

1) Was versteht man unter paralleler und serieller Übertragungstechnik? Wo wird die jeweilige Technik eingesetzt? Erklären Sie den Begriff Bitsynchronisation bei serieller Übertragungstechnik. Beschreiben Sie das Grundprinzip der asynchronen und synchronen bitseriellen Übertragungstechnik im Detail. [80 Punkte]

Information wird in der Datenwelt in Form von „0“ und „1“ verarbeitet. Das ist die kleinste mögliche Information, ein „Bit“ oder „Binary Digit“. Wie ein Bit realisiert wird, hängt von der physikalischen Verarbeitung des verwendeten Systems ab (z.B. Elektrische Übertragung: Strom ein/aus, Spannungspegel High/Low, Optische Leitung Licht ein/aus, Quantenzustände Spin links/rechts (Quantencomputer), ...)

In der parallelen Übertragung werden mehrere Bits (z.B. 8 oder 16 Bit) gleichzeitig auf mehreren Leitungen übertragen. Wenn man die dazu nötigen Adressleitungen, Datenleitungen und Steuerleitungen zusammenfasst, spricht man von einem Bus. Für die parallele Übertragung benötigt man n-Datenleitungen + Steuerleitungen um n-Bit gleichzeitig zu übertragen. Dabei werden ein oder mehrere Datenworte (8,16, 32, 64bit) zur selben Zeit übertragen. Sie wird bei schneller Datenübertragung auf kurzer Distanz verwendet. Z.B. Druckerkabel (früher), Bus im PC (für möglichst schnellen Speicherzugriff).

Bei der seriellen Datenübertragung werden die Datenwörter Bit für Bit auf einer physikalischen Leitung übertragen. Die Bits werden nacheinander auf die Leitung gelegt und müssen dementsprechend beim Empfänger richtig abgetastet werden. Der Vorteil liegt darin, dass man nur 2 Leitungen benötigt (Signal und Referenz). Diese Methode der Datenübertragung wird für die Kommunikation über größere Distanzen und in großen Netzwerken verwendet, also überall dort, wo parallele Übertragung auf Grund des Mehraufwands an Leitungen zu teuer wäre und die mögliche höhere Geschwindigkeit nicht zwingend nötig ist. Um die Daten am Empfänger zum richtigen Zeitpunkt abtasten zu können muss eine Clock Leitung zusätzlich so wie bei der parallelen Übertragung mitgeführt werden, die am Sender und Empfänger den selben Takt generiert. Dies ist deshalb nötig, da die Bits hintereinander in einem bestimmten Zeitintervall übertragen werden und somit Sender und Empfänger die gleichen Zeitintervalle zum senden bzw. wiedergewinnen der Daten verwenden müssen, da sonst zum Beispiel während einer Flanke abgetastet wird. Diese zusätzlichen Kosten sind bei Weitverkehrsnetzen (WAN) nicht akzeptabel.

Um aus Kostengründen die Clock Leitung einsparen zu können wir Bitsynchronisation (Synchronisation des Takts) betrieben. Der Empfänger betrachtet dabei die Signaländerung auf der Datenleitung und versucht daraus einen passenden Takt zu regenerieren (clock recovery). Mit diesem Signal wird dann abgetastet. Dabei ist wichtig, dass in der Mitte der Bitzelle abgetastet wird (Signal wird auf Grund des Leitungswiderstandes schwächer (Attenuation), Noise (Rauschen), Distortion: Signal wird gestreckt, verzerrt).

Bei der asynchronen Übertragung wird nur für ein Datenwort (8,16 Bit) Bitsynchronisation betrieben. Jedes Datenwort wird dabei unabhängig von den anderen gesendet. Hierbei wird die Technik des Start und Stopbits verwendet. (Wenn keine Daten übertragen werden ist die Leitung immer auf logisch 1(idle) NRZ-CODE). Jedes Datenwort beginnt mit dem Startbit (Wechsel 1- 0) und endet mit dem Stopbit (ein oder zwei Bit 1). Mit der negativen Flanke auf das Startbit wird die Übertragung eingeleitet und der Empfänger für ein Datenwort (8 Bit) synchronisiert. Das Stopbit ist nötig, damit das nächste Startbit sicher erkannt wird. Sender und Empfänger verwenden also jeder seinen eigenen Takt, die jedoch mit annähernd gleicher Frequenz arbeiten. Synchronität herrscht also nur während der Übertragung. Die Zeit zwischen zwei Datenwörter ist variabel. Nachteil: zu jedem Datenwort 8 Bit muss man 3 Bit für Synchronisierung mitübertragen.

(Bilder.: Seite 01-7)

Synchrone Übertragung wird verwendet um gleich ganze Datenblöcke zu versenden, das heißt Synchronität besteht zumindest so lange als Daten übertragen werden. Aus dem übertragenen Signal kann auf Grund der Flankenwechsel im Signal auf das Clock Signal rückgeschlossen werden. Hierfür sind jedoch häufige Signalfanken nötig, da ansonsten die Synchronität verloren geht. In Zeiten wo sich das Signal nicht ändert wird mittels PLL (Phase Locked Loop) (Bild Seite 01- 9) die Frequenz gehalten. Vorteil: Es werden nur zu Beginn des Datenblocks und nicht während des Übertragungsvorganges Synchronisationsbits benötigt. Das erlaubt kontinuierlichen Datenfluss. Es werden dabei sowohl die Frequenz als auch die Phase synchronisiert. Problem: Bei Datenwörtern mit vielen 1ern oder 0ern hintereinander ist die Clock Gewinnung bei einfachen Codes wie dem NRZ unmöglich.

Zwei Methoden um das Problem zu lösen:

- Kodierung so, dass jedes Bit einen Signalwechsel beinhaltet (Manchester, Differential Manchester, FSK; verwendet in LANs)
- Kodierung so, dass genügend Signalwechsel vorhanden sind: NRZI (mit Bitstuffing: bei vielen Einsen wird eine 0 eingefügt, die am Empfänger wieder ausgefiltert wird), RZ, AMI (Srcambler: verhindert zu viele 0en)
HDB3: mittels Codeverletzungen werden Signalwechsel erzeugt (verwendet in WANs)

2) Geben sie die Codierung für den Manchester und HDB3 Code an. Vergleichen sie die Eigenschaften dieser Codes bezüglich Bandbreite, Gleichanteil mit dem NRZ Code. In welchen Netzwerken werden diese verwendet (LAN oder WAN)? (70 Punkte)

Beim Manchestercode wird jedes übertragene Bit in 2 Teile aufgespalten , wobei der 1. Teil immer das Komplement vom Datenbit ist. Der 2. Teil ist gleich dem übertragenen Bit. Der Vorteil für die Clock Gewinnung ist, dass in jedem Bit ein Signalwechsel auftritt. Dieser tritt jeweils in der Mitte des Bit auf: Wechsel 1-0: log. 0; Wechsel 0-1: log. 1; Im Gegensatz zum NRZ-Code (Non return to Zero) benötigt der Manchestercode die doppelte Bandbreite. Der Vorteil liegt darin, dass der Manchestercode keinen oder einen konstanten Gleichanteil besitzt, was beim NRZ-Code, wo pos. Spg. für log. 1 und keine Spg für 0 steht, allgemein nicht der Fall ist. Der Manchestercode wird im LAN verwendet. (Bild: Seite 01-12)

Der HDB3 –Code (High Density Bipolar 3) hat 3 Zustände L, 0, H. Jeder 1er wird dargestellt als Puls mit alternierender Polarität abhängig vom letzten 1er Bit. Eine 0 verursacht keinen Signalwechsel.

Der HDB3 Code verwendet Codeviolations (Codeverletzungen) um die für die Synchronisation nötigen Flanken zu erzwingen: Es dürfen max 3 mal 0en hintereinander gesendet werden um die Synchronisation nicht zu beeinträchtigen. Kommen 4 mal 0en hintereinander wird nach der 3ten 0 eine Sicherheitsflanke V mit dem gleichen Vorzeichen wie das letzte 1er Bit eingefügt. Somit kann der Empfänger die Sicherheitsflanke erkennen. Damit würde aber der Gleichanteil ansteigen. Darum gibt es ein A-Bit das die Polarität wieder ausgleicht. Im Vergleich zum NRZ-CODE hat der HDB3-Code keinen Gleichanteil jedoch gleiche Bandbreite und wird deshalb im WAN verwendet.

Polarität des letzten Pulses:	Anzahl der Pulse seit der letzten Codeverletzung	
	Ungerade	Gerade
Plus	000 +V	-A 00 -V
Minus	000 -V	+A 00 +V

Diese Codierung gewährleistet die nötige Anzahl an Flanken und dass kein Gleichanteilauftritt.

Bild Seite 01 –14

Der HDB3-Code (High Density Bipolar 3 – Code) stellt logisch 1 als Pulsfolge mit alternierender Polarität dar. Logisch 0 erzeugt keine Pulsfolge. Wichtig bei diesem Code sind aber die „Ausnahmen“, die Violations: Um regelmäßig einen Pegelwechsel zu erzeugen wird jede vierte 0 durch einen Puls mit gleicher Polarität des letzten 1-Pulses dargestellt. Dieses sog. „V-Bit“ wird vom Empfänger in der Datengewinnung ignoriert und nur zur Bitsynchronisation verwendet, da das nächste gültige 1-Bit eine umgekehrte Polarität als das letzte gültige 1-Bit haben muss.

Um einen DC-Level bei einer langen Folge von Nullen (wobei ja bei jeder vierten ein Impuls gleicher Polarität erzeugt wird) zu verhindern, gibt es noch so genannte „A-Bits“: Nach jedem gesendeten 1-Bit (oder einer Reihe von 1-Bits) wird überprüft, ob die Summe der Pegel (inklusive V-Bit der letzten Violation) seit der letzten Violation Null ergibt (gleiche Anzahl von + und – Pegeln). Ist dies nicht der Fall (DC-Anteil!) wird ein A-Bit in umgekehrter Polarität des direkten Vorgängers gesetzt. Nach zwei Nullen wird (statt der vierten 0) das V-Bit in gleicher Polarität wie das A-Bit gesetzt. Man erhält nun entweder die Reihenfolge +A 0 0 +V oder –A 0 0 –V. Tritt am Empfänger dieses Pegelmuster auf, wird es ignoriert, und nur der zu erwartende Pegel des nächsten 1-Bit wird umgedreht. Das A-Bit wird natürlich (genauso wie das V-Bit) nur dann gesetzt, wenn mehr als vier Nullen hintereinander im Bitstrom auftreten.

Dadurch, dass die Bitmuster direkt in Pegeländerungen umgesetzt werden, benötigt der HDB3-Code die gleiche Bandbreite wie der NRZ-Code. Auch ist durch diesen Code kein oder konstanter Gleichanteil vorhanden. Der HDB3-Code wird in WANs verwendet (da Bandbreite gespart wird).

Bei seinen Fragen fehlt die 3.;

4) Wozu dienen Übertragungsrahmen (Framing)? Wie schaut der prinzipielle Aufbau eines Übertragungsrahmens aus. Gehen Sie kurz auf die Bedeutung der einzelnen Felder ein. Was versteht man unter Rahmensynchronisation (Framesynchronization)? Wie erfolgt Rahmensicherung (Frame Checking) und Fehlererkennung (Error Detection) prinzipiell bei serieller Übertragungstechnik?[80 Punkte]

Grundsätzlich wird bei der synchronen Datenübertragung, zwischen zwei Systemen, Information in Form von Datenblöcken begrenzter Länge, so genannten Frames ausgetauscht. Diese Aufteilung in Datenblöcke ist nötig, damit die Übertragungsstrecke von mehreren Teilnehmern benutzt werden kann und nicht durch die Datenübertragung eines einzelnen blockiert wird (TDM), oder auch um die Flexibilität eines großen Netzwerkes wie dem Internet gewährleisten können, wo die einzelnen Datenblöcke nicht notwendigerweise auf dem selben Pfad zum Ziel gelangen.

Dabei ist es nötig den Beginn und das Ende eines solchen Blocks erkennen zu können (Frame Synchronisation).

Treten bei der Übertragung Fehler auf der Leitung auf (Crosstalk, Noise,...) so kann es passieren dass Signale nicht mehr richtig erkannt werden können, deshalb benötigt man Methoden zur Fehlererkennung (Frame protection/checking, error detection).

Prinzipieller Aufbau eines Frames:

Sync	SD	Control	Data	FCS	ED
------	----	---------	------	-----	----

SYNC: (Sync Pattern) wird verwendet um nach einer langen Ruhephase(idle) den Empfänger wieder auf die richtige Taktfrequenz zu bringen. Typische Bitkombination 01010101..... bei Ethernetframes 8 Byte.

Kann aber auch dazu benutzt werden, um den Empfänger während einer IDLE Phase auf dem richtigen Takt zu halten.

SD:(Starting Delimiter)

ED:(Ending Delimiter) Das sind Bitkombinationen die den Anfang und das Ende eines Blocks anzeigen. Das Problem ist, dass diese Bitkombinationen nicht im Datenblock drinnen vorkommen dürfen, weil z.B. ein Frame zu früh geschlossen werden würde. Um diese vermeiden zu können verwendet man Daten- Transparenz (siehe Frage 5).

Es besteht auch die Möglichkeit, dass es keine Verfahren gibt, um auch diese Bitmuster innerhalb des Frames zu erlauben, dann muss die verwendende Applikation sich darum kümmern.

CONTROL: Das Control Feld enthält Infos für Protokollprozeduren. Darunter auch :

Frame Type: (Data, Ack, Nack, Connect, Disconnect, Reset)

Protocol Type:(IP, IPX, Apple Talk)

Adressinfo: Adressen von Quelle und Empfänger im Fall einer Mehrpunktleitung,

Frame length,

Sequence number: Identifiziert jedes Frame notwendig für Fehlerbehebung (error recovery) und flow control bei connection oriented services. etc.

DATA: Die zu übertragenden Daten werden in diesem Block zusammengefasst.

FCS:(Frame Check Sequenz) In der FCS, auch genannt Checksum, steht eine Check-Sequenz, die durch eine vorgegebene Regel errechnet wird (CRC, Parität,...). Nach dem Senden des Frames ermittelt der Empfänger aus dem Datenblock seine eigene Checksum. Diese vergleicht er mit dem Wert in der FCS. Somit kann festgestellt werden ob der Frame fehlerhaft ist oder nicht (error detection). Es gibt verschiedene Verfahren zur Erstellung der Checksum. Ein sehr gutes Verfahren heißt CRC (Cyclic Redundancy Check). Durch das FCS wird Control und Data geschützt.

Frame Synchronisation: Es ist wichtig zu wissen, wo ein Rahmen beginnt und aufhört. Hierfür dienen SD und ED, diese sind also für die Frame Synchronisation zuständig und dürfen natürlich im Frame nicht vorkommen, was durch Bit oder Bytestuffing realisiert wird (einfügen zusätzlicher Bits oder Bytes(Zeichen)).

Rahmensicherung: Bits können auf der Übertragungsstrecke durch äußere Einflüsse (Noise, Crosstalk) fehlerhaft werden und nicht mehr eindeutig als Null oder Eins erkannt werden. Deshalb ist es notwendig solche Fehler zu erkennen und wenn möglich zu korrigieren. Zwei Möglichkeiten:

- **Forward Error Control:** packe so viel redundante Information in jeden Block, dass der Empfänger Fehler erkennen und beheben kann (Hamming Code, Reed-Solomon Code)

Nötig unter extremen Bedingungen: hohe BER – Bit Error Rate, EMR, große Verzögerungen

- **Feedback Error Control:** packe so viel redundante Info in jeden Block, dass Fehler erkannt werden können, der Block wird dann noch mal gesendet -> FCS (frame protection)

Die FCS Methode entscheidet darüber, welche Fehler zu 100% erkannt werden können, und wie groß der Prozentsatz der nicht erkannten Fehler ist;

Jedoch ist ein zu aufwendiges Verfahren zeit und auch bandbreitenraubend.

5) Was versteht man unter Datentransparenz und wie wird diese erreicht? Erklären Sie das an Hand der bitorientierten (bitoriented) und an Hand der zeichenorientierten Methode. [80 Punkte]

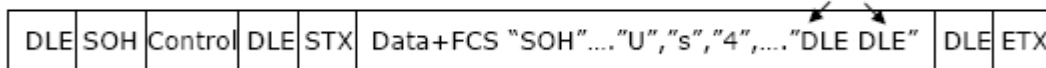
Bei der Übertragung eines Datenblocks(Frames) ist es wichtig, dass bestimmte Bitkombinationen z.B. für Frame Synchronisation SD, ED nicht im Frame auftreten dürfen. Unter Daten- Transparenz versteht man die Methoden, die angewendet werden, um diese Bitkombinationen zu verhindern. Methoden sind bit stuffing, Byte stuffing, Code violation, Byte Count technique, idle line before SD and ED (ethernet). Muss die Applikation selbst darauf achten, dass diese Bitkombinationen nicht vorkommen, dann nennt man das eine nicht Daten Transparente Methode.

Byte-stuffing:

Bild Seite 01-20

Byte stuffing ist ein zeichenbasiertes Verfahren, das heißt bestimmte Control-Sequenzen treten in Form von Zeichen also byte-weise auf (Bsp.: PPP). Hiefür wird der ASCII Code verwendet, in dem Bitmustern bestimmte Zeichen oder Controlzeichen zugeordnet sind. Wenn im Datenblock auch Steuerzeichen vorkommen, dann wird es problematisch, weil sonst wiederum ein Frame zu früh geschlossen werden kann und andere Probleme auch auftreten können. Man benutzt deshalb das Steuerzeichen DLE (Data Link Escape ASCII 0x10). Mit diesem Steuerzeichen werden alle anderen Steuerzeichen, die für die Übertragung relevant sind, eingeleitet. Beispiel: DLE STX bedeutet Start of Text während nur STX einfach ein (Steuer)-zeichen im Text ist. Soll das Zeichen DLE auch im Text vorkommen, so muss es verdoppelt werden. Somit erkennt der Empfänger, dass es sich um ein Textzeichen handelt und nicht um den Beginn eines Steuerzeichens.

Empfänger macht 1 mal DLE im Text



Verwendete Steuerzeichen: SOH (Start of Header), STX (Start of Text), ETX (End of Text)

Bit stuffing:

Hierbei wird SD und ED = 01111110 genannt flag gesetzt, diese werden auch zur Synchronisation im SYNC verwendet. Jede andere Bitkombination wird als Beginn des Frames interpretiert. Diese Bitkombination mit 6 mal 1er darf im Datenblock nicht vorkommen, da sie das Ende des Frames bedeuten würde. Deshalb fügt der Sender hinter jedem 5ten 1er einen 0er ein. Der Empfänger erkennt die 5 mal 1er und löscht den 0er wieder raus. Somit kann die Kombination 6 mal 1er nur beim Anfang und beim Ende des Frames kommen.

6. Welche physikalischen Aspekte treten bei der Übertragung von elektrischen Signalen auf? Erklären sie diese kurz. Was bedeuten diese Aspekte für die Bitsynchronisation und für die maximal erreichbare Bitrate?[80 Punkte]

Auf einem realen Übertragungssystem wird das Signal auf der Leitung teilweise abgeschwächt, verzögert und mit Rauschen überlagert.

Durch die Fourieranalyse lässt sich jedes periodische Signal[z.B. Rechteck Datenübertragung] mit Periode T durch (unendliche im Falle vom Rechteck) Summen von Sinus und Kosinus Schwingung + ev. Gleichanteil darstellen. Jede dieser Schwingungen besitzt ein Vielfaches der Grundfrequenz $f = 1/T$ und eine bestimmte durch die Analyse vorgegebene Frequenz. Jedes Signal lässt sich also durch eine sog. Fourier Reihe darstellen.

Kein Übertragungssystem kann Signale übertragen, ohne Leistung zu verlieren (Verluste auf der Leitung auf Grund Leitungswiderstand - attenuation).

Jedoch wird die Amplitude abhängig von den Frequenzen der harmonischen Schwingungen und abhängig vom jeweiligen Übertragungsmedium unterschiedlich geschwächt, wodurch die Rekonstruktion des ursprüngliche Signals noch schwieriger wird (ansonsten bloß feinere Verstärker).

Im Normalfall werden alle Schwingungen mit den Frequenzen von 0 bis zu einer bestimmten Frequenz f_c fast ungedämpft übertragen, während alle anderen Schwingungen ab einer bestimmten Frequenz f_c stark geschwächt werden. Dies hängt hauptsächlich von der physikalischen Beschaffenheit und Eigenschaft des Übertragungsmediums und von den Filtereigenschaften der Sender- Empfängerschaltung ab. Diese Frequenz ist ein Synonym für die verfügbare Bandbreite auf einem bestimmten Medium.

Ein wesentlicher Punkt ist auch die zeitliche Verzögerung des Signals. Schwingungen mit höherer Frequenz und welche mit niedriger Frequenz können von Übertragungssystemen nicht gleichschnell übertragen werden (delay distortion). Demnach könnte es zu einer Überlagerung zwischen dem schnellsten Teil des zu übertragenden Bits und dem langsamsten Teil seines Vorgängers kommen, was zu ungültige Werte führen kann.

Ein zusätzlicher Aspekt ist das ungewollte Rauschen (noise) auf der Übertragungsleitung. Rauschen entsteht durch unkontrollierte Spannungen, die durch irgendwelche Felder, auf die Leitung induziert werden. Zusätzlich kann Rauschen durch Kopplung von der Versorgung des Senders und Empfängers herrühren. Außerdem tritt auch das Übersprechen (Crosstalk) von einer Leitung auf die andere auf. (siehe Bild 01-27)

Wegen diesen ganzen Einflüssen wird die Bitsynchronisation sogar in der Mitte eines Bits schwierig, bei steigenden Bitraten. Ab einer gewissen Bitrate wird es sogar unmöglich. Die maximale Bitrate hängt grundsätzlich von der Bandbreite und von der Leitungslänge ab. Diese maximale Bit Rate kann durch das Nyquist Kriterium berechnet werden: $R = 2 * B \ln V$. (siehe Frage 6).

7. Was besagt die Theoreme von Nyquist und Shannon? Erläutern Sie diese kurz. Was versteht man unter „Baseband“, „Narrowband“ und „Broadband“ Übertragung im Zusammenhang mit Datenkommunikation? [80 Punkte]

Das **Nyquist Theoreme** gibt Auskunft über die maximale Bitrate die auf einer ideale(rauschfreie) Leitung mit möglich ist.

$$R = 2 * B * \log_2(V)$$

R= maximale Bitrate (Bits/sec)

B= Bandbreite (begrenzt den Bereich der Übertragung): der Bereich in dem das Signal nur wenig gedämpft wird.

V= Anzahl der Zustandslevel, welche das Signal annehmen kann.(z.B. Binär 0,1 zwei Zustände; QAM 16 Zustände)

Beispiel für Anwendung: Telefon: B=3000 Hz, R=6000 Bits/sec für V=2, R=18000 Bits/sec für V=8

Das **Shannon Theoreme** gilt für eine rauschbehaftete (noisy) Leitung (Rauschen verursacht durch crosstalk, Impulse, thermisch/weises Rauschen)

$$\max R = B * \log_2(1 + S/N)$$

S= Signalleistung

N= Rauschleistung(Noise)

SNR = 10 log S/N ... Signal gegen Rauschen Rate (gemessen in dB)

Beispiel Telephon Leitung: B = 3000Hz; SNR = 30 dB -> S/N = 1000

maxR = 30 kBit/s

Baseband: Die gesamte Bandbreite(gesamter Frequenzbereich) einer Leitung wird dazu verwendet, um einen einzigen Datenstrom zur gleichen Zeit zu übertragen. Die Signale werden als Rechteckimpulse übertragen. Die Grenze der Bitrate ist bestimmt durch die physikalischen Eigenschaften des Übertragungsmediums, Leistung des Senders und Sensibilität des Empfängers, S/N Rate und ergibt sich durch die Nyquist/Shannon Theoreme. Die Kodierung muss derart gehandhabt werden, dass Bitsynchronisation gesichert ist (um die einzelnen Bits richtig abzutasten) und dass ein Gleichanteil vermieden wird.

Narrowband (Schmalband): Die Bandbreite ist begrenzt, deshalb könne Rechteckimpulse($f=0$ bis ∞) nicht direkt übertragen werden, sondern müssen geeignet moduliert werden. Die Umwandlung von Rechteckimpulse in ein passendes Signal wird durch Modulation ermöglicht(z.B. Modem zur Datenübertragung über B=3000Hz Telefonnetzwerk)

Folgende Technologien zur Modulation gibt es:

Amplitudenmodulation (amplitude shift keying ASK): dabei wird ein Sinusförmiges Signal übertragen für log. 1 oder es wird nichts übertragen für log. 0 (oder auch Sinus mit anderer Amplitude).

Frequenzmodulation (FSK): hierbei dienen Sinusschwg. mit unterschiedl. Frequenz um den logischen Zustand darzustellen.

Phasenmodulation (PSK): Hierbei treten Phasensprünge in der Schwingung auf, die log. 0 oder 1 signalisieren.

Eine Kombination aus den Technologien ist die Quadraturamplitudenmodulation (QAM) (4 Bit werden in einem Schritt zur gleichen Zeit übertragen -> 9600 Bit/s max bei 2400 Baud).

Broadband (Breitband): Die verfügbare Bandbreite einer seriellen Leitung wird aufgeteilt auf mehrere Teile mit kleiner Bandbreite. Mit Hilfe von speziellen Modulationstechniken, die speziell auf die verschiedenen Bandbreiten abgestimmt sind kann auf einer Leitung mehrere verschiedene Bits unabhängig voneinander übertragen werden. In verschiedenen Frequenzbereichen existieren also mehrerer Übertragungskanäle, wobei der jeweilige Datenstrom eines Kanals mit der entsprechenden Frequenz moduliert wird (Bsp.: Kabel Fernseh).

In digitalen Systemen ist damit oft auch nur high Speed Übertragung gemeint, aber es wird nichts moduliert.

Unterschied Bitrate - Baudrate:

Baudrate: gibt an wie oft sich ein Signal ändert.

Bitrate: gibt an wie viele Bits transportiert werden.

Diese müssen nicht notwendigerweise übereinstimmen z.B. QAM. Stimmen also nicht überein, wenn mit einem Signalwechsel mehrere Bit übertragen werden.

Für die nächsten vier Fragen: Erklären sie das Grundprinzip von ARQ:

Bei der Übertragung von Daten über eine Punkt zu Punkt Leitung kommen sog. Leitungsprotokolle zum Einsatz, die sich um die Rahmensynchronisation, -sicherung und um die Fehlererkennung kümmern (in Hardware implementiert). Zusätzlich können noch Features wie Verbindungs- und Leitungsmanagement, Fehlerbehebung und Flusskontrolle in Software implementiert sein. Je nach verlangen der Applikation kann die Verbindung connection-less (nur die Basiselemente der Leitungsprotokolle sind inkludiert) oder connection-oriented (es wird ein log. Kommunikationskanal zwischen Sender und Empfänger aufgebaut) aufgebaut werden.

Bei der Connection-oriented Methode kümmert sich die Kommunikationssoftware selbstständig um die Fehlerkorrektur mittels Feedback Error Control. Hierbei werden defekte oder ausgefallene Datensätze mittels ARQ (Automatic Repeat Request) neu angefordert.

Das Grundprinzip läuft wie folgt ab: Jedes Frame wird vom Sender mit einer Nummer(Rahmen- Identifier) der Reihe nach versehen, gesendet und im Sendebuffer(Retransmission List) gespeichert. Dabei wird ein Timer für Timeout-Mechanismus gestartet. Der Empfänger bekommt das Frame übertragen und schreibt es sich in den Empfangsbuffer(Receive List). Mit Hilfe des Rahmen- Identifier wird jedes empfangene Frame mit der Liste im Empfangsbuffer verglichen und alle Duplikate gelöscht. Um den Sender mit zu teilen, dass die Übertragung erfolgreich war, wird jedes vom Empfänger erhaltene Frame mit einem speziellen Rahmentypen dem Ack (Acknowledgement) und der Nummer des Frames bestätigt. Der Sender erhält das Ack und löscht damit den entsprechenden Frame aus seiner Sendeliste. Wird keine Bestätigung erhalten, so wird der jeweilige Datensatz nach dem Timeout erneut gesendet.

ARQ bestätigt also jeden korrekt erhaltenen Datensatz per ACK – Message. Hiefür sind Identifizierer nötig um doppelte Frames erkennen zu können.

Grob unterscheidet man zwischen Idle RQ und Continuous RQ.

Idle RQ ist eine alte und langsame, simple Stopp & wait Methode. Hierbei wartet der Sender, bis er ein ACK erhalten hat, und sendet erst dann den nächsten Frame -> zwei Identifizierer sind nötig 0,1 um Duplikate zu erkennen -> Nummerierung erfolgt mod 2;

Half Duplex Protokoll -> Full duplex Leitung kann nicht voll ausgenutzt werden.

Bilder ab Seite 02-8

Verbesserung mittels NACK (not Acknowledgment Frame)

Continuous RQ: Full – Duplex; Daten werden mit der möglichen Übertragungsrage gesendet und in einem Zwischenpuffer gespeichert, aus dem sie wenn eine ACK-Message für den jeweiligen Datensatz erhalten wurde wieder gelöscht werden. Im Falle eines Timeout werden sie erneut gesandt. Der Empfänger speichert die Frames in einem Empfangspuffer, um Duplikate zu erkennen und um sie in die richtige Reihenfolge bringen zu können. (Bild Seite 02-12);

Verschiedene Möglichkeiten der Fehlerkorrektur:

- **Selective Acknowledgement:** jeder Datensatz wird bestätigt
- **Multiple and negative Acknowledgement:** GoBackN: alle Frames ab einer bestimmten Nummer werden erneut gesendet -> Reihenfolge bleibt richtig.

Hier wird die Methode Selective Acknowledgement erklärt. Hierbei wird jeder Frame gesondert bestätigt. Wenn bei der Übertragung des N+1 Frames ein Fehler auftritt, so wird dieser Frame nicht bestätigt. Alle nachfolgenden Frames werden in den Empfangsbuffer übernommen und bestätigt. Dadurch dass der Sender keinen ACK(N+1) Nachricht erhält, jedoch schon eine ACK(N+2) weiß er, dass N+1 nicht ordnungsgemäß übertragen wurde sendet es nochmals und speichert es am Ende seines Buffers. Wurde kein N+2ter Frame gesandt, dann wird der Fehler in N+1 durch den Timeout erkannt. Kommt eine ACK Message auf Grund eines Fehlers nicht beim Sender an, so reagiert ebenfalls der Timeout jedoch wird das Duplikat dann beim Empfänger verworfen und bestätigt -> keine Multiple ACK Messages möglich.

Bilder 02-14 Selective Normal

Bilder 02-15 Selective ACK Failure
Selective Timeout

Timeout: siehe letzte Frage ohne NACK;

Rahmentypen: ACK(N), Daten;

Nachteil: Daten sind nicht notwendig geordnet.

10. Erklären Sie die ARQ- Variante Continous-RQ mit „Positive Acknowledgement“ im Detail. Verwenden Sie zur Erklärung Protokollablaufdiagramme und erläutern Sie die benötigten Betriebsmittel wie verwendete Rahmentypen, Rahmen- Identifier, Retransmission List und Receive List und sowie deren Zusammenspiel. Wozu wird der Timeout- Mechanismus bei diesem Verfahren benötigt?[80 Punkte]

Continous RQ allgemein siehe letzte Frage

Hier wird die Methode Positive Acknowledgement erklärt. Wenn bei der Übertragung des N+1 Frames ein Fehler auftritt, dann bestätigt der Empfänger nur mit Ack(N), der Empfänger kann dabei auch multiple Ack verwenden, das heißt er bestätigt nicht jeden einzelnen Frame gesondert. Alle nachfolgenden Frames werden zwar in den Empfängerbuffer übernommen, jedoch nicht bestätigt. Irgendwann hat der Sender dann ein Timeout für Frame N+1. Der Sender überträgt wieder das N+1 Frame. Der Empfänger übernimmt die Daten in seine Buffer und schaut bis zu welcher Frame ID lückenlos übertragen wurde. Im Buch wurde bis zum N+3 Frame lückenlos übertragen. Somit schickt er nicht ein Ack(N+1) sondern gleich ein Ack(N+3). Wie auch beim GoBackN übernimmt jedes Ack mit höherer ID die Bestätigung aller Frames mit kleinerer ID(Multiple Ack). Deshalb gibt es auch keine Schwierigkeiten, wenn ein Ack verloren geht. Wenn die Übertragung des letzten Frames fehlerhaft war wird mittels Timeout die Neuübertragung eingeleitet.

Nachteil: Es ist eine Umordnung der Daten im Empfängerbuffer notwendig.

Vorteil: falls ein Ack beim Übertragen verloren geht ist das kein Problem, weil jedes höhere Ack die korrekte Übertragung der niedrigeren Frames als Voraussetzung hat. Demnach bestätigt jedes automatisch Ack die korrekte Übertragung vorangegangenen aller Daten bis inklusive dem gerade bestätigten Frame. Es werden nur die fehlerhaften Frames nochmals übertragen.

Bilder 02-20

Timeout: siehe letzte Frage;

Rahmen: ACK(N), Daten;

11.) Erklären Sie die ARQ-Variante Continous RQ mit „Selective Reject“ im Detail. Verwenden Sie zur Erklärung Protokollablaufdiagramme und erläutern Sie die benötigten Betriebsmittel wie verwendete Rahmentypen, Rahmen-Identifier, Retransmission List und Receive List sowie deren Zusammenspiel. Wozu wird der Timeout Mechanismus bei diesem Verfahren benötigt.[80 Punkte]

Continous RQ (Continous repeat request):

Pakete werden der Reihe nach, ohne zuerst die entsprechenden ACK Meldungen abzuwarten, gesendet. Der Empfänger speichert die Pakete in der Receive List. Ungefähr nach der doppelten Signallaufzeit sollten die dazugehörigen ACK`s eintreffen (beim Sender), worauf hin das entsprechende Paket aus dem retrans- buffer (Retransmission List) gelöscht wird. Auf verschiedene Ereignisse hin (Fehler) werden „angeforderte“ Pakete aus dem retransmission buffer heraus nochmals gesendet. Ist das ACK eines Paketes nach einer gewissen Zeit noch ausständig, so tritt ein timeout in Kraft, und das Paket wird aus der retransmission-List heraus nochmals gesendet. Kennt der Empfänger dieses Paket schon, verwirft er es, falls nicht so reiht er es in seinem Speicher ein.

Selective Reject(s.S 02-22,02-23o): Auch hier werden alle Pakete bestätigt und gespeichert, die in der angegebenen Reihenfolge ankommen. Die Methode „multiple ACK“ kann auch hier angewendet werden. Im Falle eines Übertragungsfehlers wird beim „selective Reject“ eine explizite Anforderung des fehlenden Frames gesandt anstatt eines ACK also ein SREJ(N). Somit wird nur das fehlerhafte Paket erneut gesendet. Eine Bestätigung für alle korrekt empfangenen Pakete ist die Folge (N+1 Fehler, N+2 korrekt, N+3 korrekt >> nach N+1 korrekt empfangen eine Bestätigung für N+3) -> Multiple Ack.

Jedes gesendete Paket startet einen individuellen Timer, wenn die Bestätigung(ACK) empfangen wurde wird Der Timer zurückgesetzt. Wenn Timeout eintritt wird das Paket nochmals gesendet.

Vorteil gegenüber pos. Reject: Es muss nicht jedes mal bis zum Ende des Timeouts abgewartet werden. Folgende Pakete können bereits gesendet werden.

Nachteil: Richtige Reihenfolge ist nicht gewährleistet;

Bilder 02-22

02-23

Timeout: siehe vorher;

Rahmen: ACK(N); SREJ(N), Daten;

12.) Was sind Sequence Numbers? Welche Typen gibt es? Wie wird deren Handhabung mittels Registervariablen realisiert? Wie arbeiten diese Elemente zusammen? Was versteht man unter Piggybacked Acknowledgement? Wozu dienen KeepAlive Messages? Was versteht man unter Flusskontrolle(FlowControl) und wie kann Sie realisiert werden? Warum reicht Windowing dafür alleine nicht aus? Was versteht man unter „adaptive Windowing“?[90 Punkte]

Sequence Number:

Die gesendeten Frames werden mit aufsteigenden Nummern durchnummeriert.

Die Nummer werden sowohl bei I-(Informations-Paket als send sequenz number N(S)), ACK-, NACK-, SREJ-Paketen (als receive sequenz number N(R)) verwendet.

Im Sender und Empfänger werden zusätzlich Registervariablen V(S), V(R) benötigt. Diese müssen beim Verbindungs-Aufbau initialisiert (auf 0) gesetzt werden.

V(S) enthält die sequence number des nächsten I Framest das gesendet wird. V(R) enthält die erwartete sequence Number des nächsten I Frames das empfangen werden soll, also die Nummer die bei der nächsten Ack-Message als N(R) erwartet wird. Bevor an I – Frame gesendet wird, wird der Wert von N(S) auf V(S) gesetzt und V(S) danach erhöht. Die Registervariablen sind also auch nötig um Duplikate erkennen zu können.

Für GoBackN gilt, dass der Empfänger nur I Frames akzeptiert, deren Sequenznummer N(S) = der erwarteten Sequenznummer V(R) ist. Nach dem Empfang wird V(R) um eins erhöht und danach N(R) zugewiesen -> erhält der Sender eine ACK – Msg mit N(R) = x, so bedeutet das, dass alle I Frames bis x-1 bestätigt sind.

Beispiele für Sequenznummern bei GoBackN siehe Bilder 02-25;

Keepalive Messages: Die Verbindung wird nach dem Verbindungsaufbau durch keep alive Signale während Übertragungspausen am Leben gehalten. Mit dem versenden von I Frames kann nach keep alive Signalen unmittelbar wieder begonnen werden. Eine ACK-Message mit der entsprechenden Nummer N(R) = V(R) wird sowohl für die Aufrechterhaltung als auch als ACK für I-Pakete verwendet, das heißt, wenn ein Frame bereits erhalten und bestätigt wurde und es wird später eine KeepAlive Message empfangen, so antwortet der Empfänger mit der selben Ack Message wie zuvor -> deshalb bestätigt eine Ack(N) Msg auch nur den Empfang der Frames bis N-1, da dadurch der Sender zwischen KeepAlive Antwort und Antwort auf einen neuen Frame unterscheiden kann.

Beispiel für Initializing und Keepalive siehe Bild 02-27

Piggy backed ACK:

Die Bestätigung jedes einzelnen empfangenen Frames mittels eigener Ack – Message ist auf Grund der damit verbundenen Bandbreitenverschwendung im Full – Duplex Datenverkehr nicht geeignet sondern nur im Half – Duplex Betrieb nötig.

Um dieser Ressourcenverschwendung entgegen zu wirken, geht man dazu über, die Bestätigungen der einzelnen Frames in die Daten – Frames, die ohnehin gesendet würden, zu packen, und damit den unnötigen Overhead zu beseitigen.

Sind keine Daten Frames zu senden, so werden wieder Ack Messages übermittelt.

Dadurch enthalten Daten Frames sowohl Send Sequenz number als auch die receive sn für die Gegenrichtung; dadurch können ACK/NACK Frames in beiden Richtungen auftreten und die Kommunikationspartner müssen beide Registervariablen V(S) und V(R) speichern und Retransmission und Receive Buffer haben.

Beispiel für Piggyback Acknowledgement siehe Bild 02-29

Kommen Datenrahmen beim Empfänger schneller an, als sie verarbeitet werden können, so läuft irgendwann der Buffer des Empfängers über und alle weiterhin ankommenden fehlerfreien Rahmen müssen verworfen werden. Nach Timeout werden alle diese Rahmen wieder gesendet, und vielleicht erneut verworfen.

Abhilfe liefert **Flow Control**. Hierbei meldet der Empfänger dem Sender Bufferoverflows mittels spezieller flow control messages. Danach hört der Sender auf zu senden und wartet bis der Empfänger wieder fertig ist.

Eine Möglichkeit Flow Control zu realisieren ist Windowing. Ist der Buffer voll, so sendet der Empfänger keine ACK's mehr -> das Sendefenster des Senders wird sich schließen, der Sender sendet keine Daten mehr.

Problem: Nach einem Timeout erfolgt eine erneute Übertragung. Ist der Empfänger dann noch immer nicht fertig so bleibt das Fenster weiterhin geschlossen. Nach einer gewissen Anzahl an misslungenen Versuchen betrachtet der Sender die Verbindung als unterbrochen und verwirft die noch übrigen Frames.

Somit basieren Flow-Control-Mechanismen eher auf eigene Meldungen(Stop/go) und Windowing.

Typische Flow-Control-Mechanismen sind: Stop: Receiver Not Ready (HDLC: RNR), Go: Receiver Ready(HDLC: RR)

Im Fehlerfall sendet der Empfänger ein STOP Signal, daraufhin hört der Sender auf zu senden, im schlimmsten Fall sendet er noch das was in seinem Send-Window ist, sobald der Empfänger wieder bereit ist sendet er ein GO. STOP und GO können auch als ACK Msg mitgenutzt werden.

Im Full-duplex Betrieb werden Stop und Go in beiden Richtungen benutzt; manchmal werden sie auch für KeepAlive Messages benutzt (nichts zu sende -> Go; wenn gestopt -> Stopp).

Adaptive Windowing:

Um Übertragungskapazitäten optimal ausnützen zu können, kann auch die Fenstergröße W dynamisch veränderbar sein. Sie wird dann während der Laufzeit errechnet. Beim Verbindungsaufbau wird ein Wert vereinbart und während der Datenübertragung passt der Empfänger die Größe dynamisch nach seinen Bedürfnissen (freier Buffer Speicher) an. Dabei bedeutet eine Window Size 0 -> Stop und eine Size > 0 -> Go.

(used by TCP).

13) Was versteht man unter Windowing? Wozu wird es benötigt? Was ist ein Sendefenster? Was sind die zusätzlichen Auswirkungen bezüglich Anzahl der Identifier? Welche Rolle spielt prinzipiell das Bandwidth Delay Produkt in ARQ Verfahren? Welche Auswirkungen auf das Sendefenster ergeben sich daraus? [90 Punkte]

Windowing: Ohne eine Beschränkung der nicht bestätigten Frames, würde Continuous RQ eine unendliche Anzahl von Identifier und unendlich große Buffer benötigen. Deshalb wird die Anzahl der gespeicherten Datenframes limitiert. Das Window bezeichnet den reservierten Bereich im Buffer, in dem Datenpakete für eine eventuelle Wiederholung der Sendung zwischengespeichert werden, zusammen mit den Frames die sobald die Leitung frei ist gesendet werden können.

Siehe Bild 02-30

Sobald alle Identifier verwendet sind und der Bufferspeicher voll ist, wird vom Sender nichts mehr abgeschickt. Er wartet, bis ein ACK das Sendefenster wieder „öffnet“. Die Window-Size gibt also die maximale Anzahl der unbestätigten Rahmen an. Bei „go back N“ ergibt sich als Anzahl an Identifier stets $W+1$. Sollte das Sendefenster bereits voll sein (Buffer mit W Paketen belegt) und sind alle ACK-Meldungen verloren gegangen, so muss der Empfänger noch darstellen können, welches Paket er als nächstes erwartet. Sonst kann er die nach einem timeout wieder versandten Duplikate ja nicht von neuen Paketen unterscheiden. Die Buffer Größe ergibt sich als $W * \text{maximum frame size}$, wobei W die Größe des Fensters ist. Die Nummerierung der Identifier kann mit einer Modulo Operation durchgeführt werden:

Bsp.: GoBackN: braucht $W+1$ Identifier, Nummerierung erfolgt mod $W+1$

Selective Ack: brauch $2W$, mod $2W$

Worst Case GoBackN (Seite 02-32):

Sendefenster ist nach dem Senden von 0,1,2 voll; keine ACKs kommen an; nach Timeout erneut senden; Empfänger muss erkennen dass es sich um Duplikate handelt, dass ist der Fall da $V(R) = 3$ jedoch $N(S) < 3$ ist -> Duplikate werden verworfen -> 4 Identifier nötig.

BW x RTT: Delay Bandwidth Product: gibt Auskunft über das Fassungsvermögen des Übertragungskanal

Das Produkt ergibt die Anzahl an Bytes, die sich bei einer bestimmten Bandbreite und einer Leitung mit einer gewissen Länge und damit verbunden Laufzeit, gleichzeitig auf der Leitung (hintereinander) befinden können ohne dass es zu ungewünschten Überlagerungen kommt.

RTT: round Trip Time (Antwortzeit)

BW: Bandbreite des Übertragungskanal in Bit/s

Beispiele für verschieden ausgenutzte Leitungen siehe Bilder 02-35, 02-36;

Optimale Windowsize für C-RQ ergibt aus: W (in Bytes) = $RTT \times BW$ -> dann kommen die ACKs gerade rechtzeitig um das Fenster offen zu halten -> sliding window;

Kleineres Fenster: Übertragung unterbricht, bis wieder ACKs eintreffen -> jumping window

Zu großes Fenster: im Fehlerfall müssen viele gute Frames noch mal übertragen werden.

14) Welche Stationstypen, Leitungskonfigurationen (Line Configuration) und Betriebsarten (Modes of Operation) sind in HDLC vorgesehen? Was kennzeichnen Command and Response? Welche Verwendung findet HDLC Adresse und das P/F-Bit? Charakterisieren Sie kurz das HDLC Protokoll im verbindungsorientierten Modus (ARQ Type, Transmission Methode, etc). [80 Punkte]

Allgemein:

HDLC (High level Data Link Control): Beim HDLC-Protokoll handelt es sich um einen strukturierten Satz von Standards der die Mittel bestimmt, mit denen ungleiche Geräte über Datennetze miteinander kommunizieren können. HDLC wurde ursprünglich für terminal networks entwickelt, auf Grund seiner universellen Prozeduren ist es jedoch auch in Computernetzwerken erfolgreich. Das HDLC-Protokoll ist ein bitorientiertes und damit codeunabhängiges, von ISO standardisiertes Sicherungsprotokoll für Punkt zu Punkt Verbindung und Mehrpunktverbindungen. Eine Version dieses Protokoll wird in allen X25-Netzen innerhalb der Sicherungsschicht eingesetzt und trägt in diesem Fall die Bezeichnung LAP B.

nicht notwendig:

Im HDLC – Standard sind drei Typen von Stationen definiert, die primäre, die sekundäre und die kombinierte Station.

Die Primäre Station fungiert als Master für die sekundäre Station, das bedeutet, dass die primäre Station Senderechte verteilt (siehe Token Ring). Hiefür übermittelt sie Kommandos an die sekundäre Station und empfängt daraufhin Antworten von diesen. Sie verwaltet für jede sekundäre Station auf einer Multipoint Leitung eine separate Session.

Die sekundäre Station arbeitet im Slave Betrieb, das heißt sie darf nur dann Daten senden wenn sie von der Primären dazu aufgefordert wurde. Hiefür empfängt sie Kommandos vom Master und sendet Antwort Frames. Sekundäre Stationen können nur über einen Master miteinander kommunizieren, nicht direkt.

Die kombinierte Station enthält Protokoll Komponenten sowohl der sekundären als auch der primären Station und kann damit Kommandos und auch Antworten senden und empfangen. Hiefür benutzt sie die Leitungsadresse um zwischen Antwort und Kommando zu unterscheiden:

Frame mit eigener Adresse empfangen -> Kommando

Frame mit Partneradresse empfangen -> Antwort

vielleicht für diese Fragestellung nicht nötig:

Man unterscheidet bei HDLC zwischen balanced und unbalanced Mode. Im unbalanced Mode gibt es nur eine primäre und dafür mehrere sekundäre Stationen. Der Master ist für jeden Slave zuständig und verwaltet somit die Verbindungen. Adressen haben in diesem Modus nur die Sekundären. Diese Adressen benutzt der Master um seine Kommandos an einzelne Slaves zu senden. Empfängt der Master Frames, so enthalten diese die Adressen des Absenders. Dieser Betrieb ist sowohl für Punkt zu Punkt als auch für Multipoint Verbindungen zulässig.

Der balanced Mode kann nur für Punkt zu Punkt Verbindungen verwendet werden. Dabei haben beide Partner dieselben Rechte, weshalb es sich um kombinierte Stationen handeln muss. Adressierung siehe weiter oben.

//

Die Modes of Operation für diese Modi sind nun:

Unbalanced:

- NRM: normal response Mode
- ARM: Asynchronous response Mode

Balanced:

- ABM: asynchronous balanced Mode

NRM:

Sekundäre brauchen gezielte Erlaubnis zum senden; nach der Erlaubnis senden sie auf jeden Fall eine Antwort, die nicht notwendig auch Nutzdaten enthalten muss, dann gibt sie nur die Erlaubnis wieder zurück;

Mit dem letzten Nutzframe wird die Sendeerlaubnis wieder an den Master übergeben; danach muss die Station wieder auf die Erlaubnis warten; um die Verteilung der Sendeberechtigung (polling) kümmert sich die primäre Station; wird häufig für Multipoint Leitungen und Half-duplex point to point Leitungen verwendet.

ARM:

Dabei hat der Sekundäre das Recht selbst eine Übertragung zu initiieren; Full-duplex Leitung notwendig; Overhead kann dadurch reduziert werden, da das Polling ausfällt. Um das Leitungsmanagement und die Fehlerbehebung muss sich immer noch der Master kümmern; auf einer Multipoint Leitung kann sich nur ein sekundärer im ARM Mode befinden; nur selten benutzt;

ABM:

Hierbei können die kombinierten Stationen selbst eine Übertragung ohne explizite Erlaubnis starten; jede Station ist im gleichen Ausmaß für Fehlererkennung und Leitungsmanagement verantwortlich -> beste Wahl für Punkt zu Punkt Verbindungen

Bei einem Command Frame handelt es sich um einen Frame der von einer primären an eine sekundäre Station gesendet wird. Dieser Frame kann für administrative Zwecke (Verbindungsaufbau, flow control...) gedacht sein oder auch Nutzdaten von einem anderen Kommunikationspartner enthalten. Das entscheidet sich durch die Art des Frames (Information (I) Frame, Supervisory (S) Frame, Unnumbered (U) Frame). Ein Response Frame ist ein Frame der von einer sekundären an eine primäre Station gesendet wird, dieser kann ebenfalls verschiedenen Zwecken dienen. Command und Response sind durch die HDLC - Adresse gekennzeichnet (siehe weiter oben);

Das P/F Bit dient für das Polling: P – Bit nur in Command Frames; mit P = 1 signalisiert der Master das der Slave Sendeerlaubnis hat. F- Bit nur in Response Frame; mit F = 1 gibt der Slave die Sendeerlaubnis zurück.

Im Connection oriented Mode arbeitet HDLC mit einer Art Continuous RQ, wobei der Empfänger erst dann antworten (ACK) kann, wenn er die Erlaubnis dazu hat; hierfür wird piggyback acknowledgement verwendet; max. Window size = 7 (im normal Mode), Window size = 127 (im extended Mode); zum Verbindungsaufbau dienen U – Frames, zur Übertragung von Nutzdaten dienen I – Frames, S – Frames kümmern sich um Kontroll – Funktionen (Ack, request for retransmission, flow control (RR, RNR); RR (im Falle von GO) und RNR (im Falle von STOP) können auch als keepalive dienen. Error Recovery erfolgt durch die Methode des Checkpointing – entspricht einem delayed oder triggerd GoBackN: keine eigenen NACK Frames; sobald Empfänger die Erlaubnis zum Senden hat sendet er ein Frame mit der jeweiligen Sequenznummer ab wo die Daten neu gesendet werden müssen (deshalb delayed).

Andere Methoden des Error recovery: REJ: reject Frame entspricht NACK Frame |
 SREJ: selective reject Frame: selektive Anforderung eines Frames | ABM

15) Erläutern Sie den Aufbau eines HDLC Rahmens und geben Sie die Formate des Control Feldes an. Wofür werden die einzelnen Formate bzw. Rahmentypen prinzipiell verwendet. Welche Dienste lassen sich damit realisieren? Welche Fehlerbehebungsstrategien sind beim HDLC-Protokoll vorgesehen? Gehen Sie dabei auf Checkpointing und die HDLC-Optionen REJ, SREJ im Detail ein.[90 Punkte]

Das Rahmen-Format bei HDLC sieht so aus:

Flag	Address	Control	Data	Checksus	Flag
------	---------	---------	------	----------	------

HDLC-definiert drei Typen von Frames, jeder Typ mit einem anderen Kontrollfeld-Format.

Information-Frames für die eigentliche Datenübertragung (vorher Verbindungsaufbau notwendig).

Supervisor-Frames für die Steuerung während der Datenübertragung (ACK, flow control (RR,RNR), request for retransmission, keepalive mittels RR(in GO Phase) und RNR(in STOP Phase)).

Unnumbered-Frames werden für die Verwaltungszwecke verwendet (Verbindungsverwaltung, Initialisierung, Test,...)

Im verbindungslosen Modus werden nur U Frames für allen Datentransport verwendet.

Das Flag Feld dient als SD und ED Feld.

Im Adressfeld steht die jeweilige HDLC Adresse des Empfängers (Command Frame) beziehungsweise des Senders (Response Frame). Im unbalanced Mode ist das immer die Adresse der sekundären Station.

Das Datenfeld/Informationsfeld wird nur in Informations-Frames und einigen Unnumbered-Frames genutzt und hat variable Länge.

Die Frame-Check-Sequence besteht aus einem 16-Bit oder 32-Bit Cyclic-Redundancy-Check.

HDLC ist Code transparent und arbeitet mit bitstuffing.

Allen Rahmentypen gemein ist das P/F-Bit(Poll/Final-Bit) an der 5.Stelle des Controll-Feldes. Bei Command Frames spricht man vom P-bit, und sonst vom F-Bit. Generell haben die P/F-Bit den Status 0. Im NRM: Bei dem letzten Rahmen eines Befehles setzt der Master das P Bit auf 1. Damit übergibt er dem Slave das Recht, zu übertragen. Mit dem letzten Rahmen einer Antwort gibt der Slave mit F=1 das Senderecht wieder zurück. Sonst ist P/F immer gleich 0. In den anderen Modi kann selbstständig gesendet werden. P- und F-Bits werden hierbei nicht benötigt. Für Half-duplex Leitungen markiert dieses P/F Bit Checkpoints für die Fehlerkorrektur (siehe weiter unten).

Im ARM/ABM Mode wo bei beteiligten ohne explizite Erlaubnis Senden dürfen, wird das P/F Bit nur noch zur Fehlerkorrektur verwendet: sendet der Master einen Frame mit P=1 so muss der Slave so bald als möglich mit einem F=1 Frame antworten.

Mit Hilfe dieser verschiedenen Frame Typen lassen sich nun sowohl verbindungslose als auch verbindungsorientierte Datenübertragungen realisieren.

Prinzipiell gibt es drei Fehlerbehebungsmodi in HDLC: Checkpointing, REJ, SREJ;

Checkpointing: dieses funktioniert für alle Betriebsarten, und ist die angemessene Fehlerkorrektur für half – duplex Leitungen. Im NRM darf ein Teilnehmer immer nur dann Daten senden, wenn er die Erlaubnis dafür hat. Eine sekundäre Station erhält diese Erlaubnis durch den Master mittels P=1, und gibt sie mittels F=1 wieder zurück. Tritt nun während einer Übertragung ein Fehler auf, so kann dieser erst durch den Empfänger an den Sender indiziert werden, wenn dieser die Sendeerlaubnis hat, und ausgebügelt erst wieder dann wenn wieder der Sender an der Reihe ist (deshalb delayed/triggered GoBackN -> Checkpointing). Es werden also keine eigenen NACK Frames verwendet, sondern es wird mittels eigener ACK Message oder piggyback Acknowledge angezeigt bis zu welchem Frame die Übertragung in Ordnung war.

In ARM Mode: immer dann wenn ein Frame mit P=1 oder F=1 empfangen wird: es findet eine Überprüfung statt, welche Frames bis jetzt noch nicht bestätigt wurden mit Hilfe des N(R) Feldes -> danach wird die GoBackN Methode mit dieser Sequenznummer angewendet.

In ABM Mode: hier wird das nur durchgeführt wenn ein Frame mit F=1 empfangen wird.

REJ: reject Frame: funktioniert wie NACK Frame: sobald Fehler aufgetreten ist wird ein REJ Frame mit der Sequenznummer des nicht empfangen Frames gesendet -> GoBackN

SREJ: selective reject: fordert einen bestimmten Frame an.

Diese Methoden sind natürlich im NRM nicht möglich.

16) Was versteht man unter Multiplexern im allgemeinen und Zeitmultiplexern(TDM) im speziellen? Gehen Sie im Detail auf das synchrone und das statistische (asynchrone) Zeitmultiplexen ein. Welche Eigenschaften hat dieses Verfahren hinsichtlich Übertragungszeit eines Bytes, Echtzeitfähigkeit, Handhabung von Übertragungspausen der Endgeräte, Protokolltransparenz? Wäre Flow Control erforderlich bzw. wünschenswert in diesem Zusammenhang?[100 Punkte]

Leitungsprotokolle wurden dazu entwickelt, damit zwei Geräte über eine physikalische Verbindung kommunizieren können. Dadurch wird die gesamte Bandbreite der Leitung nur von zwei Geräten genutzt. Wollen viele Geräte miteinander kommunizieren, wären viele Leitungen nötig, was sehr teuer wäre.

Ein Multiplexer ist ein Gerät, das mehrere Datenkanäle auf eine phys. Leitung legen kann. Der Demultiplexer teilt das Signal von dieser Leitung wieder in mehrere Datenkanäle. Ein Multiplexer teilt also die verfügbare Bandbreite auf einer physikalischen Leitung in mehrere logische Kanäle auf, so dass mehrere Geräte über diese eine Leitung kommunizieren können. Auf der Empfängerseite splittet ein Demultiplexer die eine Leitung wieder in die einzelnen Kanäle auf. Beim Zeitmultiplexer werden den Eingängen Zeitschlitze zugeordnet, das heißt jedem Gerät am Eingang des Multiplexers ist ein bestimmtes Zeitintervall zugeteilt, in dem seine Daten über die physikalische Leitung zum Demultiplexer transportiert werden. Alle individuellen Zeitschlitze werden dann zu einem Frame zusammengefügt und anschließend übertragen. Es gibt 2 Arten: synchrones und asynchrones (statisches) Zeitmultiplexen (**TDM=Time Division Multiplexing**).

Synchrones Zeitmultiplexen:

Der Multiplexer sendet regelmäßig Übertragungsrahmen mit einer konstanten Anzahl von Zeitschlitzen aus. Jedem Eingang wird ein bestimmter Zeitschlitz zugeordnet, wobei jedem Zeitschlitz eine fixe Position innerhalb des Rahmens zugewiesen ist. Jeder Zeitschlitz hat eine konstante Länge /Kapazität.(s.S 04-6o); hat ein Teilnehmer nichts zu senden, so wird eine spezielle Idle Bitfolge eingefügt.

Eigenschaften: minimale Verzögerungen durch packetize und depacketize, protokolltransparent(jedes Protokoll kann intern verwendet werden), Kanal sieht für ein Endsystem wie eine point to point Verbindung aus, die Bitrate ergibt sich als Summe der Einzelbitraten+sync flag , dadurch ist eine entsprechende physikal. Leitung notwendig -> teuer. Sind keine Daten zu Übertragen, werden spezielle idle-pattern vom Multiplexer in die Zeitschlitze eingefügt, -> Bandbreitenverschwendung, falls nicht ständig gesendet wird. Flow Control wäre in diesem Zusammenhang nicht erforderlich.

Statisches/Asynchrones Zeitmultiplexen:

Vermeidet beide Nachteile vom synchronen TDM (Bandbreitenverschwendung, idle pattern).

Beim asynchronen (statistischen) Zeitmultiplexen wird nur dann ein Übertragungsrahmen erzeugt, wenn auch wirklich gesendet wird. Dadurch ergibt sich die Bitrate auf der Verbindungsleitung als Summe aller (statistischen) durchschnittlichen Übertragungsraten der Endgeräte. Sendet eine Station nicht, wird diese einfach übersprungen. Wollen 2 Endgeräte gleichzeitig senden, muß der Multiplexer zwischenspeichern, und nacheinander die Rahmen senden. Hat eine Station mehr zu senden, so werden ihr in einem Rahmen mehr Plätze zugeteilt. Ein Kontrollmechanismus muss zusätzlich dafür sorgen, dass nicht ein User die Trunk-Leitung die ganze Zeit für sich allein beansprucht. Dadurch dass es nun keinen Zusammenhang zwischen Zeitschlitz und Empfängerport gibt, muss der Multiplexer zusätzlich dem Demultiplexer mitteilen, zu welchen Datenkanal der Rahmen gehört (Port-Adresse). Im Falle von Überlastungen verursacht die Bufferung der Daten zusätzliche Verzögerungen. Auf Grund des statistischen Verhaltens, sind die Verzögerungen variabel -> asynchron.

ATDM kann Protokolltransparent genutzt werden, im Falle von Bufferoverflows im Multiplexer erhalten die Geräte auf jeden Fall Übertragungsfehler (FCS errors). Deshalb sollte es eine Flowcontrol zwischen Endsystem und Multiplexer geben -> HW: Handshake Signal; SW: Connection oriented Protocol like HDLC RNR.

17) Erklären Sie das Prinzip der Leitungsvermittlung (circuit switching) im Detail. Welches Zeitmultiplexverfahren liegt zu Grunde? Welche gängige Netzwerktechnologie beruht auf diesem Verfahren? Wie erfolgt heutzutage die Übertragung von Sprache? Was versteht man unter PCM? Was stellt der DSO Kanal dar? Was versteht man unter Multiplexer-Hierarchien, welche gibt es und wozu dienen diese?[100 Punkte]

Praktisch wäre eine any-to-any Topologie(jeder hat zu jedem eine direkte eigene Verbindung), jedoch ist diese zu teuer. Eine Vielzahl an Leitungen und Übertragungsgeräten(Modems, Repeater,...) wäre notwendig. Besser/Günstiger/Billiger ist hier eine Struktur mit mehreren Vermittlungsstellen (TDM Switches) die untereinander mit Leitungen hoher Bandbreite verbunden sind und auf dieser synchrones TDM verwenden. An diese Vermittlungen sind Endgeräte über Leitungen mit nicht notwendig so hoher Bandbreite angeschlossen. Jedem dieser Geräte ist ein fixer Zeitschlitz zugewiesen, während dessen seine Daten über den Trunk transportiert werden. Alle Zeitschlitze werden wieder zu einem Frame zusammengefügt. Somit kommt es logisch auch zu einer any-to-any Topologie. Die Switches verbinden ankommende Daten einer Trunkleitung dann entweder mit einem lokalen Port oder mit einer weiteren Trunk-leitung (transit switches). Jeder Switch speichert seine Mapping Information in Circuit Switching Tabellen.

Jeder Pfad zwischen zwei Endgeräten wird beschrieben durch entsprechende Einträge in den Swiching Tabellen der die beiden Geräte verbindenden Switches.

Durch dieses Verfahren spart man viele teure Langstreckenleitungen die für einen vollen Mesh nötig wären.

Eigenschaften: minimale Verzögerungszeiten, hohe Bitraten auf den Trunks, idle pattern (Bitmuster) nötig, wenn ein Teilnehmer nichts zu senden hat, Protokolltransparent;

Um die Anzahl der lokalen physikalischen Leitungen zu reduzieren, wenn man zusätzlich TDM zwischen den Geräten und dem local switch anwendet -> mapping zwischen diesen funktioniert wie zwischen den einzelnen Switches (siehe Bild 05-7).

Die Switching Tabellen selbst können entweder statisch, oder dynamisch sein.

Statische Tabellen werden von einem Netzwerk Administrator verwaltet.

Dynamische Tabellen unterteilen sich wieder in zwei Kategorien:

- **fail safe:** Einträge werden nur dann geändert wenn eine Trunkleitung ausfällt und damit ein anderer Pfad nötig ist
- **on demand (auf Anforderung/Verlangen):** End Systeme benutzen spezielle Protokolle um einen Verbindungsaufbau anzufordern. TDM Switches richten einen Pfad ein, in dem sie spezielle Protokolle zwischen den Switches verwenden -> Pfad wird erst auf Verlangen eingerichtet (switched circuit services).

Das Telefonsystem beruht auf dieser Netzwerktechnologie, ISDN verwendet switched circuit services;

Die Übertragung von Sprache in unserem Telefonnetzwerk basiert auf dem Nyquist Theorem. Analoge Sprache kann mittels PCM (pulse-code-modulation) digitalisiert werden. Dabei wird die Sprache alle 125µsec, also 8000 mal pro Sekunde abgetastet und dieser Wert als 8Bit Datenwort codiert. Diese Daten können dann über eine mind. 64kBit/s schnelle Datenleitung übertragen und am Empfänger rekonstruiert werden. Nur zwischen dem Haus und der lokalen Vermittlungsstelle erfolgt die Sprachübertragung noch analog.

Das Nyquist Theorem besagt folgendes: Jedes analoge Signal mit begrenzter Bandbreite f kann korrekt rekonstruiert werden wenn die Abfragefrequenz $2*f$ entspricht. Die Abgetasteten Werte werden quantisiert und in ein binär-codiertes Datenwort zusammengefasst. Die Übertragung der Datenworte des Signals erlaubt somit die Rekonstruktion des gesamten Signals. Um die Qualität der Signal Rausch Rate zu verbessern fragt man bei kleinen Amplituden das Signal mit feinerer Auflösung ab. Hiefür wird eine nichtlineare Logarithmische Funktion verwendet um die Signale zu quantifizieren. (-USA: μ -law(Bell);-Europe: A-law(ITU);) PCM(pulse Code modulation) : Um die digitalen Werte in eine definierten Übertragungsform zu bringen, verwendet man die PCM codierung. Ein 8 bit PCM sample sieht folgendermaßen aus(s.S 04-15o). Das Segment besagt, in welchem Amplitudenbereich man sich befindet, wie fein also die Auflösung der digitalisierten Amplitude ist (feinere sample-Schritte bei kleinen Amplituden).

Der DS0(Digital Signal,Level 0) stellt genau einen Zeitschlitz in einem Datenpaket(„multiplexing Frame“)dar, und ist die Basis für hierarchische digitale Kommunikation.(s.S 04-17 u). Er entspricht einem PCM codierten 64kBit/s Sprachkanal. Die unterste Ebene (die Ebene die die einzelnen Teilnehmer mit dem local switch verbindet) eines Telefonnetzwerkes basiert also auf diesem Kanal. Mehrere solche Kanäle (31) werden in der nächst höheren Ebene E1 durch einen Switch (TDM: jeder Kanal hat einen fixen Zeitschlitz) in ein Datenwort/Frame gepackt, die Kanäle dieser Ebene werden in der darauf folgenden Ebene wieder zusammengefasst,... . Damit immer noch 8000 Bit/s am Empfänger ankommen, also jeder Abtastwert innerhalb von 125µs, folgt, dass die Datenraten der einzelnen Ebenen entsprechend höher liegen müssen ($E1\ 32 * 64kBit/s = 2048kBit/s$ -> selbe Bitrate wie in der untersten Ebene pro Benutzer); Bild siehe 04-19

Diese Multiplexer Hierarchien dienen also hauptsächlich dazu um physikalische Leitungen einsparen zu können und trotzdem eine Verbindung von jedem zu jedem zu ermöglichen.

Für den Aufbau derartiger hierarchischer Strukturen gibt es zwei Grundlegende Architekturen.

PDH - plesiochronous digital hierarchy: Plesio bedeutet beinahe synchron. Zeitdifferenzen zwischen den einzelnen Multiplexern werden mit „bit stuffing“ kompensiert („overhead bits“). Die Zahl der „overhead bits“ steigt mit zunehmender Rate jedoch rasch an(s.S: 04-19o) Die PDH-Technologie wird noch immer für langsame Leitungen verwendet. Jedoch dadurch, dass es unterschiedliche Standards für Europa und Nord Amerika gibt (-> unterschiedl. Multiplexing Prozeduren) und durch den unnötigen, wachsenden Overhead wird PDH zunehmend von SDH verdrängt.

SDH – synchronous digital hierarchy: macht die Nachteile von PDH weg; ist weltweit standardisiert; wurde für fiber optic entwickelt. In Nordamerika wird SONET verwendet (Substandard von SDH). Ziel ist ein gemeinsam funktionierendes echt synchrones Netzwerk.

18) Erklären Sie allgemein das Prinzip der Paketvermittlung (packet switching). Welches Zeitmultiplexverfahren liegt zu Grunde? Was sind Routingtabellen und wie können diese erstellt werden? Welche Funktionen spielt die Adressierung in diesem Zusammenhang? Erklären Sie den Datagramm-Dienst im Detail. Welche Dienstart (service) liegt zu Grunde? Wie werden dabei Pakete weitergeleitet? Geben Sie Vor- und Nachteile dieser Methode an. Welche Netzwerktechnologien beruhen auf diesem Verfahren? [100 Punkte]

Packet Switching ist die konsequente Umsetzung des Prinzips des statistischen Zeitmultiplexens in einer Netzwerkumgebung. Damit treten die Basiseigenschaften des statistischen Zeitmultiplexens wie variables Delay durch Pufferung, Adressierung und keine fixe Zuordnung von Bandbreite (Timeslots) zu Kommunikationsbeziehungen nun auch in der Netzwerkumgebung auf (Anmerkung: Das Grundprinzip des statistischen Multiplexens soll hier an dieser Stelle nicht erklärt werden, weil das Inhalt der Frage 15 ist). Der statistische Zeitmultiplexer, der nun i.a. mehr als ein Trunk-Port aufweist, heißt Packet Switch. Die Endsysteme werden über Access-Leitungen an die Ports des nächstgelegenen Packet Switch angeschlossen. Die Switches untereinander sind über bandbreitenstarke Trunkleitungen verbunden. Möchte ein Endsystem Daten senden, werden diese in kleine Stücke zerhackt, Pakete genannt werden, mit Ziel- und Ursprungsadresse versehen und an den lokalen Packet Switch übertragen. Der speichert das Paket zunächst zwischen (buffert es), wertet die Adressinformation mittels Routing- oder Switching-Tabelle aus, um festzustellen, auf welchem Port die Daten weitergesendet werden müssen, stellt das Paket in die Warteschlange der abgehenden Leitung und sendet das Paket – wenn es an die Reihe kommt - schlussendlich Richtung Ziel weiter (Store and Forward Prinzip). Nachdem die Leitungen nach statischen Werten dimensioniert sind, ist die Wartezeit abhängig vom momentanen Verkehrsaufkommen. Diese Methode des statistischen Zeitmultiplexens erlaubt somit vielen Teilnehmern miteinander zu kommunizieren, ohne dass Kapazität auf einer Leitung extra reserviert werden muss. Auch Leitungen werden dadurch eingespart und die nötige Bitrate der Trunkleitungen dadurch limitiert, dass sie für den Durchschnittswert ausgelegt wird. Jedoch ist ein Protokoll zwischen End System und Switches nötig, um flow Control und die Adressierung realisieren zu können -> beide müssen die selbe Sprache sprechen. Dadurch ist Packet switching nicht mehr Protokoll transparent. Redundante Leitungen können für alternative Pfade bei Fehlern bzw. für Lastaufteilung Verwendung finden. In der Routingtabelle/Switchingtabelle ist im Prinzip abgespeichert, welche Zieladresse über welches Port erreichbar ist. Man kann das mit einer Wegweisertechnik vergleichen, wobei in jedem Packet Switch Wegweiser für ein bestimmtes Ziel derartig aufgestellt sind, dass ein Paket entlang der Wegweiser zum gewünschten Ziel weitergeleitet werden kann. Von Switchingtabellen spricht man im Zusammenhang mit connection oriented services (virtual call service), von Packetswitching im Falle von connection less services (datagram service). Alle auf Packet Switching basierenden Netzwerke, die „routable protocols“ verwenden, benötigen für Endsysteme eindeutige und strukturierte Adressen (OSI Layer 3). Strukturiert heißt, dass sich darin die Topologie in irgendeiner Form widerspiegelt (Beispiele dafür sind Net-ID/Host-ID bei IP oder Ländercode (+43 für A) bei Telefonnetzen). (Anmerkung: Transparent Bridging (Ethernet Switching) ist auch Packet Switching (allerdings auf OSI Layer 2), verwendet aber unstrukturierte Adressen (MAC-Adressen), die keine Topologieinformation enthalten und daher auch nicht zusammengefasst werden können. Die Routingtabellen (die Wegweiser) können entweder statisch von Netzwerkadministrator konfiguriert werden oder dynamisch unter Verwendung von Routingprozessen und Routingprotokollen erstellt werden. Statisch heißt, dass bei einer Änderung der Topologie der Netzwerkadministrator händisch eingreifen muß, das heißt, die Routing Tabellen sind vorkonfiguriert und können sich nicht selbstständig optimieren. Dynamisch heißt, basiert auf eigenen Routingprotokolle, mit Hilfe derer die PacketSwitches Informationen über die Netzwerktopologie austauschen. Routing ist dabei der Prozeß der Wegefindung; wenn mehr als ein Weg zum Ziel vorhanden ist, so wird der Optimale (kann nach verschd. Kriterien entschieden werden) in die Routing Tabelle eingetragen.

Connection oriented services: Routing Tabellen werden verwendet um die Einträge in die Switching Tabellen zu generieren, darum werden sie nur für den Verbindungsaufbau benötigt, danach werden die SW Tabellen benutzt.

Datagram Services:

CL Services (Datagram Services): mittels Routing Tabellen wird die Weiterleitung jedes einzelnen Paketes , unabhängig von den vorangegangenen, realisiert -> es kann passieren, dass die Pakete außerhalb der Reihenfolge ankommen, da im Falle von Änderungen der Auslastung einzelner Leitungen eine andere Routing Entscheidung getroffen werden kann (immer der beste Weg). Die Pakete werden also gesendet ohne eine logische Verbindung aufzubauen -> haben auch keine Sequenznummer; Jedes Paket muss die vollständige Adressinfo beinhalten (Source und Destination). Pakete können auch verworfen werden, im Falle von Netzwerküberflutungen und Übertragungsfehlern.

Nachteile: Um Error Recovery (erneutes Senden im Falle eines Fehlers, verwerfen von Duplikaten) müssen sich die Endgeräte selbst kümmern und auch darum, dass die richtige Reihenfolge der Pakete eingehalten wird. Eine vorsorgliche Art des Flow Control ist nicht möglich.

Vorteile: kleiner Protokoll overhead (leicht zu implementieren); schnellstmögliche Übertragung, da keine Verbindung aufgebaut werden muss.

CL deshalb, weil keine Reservierung von Ressourcen (Bandbreite, Bufferspeicher) möglich ist;

Best Effort (größte Anstrengung): der Transport von Paketen hängt von den verfügbaren Ressourcen ab.

Inkonsistente Routing Tabellen könnten dazu führen, dass Pakete ewig im Kreis wandern und dadurch das Netzwerk lahm legen -> Mechanismen die das verhindern: TTL, hop count;

Technologien: IP, IPX, Appletalk,...

19) Erklären Sie allgemein das Prinzip der Paketvermittlung (packet switching). Welches Zeitmultiplexverfahren liegt zu Grunde? Was sind Routingtabellen und wie können diese erstellt werden? Welche Funktionen spielt die Adressierung in diesem Zusammenhang? Erklären Sie den Virtual Call-Dienst im Detail. Welche Dienstart (service) liegt zu Grunde? Wie werden dabei Pakete weitergeleitet? Welche Aufgaben haben dabei Routingtabellen? Was sind Switching Tabellen, wie werden diese erstellt und wozu dienen sie? Geben Sie Vor- und Nachteile dieser Methode an. Welche Netzwerktechnologien beruhen auf diesem Verfahren? [120 Punkte]

Allgemein siehe letzte Frage

Virtual Call Dienst ist Packet Switching (OSI Layer 3 mit strukturierten Adressen) im connectionoriented Service Mode. (Anmerkung: Prinzip von Packet Switching ist hier an dieser Stelle nicht zu beantworten, weil das Thema der Frage 20 ist). Endgeräte, die kommunizieren möchten, müssen zunächst eine logische Verbindung aufbauen, bevor Datenpakete übertragen werden können. Der Verbindungsaufbau erfolgt durch Weiterleitung von speziellen Call-Setup Paketen mittels der auch in diesem Mode vorhandenen Routingtabellen (Wegweiser für strukturierte Zieladressen). Beim Weiterleiten der Call-Setup Pakete werden allerdings zusätzlich noch Switchingtabellen aufgebaut, die dann das Weiterleiten der Datenpakete nach erfolgreichem Verbindungsaufbau bewerkstelligen. Call-Setup Paketen enthalten die vollständige, strukturierte Adresse und zusätzlich noch einen lokalen Connection-Identifizier (entspricht der Portnummer bei asynchronem TDM). Dieser ist jeweils nur auf einer Teilstrecke eindeutig und dient zur Unterscheidung der über diese Teilstrecke gelegten Verbindungen (Multiplexing mehrere Virtual Circuit möglich). Beim Weiterleiten wird ein Mapping des ankommenden Connection-Identifiziers zum abgehenden Connection-Identifizier in der Switching-Tabelle festgehalten. Datenpakete enthalten nur noch den lokalen Connection-Identifizier (aber keine komplette strukturierte Adresse), wobei sich der Connection-Identifizier von Teilstrecke zu Teilstrecke gemäß der Switchingtabellen ändert. Durch den Verbindungsaufbau wird quasi die Spur markiert, welche die Set-Up Pakete genommen haben. Die Spur ist in den Switchingtabellen festgehalten. Die Verbindung kommt zustande, wenn der gewünschte Teilnehmer den Verbindungsaufbau akzeptiert und bestätigt. Datenpakete folgen dieser Spur, das heißt die Pfadauswahl findet nur beim Verbindungsaufbau einmal statt, danach wird dieser Pfad für die weiter Übertragung beibehalten. Fällt also eine benutzte Trunk Leitung oder ein Switch aus, so wird die Verbindung unterbrochen und muss wieder neu aufgebaut werden, falls ein redundanter Pfad vorhanden ist, können die Packet Switches auch auf diesen ausweichen. Damit ist auch sichergestellt, dass die Pakete in der gleichen Reihenfolge wie beim Absenden beim Ziel ankommen (man nennt das Sequencing, die Sequenz wird eingehalten). Endsysteme selbst sehen nach erfolgreichem Verbindungsaufbau nur noch einen „point-to-point circuit“ (physikalischen Link), der durch die Connection-Identifizier am Anfang und Ende gegeben ist. Sie sehen quasi eine - durch diese Connection- Identifizier adressierbare - Transport-Röhre (pipe). Die eindeutigen Adressen sind deshalb während der Übertragung nicht mehr nötig, tatsächlich werden auch nur noch die Identifizier verwendet. Man spricht daher vom virtual (scheinbaren) circuit, weil natürlich tatsächlich Pakete von Hop-to-Hop über klassisches Store and Forward weitergeleitet werden. Durch Aufbau mehrerer virtual circuits kann ein Endsystem natürlich auch mehrere Verbindungen gleichzeitig unterhalten. Hierfür sind die Connection Identifizier die Basis; Sie dienen also dazu, mehrere verschiedene virtuelle Verbindungen über eine physikalische Leitung unterscheiden zu können. Nach erfolgreicher Abwicklung der gesamten Übertragung werden Verbindungen üblicherweise wieder abgebaut. Ein Provider kann basierend auf dieser Technik entweder ein SVC (Switched Virtual Circuit) Service - mit Circuits on Demand wie oben geschildert – anbieten oder ein PVC (Permanent Virtual Circuit) quasi als Standleitungersatz. Beim PVC fällt der Verbindungsaufbau und Abbau weg, weil die Switching Tabellen permanent vom Provider eingerichtet sind und diese Verbindungen permanent vorhanden sind. Daten-Pakete werden wie gewohnt mittels Switching Tabellen anhand des lokalen Connection Identifizier weitergeleitet.

Vorteile: Durch die Existenz einer Verbindung ist Ressourcenreservierung (Bandbreite, Bufferspeicher,...) für eine Verbindung möglich; Flow Control zur Verhinderung von Staus im Netzwerk ist möglich; kann Quality of Service anbieten, dadurch dass die nötigen Ressourcen schon beim Verbindungsaufbau reserviert werden können; Ablehnung einer Verbindung bei Nicht-Vorhandensein der gewünschten QoS ist möglich; Error Recovery ist möglich.

Nachteile: Verbindungsaufbau kostet Zeit; Implementierungsaufwand sehr groß; komplexe Protokolle

Beispiele für connection-oriented Packet Switching:

X.25: Local Connection Identifier = LCN (Logical Channel Number); zuverlässige Transportröhre durch Protokollunabhängige Error Recovery auf jeder Teilstrecke (durch Bitfehler oder Stau verloren gegangene Pakete werden netzintern durch ARQ Techniken wiederholt); Flow Control durchsetzbar; inband signaling (Call-Setup Pakete fließen in der selben Röhre wie Datenpakete); Pakete variabler Länge

Frame Relay: Local Connection Identifier = DLCI (Data Link Connection Identifier); unzuverlässig da kein Error Recovery ; Flow Control durch Congestion Indication ersetzt und daher andere Maßnahmen zur Sicherung des Netzes erforderlich (Traffic Contract, Traffic Policing, Traffic Shapping); outband signaling (Call-Setup Pakete fließen in einer separaten Röhre); Pakete variabler Länge

ATM (Asynchronous Transfer Mode): Local Connection Identifier = VPI/VCI (Virtual Path Identifier / Virtual Channel Identifier); wie frame relay jedoch Pakete mit konstanter Länge; outband signaling (Call-Setup Pakete fließen in einer separaten Röhre); Pakete konstanter Länge -> Zellen genannt (cell = 53Byte) -> Cell Switch

20) Was sind die grundlegenden Charakteristiken von LANs? Welche OSI Schichten sind für eine Kommunikation innerhalb eines LANs notwendig? Warum ist bei LANs eine Aufteilung der OSI Schicht 2 in zwei Subschichten LLC und MAC notwendig? Erklären Sie kurz die Funktion von LLC (prinzipielle Dienstarten, Funktion DSAP, SSAP) Was sind MAC Adressen und wie erfolgt die Handhabung von Rahmen beim Empfang? [80 Punkte]

In einem LAN (Local Area Network) greifen alle Geräte auf ein Medium (Kabel, shared media) zu. Die Ausdehnung des Netzes ist beschränkt (bis zu einigen km). Alle Geräte sind gleichberechtigt (keine Masters / Slaves) und können beliebig untereinander kommunizieren. Es ist für high speed Kommunikation gedacht, heute sind Datenraten bis zu 1Gbit/s möglich. Ein LAN weist ein Broadcast Verhalten auf, das heißt jeder Rechner „hört“ alles mit, was ein anderer Rechner sendet, wenn keine aktiven Netzkomponenten vorhanden sind, die den Netzverkehr regulieren. Eine solche Art von Netz nennt man auch diffuses Netz (vgl. Radio). Für den Zugriff auf die Multipoint Leitung ist ein Zugriffsmechanismus nötig -> Media Access Control; auch eine Adressierung ist nötig: MAC Adresse – unstrukturiert (jede Station hat eine individuelle). Es werden keine Netzwerkkomponenten mit Store-and-Foreward oder Routing benötigt. Es sind verschiedene Topologien wie Bus, Stern oder Ring möglich.

Für die Kommunikation in einem LAN sind die OSI Schichten 1 und 2 zuständig.

Jeder Rechner auf einem LAN erhält jedes Paket, das über das Kabel läuft, jedoch nur der Rechner mit der entsprechenden Ziel MAC Adresse leitet die Daten auch wirklich weiter an die oberen Schichten des OSI Modells. Die anderen Pakete werden direkt von der NIC verworfen. Ein LAN verwendet auch Broadcast – Adressen, das sind Adressen, die von vielen bis hin zu allen Geräten auf einem LAN akzeptiert werden (Globaler Broadcast, Gruppenbroadcast). Broadcasting wird für die Initialisierungsphase genutzt.

OSI Layer 2 ist eigentlich nur vorgesehen für Punkt zu Punkt Verbindungen, deshalb wurde er von der IEEE aufgesplittet in die beiden Subschichten LLC und MAC;

MAC regelt den Zugriff auf das geteilte Medium (verhindert Datenkollisionen, garantiert für Fairness im Netz, behandelt Prioritätsframes), Framing, Adressierung und Fehlererkennung und war bei OSI ursprünglich nicht vorgesehen.

LLC umfasst die eigentlichen Aufgaben des Data Link Layers und stellt die Verbindung der Endsysteme untereinander (Verbindungslos, Verbindungsorientiert) und Service Access Points (SAPs) für die höheren Schichten zur Verfügung. Der LLC Header stellt das Bindeglied zwischen dem Sublayer MAC und dem Layer 3 dar.

Jeder Datenblock wird in ein LAN Frame eingebunden, das aus dem MAC Header gefolgt vom LLC Header und anschließend dem MAC Trailer besteht (MAC Header und Trailer sind LAN spezifisch).

Der LLC Header besteht aus: DSAP (Destination Service Access Point), SSAP (Source Service Access Point) und Control einem Kontrollfeld.

DSAP/SSAP dienen als Kennzeichnung der höheren Protokollprozesse der Ziel- und Absendersysteme. (von 128 individuellen Werten für DSAP/SSAP sind 63 für IEEE-Protokolle reserviert bzw. weiter 63 für herstellerspezifische Protokolle bzw. Applikationen).

LLC spezifiziert 4 Dienstmethoden und zugehörige Protokolle:

(Datagram)	Class 1:	verbindungsloser ungesicherter (unacknowledged, unbestätigter) Dienst
	Class 2:	verbindungsorientierter Betrieb plus Class 1
	Class 3:	Class 1 plus verbindungsloser bestätigter Service
	Class 4:	Class 2 plus verbindungsloser bestätigter Service

Jedes Netzwerkgerät ist mit einer einzigartigen sog. „Burn-In-Adresse“ (BIA) (wird vom Hersteller des Gerätes in einen ROM gebrannt) 48 bit langen MAC-Adresse eindeutig identifiziert. Diese MAC-Adresse wird als Sender-Adresse in den Frames angegeben und dient natürlich auch als Zieladresse.

Es wird von jedem Netzwerkgerät (NIC, Network Interface Card) auf dem Medium immer alle Rahmen empfangen (aufgrund des Broadcast-Verhalten von LANs). Die NIC entscheidet dann anhand der BIA im Empfängernfeld des Rahmens (entweder sie ist gleich der BIA der NIC oder kennzeichnet einen Broadcast), ob dieser stillschweigend verworfen wird, oder an höhere Schichten weitergeleitet wird.

21) Erläutern Sie die ursprüngliche Aspekte des IEEE 802.3 LAN (Ethernet) wie Topologie, Zugriffsverfahren (Media Access Control), (Collision Window / Slot Time) und physikalische Reichweite, minimal und maximale Rahmengröße, anhand der 10Base5 und 10Base2 Techniken. Wie ist ein Ethernet-Rahmen, wie sind MAC Adressen aufgebaut. Was versteht man unter Transceiver (extern/intern)? Was ist ein Repeater bzw. was besagt die Repeater Regel? [90 Punkte]

Ethernet IEEE 802.3 wurde ursprünglich als Bus Topologie basierend auf Koaxkabeln entwickelt. Dabei breitet sich das Signal auf der Leitung in beiden Richtungen aus und wird um Signal Reflexionen zu vermeiden mittels Widerständen an den Enden der Kabel terminiert. Dadurch, dass die Übertragungsleistung der Stationen beschränkt ist, ist die Kabellänge und auch die maximal Anzahl der Stationen beschränkt. Ursprünglich wurden zwei Basisband Übertragungsvarianten mit Manchesterkodierung und eine mit Breitband (Modulation) entwickelt: 10Base5, 10Base2 und 10Broad36; dabei steht 10 für 10 MBit/s, Base bzw. Broad für die Übertragungsmethode (Basisband, Broadband, Narrowband) und die letzte Zahl für den Kabeltyp.

Ethernet ist ein LAN und weißt somit ein Broadcast Verhalten auf, das heißt, dass jeder zu jedem Zeitpunkt Daten auf den Bus legen kann und jeder der an den Bus angeschlossen ist kann diese Daten empfangen. Deshalb ist ein Zugriffsverfahren für den Bus nötig, um zu verhindern, dass zwei oder mehrere Geräte gleichzeitig senden und damit die Daten unbrauchbar werden.

Das verwendete Zugriffsverfahren ist CSMA/CD (Carrier Sense Multiple Access / Collision Detection). Bevor eine Station sendet, horcht sie das Medium ab, ob eine andere Station gerade sendet. Erst wenn das Medium frei von Übertragungen ist, beginnt die Station ihre Daten auf die Leitung zu legen. Wenn zwei Stationen gleichzeitig zu senden beginnen, kommt es zu Kollisionen; diese wird dadurch erkannt, dass der DC Level auf der Leitung überwacht wird und dann das Senden sofort eingestellt. Anschließend wird ein JAM-Signal (32 bit) gesendet, damit jede Station die Kollision registriert und die Ausweitung der Kollision eingegrenzt wird. Ein Zufallsalgorithmus sorgt dafür, dass irgendeine Station wieder zu senden beginnt. Kommt es 16mal hintereinander zu einer Kollision, wird ein Fehler an den höheren Layer gemeldet. Wenn zwei Stationen sehr weit auseinander liegen, deren Signale kollidieren resultiert aus der doppelten Laufzeit (=Kollisionsfenster) eine lange Zeitdauer, in der das Netz nicht genutzt werden kann. Das maximale Kollisionsfenster (Slotzeit) ist auf 51,2 µSec (für 10 MBit/s Ethernet 10Base2 oder 10Base5) festgelegt, wodurch die Ausdehnung eines Netzes beschränkt wird (2500-3000m) und eine minimale Framelänge von 64 Byte fordert.

Die maximale Framelänge ist durch die Forderung der fairness gegenüber den anderen Partnern gegeben (1518Byte).

Nach einer Kollision ergibt sich die Zeit, die die einzelnen Teilnehmern warten, bis sie wieder zu senden beginnen durch: $\text{total delay} = \text{basic delay (slot time)} * \text{random}$; Die Zufallszahl ist dabei eine Zahl zwischen 0 und 2^k wobei k die Anzahl der Sendeversuche, aber nicht größer als 10 ist -> 1024 potentielle Slots -> max. 1024 Stationen;

10Base 2 und 5 arbeiten beide mit Manchesterkodierung und einem DC Level von -40mA; log 1 entspricht 0mA, log 0 -80mA -> senden zwei gleichzeitig ergibt sich ein DC Level der < -40mA ist und damit als Kollision erkannt wird.

Aufbau eines Frames in Ethernet:

- 64 bit Präambel zur Taktsynchronisation
- 48 bit Destination MAC-Adress
- 48 bit Source MAC-Adress
- 16 bit Länge des Datenblocks
- LLC
- ? Payload
- 32 bit Frame Check Sequence

Es gibt jedoch auch noch den Ethernet Version 2 Frame (nicht von IEEE), bei diesem wird das Längen Feld durch ein Typ Feld ersetzt, in dem der Protokolltyp angegeben wird. Damit entfällt der LLC Layer; Beide können auf einer Leitung koexistieren, sind jedoch nicht interoperabel -> die Werte im Typefeld sind stets größer als 1518 damit zwischen beiden unterschieden werden kann;

Zwischen zwei Frames ist standardmäßig ein Gap (Abstand) von 9,6µs;

Aufbau der MAC Adresse:

DA: (48Bit)

I/G: Individual/Group: 0: Einzeladresse; 1: Gruppenbroadcast;

U/L: universal/local: 0: globale Adresse (verwaltet von IEEE); 1: lokal verwaltete Adresse

Bit 45-0: Adresse;

SA: (48Bit): I/G nicht verwendet.

Ein Repeater ist eine aktive Netzwerkkomponente, der den durchgehenden Datenstrom verstärkt, ohne die Daten unnötig lang in einem Buffer zwischenspeichern. Ein Repeater leitet ein ankommendes Signal an alle seine Ports weiter. Die Ausdehnung des Netzes wird dadurch größer, die resultierende Verzögerungszeit ist minimal. Jedoch wird durch einen Repeater eine Kollisionsdomäne (der Bereich der von einer Kollision betroffen ist) vergrößert. Lokale Repeater verbinden dabei direkt zwei LAN Segmente, remote Repeater hingegen verbinden LAN Segmente durch ein sog. Link Segment, über welches die beiden Repeater verbunden sind. Ein aktiver Hub ist ein Multiportrepeater.

Für Netzwerke, die Repeater verwenden, gilt die Repeater-Regel – oder auch 5-4-3 Regel genannt, weil Repeater keine zusätzlichen Filtermechanismen verwenden. Durch Repeater verbundene Segmente bilden eine Kollisionsdomäne, d.h. Kollisionen wirken über Repeater hinweg. Damit nun das Kollisionsfenster von 51,2µs eingehalten wird gelten folgende Repeater regel: maximal 4 Repeater dürfen zu einem Netz zusammengeschlossen werden, wobei nur an 3 der Verbindungsstränge Endgeräte angeschlossen werden dürfen. Die restlichen 2 Verbindungen dienen zum verbinden der Repeatern (maximal 500m). Bei mehr als vier solcher Geräte kann der Abstand zweier Sendeeinheiten so groß werden, dass eine an einer Kollision beteiligte Station nicht merkt, das sie beteiligt ist und auch die Datenpakete nicht neu sendet, was leider zu Datenverlust führt.

Auf 4 Segmenten mit 3 Repeatern darf die Länge der Link Segmente nicht mehr als 1000m betragen.

22) Warum und wie hat sich die Ethernet-Technik von der ursprünglichen Koax-Bus-Technologie weiterentwickelt. Gehen Sie dabei auf Linksegmente, 10BaseT, 10BaseF und Hub ein. Welche Aspekte waren bei der Entwicklung von Fast- und Gigabit-Ethernet zu beachten? Gehen Sie auf die neuen Aspekte wie PCS, MII, GMII 4B5B-Coding, 8B10B-Coding ein. Erläutern Sie die neuen Möglichkeiten wie Fullduplex Operation, Autonegotiation, Flow Control und Trunking. Wodurch wird Gigabit-Ethernet zu einer Quasi-WAN Technologie? [110 Punkte]

Aufgrund der Einschränkungen in der Dimension der Netze und den Übertragungsraten versuchte man relativ bald, diese Netzwerkarchitektur weiter zu verbessern. Hierfür wurden sogenannte Link Segmente eingeführt, die eine Repeater – Repeater Verbindung darstellen. Diese Segmente dienen dazu um die maximale Ausdehnung eines Netzwerkes vergrößern zu können, oder um zwei weiter entfernte Netze miteinander verbinden zu können. Ein solcher Link stellt eine Punkt zu Punkt Verbindung zwischen zwei Repeatern dar, über die die Repeater ihre Daten übertragen. Zur Verbindung diente zu erst FOIRL (Fiber Optic Inter Repeater Link). Dieser erlaubte eine maximale Länge von 1000m und basierte auf Glasfaser. Dies war für die überbrückbaren Distanzen schon eine sehr große Steigerung von 185m (10Base2) bzw. 500m (10Base5) auf über 1000m.

Spätere Verkabelungsstandards (Repeater – Repeater):

10BaseFL (asynchrone Übertragung, 2000m, Glasfaser)

10BaseFB (synchron (idle Signale während Pausen), 2000m)

10BaseFP passiver HUB (nicht elektrisch versorgt -> keine Verstärkung des Signals)

Durch diese Erweiterungen wurden Netzwerkausdehnungen bis hin zu 3000m möglich (Repeater Rules)

Später wurden diese Link Segmente für die Verbindung mehrere Endgeräte zu einem Multiport Repeater verwendet, jede eine eigene Punkt zu Punkt Verbindung. Das war nötig, da ein internationaler Standard zur Gebäudevernetzung basierend auf Twisted Pair und einer Stern-Technologie entwickelt wurde. Außerdem passte es sehr gut für Token Ring Verkablungen -> Überlebensstrategie von Ethernet.

Verkabelungsstandards hierfür:

10BaseT (unshielded twisted pair): max. 100m, 4 Leitungspaare: 2 Transmit, 2 Receive -> RJ45 Stecker, Manchester Kodierung ohne DC Offset -> Kollisionen werden vom HUB entdeckt, falls er zwei oder mehr Signale gleichzeitig empfängt -> JAM Signal (CSMA/CD in a Box); während Pausen: LTP (periodischer Link Test Puls) wird von den LAN Geräten gesendet; kein Signal -> keine Verbindung; dient für: Repeater – Repeater, End System - Multiport Repeater, End System – End System über Cross Over Kabel;

Auch 10BaseFL wird für End System - Multiport Repeater verwendet;

Ein Multiport Repeater in einer Sternentypigen Topologie wird HUB genannt; es ist dadurch auch möglich verschiedene Medien über einen HUB miteinander zu verbinden (Fiber, Kupfer);

Bilder zu Verkabelungen siehe Seite 07-18;

Bei einem Repeater Netzwerk handelt es sich noch immer um eine Kollisionsdomäne -> es wurden Bridges (store and forward devices) eingeführt, die eine Aufteilung des Netzwerkes in mehrere Kollisionsdomänen gestatten, dadurch dass sie nur Frames an andere Ports weiterleiten, für die dieser auch gedacht ist (Entscheidung basiert auf MAC Adresse, unstrukturierte eindeutige Adresse); ein solches Netzwerk beinhaltet keine Strukturinformation und ist noch immer eine Broadcastdomäne;

Deshalb wurden Router entwickelt, die ihre Forwarding Entscheidungen basierend auf strukturierten Layer3 Adressen treffen -> Aufteilung in mehrere Broadcastdomänen da Router nur Daten weiter leitet die an seine MAC gerichtet sind.

Die neueste Version von IEEE 802.3 spezifiziert Ethernet mit Geschwindigkeiten von 10,100 und 1000MBit/s, Full Duplex Betrieb, Auto Negotiation und Flow Control; neue Versionen wurden immer so entwickelt, dass sie rückwärts kompatibel zu älteren Versionen sind -> auch CSMA/CD (halb duplex) mit Multiportrepeatern ist noch möglich;

Full Duplex:

Mit Hilfe von Multiport Switches (fast transparent Bridges, implementiert in HW) wurde Full Duplex Kommunikation auf Punkt zu Punkt Leitungen ermöglicht -> CSMA/CD wurde überflüssig -> HUB wurden durch Switches ersetzt -> kollisionsfreies Ethernet in einer Sterntopologie. Auch für Punkt zu Punktverbindungen von Endsystemen ist CSMA/CD überflüssig;

Sehr schnelle Switches wurden nötig, Bufferoverflows waren jedoch trotzdem nicht zu vermeiden -> Flow Control wurde nötig -> MAC Control Frame wurde eingeführt (Identifiziert dadurch, dass das Längengeld des MAC Frames auf 8808hex gesetzt wird);

Flow Control:

MAC – Control Frame mit Pause Kommando wird übertragen -> Sender stoppt Übertragung für eine gewisse im Frame angegebene Zeit, oder bis ein Pause Kommando mit Zeit = 0 empfangen wird;

Autonegotiation:

Zwei Geräte können Informationen über ihre Eigenschaften austauschen (Signalrate, CSMA/CD oder Full Duplex) -> hierfür werden die NLP (normal Link pulses) von 10BaseT verwendet -> bei 100BaseTX werden FLP (fast link pulses) verwendet, das sind 33 NLPs (in der Zeit wo normal nur einer übertragen wird) wobei 16 Bit an Daten übertragen werden -> mit diesen werden die Eigenschaften der Endgeräte signalisiert; werden nur beim Verbindungsaufbau übertragen; alte Geräte werden dadurch erkannt, dass sie nur einzelne NLPs übertragen; -> automatische Konfiguration der optimalen Einstellungen;

Trunking:

Auf Trunkleitungen zwischen multiport switches ist Full Duplex Übertragung möglich -> 200MBit oder 2GBit;

Der neue Hardwaremäßige Aufbau äußert sich natürlich im Physikalischen Layer und dessen Sublayers. Das Codieren erledigt der medienabhängige Physical Coding Sublayer (PCS). Um aber das Codieren (aufgrund der verschiedenen LAN-Technologien) medienunabhängig zu machen ist vor dem PCS das Media Independent Interface (MII). Dient als Interface zwischen MAC Layer und Physikal Layer; unterstützt alle Datenraten; Für Gigabit LAN gibt es statt dem MII das Gigabit Media Independent Interface (GMII). Zusätzlich werden von der PCS entweder 4 Bits oder 8 Bits von der MII in 5 oder 10 Bits codiert (4B5B bzw. 8B10B-Block Encoding, bei Gigabit LAN). Hierbei wird jeder 4 Bit Codegruppe eine 5 Bit Codegruppe zugeordnet. Einige Codegruppen dienen zur Signalisierung, alle anderen möglichen sind ungültig, was zu einer sehr einfachen Fehlererkennung führt. In den verwendeten Gruppen ist die maximale Anzahl von Nullen und Einsen so gewählt, dass der Gleichanteil unter 10% bleibt (8B10B ist der DC-Anteil noch viel geringer). Übertragung erfolgt mittels NRZI; Effizienz: $4/5 = 80\%$;

Der PMD (physical medium dependent) Layer wurde auch hinzugefügt, der die unterschiedl. Stecker spezifiziert.

Diese Erweiterungen wurden so durchgeführt, dass sie noch immer rückwärts kompatibel zu alten Technologien sind.

Heutige Point-to-Point-Full-Duplex-Leitungen (die nicht mehr durch CSMA/CD in ihrer Länge eingeschränkt sind) des Gigabit Ethernet, die bis zu 70 km Länge (mit Glasfaser) erreichen können, und der Trend hin zum Layer 3 Switching (ermöglicht load balancing) sorgen dafür das Gigabit Ethernet immer mehr einer WAN-Technologie gleicht.

23) Erklären Sie die prinzipielle Methode des Bridgings und des Routings. Auf welchem Layer des OSI Modells, mit welchen Adressen arbeitet Bridging? Auf welchem Layer des OSI Modells, mit welchen Adressen arbeitet Routing? Erläutern Sie die Funktionsweise einer Transparenten Brücke im Detail (3 Entscheidungen bezüglich Weiterleiten von Rahmen, Aging, ohne Betrachtung der Spanning Tree Methode). Geben Sie Vor und Nachteile von Bridging bzw. Routing an. [110 Punkte]

Die Aufteilung eines Netzwerkes kann mit Hilfe von Paket Switches erledigt werden (store and forward Prinzip – Zwischenbufferung); Einen solchen Packet Switch der auf Layer 2 des OSI Modells implementiert ist nennt man Bridge. Oberhalb der Schicht 2b (LLC-Schicht und höher) sind die Brücken für alle Transportprotokolle unsichtbar (Protokolltransparenz). Die Weiterleitung von Paketen basiert dabei auf der unstrukturierten aber eindeutigen MAC Adresse. Dadurch wird ein Netzwerk zwar in mehrere Kollisionsdomänen (auf Grund des store and forward Verhaltens) aufgeteilt, es bleibt aber noch immer eine einzige Broadcast Domäne. Man unterscheidet zwischen transparentem und source route bridging. Bei letzterem wird der Pfad vom Endgerät bereits ermittelt – mehr Overhead, jedoch sind die Bridges weniger komplex.

Ein Router hingegen ist ein Packet Switch, der auf OSI Layer 3 implementiert wurde und damit mit strukturierten Layer 3 Adressen arbeitet. Er unterteilt ein Netzwerk auch in mehrere Broadcastdomänen, dadurch, dass er nur diejenigen Pakete weiterleitet, die an seine MAC Adresse gerichtet sind. Ein Router ist nicht Protokolltransparent, das heißt die End Systeme müssen dieselbe Sprache wie er sprechen. Um die Adressen zu verwalten, benutzt der Router – genauso wie einige Bridges – Tabellen, die Angaben über die Adresse des jeweiligen Zielnetzes, die Anzahl der zu durchlaufenden Router (Hops), das nächste zu wählende Teilnetz speichern. Ein Router speichert nur die Adressen von ganzen Subnetzen im Gegensatz zu einer Bridge die alle Adressen der Teilnehmer speichert.

Eine transparente Brücke ist für die Endknoten nicht sichtbar. Die forwarding Entscheidungen trifft sie an Hand der Layer 2 MAC Adresse des Ziels. Sie arbeitet mit einer Tabelle, die den Adressen der Endknoten die jeweiligen Brückenports zuordnet. Anhand dieser Tabelle – die vom Netzwerkadministrator statisch angelegt werden kann oder dynamisch über einen Selbstlernmechanismus angelegt wird – kann eine Bridge erkennen, wo – relativ zu ihr gesehen –, an welchen Ports die kommunizierenden Stationen liegen. Diese Tabelle wird, falls dynamisch, permanent aktualisiert (keine Alterung). Dieser Mechanismus erlaubt es, dass Teilnehmer ihre Standorte wechseln, ohne eine neue Adresse erhalten zu müssen. Erhält ein Teilnehmer für längere Zeit keine Nachrichten, so wird dessen Adresse aus der Tabelle entfernt (Aging). Eine Bridge muss jedes Frame auf einem Netzwerk erhalten und bearbeiten. Dadurch dass sie von den Endgeräten nicht gesehen wird ist auch keine Flow Control möglich.

Ist die Adresse am gleichen Segment, von dem der Rahmen kommt, wird der Rahmen nicht weitergeleitet. Er wird verworfen – FILTERING. Ist die Adresse an einem anderen Port als der erhaltene Rahmen, wird in diese Richtung ein Duplikat weitergeleitet – FORWARDING. Ist die Adresse gänzlich unbekannt (kein Eintrag in der Tabelle), wird der Rahmen an alle anderen Ports weitergeleitet – FLOODING. Dieses Flooding wird deshalb vor allem zu Beginn der Netzwerklebenszeit benötigt (siehe Biler 08.8), da dann noch keine Adressen bekannt sind und die Bridges erst „lernen“ müssen. Zwischen zwei Endgeräten in, über eine Bridge gekoppelten Netzen darf immer nur ein eindeutiger Weg existieren, da es sonst passieren kann bei inkonsistenten Tabellen, dass Pakete ewig im Kreis wandern und zu Bufferoverflows führen. Der Nachteil dabei ist, dass kein load balancing möglich ist und beim Ausfall eines Pfades ein statisches Netz so lange still steht, bis der Administrator es für einen redundanten Pfad umkonfiguriert hat. Im Falle von mehreren Bridges in einem Netzwerk, kann es zu einem Problem kommen. Broadcasts werden von beiden Bridges verdoppelt und kreisen dann – nachdem Broadcasts meistens an sehr viele oder alle Teilnehmer im Netz gehen – im Netz, wo sie immer wieder verdoppelt werden. Ein solcher Broadcast Storm kann ein ganzes Netz lahm legen.

Vorteile Bridge:

braucht nur die MAC Adresse, ist unsichtbar, schneller da HW und keine Adressauflösung nötig, Standortwechsel eines Teilnehmers möglich;

Vorteile Router:

Bearbeitet nur an ihn gerichtete Frames, Anzahl Tabelleneinträge = Anzahl der Subnets, load balance möglich, flow control möglich, broad- und multicasts gelangen nicht ins WAN, kennt die besten Wege;

Nachteile Bridge:

Muss jeden Frame bearbeiten, Anzahl Einträge = Anzahl Endgeräte, kein load balancing, kein flow control, LAN/WAN Kopplung auf Grund Broadcastverhalten nicht möglich;

Nachteile Router:

Strukturierte Adresse (muss konfiguriert werden), langsamer, Standortwechsel erfordert Adressanpassung, default router für Endsysteme nötig;

24) Was versteht man unter Broadcast Storm im Zusammenhang mit „Transparent Bridging“? Wie wird er verhindert? Erklären Sie Aufgabe und Funktionsweise der Spanning Tree Methode im Detail. [110 Punkte]

Ein Broadcast ist eine Rundsendung von einer Station an alle anderen. Unter einem Broadcaststorm versteht man eine Situation, wenn ein mittels Bridges aufgebautes Netz durch einen oder mehrere Broadcasts auf Grund von Konfigurationsfehlern lahm gelegt wird. Dies geschieht folgendermaßen:

Eine Brücke unterteilt ein Netzwerk nicht in mehrere Broadcast Domänen, das heißt ein Broadcast wird an alle Ports weitergeleitet. Existieren nun in einem Netzwerk zwei durch Bridges gebildete parallele Pfade, so wird ein Broadcast von beiden Bridges weitergeleitet, und gelangt somit über zwei Wege auf das andere LAN Segment. Dort sendet jede Bridge denn Broadcast an alle Teilnehmer und natürlich auch an die andere Bridge, wodurch der Broadcast wieder ins ursprüngliche Segment über wiederum zwei Wege zurückgeführt wird. So zirkuliert dieser Broadcast so lange im Netz, bis alle Buffer der Bridges überfüllt und das Netzwerk dadurch lahm gelegt wird. Dieser Storm muss verhindert werden, in dem immer nur genau ein Pfad von einem Segment in ein anderes führt. Das kann vom Administrator erledigt werden, oder es kümmert sich ein spezieller Mechanismus darum, dass Spanning Tree Protokoll (STP).

Spanning-Tree ist ein Verfahren zur Schleifenunterdrückung in brückengekoppelten Netzwerken. Bei diesem Verfahren werden physikalisch redundante Netzwerkstrukturen ermittelt und in einer zyklenfreien Struktur abgebildet. Diese Maßnahme reduziert die aktiven Verbindungswege einer beliebig vermaschten Netzwerkstruktur zu einer Baumtopologie (daher die Bezeichnung Spanning Tree, SPT). Mathematisch betrachtet ist eine Baumstruktur so geartet, dass alle vernetzten Punkte nur durch einen Weg miteinander verbunden sind. Bei einem Ausfall einer Verbindung wird, falls vorhanden, auf einen redundanten Pfad umgeschaltet. Das heißt, dass die Eindeutigkeit der Wege erhalten bleibt. Außerdem sind alle vernetzten Punkte von allen anderen vernetzten Punkten aus erreichbar.

SPT ist mit Hilfe eines speziellen Protokolls für Bridges realisiert, dass Bridge Protocol Data Units (BPDU) Pakete mit MAC multicast Adressen verwendet.

Parameter für das STP:

Bridge Identifier: jede Bridge bekommt eine Nummer die sog. Bridge ID zugeordnet. Diese Nummer ist eine Kombination aus MAC Adresse und Prioritätsnummer, meist wird die kleinste MAC Adresse aller Ports verwendet. Die Prioritätsnummer kann vom Administrator zugewiesen werden (default 32768). Die Bridge mit der kleinsten ID hat die höchste Priorität -> bei defaults die mit der kleinsten MAC.

Port Cost:

Dient dazu, um festzulegen, welche Leitungen bevorzugt benutzt werden sollen, in dem man jedem Port gewisse Kosten zuordnet. Der Pfad mit den geringsten Kosten zwischen zwei Geräten wird dann benutzt. Default: Kosten = 1000 / Übertragungsrate in MBit/s (100 für 10MBit Ethernet). Sie können wieder vom Administrator festgelegt werden.

Port Identifier:

Kombination aus Port MAC und Prioritätsnummer (von Administrator konfiguriert).

Der STP Algorithmus läuft so ab:

- **Auswählen der Root Bridge (Über Bridge Identifier -> kleinste ID, Root Bridge):**

Mittels BPDUs teilen sich die Bridges mit welche Bridge momentan als Root Bridge angesehen wird und welche Pfadkosten zu dieser existieren; außerdem übertragen sie ihre eigene ID und die Port ID; Die Bridge mit der kleinsten ID wird dann zur RootBridge; danach wird die Übertragung von BPDUs nur noch von dieser getriggert.

Strategie: erhält eine Bridge eine BPDU mit geringerer Root Bridge ID als der eigenen, sendet sie auf diesem Port keine BPDUs mehr, auf den anderen Ports sendet sie das angepasste Strategie: erhält eine Bridge eine BPDU mit geringerer Root Bridge ID als der eigenen, sendet sie auf diesem Port keine BPDUs mehr, das angepasste BPDU sendet sie auf den anderen Ports aus;

Erhält sie eine BPDU mit einer höheren ID so sendet sie ihre eigene weiter; die anderen Brücken sollten dann aufgeben;

- **Auswählen der Root Ports (Über Berechnung des kürzesten/besten Weges jeder Bridge zur Root Bridge über Port Costs – Root Path Costs = Summe aller Pfadkosten von dieser Bridge zur RB; der Port mit den geringsten Kosten wird zum Root Port, bei gleichen Kosten der mit der geringeren ID)**

- **Auswahl einer Bridge für jedes LAN Segment** (Port zum LAN-Seg heißt dann Designated Port; wieder über Pfadkosten, die Bridge mit den geringeren Kosten gewinnt)
- Root Ports und Designated Port aktivieren, alle anderen deaktivieren...
- dadurch ist ein einzelner Pfad von Root (Wurzel, Root Bridge) zu den Leaves (Blätter, LAN Segmente) erzeugt.

Fehlererkennung:

Die RB erzeugt alle 1-10sec eine BPDU Nachricht (Art Hello Msg.) die an alle Root und designated Ports versandt wird. Auch alle anderen, geblockten Ports hören diese Nachrichten. Fallen diese aus, so ist entweder die RB (neue wird ausgewählt) ausgefallen oder eine designated (falls ein redundanter Pfad vorhanden ist wird auf diesen umgeschaltet).

Der größte Nachteil der Spanning Tree Methode ist, dass kein load Balancing möglich ist, da immer nur ein Pfad freigeschaltet ist.

25) Was versteht man unter Collision Domain und Broadcast Domain im Zusammenhang mit Ethernet und Transparent Bridging? Was ist L2 Switching (Ethernet Switching)? Was sind VLANs? Was ist Tagging? Zeigen Sie kurz den Wandel auf, den gebridgede LANs durch die neuen Technologien Fast Ethernet, Gigabit Ethernet genommen haben. [90 Punkte]

Unter einer Kollisionsdomäne versteht man den Bereich eines LANs in dem Datenkollisionen auftreten können, die durch zwei oder mehrere Teilnehmer auftreten können, wenn diese gleichzeitig Daten senden. Repeater (die simple Verstärker sind und somit jedes Signal das sie erhalten an jeden ihrer Ports ausgeben), die LAN-Segmente mithilfe von Link-Segmenten oder direkt verbinden können, fügen diese zu einer Collision Domain zusammen, das heißt der Bereich in dem Kollisionen auftreten können wird vergrößert.

Unter einer Broadcast Domäne versteht man den Bereich eines LANs, in dem ein Broadcast an alle Teilnehmer weitergeleitet wird.

Bridges trennen ein LAN in mehrere Collision-Domains, da sie nicht nur simple Verstärker sind, sondern Store-and-Foreward betreiben, das heißt nur diejenigen Daten in ein LAN Segment weitersenden, die auch für dieses Segment bestimmt sind (MAC Adresse wird überprüft). Doch bleibt das Netzwerk immer noch eine Broadcast-Domäne, da ein Broadcast in jedes LAN-Segment geflutet wird, weil die Bridges selbst für die Endgeräte unsichtbar sind.

Router teilen das ganze Netzwerk vollkommen, Broadcast wird vom Router nicht weitergeleitet, da er nur solche Pakete weiterleitet, die an seine MAC Adresse adressiert sind.

Ein Ethernet Switch ist eigentlich eine transparente Bridge, die jedoch schneller ist, da sie in der Hardware implementiert ist, Multiple Ports und erweiterte Funktionalität (z.B. VLAN) aufweist. Ethernet Switching ist aber nicht vergleichbar mit WAN Switching (X25 switch)! Ethernet Switches sind natürlich für Ethernet Verkabelungen ausgelegt und für die Ethernetstandards entwickelt.

Die Grundidee hinter VLAN (Virtual LAN) ist eine logische Aufteilung eines hardwaremäßigen 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. Das 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. Heutige Switches sind in der Lage mehrere Netzwerkstationen zu einem VLAN zusammenzufassen, wofür für jedes VLAN eigene bridging/switching Tabellen, Broadcastbehandlung und Spanning Trees (falls das Netzwerk nicht sowieso in Sterntopologie über einen Multiport Switch und somit im Full duplex Betrieb aufgebaut ist) notwendig sind.

Unter einem VLAN versteht man also das Multiplexen verschiedener LANs über dieselbe Infrastruktur.

Stationen werden zu einem VLAN hinzugefügt entweder Port basiert -> jedes Port wird einem VLAN zugeordnet (kann nur einem VLAN angehören), MAC basiert -> jede MAC wird einem VLAN zugeordnet (nur einem) oder Protokoll basiert, z.B.: IP -> VLAN x,... (eine Station kann mehreren VLANs angehören).

Sind solche VLAN verwaltenden Switches über Trunkleitungen verbunden, so muss bei Datenverkehr über diese Trunks gekennzeichnet werden, zu welchem VLAN die jeweiligen Frames gehören. Dies geschieht mittels Tagging: die Frames werden markiert und können somit dem VLAN zugeordnet werden. Dies geschieht über 4 zusätzliche Byte im Frameheader;

Um trotzdem Datenaustausch zwischen verschiedenen VLANs zu realisieren werden Router benötigt, die ja nicht auf den Layer 2 Protokollen und Adressen basieren und somit Daten beliebig austauschen können -> hierfür müssen sie jedoch auch in der Lage sein, tagged Frames zu erkennen und zu modifizieren. (Bilder siehe 09-14 ff).

Wandel:

Ursprünglich verbanden Bridges zwei oder mehrere Netzwerkbusse miteinander. Dadurch wurden zwar die Kollisionsdomänen verkleinert (im Gegensatz zu einem einzigen Bus) das Netzwerk blieb jedoch noch immer eine einzige Broadcastdomäne. Die Netzwerkbusse wurden im halb duplex Modus mit CSMA/CD betrieben.

Mit Einführung der neuen Ethernet Standards Fast und Gigabitethernet war es möglich Punkt zu Punkt Verbindungen im Full Duplex Mode betreiben zu können und dadurch viel höhere Geschwindigkeiten zu erreichen. Außerdem wurde die Kollisionserkennung und damit CSMA/CD überflüssig. Ethernet Switches erlauben somit auch Full Duplex Betrieb auf Punkt zu Punkt Verbindungen -> dadurch verdrängen sie Hubs, da sie keine Kollisionserkennung brauchen. Die Netzwerktopologien haben sich dadurch vom Netzwerkbus zur Sterntopologie (jedes Endsystem über eigene Punkt zu Punkt Verbindung mit Switch verbunden) hin gewandelt und es ist dadurch ein Kollisionsfreies Ethernet entstanden (siehe Bilder 09-6). Dadurch wurden die Längenbeschränkungen von Kabeln überflüssig und heute sind mit Glasfaser bis zu 70km möglich bei 1Gbit/s -> Ethernet wird zur WAN Technologie.

26) Was passiert wenn folgende Endgeräte (auf LAN1 Host A mit MAC A und HOST C mit MAC C, auf LAN2 Host B mit MAC B und auf LAN3 HOST D mit MAC D) erstmalig miteinander kommunizieren. LAN1, LAN2 und LAN3 sind über einen Ethernetbridge EB (Port 1 zu LAN1, Port 2 zu LAN2, Port 3 zu LAN3) verbunden. Sie können davon ausgehen, dass Spanning Tree bereits eingeschwenkt ist und die Bridging Tabelle zu Beginn noch leer ist. Schildern sie die funktionsabläufe der EB an Hand der ersten sechs Rahmen, die zeitlich folgendermaßen erscheinen: A nach B, B nach A, C nach A, B nach D, D nach B, C nach A. [90 Punkte]

siehe auch 8.07

Host A sendet ein Datenpaket über LAN 1 mit SA=MAC A und DA=MAC B in sein Netzwerk. Host B befindet sich nicht auf demselben LAN Segment, erhält das Frame somit nicht direkt, Host C hingegen verwirft den Frame. Das Frame wird von der Bridge abgefangen. Diese hat keine Einträge und schreibt sich jetzt auf, dass Host A auf Port 1 erreichbar ist (Lerne A). Weil sie das Ziel B nicht kennt sendet/flutet die Bridge das Datenpaket an alle anderen Ports (Port 2 und 3) weiter (flooding). Host B erkennt auf LAN 2 anhand der DA=MAC B, dass das Datenpaket für ihn bestimmt ist und übernimmt dieses. Auf LAN 3 erkennt Host D, dass das Paket nicht für ihn bestimmt ist und verwirft es somit.

Sendet nun Host B Daten über LAN 2 mit SA=MAC B und DA=MAC A an die Bridge, so schreibt sich die Bridge auf das Host B auf Port 2 erreichbar ist, weil sie diesen noch nicht gekannt hat (Lerne B). Dann schaut die Bridge in der Tabelle nach ob das Datenpaket an einen bereits bekannten Empfänger zu senden ist. Dem ist so da DA=A vorhin schon eingetragen wurde und deswegen leitet die Bridge das Datenpaket über Port 1 an Host A weiter (forwarding). Host A erhält das Paket und Host C verwirft es. LAN 3 erfährt nichts von dieser Übertragung.

Nun sendet Host C einen Frame zu Host A. Dieser befindet sich auf demselben LAN und erhält das Frame somit direkt. Auch die Bridge fängt den Frame auf und sieht, dass sie die SA noch nicht kennt und trägt somit in seine Tabelle ein, dass sich Host C auf Port 1 befindet. Da sich Host A auf demselben Port befindet flutete die Bridge die Daten nicht an die übrigen Ports.

Sendet B Daten nach D mit SA = B und DA = D, so werden diese von der Bridge abgefangen und, da sie D nicht kennt an alle Ports geflutet. Somit erhält D auf LAN3 die Daten, A und C verwerfen sie da die DA nicht mit ihrer Adresse übereinstimmt.

Antwortet nun D B mit SA = D und DA = B, dann lernt die Bridge wo sich Host D befindet (Port 3) und sendet die Daten, da sie bereits einen Eintrag für B besitzt an Port 2 weiter, wo sie Host B erhält.

Nun kennt die Bridge alle Adressen und zugehörigen Ports und wenn nun C noch mal Daten an A sendet, so werden diese von der EB zwar inspiziert jedoch nirgends hin weitergeleitet.

27)Charakterisieren Sie kurz die wesentlichen Eigenschaften des IP Protokolls (Netzwerk Type (Packet oder Circuit Switching)/ Service Type (CO oder CL), beteiligte Komponenten (IP Host, Router), Forwarding Prinzip). Wozu ist eine Begrenzung der Lebensdauer eines IP-Datagramms notwendig, wie wird sie realisiert? Wann wird IP Fragmentierung vorgenommen, wie wird sie realisiert? Wie ist das ToS Feld ursprünglich aufgebaut, wie sieht es heute aus (DSCP) und was könnte damit umgesetzt werden. Über welchen Bereich erstreckt sich die Checksum? [100 Punkte]

IP ist ein auf der Schicht 3 des OSI Modells angesiedeltes Protokoll. Es regelt den Versandt von Daten. Es bietet einen unzuverlässigen, verbindungslosen paketorientierten Datagrammdienst mit Best-Effort-Service. Das IP-Protokoll ist ein schnelles Protokoll, das aber die Reihenfolge und fehlerfreie Übertragung der Datagramme nicht garantiert (das ist Aufgabe höhere Schichten verlegt). Der Transport erfolgt dabei über ein oder mehrere

Zwischennetze zum Empfänger. Die Anzahl der dazwischen liegenden Router ist dabei begrenzt, so dass ein Paket nicht ewig durchs Netzwerk übertragen wird. IP-Datagramme werden in Schicht 2-Frames eingepackt. Dieses Einpacken (Encapsulation) ist eine der wichtigsten Eigenschaften von IP, die Flexibilität und Unabhängigkeit von der physikalischen Schicht sichergestellt. Dadurch wurde IP ein Hardware unabhängiges Protokoll und fand dadurch weite Verbreitung. Bei IP nehmen Host und Router teil am Routingprozess. Der Host ist zuständig im Falle von direktem routing, also dann, wenn sich Source und Destination im selben Netz befinden. Um das indirekte routing kümmert sich der Router. Routing basiert auf Routing Tabellen, in denen alle Wege zu Zieladressen (next Hop, Port,...) gespeichert sind. Es kann entweder statisch (Administrator) oder dynamisch (Routing Protokolle) sein. Die Forwarding Entscheidung wird mit Hilfe der IP Ziel Adresse (einer strukturierten Layer 3 Adresse, 32 Bit) getroffen, dabei folgen die Frames einem durch die Router gegebenen Pfad Hop by Hop. Dabei muss für die physikalische Übertragung jedes mal die MAC Adresse geändert werden (mapping). Die MAC Adressen findet IP mittels des ARP Protokolls (Address Resolution Protokoll). Durch die Router wird immer der beste Pfad zu einem Ziel gefunden. Damit ein Paket nicht endlos im Netz zirkuliert (bei fehlerhaften Routingtabellen) hat es eine vorgegebene Lebenszeit. Diese ist im IP Header im TTL (Time to Life) definiert. Sie wird zu Beginn auf einen Startwert gesetzt (normal 64) und in jedem Router um die Verarbeitungs/Wartezeit reduziert, jedoch zumindest um eins verringert -> dadurch wurde daraus ein Hop Count. Wird sie 0, so wird das Paket verworfen.

Bei Übertragungen zwischen Sender und Empfänger können Datenpakete über Netze geroutet werden, deren maximale Paketlänge geringer ist als die Paketlänge des Frames. Dies ist beispielsweise beim Übergang von Ethernet mit einer Paketlänge von 1512 Bytes zu X.25 mit einer Paketlänge von 512 Bytes der Fall. In einem solchen Fall werden die Datenpakete in Teile zerlegt (fragmentiert) und einzeln über das Netz geschickt. Das Fragmentieren gehört zu den Standardfunktionen des IP Protokolls. Fragmente werden jeweils mit einem vollständigen IP-Header versehen und als unabhängige Datenpakete übertragen. Die Fragmente können unterschiedliche Wege über das Netz nehmen und die Datenstationen in unterschiedlicher Reihenfolge erreichen. Die Datenstation muss in der Lage sein, die Fragmente zu sortieren und diese in der richtigen Reihenfolge an die höhere Protokollschicht zu übergeben. Dies wird durch die Angabe eines Offsets in einem eigenen hierzu vorgesehenen Feld im IP-Header erreicht. Dieser Offset wird gemessen in Vielfachen von 8 Byte (64Bit) und gibt Auskunft darüber wie viele Byte vor dem jeweiligen Fragment noch eingefügt werden müssen. Dadurch müssen die einzelnen Fragmente auch immer eine Länge haben die ein Vielfaches von 64 Bit ist (das letzte nicht). Der Vorgang des Zusammensetzens der einzelnen Datenpakete wird Reassembling genannt. Wenn das erste Paket beim Empfänger ankommt, wird ein Reassembly Timer gestartet, wodurch nicht komplette Datagramme eine beschränkte Lebenszeit erhalten. Sollte ein Datagramm nicht fragmentiert werden dürfen, muss das DF-Bit (don't fragment) im Header auf Eins gesetzt werden. Dann wird es verworfen, falls es fragmentiert werden müsste.

TOS steht für Type of Service. Das TOS-Feld ist ein Datenfeld im IP-Header. Es gibt Auskunft über die Priorität eines Datagramms und dessen bevorzugte Netzwerk Charakteristik (Bandbreite, die Übertragungsgeschwindigkeit oder die Zuverlässigkeit der Übertragung, billige Leitung). Das Feld TOS umfasst 8 Bit. Die ersten 3 Bit stellen die Vorrangsteuerung (Precedence) dar. Mit dieser Vorrangsteuerung können Datagramme mit hoher Dringlichkeit schneller geroutet werden, es gibt also an mit welcher Priorität Datagramme in der Router-Warteschlange behandelt werden. Die folgenden vier Bit (D,T,R und C) dienen dazu um eine Pfadentscheidung zu fällen (D gesetzt: minimum delay, T: max Durchsatz, R: max Zuverlässigkeit, C: minimale Kosten).

Dieses Feld wurde neu definiert zum DSCP Feld (Differentiated Service CodePoint). Es wird benutzt um die Klasse eines flows (Flusses) zu markieren. Unter einem flow versteht man dabei eine Kommunikationsbeziehung (Session) zwischen zwei IP Hosts (Datagramme gekennzeichnet durch selbe Adressen, Protokollnummern und Source und Destination Ports). Es ist sehr wichtig für QoS (Quality of Service). Bietet ein Service Provider Quality of Service in seinem Netz an, so wird diese mit Hilfe des DSCP Feldes angefordert. Für höhere Qualität kann dabei ein Service Provider natürlich mehr Geld verdienen. Damit wäre es zum Beispiel möglich Echtzeit Verkehr wie Sprache und Video über ein Netzwerk zu gewährleisten, indem diese Frames mit höherer Priorität vom Betreiber behandelt werden. Dieses Service, falls es überhaupt implementiert wird, erstreckt sich meist nicht über die Grenzen eines Providers hinweg.

Die Checksum erstreckt sich nur über den Header.

28) Welche Aufgaben und welche Struktur haben IP-Adressen? Was bringt Subnetzadressierung und wie wird sie bewerkstelligt? Was muss in den Endgeräten konfiguriert werden, um IP Kommunikation zu ermöglichen? Welche Sichtweise (lokal oder global) haben die Endgeräte (IP Hosts) dadurch? Was muß in den Routern konfiguriert werden, um IP Kommunikation zu ermöglichen. Welche Sichtweise (lokal oder global) haben die Router (IP Gateways oder IP Router) dadurch? Worauf muss bei der Adressierung in Falle von Classful Routing achten? Welche Möglichkeiten der Adressierung hat man im Falle von Classless Routing (Stichwort VLSM und Supernetting)? [110 Punkte]

IP-Adressen sind 32 Bit lang und werden in gepunkteter, dezimaler Notation geschrieben z.B. 190.145.32.148. Sie identifizieren den Zugang zu einem Netzwerk. Die Grundstruktur setzt sich aus Netzwerknummer (net-id) und Gerätenummer/Hostnummer (host-id) (also ein zwei Level Hierarchie) zusammen. Die net-id muss einzigartig sein,

wenn ein physikalisches Netzwerk mit IP-Hosts mit dem Internet verbunden wird (zugewiesen von der Internet Registry). Host-ids werden vom Netzwerkadministrator vergeben.

Je nach Einsatzgebiet gibt es 5 unterschiedliche IP-Adressklassen:

Die Klassen A, B und C unterscheiden sich durch eine unterschiedliche Länge der Netz- und Nutzeridentifikationsfelder. Bei Klasse A Netzen ist die Net ID 7 Bit lang und die Host ID 24 (126 net-ids, um die 16 Millionen host-ids). Das most-significant-Bit ist dabei immer Null, damit reicht das erste Oktett einer Klasse A Adresse von 1 - 126.

Die Klasse B-Adressen : 14 Bit Net ID, 16 Bit Host ID; Dadurch erhält man maximal 16384 net-ids und 65.534 host-ids. Erstes Oktett von 128-191;

Bei Klasse-C-Adressen. 21 Bit Net ID, 8 Bit Host ID; Man erhält um die 2 Millionen net-ids und 254 host-ids. Die Anfangskombination ist "110" -> erstes Oktett von 192-223.

Klasse-D-Adressen sind für Multicast-Adressen vorbehalten; erstes Oktett 224-239;

Klasse-E -Adressen sind reservierte Adressen für zukünftige experimentelle Anwendungen.

Mit der Einführung von LANs wurde eine dritte Hierarchieebene für Netzwerkadressen nötig, die sog. Subnets. Hierbei werden einige Bits der Host ID für die Subnet ID also zur Unterscheidung von Subnetzen in einem LAN eingesetzt. Diese Bits werden jedoch nur lokal als Subnetz interpretiert, global interessiert nur die Netz ID;

Eine Subnet Mask gibt an welche Bits für die Subnetze verwendet werden, hierbei gilt: alle Bits bei denen die Subnetmask 1 ist repräsentieren den Netzwerk Teil, alle anderen den Host Teil; natürlich Subnet Masken für die Klasse A Netze sind zum Beispiel 255.0.0.0; bei der neuen Notation wird nur noch die Anzahl der Einsen und nicht mehr die gesamte Subnetmask wie früher angegeben werden. Um für eine gewisse Adresse zum Beispiel 172.16.3.144 die Net ID und die Host ID für eine gegebene Subnet Maske (255.255.255.192) zu erhalten, muss die Adresse nur mit der Maske verundet werden, dann erhält man die Net ID (hier 172.16.3.128) die Host ID ergibt sich als Differenz (hier 0.0.0.16);

Um IP verwenden zu können muss jedem Host eine IP Adresse zugewiesen werden, mit der Net ID des jeweiligen Netzes und einer eindeutigen Host ID. Damit kann IP jedoch noch nicht vollständig verwendet werden, es ist nur direktes Routen möglich. Für indirektes Routen muss auch noch die IP Adresse des Default Gateways, also des Routers angegeben werden. Damit hat der Host nur eine sehr beschränkte Sicht auf das Netzwerk. Der Host sieht nur seinen lokalen Teil des Netzwerkes, sein lokales LAN, die ganze Netzwerkhierarchie die dahinter steckt bleibt vor ihm verborgen. Natürlich brauchen die Geräte auch MAC Adressen um die Layer 2 Kommunikation durchführen zu können.

Ein Router kann entweder statisch oder dynamisch konfiguriert sein. Schlussendlich braucht er für die korrekte Funktion auf jeden Fall die Information über alle Netze die an ihn (direkt oder über weitere Router) angeschlossen sind und wie er diese erreichen kann. Ein Router hat mehrere IP Adressen, für jeden seiner Ports eine, die zum jeweiligen Netz passen müssen. Verwendet ein Router statisches Routing, so muss die gesamte Netzwerkinformation durch den Administrator eingetragen werden. Verwendet er hingegen dynamisches Routen, so wird die Netzwerktopologie und auch der jeweils beste Pfad automatisch durch geeignete Routing Protokolle (wie RIP) ermittelt und gespeichert. Somit hat der Router eine ganz andere Sicht auf das Netzwerk, eine globale Sicht. Er sieht zwar auch nicht die gesamte Netzwerktopologie, weiß aber zu welchem Router er als gehen muss um in ein bestimmtes Netz zu gelangen, von dort aus weiß dann wieder der nächste Router weiter.

Bei der Adressierung mit Classfull Routing muss darauf geachtet werden, dass die Subnetz Maske in einer gesamten Domäne gleich ist, da classfull Router Pakete verwerfen, wenn sie deren Subnetz nicht kennen. Das bedeutet, alle Subnetze in einem gegebenen Netz müssen nur durch Netze mit der selben Subnet ID erreichbar sein, da sonst die Router mit der ID nicht umgehen können und das Paket verwerfen.

Im Falle von Classless Routing gibt es diese Einschränkung nicht, da dabei die Routing Protokolle mit Subnetzinformationen umgehen können und diese an zwischen Routern austauschen können. Dadurch kann eben eine Subnet Mask variabler Länge (VLSM – variable length subnet mask) für die einzelnen Subnetze verwendet werden und Router verwerfen die Pakete nicht, da sie die benötigte Subnetinfo besitzen. Damit kann das Subnetting so durchgeführt werden, dass es zur benötigten Anzahl an Host auf einem Subnet passt.

Supernetting ist sozusagen das Gegenteil von Subnetting. Durch Supernetting können IP Bereiche die vorher aufgesplittet wurden wieder zusammengefasst werden. Dies geschieht durch Verkürzung der Netzmaske und hat den Effekt, dass dadurch Einträge in die Routing Tabellen eines Routers wegfallen (man braucht nur mehr die Adresse des Supernetz). Supernetting fasst also durch verkürzen der Netzmaske Netze der gleichen Klasse zu einem Netz zusammen. Ist also ein Netzwerk bestehend aus mehreren zum Beispiel Klasse C Netzen nur über ein Gateway von außen erreichbar, so braucht man in diesem Gateway nur noch eine Adresse die mittels Supernetting gewonnen wurde und die zugehörige Subnetmask und nicht mehr die Einträge aller einzelnen Netze.

29) Was passiert, wenn zwei Endgeräte (Host A mit IP Adresse 10.1.0.1/16 und MAC A auf LAN 1 (IP Subnet 10.1.0.0) und Host B mit IP Adresse 20.2.0.2/16 und MAC B auf LAN 2 (IP Subnet 20.2.0.0)) erstmalig miteinander kommunizieren. LAN 1 und LAN 2 sind über einen Router R (IP Adressen 10.1.0.254 und 20.2.0.254) verbunden (Port 1 mit MAC R führt zu LAN 1 und Port 2 mit MAC U zu LAN 2). Sie können davon ausgehen, dass die Routing Tabelle vollständig ist, aber alle ARP Caches zu Beginn leer sind und kein proxy ARP unterstützt wird. Die Endgeräte haben einen entsprechenden Default Gateway-Eintrag zum Router. Schildern Sie im Detail die Protokollabläufe, die Zustände in den Router und Endsystemen bezüglich ARP Cache, die sich einstellen, wenn zunächst ein IP Rahmen von A und B, dann ein IP Rahmen von B nach A und zuletzt noch ein weiterer Rahmen von A nach B gesendet werden soll. [100 Punkte]

Da die ARP Caches zu Beginn leer sind sendet Host A einen ARP-Request in Form eines MAC broadcast (Ziel: FF, Sender: Macadresse von Host A). Dieser Request enthält auch die Ziel-IP (Default Gateway = Router). Der Router teilt dem Host A seine MAC-Adresse mit (MAC R), welcher dieser sich speichert. Jetzt sendet Host A ein Datenpaket mit der Sender-Adresse 10.1.0.1/16, Destination-Adresse 20.2.0.2/16, MAC-Sender (MAC A) sowie die Empfänger MAC (MAC R). Das Datenpaket geht folglich an den Router. Der Router seinerseits macht nun einen ARP-Request im zweiten Subnetz (20.2.0.0) in Form eines MAC broadcast, sein gesuchtes Ziel ist 20.2.0.2/16. Host B antwortet dem Router, dass die MAC-Adresse von 20.2.0.2/16 MAC Adresse B ist. Jetzt kann der Router das IP Datagramm (IP Sender: 10.1.0.1/16, IP Empfänger: 20.2.0.2/16, MAC-Sender R, MAC-Empfänger: B weiterleiten.

Will nun Host B einen Rahmen zu Host A übertragen, so sendet er wiederum einen ARP-Request, auf diesen antwortet der Router, dass er die Destination kennt. Somit ist eine weitere Übertragung möglich, da beide Hosts über die MAC-Adressen der jeweils anderen Station Bescheid.

30) Wozu dient das ARP-Protokoll? Beschreiben Sie es im Detail. Wann und wie verwendet ein IP Host das ARP Protokoll in normalen Situationen (d.h. kein proxy ARP)? Was ist Proxy ARP und wozu kann es verwendet werden? Wozu dient das ICMP-Protokoll? Wie funktioniert es? Was lässt sich damit signalisieren bzw. realisieren? [100 Punkte]

ARP steht für Adress Resolution Protokoll. Eine IP-Adresse identifiziert den logischen Zugang zu einem IP-Netzwerk, ein Ziel kann ohne weiteres Adressieren nur dann erreicht werden, wenn das physikalische Netzwerk aus einer einzigen Verbindung (Point-to-Point) besteht, in einem LAN werden deswegen MAC-Adressen verwendet, damit Pakete an ein bestimmtes Ziel geliefert werden können. Eine Verbindung zwischen IP-Adresse und MAC-Adresse wird benötigt: das ARP (RFC 826).

Das Mapping zwischen MAC-Adresse und IP-Adresse kann in einem LAN statisch (über Tabelleneinträge) oder dynamisch erfolgen (ARP Protokoll & ARP Cache).

Verwendung von ARP von einem IP-Host (ohne proxy ARP): Möchte ein Host Verbindung zu einem anderen herstellen, fragt das IP bei ARP nach der MAC-Adresse der zugehörigen IP-Adresse an. ARP vergleicht nun seine Mapping-Tabellen (= ARP Tabellen). Gibt es keinen Eintrag (Zuordnung IP-MAC), dann wird ein ARP-Broadcast ausgeschiedt. Ist ein Host unter der gesuchten IP-Adresse vorhanden, antwortet er darauf und schickt seine MAC-Adresse mit. Übertragung kann starten.

Proxy ARP: wurde (und wird noch) dazu verwendet, (2) unterschiedliche Netze über eine einzige netID anzusprechen. Hosts in den unterschiedlichen Netzen wissen nichts über den Proxy-Host, sie glauben sich in einem homogenen Netz zu befinden. Will nun ein Host 1 etwas zu einem andern (in einem anderen Netz befindlichen) Host 2 senden, tritt der Proxy-Host als Host 2 auf (vor Host 1) und sendet die Pakete weiter.

Die proxy-ARP Methode ist veraltet, wurde aus Performancegründen oder aus Sicherheitsgründen (DMZ) eingesetzt. Wird aber auch eingesetzt, wenn ein IP host die Adresse des default gateways kennt. In Unix oder Windows NT/XP wird der default-Gateway über eine Proxy-ARP Erweiterung selbst festgestellt und gesetzt.

ICMP steht für Internet Control Message Protocol. Der Paketdienst (Pakete = Datagramms) von IP garantiert und bestätigt die korrekte Lieferung eines Pakets nicht. ICMP generiert bei Fehlern eine Fehlermeldung um die Zuverlässigkeit zu erhöhen und um Informationen über Fehler oder Packetverluste im Netzwerk bereitzustellen. Mittels von ICMP gelieferten Informationen ist es möglich eine Fehlerursache zu finden. ICMP muss dazu von jeder Station unterstützt werden, wie die Fehlermeldungen gemeldet werden ist kann aber auf Grund von unterschiedlichen Implementierungen sehr verschieden sein.

Arbeitsweise von ICMP: Der IP-Station, welche ein Übertragungsproblem feststellt generiert eine ICMP Message (Ausnahme ist das PING-Paket, wenn es fehlschlägt wird keine ICMP-Nachricht verschickt.). Diese wird an den Versender des Originalen IP Pakets geschickt. Die Nachrichten werden als normale IP-Pakete gesendet (ICMP Code und Header stehen im Daten-Feld). Analysiert nun ein Administrator die Nachricht, kann er dadurch die Fehlerursache finden. Geht allerdings das IP-Paket mit der ICMP-Nachricht verloren wird keine neue Nachricht versendet. Es gibt verschiedene Haupt-ICMP-Codes, welche auch noch einen Unter-ICMP-Code enthalten (Bsp: Code

3 bedeutet Destination nicht erreichbar, ein weiterer Code gibt die mögliche Ursache an, Netzwerk/Protokoll/Host nicht erreichbar etc.).

Aufbau einer ICMP-Nachricht:

- Type: General Message Type
- Code: Detailed Specification
- Checksum: Kalkuliert über ICMP Header und Daten
- Extension Field: Wird für spezielle Messages benutzt
- Internet Header + 64 bits Originales Datagramm

Mit ICMP ist es für Administratoren also möglich, Fehler bei der Übertragung von IP-Paketen zu finden. Weiters kann durch einen ICMP-Code dem Absender auch ein besserer, schnellerer Übertragungsweg mitgeteilt werden.

31) Charakterisieren Sie kurz die grundlegendsten Eigenschaften von TCP. Wozu dienen weiters Portnummern und Sockets beim TCP-Protokoll? Wie werden Ports in Client Server Beziehungen verwendet? Wie wird der Verbindungsaufbau und Verbindungsabbau bei TCP vorgenommen? Wie werden die Sequence- und Acknowledge Nummern verwendet? Welche Rolle haben die Flags. Wie erfolgt Error Recovery? Wie wird die Flußkontrolle bei TCP durchgeführt? Welche Besonderheit gibt es bei Handhabung der Timeouts? Über welchen Bereich erstreckt sich die Checksum? Was ist UDP? [120 Punkte]

TCP steht für Transmission Control Protocol. TCP ist ein verbindungsorientierter Dienst, zuständig für End-to-End Verbindungen, der Verbindungsaufbau erfolgt dabei über einen 3-way handshake.

Die Aufgabe des TCP-Protokolls ist die Adressierung von Diensten der Anwendungsschicht über Port- und Socketnummern. Zusätzlich soll es die Zuverlässigkeit von IP erhöhen. Dazu gibt es Mechanismen wie Erkennung und Korrektur von Fehlern, Flusskontrolle, Neuordnung der Segmente falls die Reihenfolge bei der Übertragung vertauscht wurde, Entfernung von doppelten Segmenten, Dazu werden Mechanismen wie Erkennung und Korrektur von Fehlern, Flusskontrolle, Neuordnung der Segmente, falls bei der Übertragung die Reihenfolge vertauscht wurde, und Entfernung von doppelten Segmenten verwendet. Erreicht wird das durch Sequenznummern zur Kennzeichnung der Segmente, Quittierung (piggy bagged, Fullduplex), wenn Segmente in der richtigen Reihenfolge empfangen wurden, und Wiederholung von Segmenten aufgrund eines Timeouts.

Um eindeutige Verbindungen zwischen zwei Rechnern aufbauen zu können, verwendet TCP so genannte Portnummern. Wenn aber ein Rechner mehrere Dienste über denselben Port in Anspruch nehmen will, müssen diese simultanen Verbindungen zusätzlich gekennzeichnet werden. Das geschieht über Socketnummern (zusammengesetzt aus der IP-Adresse und dem jeweiligen Port). TCP fungiert also gleichzeitig als Multiplexer und Demultiplexer. TCP unterteilt die Port in zwei verschiedene Gruppen: well-known Ports (Portnummern von 0 bis 1023) und registered Ports (Portnummern ab 1024). Gemeinsam mit dem Socket-Konzept können auf einem well-known Port mehrere simultane Verbindungen aufgebaut werden. Wenn der Client eine Verbindung zu einem speziellen Dienst des Servers aufbaut, wählt der Client einen freien Source-Port und wird mit einem well-known-Port des Servers verbunden. Einige Dienste können auch dynamisch zugewiesene Portnummern verwenden (FTP, ...).

Der Verbindungsaufbau unter TCP läuft über das so genannte 3-Wege-Handshake ab, bei dem drei Nachrichten ausgetauscht werden. Ein dreifacher Austausch ist notwendig und hinreichend (Mathematiker haben das nachgewiesen!), um ungeachtet von Paketverlusten, Duplikaten und Verzögerungen eine eindeutige Vereinbarung sicherzustellen. Die Nachrichten, die ausgetauscht werden, bestehen aus einer Sequenznummer, die zufallsverteilt generiert wird, und einem Acknowledgement. Eine solche Nachricht, die für den Aufbau einer Verbindung herangezogen wird, nennt man auch Synchronisationssegment (SYN-Segment), während eine Nachricht mit dem Zweck, die Verbindung wieder abzubauen, Endsegment (FIN-Segment) genannt wird. Eine Verbindung wird also erst bei gegenseitiger Absprache auf- oder abgebaut. Die erste sendende Station generiert eine Sequenznummer, die an die zweite Station übermittelt wird. Das Acknowledgement ist noch nicht gesetzt. Beim Empfänger wird die ankommende Sequenznummer als Acknowledgement (um eins erhöht) gesetzt und eine neue Sequenznummer wird generiert. Beides wird wieder an die erste Station übermittelt, die mit einem Rücksenden des gesamten Pakets die Verbindung bestätigt. Das Resultat ist eine "synchronisierte Verbindung". Ab diesem Zeitpunkt können Daten übermittelt werden. Nachdem immer eine neue Sequenznummer generiert wird, können gleichzeitig mehrere Anwendungen eine Verbindung auf- und abbauen. In der Kommunikation werden Time-outs benutzt, um unerwünschte Verzögerungen zu vermeiden und den Datenfluss zu verbessern. Beispielsweise werden sie benutzt zur Bestimmung der maximalen Antwortzeit beim Pollen und bei der Adressierung, bevor eine Prozedur automatisch neu initiiert wird. TCP geht mit solchen Time-outs flexibler um als das Ethernet. Es geht zwar auch von einem fixen Startwert aus, richtet die Zeit aber dann je nach Verbindung immer neu ein. Bei einer langsameren Verbindung wird anhand der Zeit, die ein Paket benötigt, um vom Sender zum Empfänger und wieder retour zu wandern (Roundtime), die Zeit für das Time-out festgelegt. Sollte ein Paket bei bestehender Verbindung länger brauchen, als der Timer es vorschreibt,

wird es verworfen und neu gesendet. TCP optimiert dadurch den Durchsatz von selbst.

Die Checksum erstreckt sich im Header von Bit Null bis 15. Sie erstreckt sich über den Header, die Nutzdaten und über einen 12 Byte langen Pseudo-IP-Header, mit dem zwar fehlerlose aber falsch geleitete Pakete erkannt werden können. Bis jetzt wurden lediglich einige grundlegende Aspekte von TCP betrachtet. Um in heutigen IP-Netzen werden allerdings weit mehr Funktionen gefordert als bisher betrachtet. Eine sehr wichtige Funktion ist Slow Start and Congestion Avoidance. TCP kann damit selbstständig festlegen, wie viele Daten ins Netz geschickt werden. Dies geschieht bereits auf Senderseite – basierend auf der Größe des Fensters – und nicht erst, wenn es bei einem Empfänger zu einem Überlaufen kommt.

Fast Retransmit und Fast Recovery: Auch im Fall eines Neusendens muss die Time-out Zeit eingehalten werden. Das führt unweigerlich zu einer Verlangsamung des Netzes. Muss neu gesendet werden, wird sofort ein Time-out durchgeführt.

Delayed Acknowledgements: Wenn auf der Empfängerseite ein Paket ankommt, wird im Normalfall sofort ein ACK gesendet. Das führt auch zu unnötig viel zusätzlichem Verkehr auf dem Netz. Bei interaktiven Anwendungen herrscht meist ein reger Verkehr auf der Empfängerseite. Wenn also das ACK erst gesendet wird, wenn im Puffer des Senders ein zweiter Frame zur Übertragung bereitsteht, der das ACK piggy-backen kann, erreicht man damit eine wesentlich kleinere Netzlast. Die interaktive Applikation wartet damit jedes Mal 200ms, ob nicht vielleicht doch noch ein ACK mitreisen will, und sendet dann erst den nächsten Frame. In diesen 200ms hat die Applikation eventuell auch etwas zu senden. Wenn nicht, macht sich das ACK alleine auf den Weg.

Portnummer: Allen Prozessen werden Portnummern zugeordnet, damit sie gleichzeitig ausgeführt werden können.

Socket: Ist die Kombination von IP-Adresse und Portnummer, somit einzigartig.

Verbindungsaufbau: "three way handshake": 1.request, 2.response, 3.response of response

Sequence Number: Position des 1. Oktets von diesem Segment im Datenstrom.

Acknowledge Number: bestätigt die korrekte Ankunft von allen Oktets bis zur Ack-Nummer minus 1 und zeigt auf die Nummer des nächsten Oktets.

Besonderheiten d. Timeouts:

- high timeouts: daraus folgen "lange" Wartezeiten
- low timeouts: daraus folgen unnötige Übertragungswiederholungen

Checksum: beinhaltet den TCP-Header und Datenbereich und einen 12 Byte Pseudo-IP-Header (bestehend aus Source- und Destination-IP-Adresse, IP-Protocolltype und IP-Segmentlength). Der Pseudo-IP-Header erlaubt Fehlererkennung.

Sliding Window:

- rechte Ecke bewegt sich nach rechts: Empfänger bestätigt Daten und leert TCP-Buffer- Space
- linke Ecke bewegt sich nach rechts: Daten sind gesendet und bestätigt.
- rechte Ecke ! links: geht nicht, weil doppelte Acks gelöscht werden.
- linke Ecke links: darf nicht passieren (!shrinking Window)

TCP-Flow-Control wird durch dynamic windowing unter Verwendung vom Sliding Window Protokoll gemacht.

Slow Start: wenn es eine TCP Verbindung gibt, wird das Staufenster zuerst auf 1 Segment initialisiert. Bei Bestätigung verdoppelt usw. bis Stau auftritt) dann muss der Sender die Senderate verlangsamen. Slow Start reduziert die Senderate durch ! Congestion Avoidance (Sender Imposed Flow Control).

UDP (User Datagram Protocol): ist einfacher als TCP, verbindungslos, Layer4 Service, wird in Situationen eingesetzt, wo Datagrammverlust nicht besonders kritisch ist bzw wo die Implementierung gering sein muss. Deshalb ist es auch leichter zu implementieren. UDP verwendet die selben Portnummern wie TCP. Im UDP-Header empfinden sich Source- und Zieladresse, die Länge des UDP-datagramms und die Checksumme.

32) Schildern Sie das Verfahren Slow Start und Congestion Avoidance sowie Fast Retransmit und Fast Recovery im Detail. Welche Performanceaspekte stellen sich dadurch bei TCP ein? Welche Rolle spielt dabei das Duplicate Ack? [120 Punkte]

Eine sehr wichtige Funktion bei TCP ist Slow Start and Congestion Avoidance. TCP kann damit selbstständig festlegen, wie viele Daten ins Netz geschickt werden. Dies geschieht bereits auf Senderseite - basierend auf der Größe des Fensters - und nicht erst, wenn es bei einem Empfänger zu einem Überlaufen kommt. Slow Start (und Congestion Avoidance) sind in heutigen TCP-Implementationen vorgeschrieben. Slow Start erfordert von TCP eine Verwaltung eines zusätzlichen Fensters: congestion window (cwnd). Es gibt eine Regel, die stets eingehalten werden muss: Der Absender kann bis zum Minimum des Congestion-Fensters und des annoncierten Fensters übertragen.

Wird eine neue TCP-Verbindung hergestellt, so wird das Congestion Fenster mit einem Segment initialisiert. Immer wenn ein Sender ein Acknowledgment empfängt, wird das Congestion Fenster um eine Segmentgröße erhöht. Auf diese Weise wird die Rate mit der gesendet wird jede Runde verdoppelt, bis eine Ansammlung im Empfänger auftritt. Dann wird die Senderate wieder verlangsamt. Eine Ansammlung (Congestion) kann durch Timeouts und duplicate acknowledgements erkannt werden.

Fast Retransmit: Ursprünglich konnte ein Packetverlust nur durch Auslaufen des Retresmission Timers erkannt werden. Auch im Fall eines Neusendens muss die Time-out Zeit eingehalten werden. Das führt unweigerlich zu einer Verlangsamung des Netzes. Muss neu gesendet werden, wird sofort ein Time-out durchgeführt. Bei Fast Retransmit hat der Empfänger sofort ein duplicate ACK zu senden um dem Sender zu zeigen, welche Segmente von ihm erwartet werden. Allerdings sendet der Empfänger auch ein duplicate Ack wenn Segmente nur in der falschen Reihenfolge auftreten. Aus diesem Grund wartet der TCP Sender noch ein drittes ACK ab. Dieser Mechanismus wird „Fast Retransmit“ genannt.

Fast Recovery: Fast Recovery geht sozusagen Hand in Hand mit Fast Retransmit um den einfachen Packetverlust zu reparieren.

Mechanismus: sstresh wird auf die Hälfte der aktuellen Window-Größe gesetzt. Das Sendefenster selbst wird auf diesen Wert + 3 gesetzt (daher kann man davon ausgehen, dass der Empfänger schon 3 Duplicate ACK's erhalten hat. Danach wird Congestion Avoidance ausgeführt. Für jedes weitere Duplicate ACK erhöht der Sender das Sendefenster um 1. Ab dem Zeitpunkt an dem der Sender ein ACK von neuen Daten erhält setzt der das Sendefenster wieder auf den Wert von sstresh und Congestion Avoidance wird erneut ausgeführt.

33) Was versteht man unter „direct“ und „indirect delivery“ im Zusammenhang mit IP Forwarding? Was ist ein Default Gateway? Wie sind statische Routen charakterisiert? Wann werden diese bzw. können diese eingesetzt werden? Was ist Default Routing? Wie wird eine Default Route gekennzeichnet? Wo kommen Default Routes zum Einsatz? Was ist grundsätzlich dynamisches Routing? Welche Rolle spielen Routing Protokolle und die Routing Metrik dabei? Charakterisieren Sie kurz die beiden Basistechniken Distance Vector und Link-State. [110 Punkte]

Im Falle des indirect routing muss das IP-Forwarding von Routern übernommen werden, wobei die Zieladresse dem IP-Header zu entnehmen ist. Die Zustellung des Pakets erfolgt dabei hop by hop, d.h. von Router zu Router. In diesem Fall spricht man auch von indirekter Zustellung (indirect delivery) von IP-Datagrammen. Der Host ist nur dafür zuständig, einen default-Router als nächste Station auszuwählen. Der Host selbst ist für die direkte Zustellung von Datagrammen zuständig (direct delivery). Welche Zustellungsart gewählt wird, hängt von der Destination-net-ID ab. Eine direkte Zustellung wird wohl nur dann verwendet, wenn die netID des Hosts mit der netID des

Zielhosts übereinstimmt. Im umgekehrten Falle ist eine indirect delivery vorzuziehen.

Alle Datenpakete, die ein Rechner nicht im eigenen Netz versenden kann, werden an das Default Gateway gesendet. Meist ist das eine eigene Hard- und Software, die die Weiterleitung übernimmt.

Mit einem Gateway werden meistens Netzwerke verbunden, die aufgrund der unterschiedlichen Protokollstruktur nicht miteinander kommunizieren können. Ein Gateway kann also alle in einem Netzwerk vorhandenen Protokollarten ineinander umwandeln.

Default Gateway: Die IP-Hosts sind bei statischen Routen selbst dafür verantwortlich einen default-router (Default Gateway) auszuwählen, über welchen der nächste Hop im Falle einer indirekten Zustellung erfolgen soll.

Statische Routen: Die Routingtabellen werden vom Netzwerkadministrator vordefiniert. Sie sind nicht responsive auf Änderungen der Topologie. Bei komplexen Netzwerken kann es dann schwer werden statische Routen zu generieren bzw. zu ändern. Allerdings entsteht bei der Verwendung statischer Routen kein zusätzlicher Overhead in der CPU und kein zusätzlicher Verkehr im Netzwerk. In manchen Technologien sind nur statische Routen möglich (z.B. X.25, ISDN). Sie werden auch manchmal wegen Security-Vorteilen verwendet.

Default Routing: Allgemein werden unbekannte Ziele vom Router verworfen. Man kann allerdings eine Default Route definieren. Jetzt werden alle unbekanntes Ziele zu einem bestimmten (default) Router geschickt. Dies kann den Vorteil haben, dass dieser die Zieladresse kennt. Es hat auch den Vorteil, dass nun nicht mehr jeder Router eine komplette Routing-Tabelle benötigt. Das Default-Network wird über die Net-ID 0.0.0.0 beschrieben. Default Routing wird verwendet, wenn man ein lokales Netzwerk mit z.B. dem Internet verbinden will. Auch können mittels Default-Routing mehrere Subnetze miteinander verbunden werden.

Dynamische Routen: Routingtabellen werden hier dynamisch upgedatet. Sie erhalten die

Informaionen über Routingprotokolle von anderen Routern. Die Routing-Protokolle müssen die momentane Netzwerktopologie kennen. Weiters sollten sie den besten Weg zu jedem erreichbaren Netz kennen. Sie sollten auch die Informationen über das Erreichen den besten Weges in Routingtabellen speichern. Um den besten Weg feststellen zu können müssen aber die Metrik-Informationen des Netzes bekannt sein. Meist werden statisch vordefinierte Variablen (z.B. hop, cost, bandwith,...) verwendet. Hier gibt es 2 grundlegende Technologien: Distance Vector und Link State

Distance Vector: Routingtabelle wird periodisch an alle schnellen Nachbarrouter gesendet, eingehende Updates werden untersucht auf neue Netze, Änderungen in der Metrik (basiert auf Hops) von bekannten Netzen etc. Beispiele für Distance Vector Protokolle: RIP, RIPv2, IGRP, IPX RIP,...

Link State Protokolle: Router haben eine globale Sicht des Netzwerks, wissen exakt über alle Router und Links bescheid, Änderungen werden von ihnen selbst festgestellt.

34) Erläutern Sie das dynamische Routing-Protokoll RIP im Detail. Welche Probleme können bei der prinzipiellen Vorgehensweise von RIP (Count-To-Infinity) auftreten? Was bewirkt dabei Maximum Hop Count, Split Horizo, Poison Reverse und Hold Down. Beschreiben Sie das im Detail. Welche Verbesserungen gegenüber RIPv1 gibt es durch RIPv2? [120 Punkte]

RIP (Routing Information Protocol) ist ein typisches IGP (Interior Gateway Protocol). Die Entscheidungen, die dieses Protokoll trifft, beruhen auf Abzählung der Hops (Distance Vector Protocol, mit Hilfe eines Vektors wird die Richtung des Routers festgelegt, der die schnellste Verbindung in ein bestimmtes Netz aufbauen kann). Die Information, mit welchem Netzwerk der RIP-Router verbunden ist, wird in die Routing Tabellen eingetragen, in denen dann die netIDs der direkt mit ihm verbundenen Netze und die Entfernung (in Hops) von ihnen steht. Alle 30 Sekunden wird über einen Broadcast die eigene Routing Tabelle an benachbarte Router gesendet, die ihre Tabellen dann dementsprechend updaten können. Die upgedateten Tabellen werden schließlich weiterversendet. Nach einer bestimmten Zeit wissen alle Router über alle Netzwerkadressen im kompletten Netz bescheid. Enthalten die upgedateten Listen Router, die dieselbe netID haben, wird die Verbindung mit den wenigsten Hops in die Liste eingetragen. Haben zwei Verbindungen dieselbe Anzahl an Hops, wird automatisch die erste eingetragen. Mit diesem Protokoll werden die Netzkapazitäten optimal ausgenutzt. Sobald eine bessere (schneller oder mit weniger Hops, bessere Metrik) Verbindung zu einem Router besteht (auslesbar aus den Update-Listen), wird diese Verbindung ohne lange Nachzufragen einfach in die Liste übernommen.

Sollte ein Update mit einer schlechteren Metrik als die für dieses Netz derzeit gespeicherte daher kommen, wird es nur in die Tabelle übernommen, wenn es von dem Router kommt, der in der Tabelle als Vektor für dieses bestimmte Netz eingetragen ist. Alle anderen für dieses Netz werden ignoriert. Wenn ein Routing-Tabellen-Eintrag nicht innerhalb von 180 Sekunden upgedatet wird, wird er als veraltet erklärt. Ohne einen speziellen Mechanismus haben alle anderen Router nach mindestens 180s wieder eine vollständige Routing- Tabelle. über spezielle Network-Unreachable-Messages (werden an alle Router gesendet) dauert dieser maximal 180s. Während dieser Übergangsphase wird nach der alten Tabelle verfahren. Bei sehr großen Netzen kommt es aufgrund der 180s Phase bei Ausfällen oder Störungen zu einer sehr langsamen Konvergenz. Weil der Inhalt eines Updates der Routing-Tabellen verbindlich ist (Trusted Information Principle), kann es bei RIP sehr leicht zu Schleifenbildung kommen. Durch die beiden oben genannten Fehler können Datagramme über redundante Wege kreisen und zu einem "Count to Infinity" Problem werden. Ein weiteres Problem ist, dass Routing Tabellen immer als ganzes verschickt werden, was für große Netze nicht sehr vorteilhaft ist, weil sehr viele netIDs in der Tabelle enthalten sind. Ein ständiges periodisches Updaten der Listen fällt bei Weitverkehrsnetzen zusätzlich ins Gewicht. Methoden, den oben erläuterten Problemen Abhilfe zu schaffen, sind Maximum Hop Count, Split Horizon, Poison Reverse, Hold Down und viele mehr. Die in der ersten Version verwendeten Datagramme enthielten oft freie Stellen. Eine Neuerung in der zweiten Version im Vergleich zur ersten ist, dass diese freien Plätze bestimmten Funktionen zugeteilt wurden. Die Neuerungen sind Routing Domains, Übertragung von Subnetmasks und Next Hop Redirect Information, Route Advertisements über EGP-Protokolle und Authentifikation. Bei Routing Domain wird ein Subnet in mehrere Domänen aufgeteilt. Routing Updates können schließlich den Zieldomänen übermittelt werden. Ein Router kann damit mehrere Domains gleichzeitig mit den entsprechenden Datagrammen versorgen. Eine weitere Neuerung im RIPv2-Header ist das SUBNET MASK. Die zu der jeweiligen IP-Adresse gehörige Subnetzmaske wird mitübertragen, wodurch Variable Length Subnet Mask (VLSM) möglich wird. Im Feld IP ADDRESS kann die IP-Adresse jenes Routers eingetragen werden, der als Next Hop für die Weiterleitung verwendet werden soll. Er muss im selben Teilnetz direkt erreichbar sein.

Die IP-Adresse 0.0.0.0 in dem Feld bedeutet, dass der aussendende Router als Next Hop für das angegebene Netz fungiert. Nicht alle Router in einem Teilnetz müssen Routing Updates aussenden (in bestimmten Szenarios). Für die Weiterleitung der Updates wird kein Broadcast mehr verwendet, was alle angeschlossenen Geräte beschäftigen würde, sondern ein Multicast mit Adresse 224.0.0.9, mit der sich Router, die zu dieser Gruppe gehören, identifizieren. Authentifikation wird verwendet bei Routing Updates. Momentan gibt es nur einen Typ von Authentifikation (Typ 2), der einem einfachen Passwortschutz entspricht. Ein Router, der ein Update ohne gültiges Passwort erhält, ignoriert dieses. RIPv2 ist abwärtskompatibel. Ein RIPv2-Router, der im RIPv1-Modus arbeitet, sendet nur RIPv1 Datagramme. Ein RIPv2-Router, der im RIPv1-Kompatibilitätsmodus arbeitet, sendet zwar RIPv2-Datagramme aus, jedoch als Broadcast, weil ein RIPv1-Router die zusätzlichen Headerfelder einfach ignoriert. RIPv2-Router im RIPv2-Modus senden Datagramme als Multicast.

Die maximale erlaubte Distanz zwischen zwei Subnetzen wird bei RIP auf 16 begrenzt. Ist im Abschnitt DISTANCE in der Routing Tabelle der Wert 16 gespeichert, ist das Netz nicht mehr erreichbar. IP-Datagramme mit dieser netID werden dann vom Router verworfen, der dann ein ICMP-Datagramm mit "network unreachable" generiert. Ein Nichterreichen eines Netzes kann also aktiv bekanntgegeben werden. Das 180s Timeout in den Nachbarroutern muss dann nicht abgewartet werden. Die Anzahl der Hops kann nicht größer als 15 sein.

Maximum Hop Count alleine reduziert aber nicht temporäre Routing Loops. Eine Methode gegen Routing Loops und Verringerung der Slow Convergence (Zählen bis 16) ist Split Horizon. Sie verhindert, dass Informationen über Netze in die Richtung geschickt werden, aus der sie gekommen sind, außer die Information enthält eine bessere Verbindung, die in die Tabelle eingetragen werden kann. Außerdem wird die Konvergenzzeit beim benachbarten Router auf die Zeit der Fehlererkennung (180s) anstatt von $16 \cdot 30s = 480s$ reduziert.

Eine alternative Methode ist Poison Reverse. Dabei geben Router in ihren Routing Updates die Nichterreichbarkeit (Message = Poison) von Netzen in die Richtung bekannt, aus der sie die Informationen über diese Netze erhalten haben, wobei beim benachbarten Router die Konvergenzzeit auf die Zeit der Fehlererkennung reduziert wird (180s). Das funktioniert ganz gut in einfachen Netzen.

Hold Down: In komplexeren Netzen benötigt man einen zusätzlichen Mechanismus, um Schleifen zu verhindern. Es veranlasst einen Router nach einer Nichterreichbarkeitsmeldung eines Netzes weitere Informationen über dieses Netz für eine bestimmte Zeit zu ignorieren. Die Informationen stammen nicht von dem Router, der die Nichterreichbarkeitsmeldung geschickt hat. Ein typischer Wert ist dabei 240s. Alle Router im Netz haben damit die Möglichkeit, die ausgeschickte Nichterreichbarkeitsmeldung zu erhalten. Außerdem wird dadurch ein gewisser

Einschwingvorgang abgewartet (die Nachricht breitet sich ja als Welle im Netzwerk aus!), wodurch Inkonsistenzen in den Routing Tabellen und damit Schleifen vermieden werden. Durch ein Hold Down wird aber die Konvergenzzeit ein wenig erhöht, was sich in manchen Fällen ungünstig auswirken kann.

35) Was ist Classful Routing? Wie erfolgt dabei der Routing Table Lookup? Was ist Classless Routing? Wie erfolgt hier der Routing Table Lookup? Welche zusätzlichen Möglichkeiten gibt es bei der Adressierung? Was ist CIDR? Was versteht man unter Route Summarization? Warum sollte aber auch bei Classless Routing die IP Adressierung der physikalischen Topologie folgen? [90 Punkte]

Classfull Routing: Routing Protokolle wie RIP, IGRP können keine Subnetz-Informationen über routing updates übertragen. Dies führt zu folgenden Konsequenzen:

- Wenn eine gegebene Klasse A, B oder C gegeben ist und diese in weitere Subnetze unterteilt wird, so muß die Subnetmask in allen Bereichen gleich sein) Es ist keine variable Länge der Subnetzmaske (VLSM) erlaubt.
- Wird ein Routing-Update zu einem Interface geschickt, dessen Netzwerknummer unterschiedlich dem des subnetted networks ist, so wird nur die Netzwerknummer des Klasse A, B oder C Netzwerkes verkündigt. So wird die Zusammenfassung der Routen (route summarize) nur über die Grenzklassen optimiert. Folglich muss ein Subnetz-Bereich kontingent sein.
- Classful routing

Routing Table lookup: Nehmen wir an, es wird ein IP-Datagramm mit einer gegebenen IP-Adresse vom Router empfangen. Jetzt kann die IP-Adresse als Klasse A, B oder C Netz

identifiziert werden. Als nächstes wird ein lookup in der Routing-Tabelle ausgeführt. Wenn sich dort kein Eintrag befindet, wird das IP-Datagramm weggeworfen. Handelt es sich aber um einen Treffer, so wird die IP-Adresse mit jedem bekannten Subnet überprüft. Existiert kein solches Subnetz, so wird das Paket weggeworfen.

Auch wenn das übergeordnete Netzwerk beim Router bekannt ist, aber das Subnetz nicht

existiert wird das Datenpaket verworfen. Das ändert auch nichts, wenn ein Default Gateway eingestellt ist. Somit muss der unterteilte Bereich der Subnetze kontingent (durchgehend) sein. Somit muß jedes Subnetz eines gegebenen Netzes nur über den Pfad mit den jeweiligen Subnet-IDs ansprechbar sein.

Classless Routing: Wird verwendet, wenn Routing-Protokolle Informationen über Subnetzmasken bei Routerupdates übertragen können. Beispiele sind: RIPv2, OSPF, eIGRP. Das hat folgende Vorteile:

- Variable Längen der Subnetzmasken können verwendet werden (VLSM). Dadurch kann der Adressbereich effizienter aufgeteilt werden.
- Route Summarize kann auf jeder Adresse durchgeführt werden (und nicht nur auf class boundaries)
- Classless routing

Routing Table lookup: Nehmen wir an, es wird ein IP-Datagramm mit einer gegebenen IP-Adresse vom Router empfangen. Diese Adresse wird nicht als Class A, B oder C interpretiert.

Es wird ein lookup in der Routing-Tabelle ausgeführt, der den besten Treffer für diese IP-Adresse zurückliefert. Dazu werden die IP-Präfixe in der Routing-Tabelle bit für bit (von links nach rechts) mit der IP-Adresse verglichen. Das IP-Datagramm wird an jenes Subnetz übermittelt, das am besten an die IP-Adresse passt. Das bietet den Vorteil, dass IP-Adressen mit beliebigem Subnetting verwendet werden können und man so unabhängig vom übergelegtem Netzwerk ist. So kann nun auch ein Sub-Subnetting betrieben werden.

CIDR (Classless Interdomain Routing): Bei diesem Verfahren werden IP-Adressen zusammengefasst, wobei ein Block von aufeinanderfolgenden IP-Adressen der Klasse C als ein Netzwerk behandelt werden. Eine Organisation bekommt dabei nicht mehr ein ganzes Netz zugeteilt, sondern nur mehr Subnetze mit einer jeweiligen Subnetzmaske. Die Routing Tabellen der Router werden dadurch auch ein wenig entlastet, in dem der IP-Adresse ein Präfix angehängt wird, mit dem eine große Firma oder ein großer ISP gekennzeichnet werden kann. Auch darunterliegende Netze können damit zusammengefasst werden (Supernetting). Bei IPclassless kann die Grenze zwischen Netzwerk- und Hostteil der IP-Adresse nicht nur an den Byte-Grenzen, sondern auch an beliebigen Bit-Positionen innerhalb der 32-Bit gesetzt werden. Durch die Subnetz-Maske wird angegeben, wie viele Bits der Adresse den Netzwerkteil bilden (Bsp.: 193.171.213.0/24 ... die ersten 24 Bit bilden die Netzwerk-Adresse).

Die IP-Adressierung sollte aber trotzdem ein wenig strukturiert und ans physikalische Netz angepasst sein. Es hat nicht viel Sinn, einen Host in einem Subnetz zu suchen, in dem er gar nicht ist, nur weil die Strukturierung nicht gegeben ist. Es ist nicht notwendig, einen bestimmten Host im kompletten Internet zu suchen; das Netz wird dadurch sicher nicht schneller werden.

36) Beschreiben Sie kurz das Grundprinzip der Link-State Routing Technologie OSPF (!!! Beschränken Sie sich dabei und auch im folgenden auf OSPF in einer Area !!!). Wie kommen in OSPF Nachbarschaftsbeziehungen zustande? Welche OSPF Messages werden dazu verwendet? Welche LSA-Typen werden in diesem Zusammenhang verwendet? Wie können Nachbarschaftsbeziehungen eindeutig in der Topology Database beschrieben werden? Wozu dienen OSPF Database Description Messages? Wie werden OSPF Messages transportiert? Wie wird tatsächlich das LSA (die Verkehrsfunknachricht) bewerkstelligt (Stichwort „Hot Potatoe“)? Welche Bedeutung hat dabei LSA Sequence-number? [140 Punkte]

Bis jetzt existierte in jedem Router eine a-priori konsistente Datenbank in jedem Router. Die grundlegende Bedeutung der so genannten link states sind anlegen und behalten der Daten in der Datenbank. Ein Link-State steht für eine lokale Nachbarschaft zwischen 2 Routern. Er wird zwischen Ihnen aufgebaut. Andere Router werden über den Link- Aufbau mittels Broadcast über die neue Verbindung informiert ("traffic news"). Die Link-States werden kontinuierlich überprüft. OSPF ist ein IP Protokoll. Die Router haben die komplette Verkehrslage des Netzwerks gespeichert. Es wird jedoch durch den Dijkstra Algorithmus ein Verkehrsnetz gebaut, welches schließlich auch benutzt wird. Der

Dijkstra Algorithmus sorgt dafür, dass es zu jedem Knoten im Netzwerk nur noch einen Weg gibt (ähnlich Spanning Tree Protocol) Wie werden Linkstates benutzt? Angrenzende Router erklären sich als Nachbarn, wenn sie ihren Link-State auf up setzen. Dieser Link-State kann mittels eines Hello-Requests überprüft werden. Jede Änderung eines Link-States wird den anderen Routern der OSPF-Domain mittels LSA (Link State Advertizements) mitgeteilt. Das ist ein Broadcast-Mechanismus. LSAs sind kürzer als normale Routing-Tabellen. Die komplette Topologie-Map vertraut LSA.

Wie kommen Nachbarschaftsbeziehungen zustande? Zuerst sendet jeder Teilnehmer einen hello-Request. Wird ein neuer Nachbar erkannt, so sendet der erste seine database description message. Er bekommt dann vom 2. einen LS request. Das bedeutet, dass er mehr über den anderen erfahren möchte. Im nächsten Schritt bekommt er mittels eines LS update die Daten des ersten. Dieser quittiert den Empfang mittels eines LS ack. Nun möchte auch der 2. Partner seine Topologie-Datenbank dem 1. übermitteln. Dazu sendet er ihm eine database description

message. Diese wird dann wiederum mit einem LS request beantwortet. Mit dem nächsten LS update werden die Daten übertragen, die mit einem LS ack quittiert werden. Nachdem sich nun diese 2 Router synchronisiert haben, melden sie ihren ganzen anderen Nachbarn die neuen Beziehungen weiter. Da dies sofort geschieht und nicht erst nach der laut Timer nächsten LSA-Message (30 min) dauert es nur eine kurze Zeit bis jedem Router das gesamte Netzwerk bekannt ist („Hot Potatoe“)

Die Database: Jeder Router besitzt eine Topologie-Datenbank. Sie ist wie eine „Network Roadmap“. Sie beschreibt somit das gesamte Netzwerk. Die Datenbank basiert auf einem Graphen. Jeder Knoten steht für einen Router. Jede Ecke steht für ein Subnetz, wobei jeder Router den Graphen als root verwendet. Anhand dieser Datenbank kann sich der Router den besten Weg in ein anderes Netz berechnen. In der Datenbank sind ja alle Wege vorhanden. So gibt es kein Warten mehr, falls ein anderer Router ein Gerücht verbreitet. Nachdem nun der kürzeste Pfad ermittelt worden ist, wird er in der Routing-Tabelle eingetragen. OSPF ist auch fähig zwischen internen und externen net-IDs zu unterscheiden. Mit einem Router-LSA (Typ1) kann ein bestimmtes Subnet beschrieben werden.

In OSPF gibt es 3 Arten von Routing:

- **intra area routing**
Hier werden Daten innerhalb einer Area übertragen. Es existieren in dieser Area Router-Link LSA (Typ1 Router LSA) und Network Link LSA (Typ2).
- **iner area routing**
Hier findet ein Datenaustausch zwischen 2 Areas über eine Backbone-Area statt. Es existiert hier ein Summary Link LSA (Typ3 oder 4). Typ3 wird zur Verbindung von Netzwerken und Typ4 zum Verbinden von IP-Adressen auf ASBRs verwendet.
- **exterior routing**

Pfade zu externen Zielen sind statisch konfiguriert oder über ASBR (Autonomous Systems Boundary Routers) mittels EGP oder BGP importiert. Dazu dient ein AS External Summary LSA (Typ5)

LSA Age: Die LSA Message wird alle 30 Minuten gesendet. Empfängt ein Router 60 Minuten lang keine LSA Messages altert der Link aus und wird somit gelöscht.

37) Was bedeutet Broadcast Umgebung (shared media wie LAN) für das OSPF Prinzip? Welche Funktion haben Designated Router und Backup Router in einer Broadcast Umgebung? Hat das auf das Weiterleiten von IP Datagrammen einen Einfluß? Welche Abläufe bzw. welche Arten von Destination Adressen gibt es in einer Broadcastumgebung bei der Übertragung von OSPF Messages? Mit welchem LSA-Typ wird eine Broadcast Umgebung bekanntgegeben?

Broadcast Mechanismus von LSA: ist extrem wichtig, da die Konsistenz der Topologie – Datenbank davon abhängt. Jede LSA Nachricht muss explizit bestätigt werden, ansonsten greift ein Timeout und die LSA Nachricht wird erneut gesendet. Wiederholt sich ein Fehler zu oft, wird Nachbarschaft aufgelöst, da es beim entsprechenden Nachbarn offenbar zu einem Fehler gekommen ist und sonst die Konsistenz des Netzwerkes nicht mehr gewährleistet wäre. Zusätzlich werden Link States alle 30 min wiederholt bzw. altern nach 60 Minuten aus. Grund: automatische Korrektur von Fehlern im Netzwerk. Der Einfluss auf die Weiterleitung von IP-Datagrammen ist gegeben, da sich aufgrund des OSPF Mechanismus „hello“-Message, LSA-Update doch erheblicher Traffic entsteht.

OSPF Broadcast Networks: Wenn sich mehrere Router in einem Multi-Access Netzwerk befinden funktioniert, das Jedermitt- Jedem Prinzip aufgrund der $N*(N-1)/2$ Problems nicht. Weiters wären die Informationen über die Nachbarn alle redundant, da jeder Router alle anderen Router als Nachbarn ansehen würde. Es würde somit ausreichen einen Zentralen „Knotenpunkt“ zu haben. Dieser heißt in OSPF „Designated Router“

Adressen: OSPF benutzt dedicated IP Multicast Adressen für den Austausch der Routing Messages. (zb 224.0.0.5 „All OSPF Routers“; 224.0.0.6 „All Designated Routers“)

Broadcast Umgebung: Sobald mehrere Router einen Multi-Access auf ein Netzwerk-Segment haben (z.B. LAN, X.25, Frame Relay) wird ein Designated Router und ein Backup Router bestimmt. Diese werden mittels der hello-Message ausgewählt. Der Grund für den Designated und Backup Router ist, dass sonst ein zu großer Netzwerk-Traffic auftreten würde, wenn sich die Router synchronisieren. Aus diesem Grund wird ein Router zum Designated Router. Er wirkt nun als Ansprechpartner für alle anderen Router. überprüft wird er durch den Backup Router. Fällt der Designated Router aus, so wird der Backup-Router zum Designated-Router und es wird ein anderer Backup-Router bestimmt.

Designated Router (DR): Er versorgt alle anderen Router dieses Segments mit Nachbarschaftsverbindungen über virtuelle Punkt zu Punkt Verbindungen. Der Designate Router ist für die Abgabe von Network-LSAs verantwortlich. Der Backup Router ist einfach die Ausfallssicherung für den Designated Router, welcher dessen Aufgabe übernimmt wenn dieser ausfällt.

38) Was ist der Grund eine OSPF Domain in Areas zu unterteilen? Welche Mechanismen kommen hier zum Tragen? Was versteht man unter Backbone Area und wie erfolgt der Anschluß anderer Areas? Welche LSA-Type kommen dadurch zusätzlich zum Einsatz? Wie erfolgt die Handhabung dieser Type durch einen Area Border Router bzw.durch einen areainternen Router? Was versteht man unter Route Summarization im allgemeinen und wie kann man das bei OSPF mit Areas nützen? Welche LSA Typen werden benötigt, um externe Netze in einer OSPF Domain bekanntzumachen? Welche speziellen Router werden benötigt? Was versteht man unter Stub Areas in Zusammenhang mit externen Netzen? Geben Sie die Reichweite (Inter-Area oder Intra-Area) der verschiedenen LSA Typen an und begründen Sie das kurz. Was versteht man unter Route Summarization im allgemeinen und wie kann man das bei OSPF mit Areas nützen? Worauf muß man bei Route Summarization in Zusammenhang mit OSPF aufpassen?

Jede Area hat ihre eigene Topologiedatenbank. Somit bleibt die Area-spezifische Routing- Information innerhalb der Area. Ändert sich die Topologie eine Area, bleibt der Routing-Traffic innerhalb der Area. Somit wird bei route summarization der Traffic drastisch reduziert. Jede OSPFArea bekommt dann ihre eigene area-ID. Diese sind ähnlich den AS-Nummern. Sie ist wie eine IPAdresse strukturiert oder nur eine einfache Nummer. Allerdings muß sie innerhalb einer OSPFDomain eindeutig sein. Eine OSPF-Domäne beinhaltet zumindest eine einfache Area. Ein Router, der mit mehreren Areas verbunden ist, wird Area Border Router (ABR) genannt. Ein ABR kennt die Topologie-Datenbanken aller mit ihm verbundenen Areas. Prinzipielle OSPF Areas müssen über eine spezielle Area verbunden sein: der Backbone Area. Sie hat die area-ID 0.0.0.0 oder 0. Existiert in dieser Domain nur eine Area, so ist sie die Backbone Area. Nicht backgebonte Areas dürfen nicht direkt miteinander verbunden werden. Diese Aufgabe übernimmt die Backbone-Area. Dieses Konzept erzwingt eine sternförmige Konfiguration aller Areas um die Backbone Area. Backbone Area Routers sind entweder über direkte physikalische Links oder über virtuelle Links miteinander verbunden. In speziellen Fällen kann ein virtueller Link dazu verwendet werden um den Verkehr von isolierten Areas innerhalb der backbone Area zu tunneln.

LSA-Typen

- **intra area routing:** Hier werden Daten innerhalb eine Area übertragen. Es existieren in dieser Area Router-Link LSA (Typ1) und Network Link LSA (Typ2).
- **iner area routing:** Hier findet ein Datenaustausch zwischen 2 Areas über eine Backbone-Area statt. Es existiert hier ein Summary Link LSA (Typ3 oder 4). Typ3 wird zur Verbindung von Netzwerken und Typ4 zum Verbinden von IP-Adressen auf ASBRs verwendet.
- **exterior routing:** Pfade zu externen Zielen sind statisch konfiguriert oder über ASBR (Autonomous Systems Boundary Routers) mittels EGP oder BGP importiert. Dazu dient ein AS External Summary LSA (Typ5)

Area Border Router: Der Area Border Router beinhaltet 2 Topologiekarten (Eigene Area, Backbone-Area). Er exportiert die Routen seiner eigenen Area zum Backbone Router mittels Summary LSA's. Der Area Border Router importiert alle Routen von anderen Areas in seine eigene Area. Auch dies wird mittels Summary LSA's gemacht.

Summary LSA's sind „Distance Vector updates“. Sie wird von den ABR generiert um die Router in einer Area bezüglich der Kosten von „außen“ zu informieren sowie vice versa. Weiters können Summary Link LSA's für Route Summarization benutzt werden.

Route Summarization: Kann entweder manuell oder vom Area Border Router konfiguriert werden (Minimierung der Routing-Tabellen-Einträge), Classless Routing, Summarization kann überall in der IP Adresse stattfinden. (zb. können mehrere Class C Netzwerke zu einer einzelnen Adresse zusammengefasst werden. [201.1.0.0 bis 2.01.1255.0 (Subnet Maske 255.255.255.0) wird zu 201.1.0.0 (Subnet Maske 255.255.0.0) zusammengefasst]) – Beim Zusammenfassen werden nur die niedrigsten Kosten gemeldet.

Wenn ein Router eine Summary LSA erhält fügt er die Kosten aus der Summary LSA zu den Kosten hinzu um den genannten Area Border Router zu erreichen. Wenn ein Area Border Router eine Summary LSA von einem Backbone erhält fügt er die Kosten aus der Summary LSA zu den Kosten hinzu um den genannten Area Border Router zu erreichen. Das Resultat wird in den Routing Tabellen festgehalten. Weiters wird eine Summary LSA in die anderen Areas mit den fertigen Kosten gesandt.

In OSPF können somit beispielsweise eine Vielzahl in IP's für die Backbone Area zusammengefasst werden.

Jeder Router weiss Bescheid über:

- Die genaue Topologie seiner Area und kennt die besten Pfade zu allen Netzwerken in seinem Netzwerk
- ABR seiner eigenen Area und den Kosten um andere ABRs zu erreichen. ABR's werden in einer separaten Liste gespeichert.

- Wenn ein Netzwerk aktiviert wird, wird ein korrespondierendes Summary LSA vom ABR ausgesandt. (mit den aktuellen Kosten um das Netzwerk vom gegebenen ABR aus zu erreichen).

Verbindung: Wenn 2 Teile eines OSPF Netzwerkes verbunden werden, werden sich die Router mit einer „hello“-Message „begrüßen“. Danach wird einer der beiden Router dem anderen seine LSA Message senden. Dieser wird daraufhin mit einem LSA-Request die komplette Topologiekarte des anderen verlangen, da sie ihm vermutlich unbekannt ist. Daraufhin wird der Router 1 dem Router 2 sein LSA-Update schicken. Danach läuft das ganze nochmals in umgekehrter Reihenfolge ab.

Trennung: Wenn 2 Teile eines OSPF Netzwerkes getrennt werden werden die eingetragenen Link States aufgrund des Timeouts von 60 min (da aufgrund dessen keine weiteren LSA-Messages mehr empfangen werden) ausaltern.

Exterior routing: Pfade zu externen Zielen sind statisch konfiguriert oder über ASBR (Autonomous Systems Boundary Routers) mittels EGP oder BGP importiert. Dazu dient ein AS External Summary LSA (Typ5) Wenn ein Router ein Summary LSA erreicht, so werden die vom Summary LSA verkündeten Kosten zu den Kosten addiert, die notwendig sind, das verkündete ABR zu erreichen. Diese Kosten werden dann in der Routing Tabelle gespeichert. Wenn ein ABR-Router ein Summary LSA vom Backbone erhält, so geht er gleich vor, wie vorher beschrieben. Weiters sendet er ein Summary LSA in die Area mit den kulminierten Kosten und setzt das ABR-ID zum aktuellen Wert.

Stub Areas: Normalerweise erhält jeder interne Router Informationen über jedes externe Ziel. OSPF erlaubt nun eine Definition von Stub Areas um Speicherbereiche der internen Router zu minimieren. Nun weiss nur der Area Border Router jeder Area über alle externen Ziele Bescheid. Jeder interne Router erhält Standardrouteinträge. Es wird nun der ganze Verkehr der nicht innerhalb der Domain bleibt an den Area Border Router weitergeleitet.

39) Geben Sie einen Überblick (Grundprinzip, Funktionsweise, Protokollabläufe, Einsatz, etc). Über das Protokoll BOOTP. Welche Konfigurations-Parameter können im Header, welche anderen wichtigen Konfigurations-Parameter können in der Vendor Specific Area transportiert des Headers werden? Was versteht man unter BOOTP Relay Agent, wann wird dieser benötigt und welches Feld im BOOTP Header ist dafür verantwortlich? Was lässt sich mit DHCP bewerkstelligen? Welcher Zusammenhang besteht mit BOOTP? Schildern Sie im Detail welche Abläufe beim Lesen einer IP Adresse zu durchlaufen sind (Welche DHCP Messages und welche Optionen werden verwendet? Wie funktioniert das mit den Timern T1, T2? etc.)

BOOTP wurde entwickelt um RARP zu ersetzen, und bietet nun Bootstrapping an. BOOTP basiert auf einem Client-Server Prinzip und benutzt UDP als Kommunikation.

Bootstrapping: Erlaubt Disk-losen Clients sowie Netzwerkkomponenten ohne flüchtigen Speicher, OS-Code zu laden Parameter von einem Zentralen Server zu konfigurieren.

Vorgang:

- Der BOOTP Client sendet einen Request an den BOOTP-Server (255.255.255.255 sowie 0.0.0.0 als Source Adresse).
- Der Server benutzt die MAC Adresse des Clients um ihn in einer Datenbank zu suchen und zu verifizieren.
 - Bei Erfolg: Der Server sendet die geforderte Boot Information mittels Broadcast zum Client.
- Ende der BOOT-P-Prozedur.

Boot-Info enthält: Die IP-Adresse eines IP-Hosts der die Bootimages enthält, sowie die Dateinamen dieser Bootfiles. Der Client benutzt nun diese Information um die Bootfiles via TFTP zu laden. Diese Trennung bewirkt, dass der eigentliche BOOTP Server nur eine kleine Reference Tabelle speichern muss – die (evtl. größeren) Bootimages können ausgelagert werden. Der BOOTP-Client ist für die Error Detection verantwortlich aufgrund des Limited Broadcasts (255.255.255.255) wäre das ganze auf ein einfaches LAN ausgelegt. Um auch BOOTP Server von anderen Subnets zu erreichen müssen die BOOTP Server als Relay Agent arbeiten können.

Konfigurationsparameter: Operation Code, Hardware Type, Length of the Hardware Address, Hops, Transaction ID, Client IP, Your IP, Server IP, Router IP, Client MAC Address, Server Host Name, Bootfilename.

Vendor Specific Area: Kann zusätzliche Information des BOOTP-Servers enthalten (zb. Subnet Maske, Hostname, Domainname, IP-Adresse des DNS-Server)

DHCP: DHCP ist ein Protokoll um Host Spezifische Konfigurationen von einem Server auf einen Client zu übertragen und ist somit ein Mechanismus um Clients temporäre oder permanente Adressen zuzuweisen. Der DHCP Server empfängt die Anfrage eines Clients und sucht sich aus einem IP Pool eine Adresse heraus, und gibt sie an den Client weiter. (auf TCP/IP Basis) Der Client kann diese Adresse nun für eine bestimmte Zeit benutzen. Nach Ablauf

dieser Zeit muss der Client erneut eine Adresse beantragen. Durch den automatischen Prozess verhindert DHCP einige Probleme, die sonst bei der manuellen Konfiguration auftreten könnten.

Der Client kann fragen nach: IP Adresse, Subnetz Maske, DNS Server, default TTL, max. Fragment Size, Default Gateways, ARP Cache Timeout, TCP Keepalives, Ethernet Encapsulation, ...

Verbindung zu BOOTP: DHCP benutzt den Header von BOOTP für die Übertragung der Daten (DHCP ist somit BOOTP basierend)

3 Methoden zur Adressgewinnung:

- *Automatisch* (DHCP gibt dem Client eine permanente Adresse)
- *Dynamisch* (DHCP gibt dem Client eine Adresse für eine bestimmte Zeit)
- *Manuell* (Adresse wird manuell erstellt, andere Parameter übernimmt DHCP)

Leasen einer IP:

- **IP Lease Request:** Wenn ein Client startet sendet er einen Broadcast an alle DHCP Server (0.0.0.0 als Source Adresse, 255.255.255.255 als Destination Adresse). Dieser Request wird in einer DHCPDISCOVER Message geschickt. IP Lease wird benutzt wenn TCP/IP zum ersten Mal gestartet wird, eine vom Client verlangte IP Adresse verweigert wird, der Client vorher schon eine IP Adresse geleased hat, welche jedoch abgelaufen ist.
- **IP Lease Offer:** Alle DHCP Server, die den Broadcast empfangen senden dem Client eine DHCP OFFER Message welche MAC-Adresse, Offered IP Adresse, Subnet Maske, Length of Lease, Server ID enthält
- **IP Lease Selection:** Wenn ein Client ein Angebot von mind. einem DHCP Server empfängt sendet er einen DHCPREQUEST ins Netzwerk um anzuzeigen, dass keine weiteren Angebote mehr akzeptiert werden. Diese Message beinhaltet die Server ID um dem einen Server anzuzeigen, dass sein Angebot akzeptiert worden ist.
- **IP Lease ACK/NACK:** Im Erfolgsfall wird ein DHCPACK gesendet, welches nochmals die IP Adresse sowie andere Konfigurationsparameter enthält. Danach kann der Client TCP/IP vollständig initialisieren.
- **DHCP Renew:** Bei der IP Vergabe wurden 2 Timer gesetzt ($T1 = 0,5 \times \text{Lease Time}$, $T2 = 0,875 \times \text{Lease Time}$). Diese werden gestartet sobald sich der Client im Bound Zustand befindet. Nach Ablauf des T1 wird ein Versuch gestartet eine neue IP Adresse erlangen. Schlägt dieser fehl greift T2 und es wird abermals nach Ablauf der Versuch gestartet eine neue IP Adresse zu erlangen. Der DHCP Server kann jetzt einfach die IP Adresser erneuern oder mittels DHCPNACK anzeigen, dass sich der Client um eine neue IP Adresse bemühen muss.

40) Geben Sie einen Überblick (Grundprinzip, Funktionsweise, Protokollabläufe, Einsatz, etc). Über das Protokoll Telnet. Was versteht man unter NVT? Was sind Telnet Commands, Optionen und Standard Functions und wozu dienen sie? Welche Portnummern werden verwendet? Was ist punkto Security zu sagen.

Telnet ist eine Methode um mit anderen Internet Hosts zu kommunizieren. Es bietet ein Standard- Interface sowie ein Terminal. Mittels Telnet kann man sich von einem lokalen Host Remote einloggen und Kommandos ausführen. Telnet bietet ein Client-Server Modell.

Basics:

- Telnet ist Connection-oriented und benutzt das TCP Protokoll auf **Port 23**
- Konzept des Network Virtual Terminals (NVT)
- Telnet war eine der ersten Internet Applikationen
- Telnet ist außerdem eine der populärsten Internet Applikationen da es flexibel ist, wenig
- Ressourcen benötigt und Telnet in jedes UNIX (sowie anderes OS) integriert ist.

Virtual Terminals: Ein Telnet Client kann das Verhalten eines realen Terminals emulieren. Intern endet jede Telnet Verbindung bei einem Network Virtual Terminal (**NVT**). Das NVT offeriert ein standardisiertes, Netzwerkweites Terminal (Printer, Keyboard, HalfDumb Mode). Somit können verschiedene Clients die unterschiedliche Telnet 's verwenden die Kommunikation auf ein gemeinsames Level übersetzen.

Telnet selbst äuft allerdings im Full-Duplex Modus – aus Benutzersicht läuft Telnet jedoch nur auf Halb-Duplex (Reduzierung der Netzwerkkosten und Server-Interrups. Der Telnet Server möchte zuerst alle Daten zum Client schicken bevor dieser weitermacht.)

Verhandlungsoptionen: Um die wenigen Möglichkeiten von NVT zu erweitern, bietet Telnet die Möglichkeit neue Optionen zu verhandeln, welche dann von den Systemen benutzt werden können.

NVT Character Set: NVT benutzt ein 8 bit Daten-Format: Trotzdem benutzt NVT den US 7 bit ASCII Code (Druckbare Zeichen + einiger Kontrollzeichen)

Interne Telnet Kommandos: Für Verhandlungs- und Signalzwecke benutzt Telnet spezielle Kommandos (8 bit lang). Die Kommandos werden mit einem Speziellen „IAC“ (Interpret as Command) prefixt. (Wenn dieser im Datenstrom vorkommt Bytestuffing). Alle Kommunikationen werden mit diesen Kommandos geführt (Länge von 2-3 Bytes, IAC, Command, mögliches 3tes Byte). Bei weitergehenden Verhandlungen können Kommandos auch länger sein (Wird durch SB (Subnegotiation Begin) und SE (Subnegotiation End) eingeschlossen)

Standard-Funktionen: Um die Kompatibilität zu vereinfachen wurden gewisse Standard-Funktionen definiert. Jedes dieser Kommandos inintiiert eine Kontrollfunktion

Sicherheit:

- Telnet Clients können zu einer Vielzahl von Server-Ports Verbindung aufnehmen (Port 25: SMTP, Port 80: http,)
- Telnet verschlüsselt Passwörter nicht – Sniffers !! (Daher sollte man Telnet Benutzer nie Root-Privilegien geben bzw. SSH benutzen)
- Einige Versionen von Telnet unterstützen „Telnet Enviroment Option“ und können angegriffen werden (Benutzer bekommen Zugriff auf das Rootverzeichnis)
- Trojanische Pferde klonen Virtuelle Terminals

41) Geben Sie einen Überblick (Grundprinzip, Funktionsweise, Protokollabläufe, Einsatz, etc). über das Protokoll FTP. Was versteht man unter Virtual File und Reduktionsansatz? Wie ist die Abgrenzung von FTP zu FileServer OS? Was versteht man unter PI und DTP? Wie verläuft die Kommunikation über die Kontrollverbindung? Wie unterscheiden sich die Abläufe von normalen FTP vom passiven FTP? Welche Portnummern werden verwendet? Was ist punkto Security zu sagen? Vergleichen Sie es abschließend mit TFTP.

Grundsätzlich gibt es **2 verschiedene Methoden** Daten zum Austausch anzubieten:

- Definition von virtuellen Daten welche für den Transfer in reale Daten übersetzt werden müssen. Es müssen alle Varianten berücksichtigt werden. Die Übersetzung vom realen zum virtuellen Dateisystem muss implementiert werden (komplex). Der Vorteil in dieser Methode liegt darin, dass die virtuellen Dateisysteme leicht eine Vielzahl von realen Dateisystemen unterstützen können. (zb. ISO FTAM Protokol)
- Reduktion: Extrahiert einige wenige Eigenschaften von vielen verschiedenen Formaten. (Dateitypen, Dateiorganisation, Benutzerverwaltung, Passwort, Symbolische Namen, I/OOperationen, einige rudimentäre Betrachtungs- und veränderungsoptionen). Bei dieser Methode ist keine Übersetzung zwischen verschiedenen Endsystemen notwendig.

FTP: „Sharing by File Transfer“ – Die Dateien werden kopiert und haben danach keinen Bezug mehr zueinander. Daher kann die heruntergeladene Datei beliebig verändert werden, was den FTP-Server nicht zu kümmern braucht.

File Server OS: „Online Sharing Systems“: Erlaubt mehreren Usern eine Datei über das Netzwerk zu benutzen. Diese können die Datei direkt am Server bearbeiten (Allerdings nur immer einer !) (zb. Novell File Server, Sun NFS)

Datei-Representation durch FTP: ASCII (8 bit NVT), EBCDIC (8 bit für IBM to IBM), IMAGE (8 bit binary)

Datei-Organisation durch FTP: Dateistruktur (Strings von Bytes, Ende durch EOF) Record-Struktur (Liste von Records, Ende durch EOR)

Transfertypen:

- **Stream:** Die Daten werden in einem kontinuierlichen Stream übertragen, EOF, EOR bezeichnen Ende der Datei
- **Block:** Die Daten werden in Blöcke unterteilt, EOR: Ende eines Blocks, EOF: Ende der Datei. Diese Übertragungsmethode ermöglicht das wiederaufnehmen von abgebrochenen Downloads)

- **Compressed:** Die Daten werden komprimiert übertragen. Selbe Dateisequenz wird nur einmal übertragen, danach wird dem Client mitgeteilt wie er diese Sequenz zu wiederholen hat.

Grundlegendes:

- FTP basiert auf dem Client-Server Prinzip
- Es wird über 2 TCP Verbindungen kommuniziert (Server-Controll-Verbindung well-known Port 21), Datenverbindung: Well-known Port 20
- TCP bedeutet, dass FTP keine zusätzliche Error-Recovery benötigt
- Access Protection via Username, Passwort. Wird allerdings im Klartext übertragen Sicherheitsproblem (zb durch Sniffen)

Nach der Verbindung unterhalten sich Client und Server via Protokoll Interpreter (PI) via dem NVT Format. PI ist hierbei dafür verantwortlich, den lokalen Syntax nach NVT zu übersetzen. Der Client sendet Kommandos zum Server, dieser antwortet in die andere Richtung. Wenn ein Kommando einen Datentransfer einleitet werden ein Client DTP sowie ein Server DTP (Data Transfer Process gestartet. Danach öffnet der Server über den Port 20 eine weitere TCP Verbindung. Wenn die Verbindung beim Startvorgang auf „Passive Mode“ eingestellt wurde öffnet der Client diese weitere TCP Verbindung (Firewall Friendly). Nach der Übertragung wird die Verbindung wieder geschlossen.

Sicherheit ist wie schon angesprochen nur relativ wenig vorhanden, da zwar Username und Passwort abgefragt werden, dies jedoch im Klartext geschieht.

Unterschied zu TFTP: TFTP ist weit weniger komplex als FTP und wird zb von BOOTP Verwendet. Es wurde geschaffen um einfachste Datenübertragung zu bieten und bieten keinerlei Funktionen zum Lesen von Verzeichnissen bzw. Sicherheitsfeatures.

42) Charakterisieren Sie kurz die grundlegenden Eigenschaften von DNS. Warum erfolgt die Namensvergabe in einer baumartigen Hierarchie? Womit läßt sich diese vergleichen (Stichwort: Filesysteme)? Welche Grundregeln gelten bei der Bildung von Namen und bei der Zuordnung von Namen zu IP Hostrechner? Was versteht man unter Domain, Domain-Name und Label? Was ist ein FQDN? Welche Top-Level-Domains gibt es? Was versteht man unter IN-ADDR.ARPA? Wie ist diese aufgebaut? Wofür wird diese verwendet? Wie erfolgt die Handhabung der verteilten DNS Namensdatenbank? Was versteht man dabei unter Zone-Files? Was ist SOA bzw. was kennzeichnet es? Was versteht man unter Primary und Secondary DNS Server? Was sind Master Files? Was sind Root-Hints? Welche Komponenten gibt es? Wie arbeiten diese zusammen? Wie erfolgt üblicherweise die Namensauflösung, wenn der Resolver nicht unmittelbar den autoritativen DNS Server befragt (Stichwort rekursiv, iterativ)? Schildern Sie kurz das DNS Protokoll. Wann wird UDP, wann wird TCP verwendet?

Historisches: Ursprünglich wurden alle Domainnamen unitär gespeichert. Mit dem zunehmenden Wachstum des Internets stellte sich jedoch schnell heraus, dass dies heute nicht mehr möglich ist. Daher wurde 1984 das Domain Name System (DNS) ins Leben gerufen. DNS ersetzt eine IP Adresse eines Hosts in einen lesbaren Namen. (Hostname Resolution). Dabei geht DNS nach einer Art Baumstruktur vor. Jeder Teil der Hierarchie wird „Domain“ genannt, jeder Hierarchielevel wird „Label“ genannt „Domain Name“. Der DNS-Baum wird durch Name Server realisiert. Jeder dieser Server nimmt sich einem Subnet des DNS-Baumes an – so genannten Zonen. (Der lokale Ort des Servers hat nichts mit dem DNS-Baum zu tun. Der DNS Baum lässt sich mit einem Filesystems (Root-Pfad) eines Computers vergleichen (zb C:\ „...“) – Es wird aber umgekehrt gelesen. Wenn jemand einen Domainnamen in eine IP Adresse auflösen will fragt er einen DNS-Server über das DNS-Protokoll. Der Nameserver wird entweder manuell konfiguriert oder mittels DHCP ermittelt.

Grundregeln:

- Hosts mit mehreren Netzwerkadressen können über einen einzelnen Domainnamen erreicht werden.
- Hosts mit einer einzelnen IP-Adresse können über mehrere Domainnamen erreicht werden.
- Das Root-Verzeichnis des DNS-Baumes ist ein „.“
- Das Root-Verzeichnis wird durch mehrere Root-Server repräsentiert.
- Unter dem Root heißen die Domains: Top-Level-Domain, Second-Level-Domain, ... (zb. .com, .de, .at, .mil, .gov, .edu, ...)

FQDN Fully Qualified Domain Name bedeutet alle Labels inkl. dem „.“

IN-ADDR.ARPA: Möchte man die zu einer IP-Adresse die zugehörige Domain wissen kann man auf IN-ADDR.ARPA zurückgreifen. Ohne diesen Service müsste die komplette DNS-Datenbank nach einer IP-Adresse durchsucht werden. Die zu suchende IP-Adresse muss allerdings verkehrt eingegeben werden. Die IN-ADDR.ARPA-Datenbank ist daher nach der IP-Adresse und nicht nach dem Domainnamen geordnet.

Die Handhabung von DNS erfolgt durch Zonen. (. dot) ist die Hauptzone. Jeder Domaineintrag ohne einen solchen DOT ist eine relative Domain. Jeder DNS-Server kennt nur die eigenen Einträge, seine Zone Files und die Links zu den anderen Hauptdomainservern die er in seinem Cache hat (com org ..). Kennt ein interner DNS-Server eine Unterdomain nicht so leitet er die den

Unterdomainserver weiter. Das **SOA (Start of Authority)** markiert die Grenzen der Zuständigkeiten der einzelnen DNS-Server. Die **Handhabung verteilter DNS** Namensdatenbanken erfolgt durch pruning (Unterteilung einer domain in unterdomains mit eigenem Dns (BIND berkeley internet domain server www.foo.org > pub.foo.org)

Zone files sind eben diese unterdatenbanken

Master files enthalten die IP-Einträge der für die gesuchte Domain zuständigen Nameserver

Primary DNS nur einer pro Domain er hat die Einträge in seiner Masterfile für alle Unterdomains.

Secondary DNS mehrere Server möglich sie enthalten eine Kopie des Masterfiles des Master-DNS-Servers. Haben auch Autorität im Primary-Bereich und werden für Redundanz und Lastausgleich verwendet. Empfohlen durch RFC 1035.

Root.hints sind Anfragen an einen Hauptdomainserver Root NS (momentan 13)

BIND besteht aus einem Server named genannt, einer „resolver library“ und gibt Unterzonen an weitere BIND-Server ab.

Aufbau: Das User-Programm macht eine Anfrage an den Resolver. Dieser fragt den ForeignNS (das äußere Netz betreffend) ab und bekommt eine Antwort die er in seinen Cache schreibt (Shared Database) sowie dem Client-Programm mitteilt. Die Shared Database wird vom internen NS durch das Masterfile refresh't und umgekehrt. Der NS arbeitet andere Anfragen von anderen Resolvern von außerhalb ab und gleicht sich mit maintenance queries/responses mit anderen außerhalb liegenden NS ab. Zusammenarbeit von **BIND u DNS** sie sprechen über Zonen miteinander.

Rekursibe DNS Abfrage die Anfrage wird an einen Default-DNS-Server weitergegeben dieser forwardet, wenn sich diese Domain nicht im Zuständigkeitsbereich des Servers befindet, die Anfrage einem Root-NS. z.B. docs.foo.org Dieser antwortet dann mit der IP des zuständigen Hauptservers z.B. für .org. Dieser Root-Server wird dann mit der Sucher nach www.foo.org befragt und gibt die IP des foo.org Servers zurück. Der www.foo.org NS wird mit der Anfrage auf docs.foo beauftragt. Schlussendlich bekommt der Client die IP des gesuchten Servers.

Alterative DNS Abfrage: Dabei wird eine Liste von bestimmten zuständigen NS direkt an den Clienten übermittelt.

43) Charakterisieren sie kurz das Prinzip von Email und SMTP. Was beschreibt RFC821/822? Gehen Sie auf die Abläufe des SMTP Protokolls näher ein (SMTP Commands). Wie schaut die Struktur von Emails aus? Welche Rolle haben MUA und MTA? Welche Protokolle kommen zwischen MUA-MTA bzw. MTA-MTA zum Einsatz (Unterscheiden Sie dabei zwischen Mail-Upload und Mail-Download)? Wie sind Email-Adressen aufgebaut? Wie erfolgt das Zusammenspiel mit DNS (Stichwort MX-Records)? Welcher Default-Transport ist mit SMTP möglich? Wozu dienen POP und IMAP? Beschreiben Sie diese kurz. Welche POP Commands gibt es und wozu dienen diese? Was kann mit IMAP verbessert werden?

Email bietet die Möglichkeit elektronische Post zu versenden, es ist die am weitesten verbreitete Anwendung im WWW. Es verwendet ein Mailbox-Prinzip - die elektronischen Nachrichten müssen auf einem Mailserver zwischengespeichert werden, da der Empfänger den Rechner nicht immer in betrieb ist.

SMTP dient zum Austausch elektronischer Post auf Grundlage einer TCP-basierenden verbindungsorientierten Rechner-zu-Rechner-Kommunikation. In RFC821/822 wird ein Textstandard dafür definiert.

Im Nachrichtenaustausch hat SMTP verschiedene Kommandos: HALO – Vorstellung, MAIL – Angabe des Absenders, RCPT – Angabe des Empfängers, DATA – Senden der Nachrichten, QUIT – Ende, VRFY – Verifizieren des Benutzernamens

Die Struktur eines Emails besteht aus 3 Teilen; den Envelope oder Header, den Body und der Signature.

MUA (Mail User Agent) ist ein Programm zum Schreiben und Lesen von Emails. Der MTA (Mail Transfer Agent) liest Emails von einem „spool-file“ und leitet diese in die Mailbox des Empfängers weiter.

Zwischen MUA und MTA kommen die Protokolle POP3/IMAP4 zum Mail-Download (Empfangen) und SMTP zum Mail-Upload (Versenden) zum Einsatz. Dagegen wird zwischen MUA und MTA nur SMTP für Up- und Download verwendet.

Die Protokolle **POP (Post Office Protocol)** und **IMAP (Internet Access Message Protocol)** dienen zum Holen von Nachrichten vom Server und zum Verwalten von empfangenen Nachrichten am Server.

POP3 unterstützt Kommandos zum Abrufen, Speichern und Löschen von Emails. POP3-Protokoll basiert auf TCP und verwendet Port 110, es muss am Server und am Client laufen. IMAP4 ist ähnlich POP allerdings ist es weit fortschrittlicher. Es basiert auch auf TCP, verwendet allerdings das Port 143.

POP Kommandos: Einloggen, Ausloggen, Nachrichten abholen und löschen.

Zusätzlich zu den Funktionen die POP zur Verfügung stellt unterstützt IMAP4 noch das Manipulieren von Nachrichten am Server, das Erstellen, Löschen und Umbenennen von Mailboxen und Kommandos zum selektiven Download von Nachrichten. Weiters kann man nach Emails unter Berücksichtigung von bestimmten Kriterien suchen, read-only Mailboxen verwenden und es werden die Flags SEEN, ANSWERED, DRAFT, DELETED und FLAGGED unterstützt.

44) Geben Sie einen Überblick über das Grundprinzip von WWW (Hypertext, HTML, URL, HTTP, Web-Browser, Web-Server). Welche Methoden für Dynamic WWW auf der Browserseite gibt es? Schildern Sie diese kurz. Welche Methoden für Dynamic WWW gibt es auf der Serverseite gibt es? Schildern Sie diese kurz.

Das **World Wide Web (WWW)** besteht aus Clients, Servern und Objekten. Web-Server sind im Grunde genommen http-Server und verbinden zum Port 80. Die Clients werden als Web-Browser bezeichnet und dienen zum Abrufen der Objekte von den Web-Servern um sie diese auszuwerten. Objekte sind elektronischen Dokumente und Daten jeglicher Art, insbesondere jedoch Hypertext- und Hypermedia-Dokumente. Das WWW integriert weitere Internetdienste mit Hilfe der einheitlichen Benutzerschnittstelle des Browsers. Hypertext ist Text, der durch Links ergänzt wird. Links sind Verweise auf andere Textstellen oder andere Dokumente (Objekte). Sie können insbesondere auf andere Stellen im selben Objekt, Objekte (Dateien) innerhalb eines Dateisystems, Computers oder im Netz. URLs (Uniform Resource Locator) entspricht einem Link, er verweist auf Ressourcen im Internet. Hypermedia enthält Text und Links zusätzlich zu multimedialen Anteilen wie Grafik, Bilder, sowie Sounds. Websites basieren auf **Hypertext Transport Protocol (HTML)**, einer beschreibenden Sprache, die vom Browser umgesetzt wird. Das Problem mit HTML ist das es nur teilweise genormt ist und deshalb auf verschiedenen Browsern unterschiedlich dargestellt werden kann.

Möglichkeiten für Dynamic WWW auf der Browserseite sind unter anderem JavaScript/JScript, JavaApplets, ActiveX und Flash.

JavaScript erweitert HTML und wird wie direkt in HTML-Dokumente geschrieben. Es wird vom Browser ausgeführt während das Dokument geladen wird. Es kann alle möglichen Verhaltensweisen von Formularen, Buttons und Textelementen beeinflussen. Außerdem kann es noch Formulare erstellen die eingebaute Fehlerüberprüfung haben. JScript ist Microsofts Antwort auf JavaScript. JavaApplets werden mit der Programmiersprache Java erstellt, welche

Plattformübergreifend eingesetzt werden kann. Sie werden in eigenen Dateien am Server gespeichert und nur ins HTML-Dokument eingebunden.

JavaApplets sind nicht dafür gedacht auf lokale Dateien zuzugreifen und können seit Java 1.1 zertifiziert werden und außerdem für Autorisation verwendet werden.

ActiveX ist Microsofts Antwort auf Java und wird hauptsächlich von Microsoft unterstützt.

Flash ist mittlerweile im Internet weit verbreitet und sehr mächtig. Es kann nicht nur zum Animieren von Websites verwendet werden sondern auch zum Erstellen von komplexen Programmen wie Browser Spiele.

Auf der Serverseite gibt es CGI, PHP, ASP, Servlets, SSI und JSP.

CGI (Common Gateway Interface) Programme erlauben Web-Server dynamische Antworten auf die Eingabe des Benutzers. Die Programme werden am Server ausgeführt. Es können verschiedene Programmiersprachen verwendet werden, hauptsächlich Pearl, aber auch C, Pascal, usw.

PHP (Hypertext Preprocessor) ist eine Alternative zu CGI/Pearl, ist aber für Web-Sites optimiert.

ASP (Active Server Pages) ist Microsofts Antwort auf PHP.

Servlets sind JavaApplets die auf der Serverseite ausgeführt werden.

SSI (Server-Sides-Include) erlaubt die serverseitige dynamische Erstellung von HTML-Seiten. So erstellte Dokumente haben die Endung .shtml.

JSP (Java Server Pages) ist eine einfache Möglichkeit zum erstellen von HTML-Seiten mit dynamischen Inhalt. Sie haben die Endung .jsp.