

Kapitel 1: Einführung

Rechnerbasierte Kommunikation wird dominieren

- Paradigmenwechsel: Früher dominierte Sprachkommunikation

"Klassische" Telekommunikation (Sprache) vs. "Datennetze"

- Früher völlig getrennte Entwicklungen
- Heute Trend zu "Multiservicenetzen" für alle Dienste und Anwendungen

Unterschiedliche Dienste/Anwendungen – unterschiedliche Anforderungen

- Datenrate (tendenziell niedrig für Sprache und Audio, hoch für Video)
- Toleranz gegen Verzögerungen, Verzögerungsschwankungen und Datenverlusten

Unterschiedliche Anforderungen und Konzepte für

- Lokale Netze
- Weitverkehrsnetze

Kapitel 2: Grundlagen

Symbolrate

- Die Symbolrate oder Baudrate ist ein Maß, welches die Schrittgeschwindigkeit bei der Datenübertragung beschreibt. Die Baudrate beschreibt die Anzahl der Signalcodes (Symbole), die pro Sekunde übertragen werden können. Jeder Signalcode entspricht einer definierten messbaren Signaländerung im physikalischen Übertragungsmedium. Die Symbolrate entspricht der Bitrate, wenn nur ein einziges Bit pro Symbol übertragen wird.
- Berechnung: Kehrwert der Symboldauer
- Einheit: Symbole/s (Baud, Bd)

Nominale Übertragungsrate (Bitrate)

- Die Bitrate (oder nominale Übertragungsrate) gibt die pro Sekunde (Zeiteinheit) maximal übertragbare Anzahl von Bits an. Sie ergibt sich deshalb aus der Anzahl der Bits, die pro Symbol übertragen werden können, und der Symbolrate. Die nominale Bitrate gibt eine oberste Grenze für die Kanalkapazität an.
- Berechnung: Symbolrate * Anzahl Bits pro Symbol
- Einheit: Bit/s

Kanalkapazität (Bandbreite)

- Die Kanalkapazität (oder Bandbreite) gibt die technisch tatsächlich mögliche Übertragungsrate an. Wenn Symbole nicht genutzt werden können, ist die Kanalkapazität kleiner als die nominale Übertragungsrate. Beispiel: Der Ethernet-Standard legt fest, dass zwischen zwei aufeinanderfolgenden Rahmen mindestens ein Abstand von 96 Bitdauern eingehalten werden muss (Inter Frame Gap, IFG). Dadurch reduziert sich die Kanalkapazität auf ~ 9,92 Mbit/s bei einer nominalen Übertragungsrate von 10 Mbit/s.
- Berechnung: $\frac{\text{Anzahl der tatsächlich nutzbaren Symbole}}{\text{Gesamtanzahl der Symbole}} * \text{Bitrate}$
- Einheit: Bit/s

Durchsatz

- Der Durchsatz gibt die Anzahl der pro Sekunde übertragenen Bits der betrachteten Instanz (z.B. Verbindung) an. Man muss dabei spezifizieren auf welche Instanz sich die Aussage bezieht und wo (im Protokolls tack) genau gemessen wird.

Gesamtdurchsatz

- Zum Gesamtdurchsatz einer Instanz zählen alle Bits, die von ihr übertragen wurden – egal ob sie dieser Instanz einen Nutzen bringen oder nicht. Beispiel: Eine Station am Ethernet sendet pro Sekunde 992 Rahmen von jeweils 1000 Bit Länge. Sie hat also einen Gesamtdurchsatz von 992000 Bit/s. Auch wenn Rahmen kollidieren oder wenn Rahmen vom Empfänger wegen Bitfehlern verworfen werden, zählen die dabei übertragenen Bits zum Gesamtdurchsatz. Der maximal erreichbare Gesamtdurchsatz entspricht der Kanalkapazität, d.h. alle nutzbaren Symbole (und damit Bits) werden tatsächlich genutzt (belegt).
- Einheit: Bit/s

Nutzdurchsatz

- Beim Nutzdurchsatz wird nur der Anteil der übertragenen Bits der Instanz gewählt, die der Instanz einen Nutzen bringen. Beispiele: Aus Sicht einer Ethernet-Instanz bringen Pakete mit Bitfehlern (oder Kollisionen) keinen Nutzen, da sie beim Empfänger verworfen werden und neu übertragen werden müssen → Übertragungsfehler mindern also den Nutzdurchsatz. Aus Sicht der darüberliegenden IP-Instanz stellt nur das im Datenfeld des Ethernet-Rahmens übertragene IP-Paket Nutzbits dar. Der Overhead des Ethernet-Rahmens (Header, CRC, Skript Seite 109) vermindert aus Sicht der IP-Instanz den Nutzdurchsatz → Overhead reduziert den Nutzdurchsatz. Beim Nutzdurchsatz muss also genau definiert werden, aus Sicht welcher Instanz die Angabe erfolgen soll.
- Einheit: Bit/s

Merke: Bitrate \geq Kanalkapazität \geq Gesamtdurchsatz \geq Nutzdurchsatz!

Auslastung

- Generell bezeichnet die Auslastung den Anteil der Gesamtkapazität einer Ressource, der tatsächlich genutzt wird. Die Auslastung wird über ein Zeitintervall bestimmt. Beispiele: Bei einer Rechner-CPU ergibt sich die Auslastung als Verhältnis der Rechenzyklen in denen der Prozessor arbeitet zu der Gesamtzahl der Rechenzyklen, die der Prozessor in dem Betrachtungsintervall verfügbar ist. Bei einer Übertragungsleitung ergibt sich die Auslastung als Verhältnis der (insgesamt) genutzten (belegten) Bits zu der Gesamtzahl nutzbarer Bits, die in dem Betrachtungsintervall verfügbar sind. Wenn mehrere Verbindungen gleichzeitig bestehen, geht die Summe der einzelnen Gesamtdurchsätze in die Berechnung ein.
- Berechnung: $\frac{\text{Anzahl der belegten (genutzten) Bits}}{\text{Anzahl der insgesamt nutzbaren Bits}}$ bzw. $\frac{\text{Gesamtdurchsatz}}{\text{Kanalkapazität}}$
Die maximal erreichbare Auslastung ist 1, d.h. die komplette Kapazität der Ressource wird tatsächlich genutzt.
- Einheit: keine, wird in Prozent angegeben

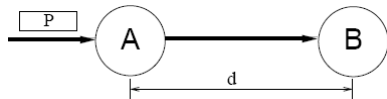
Effizienz

- Generell gibt die Effizienz an, wie gut die Kapazität einer Ressource tatsächlich ausgenutzt werden kann. Beispiele: Die Effizienz eines Paketübertragungs-Verfahrens entspricht (im fehlerfreien Fall) der Länge des Informationsfelds geteilt durch die Gesamtlänge des Pakets (Skript Seite 35, Fehler auf der Folie wurde in der Vorlesung korrigiert). Die Effizienz eines fehlerbehafteten Übertragungskanals entspricht der Anzahl der korrekt übertragenen Pakete geteilt durch die Anzahl aller übertragenen Pakete (Vortragsübung). Wenn die Pakete unterschiedlich lang sind, muss dies bei der Berechnung berücksichtigt werden.

- Berechnung: $\frac{\text{Maximale Anzahl der Nutzbits}}{\text{Anzahl der insgesamt nutzbaren Bits}}$ bzw. $\frac{\text{Maximal erreichbarer Nutzdurchsatz}}{\text{Kanalkapazität}}$
- Einheit: keine, wird in Prozent angegeben

Bestandteile der Knoten-Verzögerung bei der paketorientierten Kommunikation

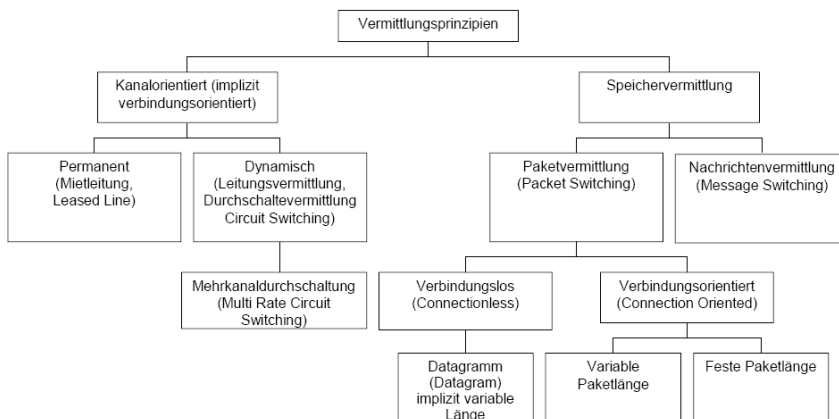
Die für die Übertragung eines Datenpakets zwischen zwei Nachbarknoten benötigte Zeit besteht aus der Summe von mehreren Komponenten, die von der Netzauslastung und den Eigenschaften der Netzelemente abhängen. Die Bestandteile der Verzögerung werden anhand der abgebildeten Struktur analysiert, wo ein Datenpaket *P* beim Zeitpunkt t_0 am Knoten *A* eintrifft:



- **Bearbeitungsverzögerung:** Der Knoten A muss einen Teil der im Kopfteil von P enthaltenen Information lesen und bewerten, um die für die Weiterleitung notwendigen Parameter ermitteln zu können. Die dafür notwendige Zeit t_{proc} wird Bearbeitungsverzögerung genannt.
- **Pufferungsverzögerung:** Bevor ein Paket weitergeleitet werden kann, muss man auf die vollständige Bearbeitung der bereits im System wartenden Pakete warten. Die Länge des Aufenthalts t_{queue} in der Warteschlange wird Pufferungsverzögerung genannt. Der Aufenthalt im Puffer ist von der Netzlast abhängig und für nicht überlastete Netze meist vernachlässigbar.
- **Ausbreitungsverzögerung:** Entlang eines Übertragungsmediums erfolgt die Signalausbreitung nur mit einer endlichen Geschwindigkeit v . Die Ausbreitungsverzögerung t_{prop} entspricht der Zeitspanne, die ein Signal benötigt, um sich bis zum nächsten Knoten auszubreiten (d/v).
- **Übertragungsverzögerung:** Wenn die Datenübertragung angefangen hat, werden die Daten mit einer Rate erzeugt, die der nominalen Datenrate entspricht. Die für das Senden des gesamten Datenpakets benötigte Zeit t_{trans} (Paketgröße/Datenrate) wird Übertragungsverzögerung genannt.
- Die von einem Knoten verursachte Verzögerung beträgt also:

$$t_{nodal} = t_{proc} + t_{queue} + t_{prop} + t_{trans}$$

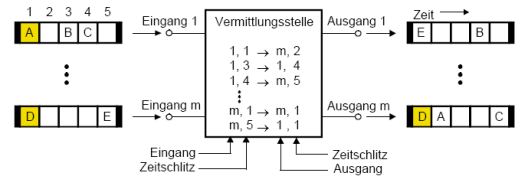
Vermittlungsprinzipien



Vermittlungsstellen

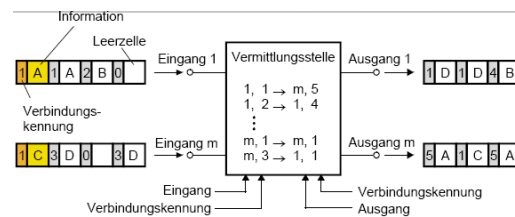
▪ **Kanalorientierte Kommunikation**

- Feste Zuordnung Eingang/Zeitschlitz → Ausgang/Zeitschlitz (wird beim Verbindungsaufbau festgelegt)
- Zuordnung der Daten zu einer Kommunikationsbeziehung anhand der Position
- Keine gegenseitige Beeinflussung da feste Zeitbeziehung (innerhalb einer Verbindung konstante Verzögerung wegen Zeitschlitzumsetzung)



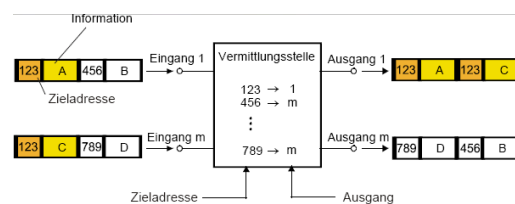
▪ **Paketorientierte Kommunikation (verbindungsorientiert)**

- Zuordnung Eingang/logische Kanalnummer → Ausgang/logische Kanalnummer (wird beim Verbindungsaufbau festgelegt)
- Bei momentaner Überlast erfolgt Zwischenpufferung
 - Gegenseitige Beeinflussung der Verbindungen
 - Variable Verzögerungen innerhalb einer Verbindung
 - Im Extremfall Verluste durch Pufferüberlauf



▪ **Paketorientierte Kommunikation (verbindungslos)**

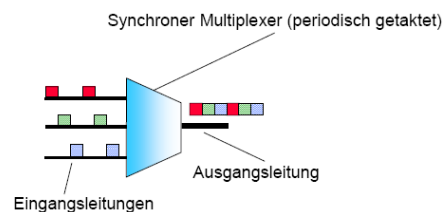
- Zuordnung Zieladresse → Ausgang (wird durch eigene Mechanismen (Routingprotokolle) festgelegt)
- Bei momentaner Überlast erfolgt Zwischenpufferung (siehe verbindungsorientiert)



Zeitmultiplex

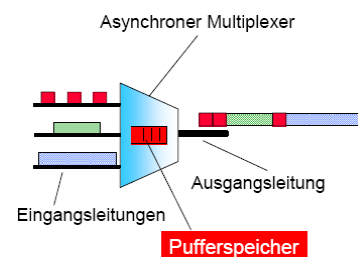
▪ **Synchron** (kanalorientiert)

- Daten kommen periodisch an, Synchronisation kann durch systematische Verschiebung erreicht werden
- Belegung eines Zeitschlitzes pro Verbindung und Periode, feste Datenrate (bzgl. Spitzenrate und zeitlichem Verlauf)



▪ **Asynchron** (paketorientiert)

- Datenpakete kommen asynchron (unkoordiniert) an
 - Es kann nur jeweils ein Paket auf der Ausgangsleitung übertragen werden
 - Bei gleichzeitigen bzw. überlappenden Ankünften gehen Pakete verloren oder es werden Pufferspeicher vorgesehen
- Pufferspeicher vermeiden Verluste auf Kosten von Verzögerungen und Verzögerungsschwankungen
- Belegung der Übertragungskapazität durch die einzelnen Verbindungen nur bei Bedarf
 - Unterstützung beliebiger und zeitlich veränderlicher Datenraten



Verbindungskonzepte

verbindungsorientiert	verbindungslos
<ul style="list-style-type: none"> ▪ Aufwand zum Auf- und Abbau der Verbindungen ▪ Wegewahl einmal pro Verbindung ▪ Komplexe Netzknoten (Zustandsspeicherung, Steuerungskommunikation) ▪ Nur (kurze, pro Link eindeutige) Verbindungskennung pro Paket ▪ Gleicher Weg für alle Pakete, keine Überholungen (Sendereihenfolge bleibt erhalten) ▪ Reservierung von Betriebsmitteln (Bandbreite, Speicher, ...) möglich 	<ul style="list-style-type: none"> ▪ Aufwand für Wegewahl pro Paket ▪ Einfachere Netzknoten (gedächtnislos) ▪ Komplette (lange, netzweit eindeutige) Zieladresse im Paket ▪ Unterschiedliche Wege, Überholungen möglich (Resequencing beim Empfänger notwendig) ▪ Reservierungen von Betriebsmitteln schwierig

kanalorientiert	paketorientiert
<p>Physikalische Verbindung</p> <ul style="list-style-type: none"> ▪ Es wird ein Weg durch das Netz aufgebaut (Laden der verbindungs-spezifischen Tabellen in den Vermittlungsstellen) ▪ Die Übertragungskapazität (z.B. PCM-Zeitschlitz) wird fest der Verbindung anhand der belegten Ressourcen zugeordnet 	<p>Virtuelle Verbindung</p> <ul style="list-style-type: none"> ▪ Es wird ein Weg durch das Netz aufgebaut ▪ Eine bestimmte Übertragungskapazität wird zwar logisch der Verbindung zugeteilt, es werden jedoch keine Ressourcen (Zeitschlitz) fest zugeordnet (Entkopplung des Weges durch das Netz von den Übertragungsressourcen, den Nutzdaten muss eine Kennung mitgegeben werden, um sie einer Verbindung zuordnen zu können)
<p>Synchrones Zeitmultiplex</p> <ul style="list-style-type: none"> ▪ Optimiert für konstante Datenströme (Sprache) ▪ Feste Datenrate (Kanalrate) ▪ Minimale Verzögerung ▪ Praktische keine Verzögerungsschwankungen ▪ Praktisch keine Datenverluste 	<p>Asynchrones Zeitmultiplex</p> <ul style="list-style-type: none"> ▪ Optimiert für sporadische Datenströme (Daten) ▪ Variable Datenraten (Spitzenrate, zeitlicher Verlauf) ▪ Zusätzliche Verzögerungen und Verzögerungsschwankungen durch Pufferspeicher ▪ Datenverluste durch Pufferüberlauf möglich

LAN (Local Area Network)

- Optimiert für geringe räumliche Ausdehnung (Gebäude, Firmengelände, Campus)
- Konzept: Direkte, verteilte Kommunikation ohne dedizierte Vermittlungsknoten (Peer-to-Peer-Kommunikation)
- Mittlere bis hohe Datenraten bei kurzer Verzögerung (1 – 1.000 Mbit/s)
- Besitz, Nutzung und Betrieb durch eine Organisation

MAN (Metropolitan Area Network)

- Optimiert für mittlere räumliche Ausdehnung (Firmengelände, Campus, Stadt, Region; Vernetzung von LANs)
- Konzept: Direkte, verteilte Kommunikation ohne dedizierte Vermittlungsknoten (Peer-to-Peer-Kommunikation)
- Mittlere bis hohe Datenraten (1 – 150 Mbit/s)
- Besitz und Betrieb durch eine Organisation, Nutzung durch viele Organisationen und Individualnutzer

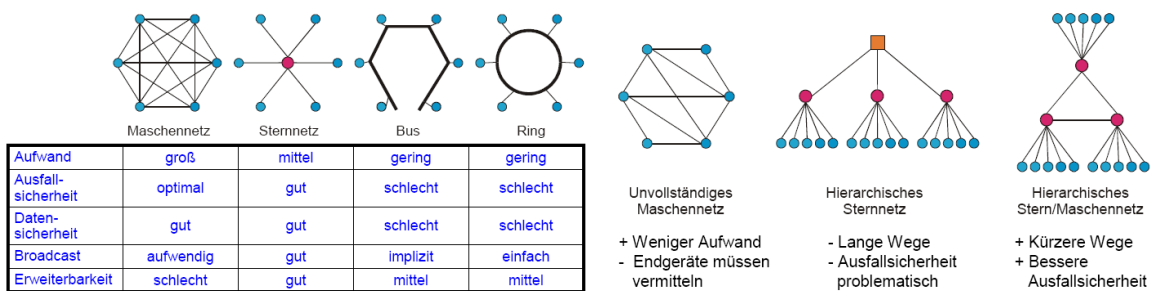
WAN (Wide Area Network)

- Optimiert für unbegrenzte räumliche Ausdehnung (Region, Land, weltweit)
- Konzept: Spezielle Infrastruktur für Übertragung und Vermittlung, Nutzung durch Endsysteme
- Niedrige bis hohe Datenraten, mehr Verzögerung (kbit/s bis 622 Mbit derzeit)
- Besitz und Betrieb durch große (öffentliche) Netzbetreiber, Nutzung durch unbegrenzte Anzahl von Geschäfts- und Privatkunden (öffentliche, für jeden verfügbare Infrastruktur)

Verbindungseigenschaften

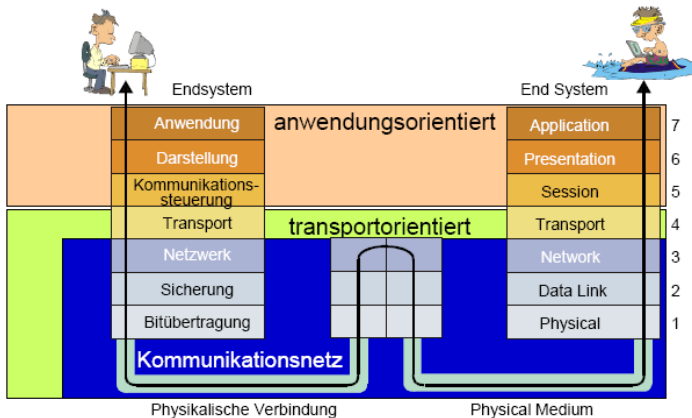
- Unidirektional: Simplex / Bidirektional: Halb-/Voll-Duplex
- Asymmetrisch / Symmetrisch
- Punkt-zu-Punkt / Punkt-zu-Mehrpunkt / Mehrpunkt-zu-Mehrpunkt

Netztopologien



Kapitel 3: Geschichtete Protokollarchitekturen (OSI-Modell)

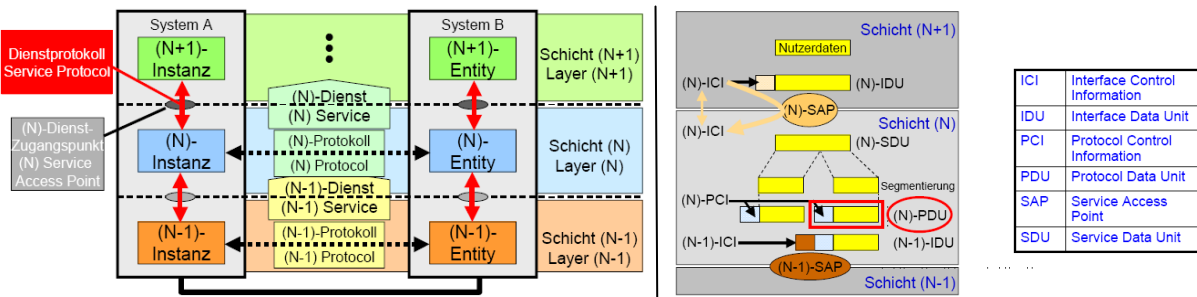
Das ISO-OSI-Modell



- Schicht 1: Bitübertragungsschicht
 - Festlegung der Steckertypen (RJ45, ...): mechanische Eigenschaften
 - Festlegung von Kabeltypen und -längen: elektrische Eigenschaften
 - Festlegung der Codierung und der Signalpegel auf der Leitung
- Schicht 2: Sicherungsschicht
 - LAPD: Sicherungsprotokoll für die ISDN-Teilnehmersignalisierung
 - CSMA-CD: Medienzugriffsprotokoll für Ethernet
 - PPP: Paketorientierte Übertragung über serielle Punkt-zu-Punkt-Links
- Schicht 3: Netzwerkschicht
 - IP: Schicht 3-Protokoll in TCP/IP-basierten Netzen (Internet)
 - RIP: Distance Vector Routingprotokoll für TCP/IP-basierte Netze

- Schicht 4: Transportschicht
 - TCP: Verbindungsorientiertes Transportprotokoll für TCP/IP-basierte Netze
 - UCP: Verbindungsloses Transportprotokoll für TCP/IP-basierte Netze
- Schicht 5: Kommunikationssteuerungsschicht
 - X-Window: Zugang zu Unix-Rechnern von abgesetzten Terminals
- Schicht 6: Darstellungsschicht
 - Standardisierte Darstellung, Formatierung und Verschlüsselung von Daten (ASCII, EBCDIC, PCIT, TIFF, JPEG, MPEG, MP3, MIDI, ...)
- Schicht 7: Anwendungsschicht
 - WWW
 - FTP: Dateiübertragung
 - SNMP: Netzmanagement
 - SMTP: Electronic Mail

Zusammenarbeit der Funktionsschichten

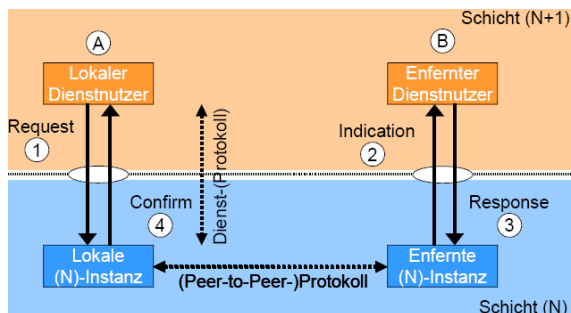


Um eine Kommunikationsbeziehung zu unterstützen, müssen zunächst die verschiedenen Funktionsschichten innerhalb eines Systems zusammenarbeiten. Dabei kann eine Schicht (N) den Dienst, d.h. den durch die Gesamtheit der Funktion erbrachten Leistungsumfang, der darunterliegenden Schicht (N-1) nutzen.

Die Kommunikation an der Dienstschnittstelle – und damit die Inanspruchnahme des Dienstes - erfolgt durch den Austausch von Dienst-Primitiven, die gemäß einem *Dienst-Protokoll* zwischen den benachbarten Schichten ausgetauscht werden. Dafür existieren zwischen benachbarten Schichten standardisierte Schnittstellen, die als Dienst-Zugangspunkte (SAP) bezeichnet werden.

Um einen bestimmten Dienst erbringen zu können, müssen die Instanzen der jeweiligen Schicht in den beteiligten Systemen (logisch) miteinander kommunizieren. Diese Kommunikation erfolgt nach einem einheitlichen festgelegten Schicht (N)-*Kommunikationsprotokoll*, das Syntax und Semantik der Kommunikation festlegt.

Dienstprimitive

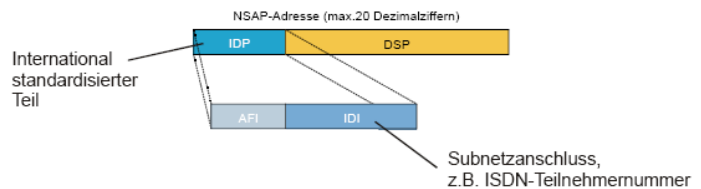
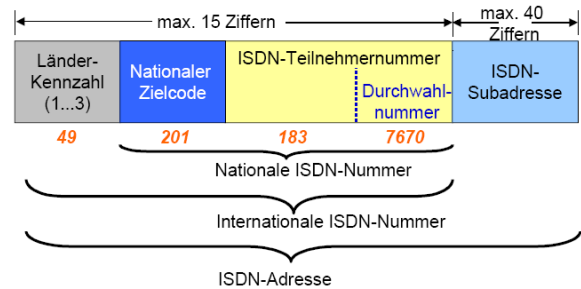


- 1) Request
- 2) Indication
- 3) Response (nur bei bestätigten Diensten)
- 4) Confirm (nur bei bestätigten Diensten)

Kapitel 4: Adressierungskonzepte

Vergleich der Adressierungskonzepte

- MAC-Adressen
 - Permanente in der Netzkarte gespeichert
 - Unabhängig von höheren Protokollen
 - Weltweit eindeutig
 - Unstrukturiert, nicht für große Netze geeignet
- IP-Adressen
 - Vom Netzverantwortlichen vergeben (fest über Konfigurationsdatei, dynamisch über Protokolle)
 - Offiziell registrierte IP-Adressen weltweit eindeutig
 - Adressbereiche an einzelne Organisationen vergeben (keine geografische oder nationale Zuordnung)
 - Strukturiert, keine effiziente Ausnutzung möglich
- ISDN-Adressen
 - Von ITU-T international standardisiert
 - Weltweit eindeutig
 - Adressraum nach Ländern aufgeteilt, innerhalb der Länder zentral verwaltet
 - Bei Einrichtung des Netzanschlusses (permanent) vergeben
 - Streng strukturiert, effiziente Ausnutzung
- OSI NSAP-Adressen
 - Von OSI und ITU-T international standardisiert
 - Weltweit eindeutiges Adressformat
 - Verwaltung der Adressen durch ISO und ITU
 - Streng strukturiert, sehr allgemeines Format



IP-Adressbereiche

- Class A: 0.x.x.x – 127.x.x.x, beginnt immer mit 0
- Class B: 128.x.x.x – 191.x.x.x, beginnt immer mit 10
- Class C: 192.x.x.x – 223.x.x.x, beginnt immer mit 110
- Class D: 224.x.x.x – 239.x.x.x, beginnt immer mit 1110, Multicast-Adressen
- Class E: 240.x.x.x – 255.x.x.x, beginnt immer mit 11110, reserviert
- Hinweis: nach RFC 949 ist es nicht möglich, nach den klassifizierenden Netz-Bits nur 0er oder nur 1en zu verwenden
- sind jeweils x.0 und x.255 reserviert, so umfasst der Class A-Bereich nur noch 0.1.x.x – 126.x.x.x und Class B nur noch 128.1.x.x – 191.254.255.255
- Private Bereiche:
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0.0 – 172.31.255.255
 - 192.168.0.0 – 192.168.255.255

Probleme mit dem Adressraum (IPv4)

- Starre, relativ unflexible Aufteilung
 - Adressraum kann nur lückenhaft genutzt werden
 - 1994 bereits 60 % des Adressraums vergeben
- Subnetting
 - Ein Teil der Host-ID wird für (interne) Netzadresse mitgenutzt
 - Subnet Mask definiert die Anzahl der Bits für Netzadresse
- Classless Interdomain Routing (CIDR)
 - Anzahl der Bits für Netzadresse wird explizit angegeben, Prefix Notation
 - IP-Adressklassen verlieren an Bedeutung (Classless)
- Network Address Translation
 - Pro Firmensitz nur eine oder wenige "Public" IP-Adressen
 - Adressumsetzung am Übergang zum öffentlichen Internet
- IPv6
 - 128 Adressbits, flexiblere Aufteilung

Kapitel 5: Protokollmechanismen

Funktionsübersicht von LAPD (Schicht 2)

- Bereitstellung einer oder mehrerer Schicht 2-Verbindungen über einen D-Kanal
 - Unterscheidung durch DLCI (Data Link Connection Identifier)
- Erkennung der Struktur der Schicht 2-PDUs (Rahmen)
 - Rahmenbegrenzung, Synchronisation, Transparenzfunktion
- Reihenfolgesicherung
 - Folgenummernsteuerung
- Fehlersicherung
 - Erkennung und Behebung von Übertragungs-, Format- und Betriebsfehlern
 - Benachrichtigung der Managementinstanz bei nicht korrigierbaren Fehlern
- Flusststeuerung

Dienstprimitive

- Beim *unquittierten* Übertragungsdienst werden einzelne Schicht 3-Nachrichten übertragen. Es erfolgt innerhalb der Schicht 2 keine Überprüfung, ob die gesendete Information bei der empfangenden Schicht 2-Instanz (fehlerfrei) angekommen ist, d.h. falls eine Fehler- oder Reihenfolgesicherung oder eine Flusststeuerung benötigt wird, muss diese Funktion in der Schicht 3 (oder einer höheren) bereitgestellt werden. Zur Benutzung des unquittierten Übertragungsdienstes stehen die Primitive REQUEST und INDICATION zur Verfügung. Der unquittierte Dienst kann aus jedem Zustand eines Schicht 2- Verbindungs-Endpunkt erfolgen.
- Beim *quittierten* Übertragungsdienst muss zunächst eine Verbindung aufgebaut und bestätigt werden, erst danach kann eine Übertragung der Nutzdaten erfolgen. Zum Schluss wird die Verbindung abgebaut, was die Gegenüberseite auch wieder bestätigen muss.

Transparenzfunktion

Von der Schicht 2 muss sichergestellt werden, dass die Begrenzungs-Flags nicht innerhalb der anderen Felder des Rahmens (durch Zufall) imitiert werden, weil dadurch die Rahmen-Erkennung durcheinander kommen würde. Dies wird dadurch erreicht, dass vor dem Senden jedesmal, wenn in der Bitfolge zwischen den beiden Flags fünf aufeinanderfolgende binäre EINSen vorkommen, eine binäre

NULL eingefügt wird. Der Empfänger wiederum entfernt aus dem Bitstrom zwischen den Flags alle binären NULLen, die direkt auf fünf aufeinanderfolgende binäre EINSen folgen. Die Stopfbits werden bei der Berechnung der Prüfbits auf beiden Seiten ignoriert.

Die Typen der Schicht 2-Rahmen

- Informations-Rahmen (I-Rahmen): Für die Übertragung durchlaufend nummerierter Rahmen mit Nutzinformationen bei der quitierten Übertragung. Das Kontrollfeld enthält eine **Sende-Folgenummer N(S)** und eine **Empfangs-Folgenummer N(R)** von jeweils 7 Bit Länge für die Reihenfolge-Sicherungs-Protokolle. Damit können 128 Rahmen eindeutig nummeriert werden (Modulo 128 Operation). Außerdem ist noch ein weiteres Bit (Poll-Bit) vorhanden, das für die Quittierung verwendet wird.
- Steuer-Rahmen (S-Rahmen): Für die Steuerung der Schicht 2-Verbindung im Zusammenhang mit der Übertragung von I-Rahmen, z.B. Quittierung und Wiederholungsanforderung für I-Rahmen oder die Flusssteuerung. Das Kontrollfeld enthält eine Empfangs-Folgenummer (7 Bit) und ein Poll-/Final-Bit (in Befehlsrahmen wird das Bit als P-Bit bezeichnet, in Meldungs-Rahmen als F-Bit).
- Steuer-Rahmen ohne Folgenummern (U-Rahmen): Für zusätzliche Steuerungsfunktionen und für die unquitierte Übertragung von Nutzdaten.

Verwendete Symbole

I I(N(S), N(R))	I-Rahmen	N(R) ist außer in I-Rahmen auch in S-Rahmen enthalten und dient zur Quittierung der empfangenen I-Rahmen. Mit N(R) wird der korrekte Empfang aller Rahmen angezeigt, deren Folgenummer kleiner oder gleich N(R) - 1 ist.
I RR(N(R))	S-Rahmen (Beispiel: RR)	
I RR(P, N(R))	S-Rahmen mit gesetztem Poll-Bit	
I ↔	Gestörter Rahmen	
II	Wiederholter Rahmen	

Zähler für die Reihenfolge-Sicherung

- Sende-Folgezähler V(S)
 - Zeigt die Sende-Folgenummer N(S) des nächsten zu sendenden I-Rahmens an
 - Wird nach dem Senden eines I-Rahmens um 1 inkrementiert
- Empfangs-Folgezähler V(R)
 - Zeigt die Sende-Folgenummer des nächsten erwarteten I-Rahmens an
 - Ist $V(R) = N(S)$, wird der Rahmen akzeptiert und V(R) um 1 inkrementiert
 - Für andere Folgenummern wird ein Reihenfolgefehler erkannt und eine Wiederholung der Übertragung eingeleitet
- Quittungs-Folgezähler V(A)
 - V(A) wird beim korrekten Empfang eines I- oder S-Rahmens auf den in diesem Wert enthaltenen Wert von N(R) gesetzt
 - $V(A) - 1 =$ Folgenummer des letzten korrekt empfangenen I-Rahmens
 - Gültige N(R)-Werte: $V(A) \leq N(R) \leq V(S)$

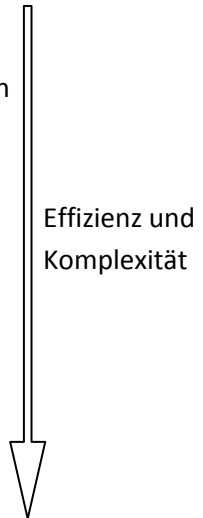
Beispiele

- Quittierung mit S-Rahmen
 - A schickt I-Rahmen 0: I (0, 0)
 - B quitiert mit S-Rahmen: RR (1)
- Quittierung mit I-Rahmen (Piggybacking)
 - A schickt I-Rahmen 0: I (0, 0)

- B schickt I-Rahmen 0 und quittiert I-Rahmen 0 von A: $I(0, 1)$
- Gemeinsame Quittung
 - A schickt I-Rahmen 0 bis 2: $I(0, 0), I(1, 0), I(2, 0)$
 - B schickt einen S-Rahmen und quittiert drei I-Rahmen von A: $RR(3)$
- Fehlererkennung beim Empfänger (Go-Back-N-Verfahren)
 - A schickt I-Rahmen 0 bis 2, I-Rahmen 0 wird gestört und verworfen: $\cancel{I(0, 0)}, I(1, 0), I(2, 0)$
 - Bei I-Rahmen 1 von A: $N(S) \neq V(R)$ bei B \rightarrow Folgefehler wird erkannt
 - B fordert Wiederholung ab $N(S) = 0$ an: $REJ(0)$
 - Nachfolgende Rahmen mit $N(S) \neq V(R)$ werden von B verworfen
 - $V(S)$ und $V(A)$ bei A werden auf $N(R)$ gesetzt. Alle Rahmen ab $N(S) = N(R)$ werden wiederholt
- Fehlererkennung beim Sender durch Zeitüberwachung
 - A schickt I-Rahmen 0, dieser wird gestört und verworfen: $\cancel{I(0, 0)}$
 - Zeitüberwachung (Timer) beim Sender, bei Ablauf wird S-Rahmen mit gesetztem Poll-Bit gesendet: $RR(P, 0)$
 - Sofortige Antwort von B: S-Rahmen mit gesetztem Final-Bit und aktuellem $V(R)$ von B in $N(R)$: $RR(F, 0)$
 - $V(S)$ und $V(R)$ bei A werden auf den Wert von $N(R)$ gesetzt
 - Wiederholung des I-Rahmens 0: $I(0, 0)$

Fehlerbehebung durch Wiederholung

- Go-Back-N
 - Alle Rahmen ab dem ersten verlorenen werden wiederholt
 - Bereits korrekt empfangene Rahmen mit höherer Nummer werden verworfen
- Selective Repeat
 - Nur der verlorene Rahmen wird zur Wiederholung angefordert
 - Bereits korrekt empfangene Rahmen mit höherer Nummer werden zwischengespeichert
- Multiple Selective Repeat
 - Mehrere verlorene Rahmen können gezielt einzeln und in Gruppen zur Wiederholung angefordert werden
- Preventive Cyclic Retransmission
 - Zyklische Wiederholung nicht quittierter Rahmen
 - Bei langen Verzögerungszeiten (Satellitenstrecken)



Flusssteuerung

- Flusssteuerung mit Fenstermechanismus
 - Der Parameter *Fenstergröße* k begrenzt die maximale Anzahl von unquitierten Rahmen auf einen Wert unterhalb des Modulo Wertes ($1 \leq k \leq 127$). Für den Sender gilt nun die Vorschrift, dass keine neuen I-Rahmen mehr gesendet werden dürfen, wenn $V(S) = V(A) + k$ ist.
- Flusssteuerung mit RNR-Rahmen
 - A schickt I-Rahmen 0: $I(0, 0)$
 - Korrekter Empfang bei B, aber B kann keine weiteren I-Rahmen annehmen, quittiert aber I-Rahmen 0: $RNR(1)$
 - B im Zustand "Busy", A sendet keine weiteren I-Rahmen
 - B kann wieder Rahmen annehmen: $RR(1)$

- A sendet weiter

Überlastproblematik

- Ursprünglich wurde die Flusssteuerung und Fehlersicherung in Paketnetzen auf der Schicht 2 (Sicherheitsschicht) durchgeführt. Die Schicht 2 Protokolle arbeiten abschnittsweise, d.h. über einen Übertragungsabschnitt zwischen zwei Vermittlungsknoten. Dadurch konnte jeder Vermittlungsknoten seine direkte Umgebung kontrollieren. Die abschnittsweise Flusssteuerung und Fehlersicherung ist sinnvoll, wenn relativ viele Fehler und Verluste auf den Abschnitten auftreten. In einer fehlerfreien Umgebung wird dadurch aber der Nutzdurchsatz unnötig beschränkt und die Durchlaufverzögerung unnötig erhöht.
- In modernen Paketnetzen, die auf Übertragungssystemen mit sehr geringen Fehlerraten aufbauen, wurde zur Reduktion der Durchlaufzeiten und zur Erhöhung des Nutzdurchsatzes die abschnittsweise Flusssteuerung und Fehlersicherung durch entsprechende Mechanismen auf einer Ende-zu-Ende-Basis ersetzt. Dadurch haben die einzelnen Vermittlungsknoten keine Möglichkeit mehr, ihre direkte Umgebung zu kontrollieren und so lokale Überlasten zu verhindern. Deshalb sind in diesen Netzen zusätzliche Flusssteuerungsmechanismen notwendig. Beispiele:
 - Adaptive Fenstergröße (implizite Erkennung)
 - Explizite Benachrichtigung des Senders, Sender drosselt Senderate
 - Ratenbasierte Flusssteuerung (Rate Based Flow Control)
 - Kreditbasierte Flusssteuerung (Credit Based Flow Control)

Kapitel 6: Lokale Netze

Mehrfachzugriffsverfahren der MAC-Protokolle

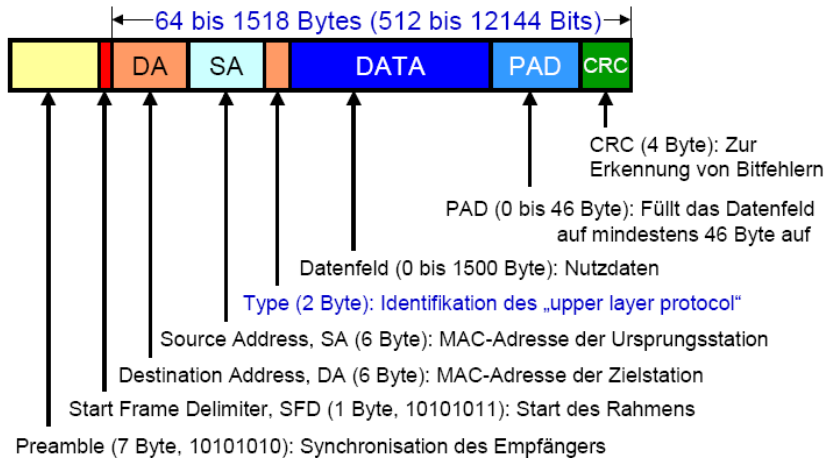
- Kanalaufteilung: Den Kommunikationspartner steht hierbei jeweils nur ein Teil der Kanalkapazität zur Verfügung, auch wenn sonst niemand kommunizieren will. Mögliche Methoden: Zeit-, Frequenz- oder Codemultiplex.
- Random Access Protokolle:
 - ALOHA: Jede Station sendet sofort, Kollisionsauflösung durch zufällige Verzögerung, max. Durchsatz: 18,5 % der Gesamtkapazität
 - Slotted ALOHA: Synchronisation auf Zeitschlitze, jede Station sendet beim nächstmöglichen Zeitschlitzanfang, Kollisionsauflösung durch zufällige Verzögerung, max. Durchsatz: 37 % der Gesamtkapazität
 - CSMA: Sendebeginn kann zu beliebigem Zeitpunkt erfolgen. Jede Station hört den Kanal ab und sendet nur, wenn keine Sendungen anderer Stationen erkannt werden. Kollisionen können nur auftreten, wenn der Sendebeginn der Stationen nahezu gleichzeitig erfolgt (Kollisionswahrscheinlichkeit wird minimiert). Collision Detection (CSMA-CD): Sendende Stationen überwachen den Kanal, bei Erkennung einer Kollision wird die Übertragung sofort gestoppt. Nach der Kollisionserkennung wird ein JAM-Signal (48 Bit) gesendet, damit Kollisionen von allen Stationen sicher erkannt wird (Kollisionsdauer wird minimiert). Nach dem Senden des JAM-Signals tritt die Station in die Backoff-Phase ein. Mit Hilfe eines Algorithmus wird die Wartephase ermittelt.

Ethernet-Varianten

- 10 Mbit/s Ethernet
 - 10Base5: dickes Koaxkabel, 500 m Segmentlänge, Busstruktur
 - 10Base2: dünnes Koaxkabel, 200m Segmentlänge, Busstruktur

- 10BaseT: UTP-Kabel, Sternstruktur
- 100 Mbit/s Fast Ethernet
 - 100BaseTX: 2 UTP-Doppeladern
 - 100BaseFX: 2 Glasfasern
- 1 Gbit/s Gigabit Ethernet
 - Über Glasfaser und über UTP möglich

Ethernet-Rahmenformat (Ethernet II)



Ethernet-Netzstrukturen / Netzkopplung

- **Repeater:** arbeitet auf Schicht 1, verstärken und entzerren die empfangenen Bits vor der Weiterleitung in Busverkabelungen. Können auch zur Kopplung von Segmenten mit unterschiedlichen Übertragungsmedien verwendet werden, wobei diese allerdings mit der gleichen Übertragungsrate betrieben werden müssen, da Repeater nicht über Pufferspeicher verfügen. Über Repeater verbundene Segmente bilden weiterhin eine Kollisionsdomäne.
- **Hub:** funktioniert wie ein Multiport-Repeater, jedoch für mehrere Segmente in einem sternförmigen Netz. Auch hier können keine unterschiedlichen Geschwindigkeiten verwendet werden, und die Segmente bilden weiterhin eine einzige Kollisionsdomäne.
- **Bridge:** erlauben eine Kopplung auf Schicht 2, indem sie MAC-Rahmen analysieren, filtern und bei Bedarf zwischenspeichern können. Durch die Zwischenspeicherung können Segmente mit unterschiedlicher Geschwindigkeit gekoppelt werden, außerdem bilden die verbundenen Segmente getrennte Kollisionsdomänen. Im Vergleich zur Konfiguration mit einem zentralen Hub steht im Netz mit einer Kopplung über eine Bridge insgesamt mehr Kapazität zur Verfügung, da lokaler Verkehr in den Segmenten die anderen Segmente nicht mehr beeinflusst.
- **Switch:** funktioniert wie eine Multiport-Bridge, die eine parallele Architektur mit hohem Datendurchsatz und vielen Interfaces bietet. Dies ermöglicht eine gleichzeitige Übertragung zwischen mehreren Ein- und Ausgangspaaren. Durch den Einsatz von UTP-Verkabelung (getrennte Adernpaare für die beiden Übertragungswege) ist ein Vollduplex-Betrieb möglich.
- **Router:** arbeitet auf Schicht 3 und schafft den Zugang zum Weitverkehrsnetz. Er filtert alle lokalen Broadcast aus und realisiert Firewall-Funktionen, mit denen der externe Zugriff auf das lokale Netz kontrolliert werden kann.

Transparent Bridging

Behandlung der gesendeten Rahmen in der Bridge/Switch:

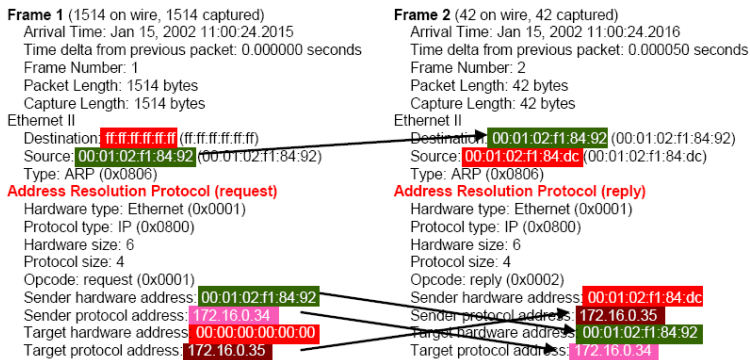
- Wenn Ursprungs- und Zieladresse im gleichen LAN sind: Rahmen verwerfen

- Wenn Ursprungs- und Zieladresse nicht im gleichen LAN sind: Rahmen in das LAN weiterschicken, in dem sich die Zieladresse befindet
- Wenn die Zieladresse unbekannt ist und für Broadcasts: Rahmen an alle anderen LANs weiterschicken (Flooding)

Das Bridging ist transparent, weil sich die Station nicht selber um das Bridging kümmern muss.

ARP-Request

Mit dem ARP-Protokoll erfragen Stationen die zu einer IP-Adresse gehörenden MAC-Adresse, damit die Rahmen dann direkt an die Zielstation gesendet werden können.



Station A:
 MAC 00:01:02:f1:84:92
 IP 172.16.0.34

Station B:
 MAC 00:01:02:f1:84:fc
 IP 172.16.0.35

Broadcast Storms und Spanning Tree Protocol

Rahmen mit unbekannter Zieladresse und Broadcasts werden endlos über die Bridges (Switches) weitergeleitet und belegen die gesamte Kapazität (Broadcast Storms). Lösung: Die Bridges (Switches) kommunizieren untereinander. Die Bridge mit der kleinsten ID (Priorität plus MAC-Adresse) wird als Root Bridge definiert. Anschließend wird ein Erreichbarkeitsbaum von der Root zu allen LANs berechnet (Anzahl der Links und Bandbreite als Kriterium für den besten Weg). Redundante Wege werden auf blockiert gesetzt und sind inaktiv. Bei Ausfällen wird der Baum neu konfiguriert. Bridges können einen Spanning Tree verwalten, Switches mehrere.

Broadcastproblematik

Ein Switch kann nur auf MAC-Adressen filtern. Somit gehen Broadcasts an alle Ports und belegen Bandbreite auf allen Segmenten (alle auf der Schicht 2 gekoppelten Segmente bilden eine Broadcast-Domäne). Router können Broadcast-Domänen trennen, in dem sie IP-Adressen filtern. Alternativ gibt es die Möglichkeit, virtuelle LANs einzurichten.

Virtuelle LANs (VLAN)

Gängige Switches erlauben die Einrichtung von virtuellen LANs. Dabei werden z.B. bestimmte Switch-Ports einem bestimmten VLAN zugeordnet und damit logisch gruppiert. Auf den Verbindungsleitungen zwischen den Switches werden VLAN-Trunks konfiguriert. Für eine Station erscheinen alle Stationen im gleichen VLAN so, als ob sie in einem gemeinsamen Netzsegment angesiedelt wären. Während in einem klassischen LAN die Zugehörigkeit einer Station durch den physikalischen Anschluss festgelegt wird, ist diese in VLANs freizügig definierbar und konfigurierbar.

Schicht-2-Broadcasts werden von einem Switch nur an die Ports weitergeleitet, die dem gleichen VLAN zugeordnet sind. Über die VLAN-Trunks werden sie aber an alle Stationen innerhalb des VLANs weitergeleitet – unabhängig davon, an welchen Switch diese angeschlossen sind. Zur Kommunikation zwischen den VLANs ist eine Kopplung auf der Schicht 3 durch Router erforderlich.

Vorteile von VLANs:

- Definition der VLANs unabhängig von der physikalischen Konfiguration: Arbeitsgruppen können flexibel definiert und umkonfiguriert werden
- Leistungsverbesserung: Weniger unnötiger Broadcastverkehr, weniger Verkehr durch Router
- Verbesserte Managementmöglichkeiten: Zentrale Konfiguration räumlich verteilter Geräte, logische statt physikalische Rekonfiguration der Netze
- Verbesserte Datensicherheit: Sensitive Daten können in separaten VLANs transportiert werden, erschwertes Abhören

Kapitel 7: Router und Routingprotokolle

Grundfunktionen eines Routers (OSI-Schicht 3)

- Paketfilterung: Trennung von Broadcastdomänen, Firewalling
- Routing (Wegewahl) auf der Basis der Zieladresse (erfolgt für jedes Paket und in jedem Router)
- Forwarding: Weiterleitung der Pakete vom Eingang zum richtigen Ausgang, evtl. Zwischenpufferung, Verwendung von Routingtabellen

Geroutete Protokolle vs. Routingprotokolle

Geroutetes Protokoll	Routingprotokoll
<ul style="list-style-type: none"> ▪ Protokoll, das über Schicht 3-Adressen verfügt ▪ Definiert Paketformate und Mechanismen für den Transport der Pakete durch das Netz von einem Endsystem zum anderen ▪ Wird (primär) zum Austausch von Nutzdaten verwendet ▪ Beispiele: IP, IPX (Novell), Appletalk (Apple) 	<ul style="list-style-type: none"> ▪ Protokoll wird zum Austausch von Routinginformationen zwischen Routern ▪ Wird zum Austausch von Topologieinformationen verwendet ▪ Topologieinformationen werden zum Aufbau und zur Pflege der Routingtabellen verwendet ▪ Kein Austausch von Nutzdaten ▪ Beispiele: RIP, IGRP (Cisco), OSPF

Metriken

- Routingprotokolle verwenden "Metriken" für jeden Pfad durch das Netz
 - Niedrigster Metrikwert kennzeichnet den "optimalen" Pfad
 - Bei Topologieänderungen erfolgt eine Neuberechnung des optimalen Pfads auf der Basis der zwischen den Routern ausgetauschten aktualisierten Metriken
- Anzahl der zu durchlaufenden Netze zum Ziel (Hop Count)
 - Einfachste Metrik
 - Unterschiedliche Bandbreite alternativer Wege nicht berücksichtigt
- Weitere Metriken
 - Bandbreite, Verzögerung, Belastung, Zuverlässigkeit, maximale Paketgröße der Links
 - "Kosten", frei definierbar
- Oft werden Kombinationen gewichteter Metriken verwendet
 - Defaultwerte für Metriken der Links und Gewichtung
 - Können zur Optimierung manuell geändert werden

Laden der Routingtabellen

- Statische Routen
 - Einträge in Routingtabellen werden manuell vorgenommen
 - Hoher Aufwand, da jedes Netz in jedem Router konfiguriert werden muss
 - Bei Änderungen müssen betroffene Router manuell umkonfiguriert werden
 - Volle Kontrolle über die Wege im Netz

- Sonderfall: Default Routen
 - In Netzen mit nur einem Ausgang zum Internet (Stub network)
 - Als Ziel, wenn kein Eintrag existiert (Gateway of last resort)
 - Alle Pakete (mit externem Ziel) werden zu diesem Ausgang geschickt
- Dynamische Routen
 - Router tauschen über Protokolle Routinginformationen untereinander aus
 - Automatische Konfiguration, weniger Konfigurationsaufwand
 - CPU-Belastung für Router durch Routingprotokolle
 - Belegung von Bandbreite im Netz durch Austausch von Routinginformation
 - Normalfall in großen Netzen

Longest Prefix Match

Durch die unterschiedliche Anzahl von für das Routing relevanten Bits (unterschiedliche Subnetzmasken) ist es möglich, dass mehrere Einträge in der Routingtabelle beim Vergleich mit der Zieladresse eines Pakets zu einer Übereinstimmung führen. Deshalb darf der Vergleich nicht nach dem ersten "Treffer" abgebrochen werden, sondern es muss sichergestellt werden, dass der Eintrag mit der maximalen Übereinstimmung (größte Anzahl von "1"-en in der Maske) gefunden und verwendet wird.

Distance Vector vs. Link State Routing

Distance Vector Routing Protokolle (Bellmann-Ford Algorithmus)	Link State Routing Protokolle (Shortest Path First Algorithmen)
<ul style="list-style-type: none"> ▪ Senden den kompletten Inhalt ihrer Routingtabellen an alle Nachbarn ▪ Metriken werden inkrementiert während sie durchs Netz propagieren ▪ Häufige, periodische Updates mit großen Datenmengen ▪ Wenig CPU-Belastung im Router, hoher Bandbreitenbedarf im Netz ▪ Lange Dauer bis nach einer Topologieänderung alle Routingtabellen wieder stabil sind (Konvergenz) ▪ Gut geeignet für kleine Netze, Beispiel RIP 	<ul style="list-style-type: none"> ▪ Senden Informationen über ihre Links an alle Router im Netz ▪ Jeder Router berechnet daraus die besten Wege zu allen Zielnetzen (Shortest Path Tree, Dijkstra-Algorithmus) ▪ Updates nur bei Änderungen der Topologie, wenig Daten pro Update ▪ Hohe CPU-Belastung im Router, wenig Bandbreitenbedarf im Netz ▪ Schnelle Konvergenz ▪ Gut geeignet für größere Netze, Beispiel OSPF

Lösungen für das Count to Infinity Problem

- Wert für "Infinity" möglichst klein wählen
 - Default bei RIP ist 16 Hops
- Split Horizon
 - Keine Informationen über eine Route an denjenigen schicken, von dem die Information über diese Route ursprünglich stammt
- Poison Reverse (in Kombination mit Split Horizon)
 - Routen, bei denen sich die Metrik signifikant vergrößert, explizit als nicht erreichbar kennzeichnen und entsprechend weitermelden
- Holddown (bis Konvergenz angenommen werden kann)
 - Nach Anzeigen eines Routenausfalls diese als nicht erreichbar kennzeichnen und einen Hold-down-Timer starten
 - Falls während der Holddown-Zeit die Router erreichbar gemeldet wird

- Akzeptieren wenn Anzeige vom gleichen Nachbar kommt
- Akzeptieren wenn Anzeige von einem anderen Nachbarn kommt und eine bessere Metrik hat als die ursprüngliche
- Ansonsten ignorieren

Kapitel 8: Die TCP/IP-Protokollfamilie und das Internet

Grundlegende Eigenschaften von IP-Netzen

- Paketorientiert, asynchrones Zeitmultiplex
- Datenpakete mit variabler Länge (IP-Pakete): optimiert für Datenverkehr
- TCP/IP-Protokolle sind sehr robust: jede Infrastruktur kann für IP-Transport verwendet werden
- Verbindungslose Kommunikation: ideal für burstartige Kommunikation, aber keine garantierte Dienstgüte möglich (IP+- Verfahren soll in Zukunft Abhilfe verschaffen)
- Hop-by-Hop Routing: Wegwahl in den Knoten (Routern) erfolgt abschnittsweise
- Keine Reihenfolgesicherung, IP-Pakete können verloren gehen: Mechanismen zur Behebung solcher Fehler müssen bei Bedarf in den höheren Protokollschichten (z.B. TCP) realisiert werden

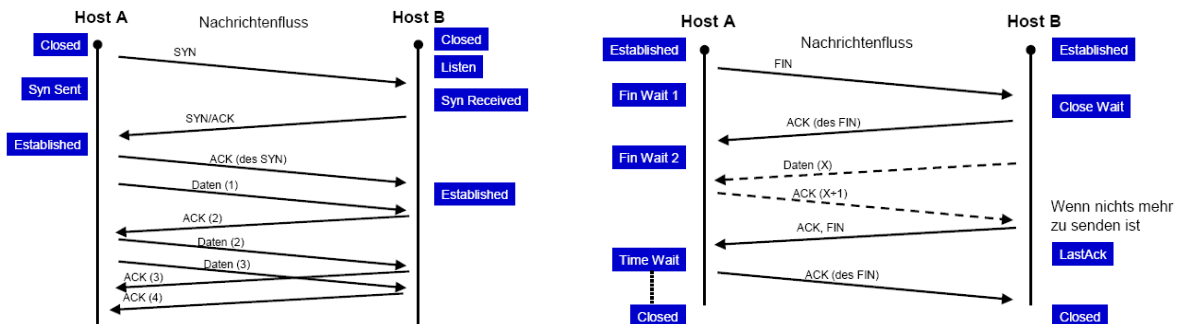
Das Portkonzept

- Die Dateneinheiten von TCP (Segmente) und UDP (Datagramme) enthalten jeweils zwei Felder (je 16 Bit), die die Quellenanwendung und die Zielanwendung der Daten identifizieren. Diese Adressen werden als Ports bezeichnet.
- Portnummern kleiner 255 sind für öffentliche, standardisierte Anwendungen reserviert
- Portnummern von 255 bis 1023 werden an Firmen für kommerziell vermarktete Anwendungen vergeben
- Portnummern über 1023 sind nicht reguliert und können beliebig verwendet werden

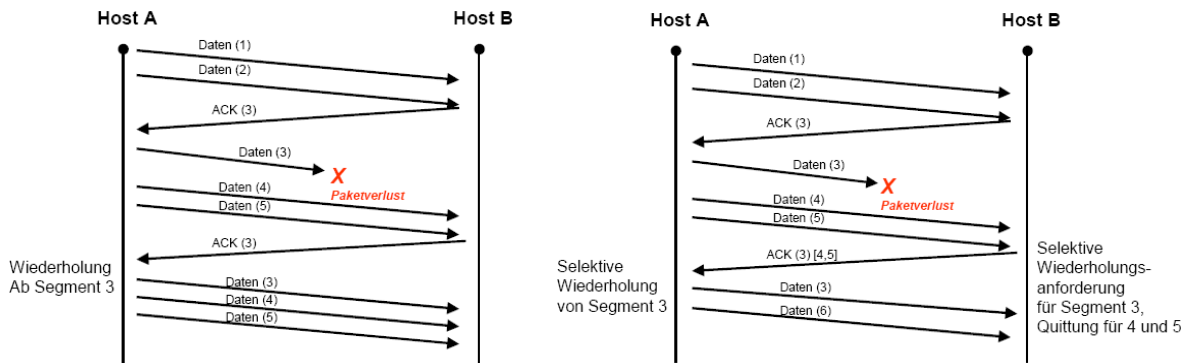
UPD und TCP

- UDP ist ein einfaches, verbindungsloses (datagramm-orientiertes) Protokoll. Es wird bei UDP keine Reihenfolgesicherung, keine Erkennung und Behebung von Verlusten und keine Flusssteuerung durchgeführt, lediglich eine Erkennung von Übertragungsfehlern wird (als Option) gewährleistet. Die von der Anwendung übergebenen Nutzdaten werden in einem Stück zusammen mit dem UDP-Header an die IP-Schicht übergeben und werden deshalb in der Regel in ein IP-Paket eingebettet bzw. bei Bedarf in der IP-Schicht fragmentiert.
- TCP ist ein hoch funktionales, verbindungsorientiertes Protokoll zur gesicherten Übermittlung von Byteströmen.

Verbindungsauf- und -abbau



Fehlerbehebung Go-Back-N und SACK



- Im Zustand ESTABLISHED werden Daten ausgetauscht, wobei alle empfangenen Daten bestätigt werden müssen. Der Datenaustausch erfolgt voll duplex. Damit nicht zu viele Bestätigungsmeldungen geschickt werden, werden die Acknowledgements verzögert gesendet und zwar entweder
 - sofort nach Eintreffen von 2 Daten-Paketen oder
 - 200 ms nach dem letzten Paket,
 je nachdem, was zuerst zutrifft. Der ursprüngliche TCP-Standard definierte nur eine normale Bestätigung (mit Go-Back-N Wirkung), die bei Verlust eines Pakets die Neuübertragung aller bis zum letzten in Reihenfolge empfangenen (und bestätigten) Byte erfordert. Natürlich ist dies nicht besonders effizient, da schon erhaltene Daten noch einmal übertragen werden.
- RFC 2018 definiert daher eine Erweiterung der TCP Acknowledgement-Meldungen, das sogenannte Selective Acknowledgement (SACK). Dieses ermöglicht es, neben der negativen Quittung für ein verlorenes Segment auch gleichzeitig positive Quittungen für bereits erhaltene Segmente zu senden. Die verlorenen Segmente können dadurch selektiv wiederholt werden, was die Effizienz des Verfahrens steigert.

Flusssteuerung

- TCP verfügt sowohl über eine empfangerbasierte als auch über eine senderbasierte Flusssteuerung.
- Zur empfangerbasierten Flusssteuerung sendet jede TCP-Instanz im TCP-Header die Fenstergröße mit die angibt, wie viele Bytes die Instanz noch akzeptieren, d.h. zwischenspeichern, kann ohne dass der Prozess, der die Daten verarbeitet, diese abholt. Wird z.B. ein rwnd-Wert von 1024 übertragen, so darf ein Sender, der dieses Segment empfängt, nur noch maximal 1024 Bytes senden, und muss dann auf ein Acknowledgement warten, bevor er weitere Daten senden darf.
- Die sendebasierten Flusssteuerung soll ein Netzwerk davor schützen, nach dem Verbindungsaufbau zu schnell überlastet zu werden. Dazu werden zwei Zustände definiert: *Slow Start* und *Con-gestion Avoidance*.