abgeglichen. Diese Änderungen werden beim nächsten periodischen Update weitergegeben. Die Metrische Information basiert dabei auf Hops. Der Router hat nur eine eingeschränkte Sicht der Topologie.

9.10 Welches fundamentale Problem gibt es bei der Distance Vector Methode? Welche Maßnahmen wurden dagegen entwickelt (Aufzählung)?

Beschränkte Sicht der Router auf das Netzwerk, als Probleme ergeben sich Count to infinity, Routing Loops, lange Konvergenzzeiten.

Lösungsversuche:

- max. hop Count
- split horizon, poison reverse
- triggered update
- hold down, route poisoning

9.11 Charakterisieren Sie kurz die Link State Methode. Bewirkt diese Methode am Router eine limitierte Sichtweise (Begründung)? Wird alle Information eines empfangenen Routing-Updates von einem Router weitergegeben? Wie kommt das Flooding von Routing-Updates zum Stillstand? Zählen Sie drei bekannte Routing-Protokolle, die auf Link State Technik basieren, auf.

Bei Link State Protokollen haben die Router eine globale Sicht der Netzwerktopologie, also exakte Kenntnis über alle Router und Verbindungen sowie deren Kosten (Metrik) eines Netzwerks. Diese Informationen werden in einer TopologieDatenbank (?roadmap?) gespeichert, man spricht dabei auch vom StraßenkartenPrinzip (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 erkannt die für die Überwachung dieser Verbindungen zuständig sind und ins restliche Netzwerk verschickt.

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

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. Nachrichten von einem besseren (metrisch) Pfad werden als good news bezeichnet und von jeder Quelle angenommen und in der Routing tabelle verwendet. Bad News sind Meldungen über einen Pfad zu einem Netzwerk, der schlechter ist, als der, den man selbst derzeit kennt. Diese werden nur angenommen, falls sie vom nächsten hop router in dieses netzwerk kommen, sonst ignoriert.

9.13 Was ist das „Count-to-Infinity“ Problem bei RIP und wie kann es dazu kommen (kurze Beschreibung)?

Das hochzählen des Hopes eines Ziels bis ins unendliche. Ein Netz das direkt an einen Router angebunden ist fällt aus. Nach 180 sek altert der Eintrag des Routers aus und er weiß nicht mehr wie er das Netz erreicht und mit welcher Metrik. Nun erhält er aber ein Routing Update von einem benachbarten Router, dieser hat vom Ausfall noch nichts mitbekommen, kann also einen Pfad zum ausgefallenen Netzwerk vorweisen. Der Router empfängt also 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 ja 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 Unendlich.

9.14 Was bewirkt der Max-Hop-Count im Zusammenhang mit dem „Count-to-Infinity“Problem? Kann dadurch ein temporärer Routing-Loop verhindert werden? Welche Auswirkungen hat das auf die Topologie eines IP Netzwerkes?

Maximum Hop Count beschränkt die maximale Distanz zwischen zwei Subnetzen auf 16, der Hop Count zwischen zwei Endsystemen kann also 15 nicht überschreiten. Diese Methode reicht allerdings nicht aus um Schleifen zu verhindern. Alle Datagramme müssen innerhalb des Max Hop Count zugestellt werden.

9.15 Was ist „Split Horizon im Zusammenhang mit RIP? Was ist „Poison Reverse im Zusammenhang mit RIP? Kann durch diese Methoden ein temporärer Routing-Loop immer verhindert werden?

Split Horizon wurde entwickelt um die langsame Konvergenz und Routing Loops entgegenzuwirken, es hält Router davon ab Informationen über die Erreichbarkeit eines Netzwerks in die Richtung aus der die Information ursprünglich kam weiterzusenden. Eine Ausnahme von dieser Regel ist wenn der Router einen besseren Pfad kennt. Don't tell me what I have told you!

Poison Reverse ist eine alternative Methode gegen Routing Loops und langsame Konvergenz. Der Router sendet Unerreichbarkeitsnachrichten (?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. Loop kann nicht immer verhindert werden.

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

Der Router ignoriert Meldungen über Netzwerke für eine gewisse Zeit, wenn vorher ein Fehler in diesem Netzwerk über ein Update gemeldet wurde.

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

Das Grundprinzip ist gleich aber es gibt neue Techniken:

- Routing Domain und Route Tags
- Transmission of subnet masks
- Transmission of next hop redirect information
- Authentication

RipV2 ist:

- Classless Routing Protocol weil Subnetmask bekannt
- uses Multicast-Address instead of Broadcast Addresses.
- Authentication lässt nur updates von authentifizierten Routern zu.

9.18 Welche prinzipielle Eigenschaft eines Routing-Protokolles bewirkt Classful Routing? Kann VLSM Technik verwendet werden (Y/N)? Werden IP Subnetze an der Klassengrenze zusammengefasst, wenn diese in Updates in Richtung anderen IP Netze gemeldet werden (Y/N)? Wie läuft der „Routing Table Lookup ab (Aufzählung)? Können IP Netzwerke bezüglich Adressierung in diesem Zusammenhang „discontiguous sein (Begründung)?

Routing Protokolle wie RIP, IGRP können keine Subnetzinformationen in ihren Routing Updates übertragen. 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 Netzwerknnummer verschieden zu 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.

- IP Adresse wird der Klasse A, B oder C zugeordnet, das Hauptnetz wird bestimmt.
- Der Eintrag in der Routingtabelle für das Hauptnetz wird gesucht. Keiner vorhanden dann wird das Paket verworfen.
- Die IP Adresse wird mit jedem gespeichertem Subnetz verglichen, bei keiner Übereinstimmung wird das Paket verworfen.

9.19 Welche prinzipielle Eigenschaft eines Routing-Protokolles bewirkt Classless Routing? Kann VLSM Technik verwendet werden (Y/N)? Werden IP Subnetze an der Klassengrenze zusammengefasst, wenn diese in Updates in Richtung anderen IP Netze gemeldet werden (Y/N)? Wie läuft der Routing Table Lookup ab (Aufzählung)? Was ist die „Longest Match Routing Rule in diesem Zusammenhang?

Classless Routing Protokolle wie RIPv2, OSPF, eIGRP können Subnetzinformationen in Routing Updates übertragen. 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.

- IP Datagram mit IP Adresse wird vom Router empfangen.
- IP Adresse wird mit Einträgen in der Routingtabelle Bit für Bit von Links nach Rechts verglichen.
- IP Datagramm wird weitergeleitet an das Netzwerk das am besten passt.
- Longest Match Routing Rule

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

VLSM ist Variable Length Subnetting Mask.

Bezeichnet die Möglichkeit, unterschiedlich lange Subnetzmasken für die gleiche Netzwerknnummer in

verschiedenen Subnetzen angeben zu können. VLSM hilft damit, den verfügbaren Adressraum besser auszulasten, wird bei classless routing eingesetzt,

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

Mehrere Netzwerke werden nach außen zu einem zusammengefasst. Die Subnetmaske ist dann kleiner als die "natürliche" Subnetmaske dieser Klasse. Positiver Effekt: Die Routing-Tabellen werden kleiner. Statt aller einzelner Netze müssen die Router nur mehr das eine Supernet kennen, wird bei Classless Routing eingesetzt.

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

Um die Anzahl der Einträge in der Routingtabelle klein zu halten sollte die Adressierung der Netze allerdings 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.

9.23 Wozu dienen die privaten IP Adress-Bereiche? Zählen Sie diese kurz auf. Welche Rolle spielt NAT in diesem Zusammenhang? Was wird dabei bei statischen Mapping getan? Was erlaubt dynamisches Mapping?

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-Adress ins Internet verbinden will, so geht das erstmal 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.

9.24 Was sind die prinzipiellen Vorteile von OSPF im Gegensatz RIP (Aufzählung und kurze Begründung)?

OSPF bedeutet Open Shortest Path First

- Netzwerklast ist kleiner als bei Distance Vektor Protokollen, Es werden nur Hello-Messages übertragen anstatt die gesamte Routingtabelle.
- Selbst bei Netzwerkänderungen ist die Netzwerklast kleiner da nur die Änderungen übertragen werden.
- Jeder Router kennt die gesamte Topologie und berechnet daraus die kürzesten Wege, dies führt zu kurzen Konvergenzzeiten.
- Jeden Port sind Kosten zugeordnet. Verbindungen mit gleichen Kosten können die Netzwerklast teilen.
- OSPF Update Messages können verifiziert werden. (Security)

9.25 Wie kommt ein OSPF Router ausgehend von seiner „Topology Database“ zu seiner Routing-Tabelle? Welche Informationen dienen dabei zur Kennzeichnung der Wege (Links)? Womit könnte man das Verfahren des „Shorted Paths First“ in Anlehnung zum L2 STP bezeichnen (kurze Begründung)?

Ausgehend von der Topologie Database verwendet der Router Shortest Path First um den kürzesten Weg zu einem Netz zu finden. (Dijkstra Algorithmus). Werden in der Topologie Database als Pfade und Router als Knoten dargestellt. INFO

9.26 Wozu dient der Dijkstra Algorithmus bei OSPF? Wie funktioniert das Verfahren prinzipiell (kurze Schilderung)?

Dienst zur Ermittlung des kürzesten Weges zu einem Ziel.

- Bestimme des Roots
- Füge die unmittelbaren Nachbarn dazu
- wähle den Nachbarn X mit den geringsten Kosten aus
- füge die Nachbarn von X hinzu
- für diese Nachbarn berechne die Kosten mit X als Vorgänger

9.27 Wofür steht ein Link State bei OSPF? Wie kommt er zustande und wann wird ein Link-State auf UP gesetzt? Wie erfolgt die Überwachung eines Link-States? Wie ist das Standard-Timeout eines Link-States bei OSPF?

Das Erzeugen und Warten der Topologie Database wird Link State genannt und bedeutet eine logische Verbindung zwischen zwei Routern. Der Link State wird mittels Hello Messages überprüft.

- Hello Messages werden versandt
- Router antwortet mit Topologie Database Description
- Falls unbekannt Einträge für den anderen Router dabei sind schickt dieser eine Anfrage für die Details
- Router schickt die Details als eine LS Update Message
- selbes Spiel in die andere Richtung
- Der Aufbau der Verbindung wird über Router LSA Messages als Broadcast im gesamten Netz verteilt

Timeout ?? INFO

9.28 Schildern Sie kurz die Kommunikationsabläufe beim Kennenlernen zweier benachbarter OSPF Router bis zum Ereignis Link-State UP. Welches LSA wird am Ende dieses Prozesses generiert?

siehe oben

9.29 Wie werden Änderungen des Link-States in OSPF kommuniziert (Stichwort LSA)? Wer ist für das Aussenden eines LSA verantwortlich? Was bewirkt ein LSA bei anderen OSPF Routern? Wie lange bleibt ein LSA in einem Router gespeichert (Stichworte „Message Age and LSA Refresh“)? Wogegen zielt das LSA Refresh ab?

Bei einer Änderung des Netzes schicken die beiden betroffenen Router LSA ins Netz. Ein Eintreffen eines LSA bringt ein Update der Database und eine Neuberechnung der Shortest Path mit sich. LSA Updates altern nach 180 Sekunden aus wenn sie nicht refreshed werden. Wird in dieser Zeit kein Refresh gemacht wird angenommen dass dieser Link nicht mehr verwendet werden kann.

9.30 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? Hat ein LSA Refresh eine neue LSA Sequence-Number?

Ein betroffener Router sendet die LSA an seine direkten Nachbarn aus, diese antworten mit einer Empfangsbestätigung und leiten diese LSA wiederum weiter (ausser an den Ursprung). Anhand der Sequenznummer kann ein Router erkennen ob der die LSA schon erhalten hat und ob sie weiterleiten muss.

9.31 Welche OSPF Messages gibt es (Aufzählung)? Wie werden diese transportiert? Warum benötigt man ein LS-Acknowledgement? Wie erfolgt die L3 Adressierung von OSPF Messages prinzipiell und wie ist die L2 Adressierung auf LANs?

- Router LSA
- LSA refreshed
- Hello Message
- LS updates
- LS ack
- LS request
- DataBase description
- Network LSA

Die Übertragung läuft über IP, da die Zustellung nicht garantiert ist muss mit einem ACK bestätigt werden. Messages werden über Multicast transportiert, oder über Point to Point Verbindung.

9.32 Welches Problem tritt bei OSPF in einer Broadcast Umgebung (LANs) auf? Welche Funktion hat der Designated-Router in einer Broadcast Umgebung? Wozu dient der Backup-Router? Mit welchem LSA-Typ wird eine Broadcast Umgebung bekannt gegeben und wer gibt es bekannt? Hat das auf das Weiterleiten von IP Datagrammen einen Einfluss?

OSPF benutzt Point To Point Verbindungen, jeder Router müsste zu jedem Punkt einen Pfad berechnen. Das Basiskonzept von LinkState beruht auf pointtopoint Verbindungen. Dieses Konzept passt am besten für pointtopoint Netzwerke wie Serial Lines. Das verursacht jedoch ein Problem mit shared media

multiaccess networks, zum Beispiel in LANs. Hello, Database Description und LSA Updates zwischen all diesen Routern kann hohen NetzwerkTraffic und CPU Belastung verursachen. Wenn mehrere Router ein multiaccess Netzwerk teilen skaliert anytoany sehr schlecht ($N*(N-1)/2$ problem). Die Information über sämtliche möglichen Nachbarschaftsbeziehungen erscheint redundant, das Konzept des Virtual (network) Node (or 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 Designated Routers würde dies einen ?single point of failure? darstellen, daher wird ein zusätzlicher Backup Designated Router (BR) benutzt. Der Designated Router sendet network Lsa. Hat nur Einfluss darrauf, wie Routing-Informationen übertragen werden, NICHT auf das Routing an sich.

10 Chapter 11/ 12 Internet Transport Layer, Applications for Admin (Version 1.1)

10.1 Was sind die grundlegenden Eigenschaften von TCP (OSI Layer, Protokoll Service (CO / CL), 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. Datenverluste werden erkannt und automatisch behoben, Datenübertragung ist in beiden Richtungen möglich, Netzwerküberlastung wird verhindert (Flow Control: Ja). Nur auf IP Hosts präsent.

10.2 Welche Klassifizierung gemäß Kapitel „Protocol Principles“ kann man für TCP treffen? Welche Spielart des Error Recovery wird dabei realisiert (genaue Bezeichnung)? Welche Spielart der Flow Control wird dabei realisiert (genaue Bezeichnung)?

Full Duplex Protocol - Piggy Packed ACKs. Error Recovery: Sequence Numbers, Positive Acknowledgments. Flow Control durch Dynamic (Adaptive) Windowing.

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

TCP Ports dienen um verschiedene Services auf einem Server zur Verfügung zu stellen. 1 bis 1023 sind die „WellKnown“, Ports, also vordefinierte Ports, die für bestimmte Services reserviert sind (z.B. HTTP 80) und >1023 sind die registrierten Ports. Der Client ist derjenige der das Service, das durch den Server zur Verfügung gestellt wird, verwendet. Der Client stellt die Verbindung her, der Server wartet. INFO ?

10.4 Was sind „well-known“ TCP Port Nummern? Was kennzeichnen sie? Wie erfolgt die Handhabung der TCP Portnummer auf der Client Seite einer TCP Verbindung? Was sind „registered“ TCP Ports?

1-1023 sind well-known Ports. Die Server Applikationen lauschen auf ihren well-known Ports. Für diese Port ist je nur ein Protokoll definiert. Sie sind reguliert und werden von der IANA für einen bestimmten Dienst vergeben. Client Application wählt freien Port (zwischen 1024 und 65535). Registeres Ports beginnen bei 1024 und sind Protokollen zugeordnet, können aber auch von anderen verwendet werden. Sie sind nicht von der IANA registriert aber in einer RFC angeführt.

10.5 Was ist ein Socket prinzipiell? Wozu benötigt man Source-Socket und Destination-Socket?

Socket ist eine Kombination aus IP Adresse und Port. Mit einem Socket kann man einen bestimmten Port auf einem Host / Server ansprechen. Destination Socket ist normalerweise ein Well known Port auf einen Server und der Source Socket kennzeichnet die Applikation die den Verbindungsaufbau veranlasst hat. So können mehrere Applikationen das selbe Protokoll verwenden.

10.6 Wie erfolgt der TCP Verbindungsaufbau im Detail? Wie werden die Startnummern in der Praxis gewählt?

Mit dem Three-Way-Handshake. Also der 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 das SYN vom Server. Nach dieser Aktion ist die Verbindung aufgebaut und die Gesprächspartner sind synchronisiert. Startnummern werden zufällig gewählt.

10.7 Warum müssen beim TCP Verbindungsaufbau die Startwerte der Sequence Numbers synchronisiert werden? Warum wähle man diesen Ansatz? Warum ist der Bereich der Nummern so groß?

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

10.8 Wie erfolgt das Error Recovery ursprünglich (d.h. ohne Verwendung eines „Duplicate ACKs“) bei TCP (kurze Beschreibung was „Positiv Acknowledgement“ bedeutet)?

Paket geht verloren, Empfänger sendet also kein ACK, Sender wartet auf Timeout, Retransmission.

10.9 Welche Änderung des Error Recovery hat man beim aktuellen TCP vorgenommen (kurze Beschreibung unter Einbeziehung von „Duplicate ACKs“)? Warum hat man diese Änderung vorgenommen?

Paket geht verloren, Empfänger sendet Duplicate ACKs für das verlorene Paket, nach 3 Duplicate ACKs sofortige Retransmission. Warum: Weniger unnütze Wartezeit, bessere Ausnutzung der Bandbreite.

10.10 Wie erfolgt der TCP Verbindungsabbau im Detail? Warum spricht man vom Schließen von Half-Sessions?

Die Verbindung muss in beiden Richtungen getrennt werden (Half Sessions). Das Ende wird mit dem FIN-Flag gekennzeichnet und muss mit einem ACK von der Gegenseite bestätigt werden.

10.11 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? Geben Sie ein Beispiel der Handhabung/des Zusammenspiels dieser Nummern für zwei unmittelbar hintereinander folgenden TCP Segmente (Block 1 Länge 550 Byte, Block 2 Länge 340 Byte).

Die Sequenze Number kennzeichnet die Position der ersten Nutzdaten dieses TCP-Segments im Datenstrom. Die Acknowledgement Number kennzeichnet das Byte das als nächstes erwartet wird.

(Block 1): Seq = z.b 100

Ack = 650

(Block 2): Seq = 650

Ack = 990

10.12 Wieso benötigt man bei TCP ein Timeout? Wie wird das Timeout bei TCP ausgelegt? Warum macht man das so?

Über das Timeout wird erkannt falls ein Paket erneut übertragen werden muss (z.B ACK ging verloren). Die Timeout Zeit wird bei TCP adaptive ausgelegt um möglichst wenig Pakete erneut senden zu müssen.

10.13 Über welche Bereiche erstreckt sich die TCP Checksum? Welche Länge kann ein TCP Segment unter Verwendung des Basis-Headers maximal aufweisen? Welcher Fenstergröße würde dieser Wert entsprechen? Mit welcher TCP Option lässt sich dieser Wert beliebig vergrößern?

TCP Checksum erstreckt sich über TCP HEADER, TCP DATA und 12 Byte PSEUDO IP HEADER. Dieser enthält: Source+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. INFO

10.14 Wie wird die TCP Flow Control exakt realisiert (Stichwort: adaptive Windowing)? Beschreiben Sie kurz das Zusammenwirken von Window und Acknowledgement Number im TCP Header eines empfangenen TCP Segments und die daraus resultierende Auswirkungen auf das Sliding Window bezüglich rechter Kante des Fensters im Zahlenraum der Sequence Numbers)?

Der Sender darf nur so viele Bytes unbestätigt haben, wie der Empfänger ihm im Window Feld mitgeteilt hat. Trifft ein Ack für n Byte ein wird die rechte Kante um n Byte verschoben, es können neue Daten versendet werden.

10.15 Wozu dienen die TCP Flags PUSH und URG?

Das URG Flag dient dazu wichtige Daten zu kennzeichnen. Die Applikation wird informiert dass wichtige Daten kommen. Das PUSH Flag signalisiert dem System die Daten nicht zwischenzupuffern (wie sonst üblich) sondern die Daten sofort dem nächstem Layer weiter zu leiten. (Notwendig für schnelle Reaktionen)

10.16 Welches Problem hatte man mit TCP bevor der neue Mechanismus „Slow Start and Congestion Avoidance Algorithm“ eingeführt wurde? Welche Grundannahme gibt es beim TCP „Slow Start and Congestion Avoidance Algorithm“ bezüglich Verlust von TCP Segmenten?

Router haben einen Zwischenspeicher für Pakete. Kommt es zu einem Überlauf gehen Pakete verloren und diese werden erneut übertragen was den Überlauf noch mehr verstärkt. Der Slow Start and Congestion Avoidance Algorithmus ist dagegen eine Abhilfe. Grundidee: TCP Segmente gehen vor allem durch Überlastung verloren und nicht durch Bitfehler auf den Leitungen, da die Übertragung sehr robust ist (Optisch und Digital).

10.17 Was ist die Grundidee des „Slow Start and Congestion Avoidance Algorithm“? Welche Änderung in TCP Error Recovery musste man bezüglich Acknowledgement einführen?

Man versucht, sich an die maximale Kapazität des Netzes heranzutasten, Balance zwischen möglichst hohem Durchsatz und niedrigem Packet Loss. Duplicate Ack muss eingeführt werden um grosse und kleine Staus unterscheiden zu können.

10.18 Wie lässt sich beim TCP „Slow Start and Congestion Avoidance Algorithm“ leichter Stau (Congestion) von einem schweren Stau unterscheiden? Welche Auswirkungen hat das auf den Algorithmus?

Geht ein Paket verloren, die unmittelbar danach kommen aber durch, so schickt der Empfänger Duplicate ACKs -> leichter Stau. Gehen ab einem gewissen Punkt alle Pakete verloren, schickt der Empfänger auch keine Duplicate ACKs, der Sender merkt nur durch den Timeout, dass was schief gegangen ist -> schwerer Stau. Die Art wie der Neustart des Sendens abläuft hängt von dem Art des Staus ab.

10.19 Welche Performanceaspekte stellen sich durch den TCP „Slow Start and Congestion Avoidance Algorithm“ für zwei Rechner, die über eine TCP Verbindung kommunizieren, prinzipiell ein (Stichwort „Wave Effect“)? Welches grundsätzliche Größe limitiert die Performance im „worst case“, falls die vorhandene Bandbreite von den beiden Rechnern alleine verwendet wird?

Bzgl der Übertragungsrate: Ein Wave-Effect. Sie pendelt zwischen maximaler Übertragungskapazität und der Hälfte. Die Bandbreite und die Verarbeitungsgeschwindigkeit der Hosts begrenzt die Performanz.

10.20 Was ist die MSS? Wann und wie wird sie signalisiert? Was hängt davon beim TCP „Slow Start and Congestion Avoidance Algorithm“ ab?

MSS ist die Maximum Segment Size und wird in einem TCP Option Feld übergeben. Der Anstieg von cwnd im Falle eines linearen Anstiegs (Window Size > slow start threshold)

10.21 Was sind die grundlegenden Eigenschaften von UDP (OSI Layer, Connectionless oder Connectionorientated 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)?

UDP ist befindet sich im Layer 3 des OSI Modells. Es ist ein verbindungsloses Protokoll und verwendet die selben Ports wie TCP. Jedoch ist UDP bei weitem nicht so komplex wie TCP. Es ist keine Flow Control vorhanden.

10.22 In welchen drei charakteristischen Situationen wird UDP eingesetzt (Aufzählung und kurze Begründung)?

- Wenn der Overhead des Herstellens einer TCP Verbindung nicht erwünscht ist. zB für sehr kurze Anfragen wie DNS
- Wo die Implementation so klein wie möglich sein muss, TCP ist komplex, UDP einfach. zB in kleinen Routern
- Wo die Neuübertragung von verlorengegangenen Datenpakete nicht erforderlich ist. zB VoIP

10.23 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 L3 und L2 mäßig adressiert (ohne Einsatz eines BootP Relay Agents)?

Grundidee: BootP wurde entwickelt, um Computer über das Netzwerk booten zu können. Die Konfiguration notwendiger Parameter und das Laden des Betriebssystems soll über das Netzwerk erfolgen, Transportmechanismus ist UDP. Die Datenbank muss Einträge über die MAC-Adressen, IP-Adressen, Filenamen des Bootimages und die IP des Hosts mit dem Bootimage. Adressierung: IP Limited Broadcast (Source-Adresse 0.0.0.0, Dest 255.255.255.255)

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

Konfigurationsparameter in der Antwort (Transaction ID etc. sind keine Konfig.parameter):

- YOUR IP: IP Adresse für den Client.
- SERVER IP: IP Adresse vom Server, der das Boot-Image zur Verfügung stellt.
- SERVER HOST NAME: Hostname diese Servers.
- BOOTFILENAME: Beinhaltet den Pfad und Filenamen des Bootfiles
- ROUTER IP: IP Adresse vom BootP Relay Agent

Nach dem BootP Prozess lädt sich der Client ein Image von einem FTP Server.

10.25 Warum und wann benötigt man ein BootP Relay Agent? Was passiert in diesem Fall? Wie spiegelt sich das im BootP Basis Header wieder?

Broadcasts funktionieren nicht über Subnetzgrenzen (bzw Router) hinweg. Wenn der BootP-Server in einem anderen Subnetz steht als ein Client, braucht man einen Relay-Agent, um die BootP Broadcasts dorthin weiterzuleiten. Der Relay-Agent setzt ROUTER IP ADDRESS auf seine IP-Adresse und leitet das Paket an den BootP Server weiter. Der BootP Server antwortet an diese ROUTER IP ADDRESS.

10.26 Wofür steht die Bezeichnung DHCP? Was kann man damit alles bewerkstelligen? Was versteht man unter „Automatic“, „Dynamic“ und „Manual Address Allocation“?

DHCP ist Dynamic Host Configuration Protocol. DHCP erlaubt es einen Host von einem Server aus zu konfigurieren (IP Adress, DNS Server Adress, Gateway, Netmask)

Automatic: DHCP vergibt eine permanente Adresse

Dynamic: DHCP vergibt eine temporäre Adresse die nur eine bestimmte Zeit Gültigkeit hat. Erneuert der Host diese Adresse nicht so verfällt sie wieder.

Manual: IP Adresse sind händisch vom Administrator vergeben, der Host übernimmt allerdings andere Parameter vom DHCP Server.

10.27 Wodurch besteht ein Zusammenhang zwischen DHCP und BootP? Schildern Sie kurz unter Verwendung der DHCP Message Typen die Abfolge des Protokolls, wie ein DHCP Client zu einer dynamischen IP Adresse kommt?

DHCP ist eine Erweiterung von BootP. DHCP verwendet das "VENDOR SPECIFIC AREA" Feld von BootP für weitere Konfigurationsparameter.

- DHCP Discover
- DHCP Offer (from Server)
- DHCP Requests
- DHCP PACK (from Server)

10.28 Woran erkennt ein DHCP Client, wie lange er eine dynamische Adresse verwenden kann? Was passiert, um die Adresse zu erneuern (kurze Beschreibung der Abläufe unter Berücksichtigung der Timern T1, T2)?

Beim DHCP Offer ist ein Length of Lease eingetragen, darin steht die Zeit die der Client die Adresse verwenden darf. Nach $0,5 * \text{Leasetime}$ (T1) versucht der Client mit einem DHCP Request (Unicast) die Zeit zu verlängern. Verweigert der Server versucht der Client nach $0,875 * \text{Leasetime}$ (T2) eine neue IP Adresse von irgendeinem DHCP Server zu bekommen. Konnte der Client den Lease nicht verlängern, so sendet der DHCP Server ein DHCPNACK an dem Client die in veranlasst die IP Adresse wieder freizugeben.

10.29 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 TFTP Protokoll ist ein simples Protokoll zum Austausch von Daten und wird eingesetzt wo zu wenig Speicher vorhanden ist um FTP zu ermöglichen. (Router, SNMP zum Firmwareupdate) TFTP erlaubt einfachstes Versenden von Daten, aber hat keine Möglichkeit zum Auslesen von Verzeichnissen, oder Authentication. IdleRQ, UDP, Connection Oriented, Sequence Numbers.

10.30 Was macht DNS prinzipiell? Warum benötigt man symbolische Namen? Wie ist der Aufbau des DNS Directories (Verzeichnis, „Telefonbuch“) gelöst? Wie wird das DNS Directory realisiert?

DNS ist das Domain Name Service. Es löst alphanumerische Namen in IP Adressen auf. Symbolische Namen werden verwendet, weil es leichter ist, sich diese zu merken. Die DNS Server Datenbank ist nach einer Baumstruktur aufgebaut. Der Baum spiegelt nicht die tatsächliche Netzwerkstruktur wieder. Das DNS Directory ist eine weltweit verstreute Datenbank um die grosse Menge an Einträgen bewältigen zu können.

10.31 Warum ist der gesamte DNS Namensbaum auf viele DNS Server aufgeteilt? Wie erfolgt die Aufteilung und wie ist die Beziehung der DNS Server untereinander gelöst? Warum benötigt man trotz der offensichtlichen Verkettung der DNS Server zusätzlich noch die Root Hints?

10.32 Was versteht man unter einer Domain? Was versteht man unter einem Domain Name? Wie wird ein Domain Name an einer bestimmten Stelle (Knoten) des DNS Trees gebildet? Was ist ein FQDN?

Ein Domain Name der symbolische Name einer bestimmten Node. Der Domain Name wird gebildet indem man von der Wurzel (.) ausgeht und alle Folgenden Labels mit „.,,verknüpft. FQDN ist Fully Qualified Domain Name.

10.33 Wie ist der Transportmechanismus für DNS Messages? Welche Portnummer wird verwendet? Über welches Protokollmerkmal im DNS Header sind DNS Requests und DNS Replys korrelierbar?

DNS-Anfragen werden auf Port 53 verschickt. TCP wird bei Zone Transfers und UDP für Standartanfragen benutzt. Im Header ist eine 16 Bit Identifikationsnummer (wird vom Client vergeben) die auch der Antwort hinzugefügt wird.

10.34 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 Autoritativ. Außerdem: Welche Bereiche einer Domain wohin delegiert wurden.

10.35 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. Authorative: Nein. DNS-Caches findet man auf Clients UND auf Servern.

10.36 Welche Parameter lassen sich prinzipiell über DNS erfragen (Aufzählung von mindestens vier Ressource Records plus ihrer Bedeutung)? Was ist ein reverse/inverse DNS Lookup?

- 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. zB: PTR für 43.34.0.192.in-addr.arpa gibt 192.0.34.43.
- CNAME: autorisierter Name für einen Alias.
- SOA: Autoritätsursprung

Mit der In-Addr.Arpa Domain kann man Reverse Lookups machen, also zu einer gegebenen IP-Adresse den dazugehörigen Hostname finden.

10.37 Wozu benötigt man „primary und „secondary master“ Name Server und was ist der wesentliche Unterschied? Können beide gleich gute Antworten liefern? Wie kommunizieren sie untereinander (TCP oder UDP) und was ist ein Zone Transfer?

Der Primary hat das Original der Zone File, hier kann der Admin es ggf. ändern. Der Secondary holt sich das Zone File per TCP, was dann Zone Transfer genannt wird. Der Secondary DNS Server ist zur Redundanz und zum Load Balancing vorgesehen.

10.38 Was versteht man unter rekursiven bzw. iterativer DNS Abfrage? Wozu dient die In-Addr.Arpa Domain? Was kann man damit machen?

Rekursiv: Ich frage einen DNS nach einem Domain Name, dieser kümmert sich um alles (der Job wird delegiert; er fragt zB andere DNS Server) und gibt mir die IP-Adresse (oder was auch immer ich haben will). Iterativ: Ich frage einen DNS nach einem Domain Name, und wenn dieser nicht zuständig ist, sagt er mir nur eine Liste von Nameservern, die ich seiner statt fragen soll. Die Root Server antworten nur iterativ.

10.39 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.". Der gibt eine Liste von zuständigen Nameservern für "at.," zurück.
- 2 Frage einen dieser NameS nach "a.www.orf.at.,". Der gibt eine Liste von zuständigen Nameservern für "orf.at.," zurück.
- 3 Frage einen dieser NameS nach "a.www.orf.at.,". Der gibt eine Liste von zuständigen Nameservern für "www.orf.at." zurück.
- 4 Frage einen dieser NameS nach „a.www.orf.at.“. Der sagt mir, dass es diesen Domain Name nicht gibt ;)