TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

Institut für Breitbandkommunikation

Unterlagen zu den Vorlesungen

DATENKOMMUNIKATION

und

KOMMUNIKATIONSPROTOKOLLE

Teil 2

o. Univ. Prof. Dr. Harmen R. van As

Technische Universität Wien, Institut für Breitbandkommunikation

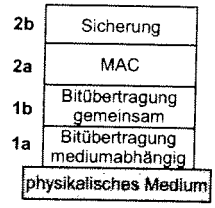
A-1040 Wien, Favoritenstr. 9-11/388

Datenkommunikation: Teil 2

2. OSI-Referenzmodell und dessen Realisierung

Version: Mai 2003

- Schicht 1: Leitungen, Übertragung; Synchronisierung
- Schicht 2: Fehlersicherung, Zugriffsprotokolle, Vernetzung
- Schicht 3: Vermittlung
- Schicht 4: Transport
- Schicht 5: Sitzung
- Schicht 6: Darstellung
- Schicht 7: Anwendung



Teilschichten in lokalen Netzen

Das OSI-Modell

Die Begriffe Protokoll (protocol) und Dienst (service) sind grundlegend. Protokolle (einer Schicht) sind präzise Festlegungen der Protokollelemente und Formate, die zwischen gleichrangigen Instanzen zweier Systeme ausgetauscht werden. Eine Instanz (entity) ist die Abstraktion der von einer Schicht in einem bestimmten System erbrachten Dienste. Die Gesamtheit der Protokolle aller Schichten wird als Protokollstapel (protocol stack) bezeichnet. Dienste (einer Schicht) sind Funktionen der jeweiligen Schicht, die der nächsthöheren Schicht zur Verfügung gestellt werden. Schichten können somit als Diensterbringer (service provider) bzw. Dienstnutzer (service user) aufgefasst werden.

OSI *(Open Systems Interconnection)* beschreibt Funktionalitäten und Regeln für einen Informationsaustausch zwischen offenen Systemen

(1) Reales System *(Real System)*
Rechner (inklusive Software, Peripheriegeräte, menschlicher Operatoren usw.), der in der Lage ist, Informationen autonom zu verarbeiten und/oder zu übertragen

(2) Reales Offenes System *(Real Open System)*
System, das den Anforderungen von OSI in Bezug auf den Informationsaustausch mit anderen realen Systemen genügt

(3) Anwendungsprozeß *(Application Process)*
Element innerhalb eines realen offenen Systems, das für eine bestimmte Anwendung die Aufgaben der Informationsverarbeitung übernimmt, z.B. der Benutzer an einem Terminal oder ein Programm, das auf eine entfernte Datenbank zugreift

(4) Offenes System *(Open System)*
Darstellung derjenigen Aspekte eines realen offenen Systems innerhalb des Referenzmodells, die für OSI von Bedeutung sind

Bild: OSI- Referenzmodell

Schichtenmodelle spielen in der Kommunikationstechnik und allgemein in der Informatik an verschiedenen Stellen eine wichtige Rolle.

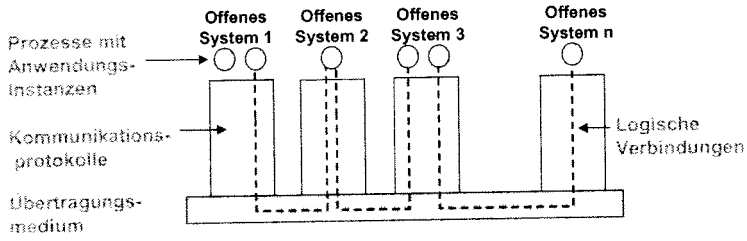
Sie basieren auf den folgenden Überlegungen:

Teilung und Beherrschung der Aufgaben: Ein komplexes System wird zerlegt, um es für Synthese und Analyse besser beherrschbar zu machen.

Unabhängigkeit der Schichten: Eine Schicht nutzt nur die Schnittstellenspezifikation zur unmittelbar darunter liegenden Schicht. Das bedeutet, der innere Aufbau der Schichten ist unwichtig, solange ihr Verhalten an der Schnittstelle gleich bleibt. Damit kann eine Schicht ausgetauscht oder ihr innerer Aufbau (Hard- oder Software) verändert werden, ohne dass das Gesamtsystem beeinflusst wird. Somit können Schichten modular (baukastenartig) kombiniert werden.

Abschirmung tiefer liegender Schichten: Eine Schicht sieht nur das Verhalten der unmittelbar darunter liegenden Schicht, nicht aber das der anderen Schichten. Damit wird die wahrgenommene Komplexität des Systems reduziert (Kapselung oder Geheimnisprinzip).

Standardisierung: Die Definition einzelner Schichten erleichtert die Standardisierung. Eine Schicht kann wesentlich schneller und leichter standardisiert werden als ein komplexes Gesamtsystem.



Vier Grundelemente, auf die sich das Referenzmodell bezieht:

(1) **offenes System** (Open System)

(2) **Anwendungs-Instanz** (Application Entity)
jener Teil eines Anwendungsprozesses, der für den Informationsaustausch verantwortlich ist

(3) **Logische Verbindungen** (Connections)
darüber werden Informationen zwischen Instanzen ausgetauscht

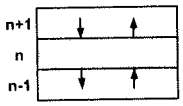
(4) **physikalisches Übertragungsmedium** (Medium)

Offene (Kommunikations-)Systeme bestehen aus (Hard- und Software-) Komponenten verschiedener Hersteller und sind bezüglich ihrer Anzahl und ihrer Ausdehnung nicht begrenzt. Die Offenheit wird durch eine Reihe von offenen, d.h. frei zugänglichen und nutzbaren Standards für den Informationsaustausch gewährleistet. Offene Teilsysteme können mit anderen offenen Teilsystemen, die dieselben Standards verwenden, problemlos kommunizieren. Anwenderprogramme oder Anwenderprozesse kommunizieren miteinander über logische Verbindungen, die alle das physikalische Übertragungsmedium, das Netz, benutzen.

Bild: Grundelemente des OSI- Referenzmodells

Strukturierungskonzept
Das Referenzmodell beschreibt die Kommunikation zwischen Systemen, die über Übertragungsstrecken untereinander verbunden sind. Es unterscheidet drei Grundelemente: Verarbeitungsinstanzen, Systeme, Übertragungsstrecken.

Verarbeitungsinstanzen sind logische Einheiten, zwischen denen Kommunikation letztlich stattfindet. Der Begriff der Verarbeitungsinstanz stellt eine Abstraktion dar, hinter der real zum Beispiel ein menschlicher Benutzer an einer Benutzerstation stehen kann, oder auch ein Programm, das auf einem Rechner ausgeführt wird.
Systeme sind entweder Endsysteme, welche Verarbeitungsinstanzen enthalten, oder Transitsysteme, die Verbindungen zwischen Endsystemen herstellen, falls diese nicht direkt miteinander verbunden sind. Der Begriff des Systems stellt eine Abstraktion dar, hinter der real beispielweise ein oder mehrere Verarbeitungsrechner mit Software, Peripheriegeräten, Benutzerstationen, Übertragungsmitteln oder auch Vermittlungsknoten stehen können.
Übertragungsstrecken verbinden Systeme untereinander.



Grundlegende Entwurfsprinzipien:

- jede Schicht erfüllt eindeutige und spezifische Aufgaben
- ähnliche Funktionen werden in einer Schicht zusammengefaßt
- interner Aufbau einer Schicht ist unabhängig von deren Funktionen
- Grenzen zwischen Schichten sind so definiert, daß möglichst wenig Steuer- und Kontrollinformationen zwischen diesen Grenzen erforderlich werden
- Informationsaustausch soll nur zwischen benachbarten Schichten stattfinden
- eine Schicht nutzt Dienste der unterliegenden Schicht und bietet ihre Dienste der nächsthöheren Schicht an

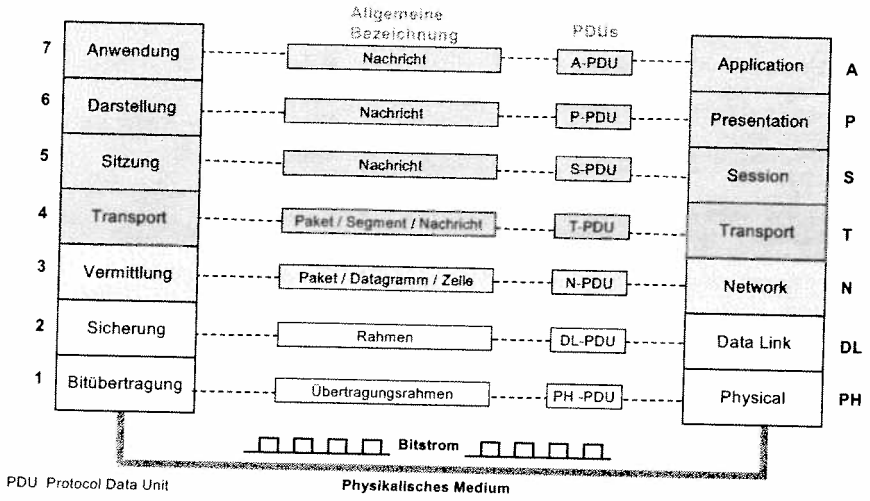
Anzahl der Schichten einerseits so groß, dass eine Schicht nicht völlig verschiedenartige Funktionen bearbeiten muss, andererseits auch hinreichend klein, damit die Architektur nicht zu unüberschaubar wird und der Kontrollaufwand nicht zu groß wird.

Das Schichtungsprinzip (Layering)

Die Verarbeitungsinstanzen stützen sich in ihrer Kommunikation auf eine Hierarchie von Kommunikationsdiensten, die aus der funktionalen Zerlegung der in jeder Kommunikation auftretenden allgemeinen Komponenten hervorgeht. Ein in der Hierarchie höherer Kommunikationsdienst umfasst dabei alle in der Hierarchie niedrigeren Kommunikationsdienste. Auf diese Weise entstehen Funktionsschichten. Sie erstrecken sich ebenso wie die Kommunikationsdienste über Systemgrenzen hinweg.

Bild: Schichten-Konzept im OSI-Referenzmodell

Was eine derartige Funktionsschicht zu leisten hat, ist durch die sie unmittelbar eingrenzenden Kommunikationsdienste als Differenz zwischen dem jeweils höheren und niederen Kommunikationsdienst bestimmt. Die Kommunikationsdienstleistung, die in einer Schicht zu dem sie begrenzenden niederen Kommunikationsdienst addiert werden muss, um den sie begrenzenden höheren Kommunikationsdienst zu erfüllen, muss nun wieder in einem durch ein Schichtenprotokoll geregeltes Zusammenspiel zwischen Instanzen erbracht werden, die verschiedenen Systemen, aber derselben Schicht angehören. Auf diese Weise entsteht aus der Hierarchie von Kommunikationsdiensten eine Hierarchie von Instanzen und Protokollen. Die Bilder zeigen die diversen Betrachtungsweisen zur Einteilungsmöglichkeiten der Schichten.



Je nach Protokollschicht werden die Dateneinheiten (Data Unit, DU) verschieden bezeichnet. Allgemein werden Protocol Data Units (PDU) zwischen gleichen Protokollschichten der beiden Endsystemen ausgetauscht, zum Beispiel T-PDU auf der Transport Schicht.

Bild: Übermittlungs- und Übertragungseinheiten

Je nach Schicht sind Bezeichnungen für die Dateneinheiten:

- **Daten (data):** E-Mail, File, Bild, Audiostrom, Videostrom.
- **Nachricht (message):** Dateneinheit der Ende-zu-Ende Kommunikation.
- **Segment (segment):** Segmentierter Nachrichtenteil der Ende-zu-Ende Kommunikation.
- **Paket (packet):** Vermittelte Dateneinheit durch das Netz über einer logischen Verbindung.
- **Datagramm (datagram):** Vermittelte Dateneinheit ohne logische Verbindung.
- **Zelle (cell):** Vermittelte Dateneinheit mit fester Länge über einer logischen Verbindung.
- **Rahmen (frame):** Dateneinheit der Schicht-2.
- **Übertragungsrahmen (transmission frame)** Übertragungsstruktur auf Schicht 1.

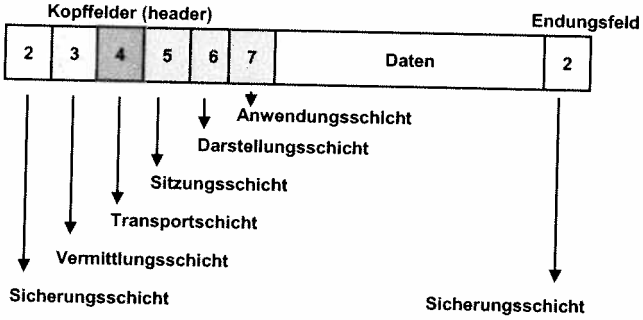


Bild: Struktur der Datenkommunikation nach OSI

Bild: Elemente des OSI-Referenzmodells

Die Aufgaben eines Protokolls innerhalb einer Schicht n hängen von der betreffenden Schicht ab.
In vielen Fällen sind dies:

- Auf- und Abbau von Verbindungen der Schicht n,
- Übertragung von Schicht-n Datenblöken,
- Reihenfolgeeinhaltung der übertragenen Dateneinheiten,
- Flusskontrolle zur Anpassung der sendenden Instanz an die empfangende Instanz,
- Fehlererkennung (z. B. fehlende Dateneinheiten),
- Fehlerbehebung (z. B. durch wiederholte Übertragung),
- Quittierung von richtig empfangenen Dateneinheiten,
- Zeitüberwachung zur Erkennung und Behebung von Verklemmungszuständen (deadlock),
- Kommunikation mit den benachbarten Schichten (n-1) bzw. (n+1) über das Adjacent Layer Protokoll (Dienstprotokoll).

Schicht 1

1) Mechanisch 2) Elektrisch
3) Funktional 4) Prozedural

Schicht 2

1) Auf- und Abbau der Schicht-2 Verbindung
2) Übertragung von Schicht-2 Datenblöcken
3) Rahmensynchronisation
4) Reihenfolgeerhaltung
5) Flusskontrolle
6) Fehlersicherung

Schicht 3

1) Auf- und Abbau der Schicht-3 Verbindung
2) Übertragung von Schicht-3 Datenblöcken
3) Wegelenkung (routing)
4) Reihenfolgeerhaltung
5) Flusskontrolle, Überlastabwehr
6) Fehlersicherung

Schicht 4

1) Auf- und Abbau der Schicht-4 Verbindung
2) Übertragung von Schicht-4 Datenblöcken
3) Reihenfolgeerhaltung
4) Flusskontrolle
5) Fehlersicherung

Schicht 5

1) Auf- und Abbau der Schicht-5 Verbindung
2) Übertragung von Schicht-5 Datenblöcken
3) Dialog-Management
4) Synchronisation mehrerer Datenflüsse
5) Flusskontrolle
6) Fehlerbehandlung

Schicht 6

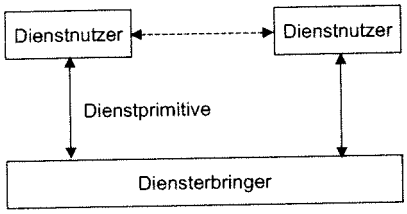
1) Auf- und Abbau der Schicht-6 Verbindung
2) Übertragung von Schicht-6 Datenblöcken
3) Anpassungen von Formatierung, Codierung und Komprimierung von Daten

Schicht 7

1) Auf- und Abbau der Schicht-7 Verbindung
2) Übertragung von Schicht-7 Datenblöcken
3) Identifizierung der gewünschten Kommunikationspartner
4) Authentisierung der Kommunikationspartner
5) Feststellung der momentanen Verfügbarkeit der Partner
6) Festlegung der Verantwortlichkeit bei Fehlerbehebung
7) Feststellung von eventuellen Einschränkungen bezüglich der Syntax
8) Einigung auf ein Verfahren zur Ressourcenaufteilung
9) Aushandlung der akzeptablen Dienstqualität
10) Synchronisation kooperierender Anwendungen

Spezielle Schichtaufgaben:
Schicht 2:
Rahmensynchronisation.
Schicht 3:
Wegelenkung (Routing),
Überlastabwehr
Schicht 4:
-
Schicht 5:
Dialogmanagement,
Synchronisation von Flüssen.
Schicht 6:
Anpassungen (Formatierung, Codierung, Komprimierung)
Schicht 7:
Authentisierung der Partner-anwendung,
Aushandlung verschiedener Kommunikationsparameter.

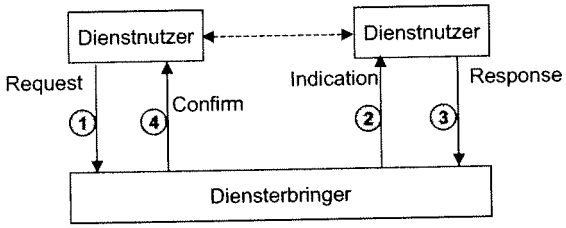
Bild: Aufgaben der sieben OSI-Schichten.



Diensterbringer:
z.B. gesamtes Kommunikationssystem, einzelne Schicht

Dienstbenutzer:
z.B. Benutzer, einzelne Schicht

Bild: Dienstnutzer / Diensterbringer



4 Typen von Dienstprimitiven:
- Anforderung (Request)
- Anzeige (Indication)
- Antwort (Response)
- Bestätigung (Confirm)

Bild: Austausch von Dienstprimitiven

Dienstprimitive (primitives, Dienstelemente)

Damit ein Dienst in Anspruch genommen werden kann, müssen sogenannte Dienstprimitve (Dienstelemente) zwischen benachbarten Schichten im selben Protokollstapel (protocol stack) ausgetauscht werden. Dies geschieht immer über einen Dienstzugangspunkt (SAP, Service Access Point).

- Es gibt vier Typen von Dienstprimitiven: Request, Indication, Response und Confirm.
- Es gibt einen bestätigten (alle vier Primitive) und einen unbestätigten Dienst (erste zwei Primitive).
- Eine Dienstprimitive wird wie folgt gekennzeichnet: Schichtabkürzung-Meldung.Dienstprimitiventyp (z.B. T-connect.request., T-connect.indication, T-connect response, T-connect.confirm).

Dienste werden mittels einer Anzahl von **Dienstelementen** (primitives) realisiert:

- **Request** (Anforderung): Eine Instanz (ein Dienstnutzer) veranlasst einen Diensterbringer zu einer bestimmten Operation, die ein Ereignis auslöst.
- **Indication** (Anzeige): Eine Instanz wird über ein Ereignis informiert.
- **Response** (Antwort): Eine Instanz antwortet auf eine Indication.
- **Confirm** (Bestätigung): Eine Instanz wird über das Ergebnis ihrer Anforderung informiert.

Diese vier Dienstelemente bilden zusammen einen bestätigten Dienst. Zur Darstellung der zeitlichen Abläufe werden Zeitdiagramme verwendet. Die Dienstelemente können in verschiedenen Dienstgruppen genutzt werden, z.B.

- CONNECT für den Verbindungsaufbau,
- DATA für den Datentransport und
- DISCONNECT für den Verbindungsabbau.

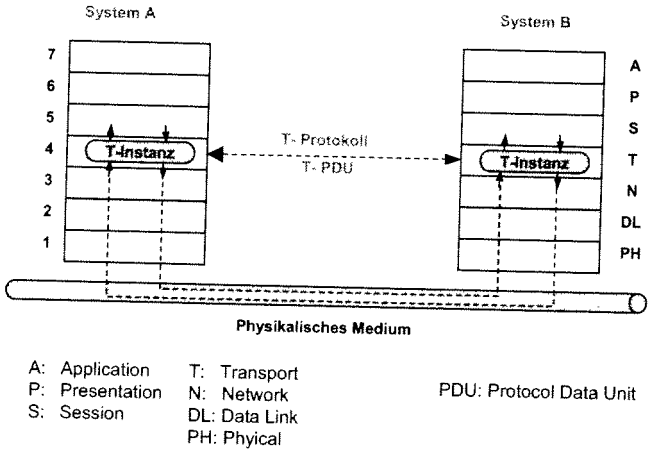
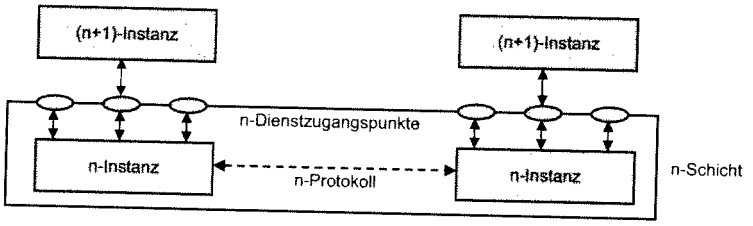


Bild: Kommunikation innerhalb einer Schicht

Das Bild zeigt eine logische Verbindung zwischen einem T-Instanzen-Paar in den Endsystemen A und B (Transportschicht). Sie dient als Diensterbringer für ein S-Instanzen-Paar als Dienstnutzer auf der Sitzungsschicht.



- n-Instanz:
  erbringt einen n-Dienst, der von (n+1)-Instanzen über n-Dienstzugangspunkte genutzt werden können
- n-Schicht:
  Abstraktionsebene mit definierten Aufgaben. Sie besteht aus allen n-Instanzen.
- n-Protokoll:
  bestimmt den Ablauf und Regeln zum Datenaustausch zwischen n-Instanzen

Bild: Instanz, Schicht und Protokoll

Im Bild ist die Kommunikation zwischen zwei Partner-Instanzen auf der (n+1)-Schicht unter Verwendung des n-Dienstes dargestellt. Dazu wird dieser n-Dienst über einen n-Dienstzugangspunkt (n-SAP) auf beiden Seiten adressiert, um die entsprechenden n-Instanzen zu identifizieren. Diese n-Instanzen auf beiden Seiten tauschen n-PDUs (Protocol Data Unit) über eine logische Verbindung mit Hilfe des n-Protokolls aus. Für jedes (n+1)-Instanzen-Paar ist auf beiden Seiten einen eigenen n-Dienstpunkt und einen eigenen n-Instanz notwendig. Für jedes (n+1)-Instanzen-Paar existiert auch eine eigene logische Verbindung.

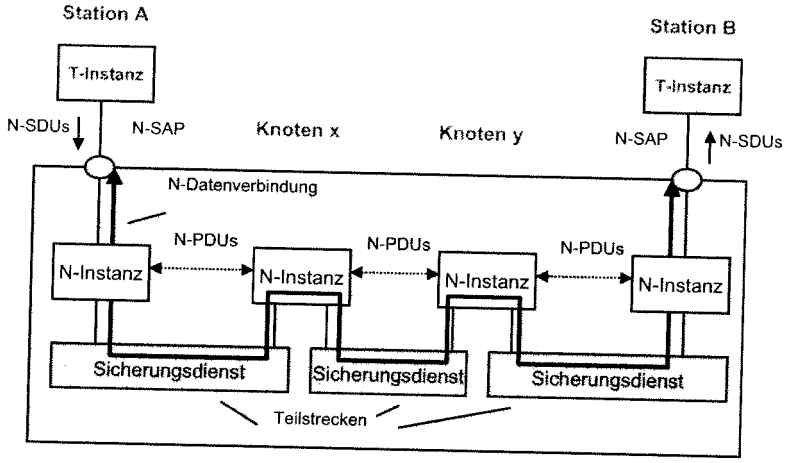


Bild: Logische Verbindung zwischen zwei T-Instanzen

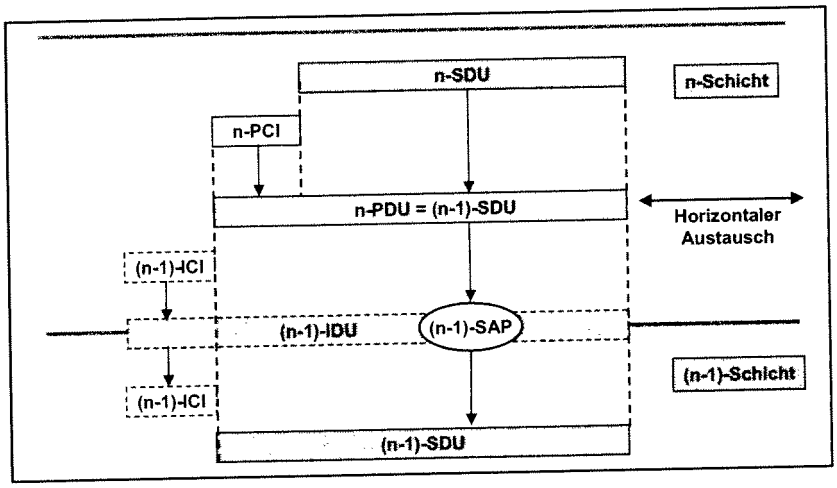
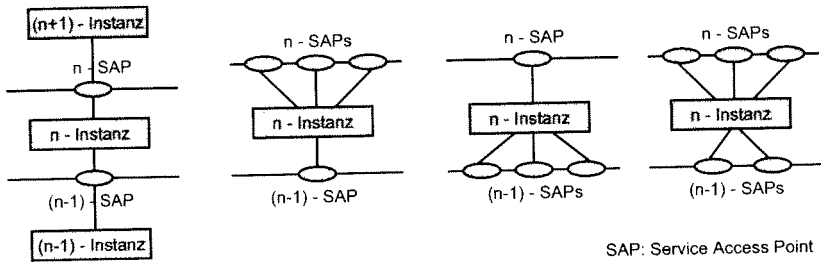


Bild: Schnittstellenübergabe von der n-Schicht zur (n-1)-Schicht



In Zusammenhang mit Multiplexen und Aufspreizen sind auch mehrere SAP-Kombinationen möglich.

Bild: Beziehungen zwischen SAPs und Instanzen

- zu einem gegebenen Zeitpunkt ist ein n-SAP mit genau einer (n+1)-Instanz und genau einer n-Instanz verbunden
- n-SAP kann von einer n-Instanz und/oder einer (n+1)-Instanz getrennt und einer anderen n-Instanz und/oder (n+1)-Instanz zugeordnet werden
- n-SAP wird über seine n-Adresse lokalisiert
- Adresse wird von (n+1)-Instanzen bei der Anforderung einer n-Verbindung benötigt

Bild: Temporäre Beziehungen zwischen SAPs und Instanzen

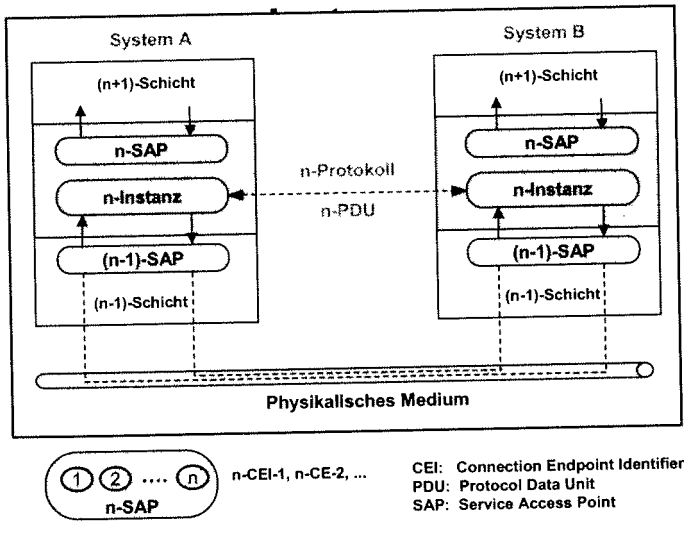


Bild: Logische Verbindungen

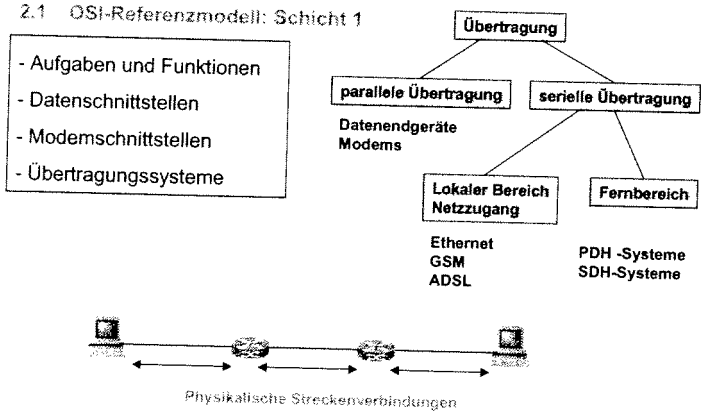
Verbindungskonzepte

Zur Unterstützung des Datenaustausches zwischen zwei n-SAPs wird das Konzept einer Verbindung (Connection) eingeführt. Dabei kann die n-Verbindung, die logisch zwei n-SAPs miteinander verknüpft, als Funktion der Schicht n aufgefasst werden muss, welche ihrerseits auf Funktionen unterer Schichten zurückgreift. Innerhalb eines n-SAP können mehrere Endpunkte von n-Verbindungen liegen, welche jeweils durch Verbindungsendpunkt-Kennungen (Connection Endpoint Identifier, CEI) unterschieden werden

2.1 OSI-Referenzmodell: Schicht 1

Version: Dez. 2003

Inhalt



Ziel:
Ungesicherte Übertragung einzelner Bits zwischen benachbarten Netzknoten

Aufgaben:

1) Auf- und Abbau der Schicht-1 Verbindung
2) Übertragung von Schicht-1 Datenblöcken

Mechanisch: Definition der Steckverbindung, Pinbelegung

Elektrisch: Definition der Codierung, Signale, ...

Funktional: Festlegung der einzelnen Funktionen
z.B. die Bedeutung der möglichen Spannungspegel an einzelnen Pins

Prozedural: Beschreibung der Abläufe
- Aktivierung und Deaktivierung von physikalischen Verbindungen
- bitserielle abschnittsweise Übertragung von Schicht-1 Datenblöcken

Bild: Bitübertragungsschicht

Die Übertragung lässt sich in die parallele und die serielle Übertragung unterteilen. Dabei sind alle Übertragungen, die nicht zum Verbinden eines Datengerätes oder Modems mit einem Kabel dienen, seriell. Hier unterscheidet man zwischen der Anschlusstechnik und der Fernübertragungstechnik. Die PDH-Übertragungssysteme werden heute nur noch als Zugangsleitungen verwendet.

Schicht 1: Bitübertragungsschicht (Ph: Physical)
Diese Schicht bewirkt eine ungesicherte Übertragung von Bits zwischen benachbarten Netzelementen (Netzknoten, Endgeräte, Rechner). Ihre beiden Aufgaben sind im Bild aufgeführt. Zu beachten ist, dass ein Übertragungsabschnitt zuerst physikalisch aktiviert werden muss, bevor die bitserielle Übertragung von Schicht-1 Datenblöcken stattfinden kann. Auf der Schicht 1 werden also die bitübertragungs-technischen Eigenschaften einer Übertragungsstrecke mechanisch, elektrisch, funktional und prozedural beschrieben. Hierbei werden einzelne Bits zwischen benachbarten Stationen übertragen. Die logische Gruppierung mehrerer Bits wird erst auf der Sicherungsschicht eingeführt.

Im Einzelnen erfüllt die Bitübertragungsschicht folgende Aufgaben:

- **Mechanisch:** definiert die Schnittstelle zwischen der Station (genauer: dem Netzadapter einer Station) und dem Übertragungsmedium. Dies ist in der Regel eine mehrpolige Steckverbindung.
- **Elektrisch:** definiert die Codierung der Bits (Spannungspegel, Impedanzen, Signalform, Frequenzbereich, etc.) und die Datenübertragungsrate.
- **Funktional:** legt die einzelnen Funktionen fest, die im Netzadapter vorhanden sind.
- **Prozedural:** beschreibt die Abläufe, die für die Bitübertragung erforderlich sind.

Auf der Schicht 1 werden die physikalischen Eigenschaften einer Übertragungsstrecke festgelegt. Dazu gehören. Eigenschaften des Übertragungsmediums, das verwendete Übertragungsverfahren sowie Belegung und Bauform der Steckverbindungen zwischen DTE (Data Terminal Equipment) und DCE (Data Communications Equipment). Die Datenendeinrichtung DTE ist das Endgerät (Rechner) des Benutzers, die Datenübertragungseinrichtung DCE als Netzanschlussmodul ist je nach Übertragungsverfahren ein Modern, ein ISDN-Adapter oder ein sonstiger Netzadapter. Die aktivierte physikalische Verbindung läuft über eine elektrische Leitung, eine Glasfaser oder eine Funkverbindung.

(1) Aktivierung und Deaktivierung von physikalischen Verbindungen
Verbindungen zwischen Instanzen der Sicherungsschicht werden auf Aufforderung einer dieser Instanzen aktiviert bzw. deaktiviert

(2) Übertragung von physikalischen Dienstdateneinheiten
sowohl synchron als auch asynchron

Bild: Funktionen der physikalischen Schicht

(1) Verbindungsbetrieb
erlaubt die Übertragung eines Bitstroms zwischen Instanzen der Sicherungsschicht

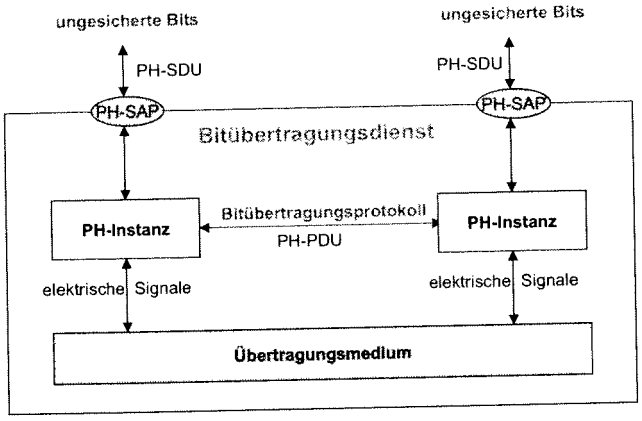
(2) Übertragung von physikalischen Dienstdateneinheiten
(*Physical Service Data Units*, Ph-SDUs)
Dienstdateneinheit besteht entweder aus einem Bit (serielle Übertragung) oder n Bits (parallele Übertragung); Halbduplex- und Vollduplexbetrieb möglich

(3) Physikalische Verbindungs-Endpunkte (*Physical Connection Endpoints*)
physikalische Verbindung kann mehrere Endpunkte haben; Verbindungsendpunkt-Identifikatoren bereitgestellt und von Instanzen der Sicherungsschicht benutzt, um physikalische Verbindungen zu identifizieren

(4) Reihenfolgeerhaltung (*Sequencing*)
Bits werden in der gleichen Reihenfolge ausgeliefert, in der sie gesendet wurden

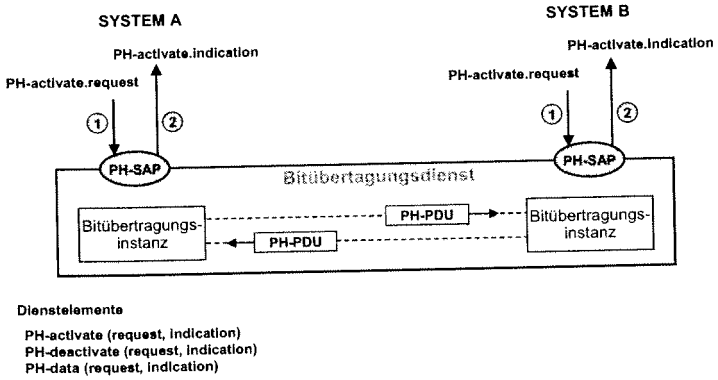
(5) Dienstgüte-Parameter (*Quality of Service*)
- Fehlerrate
- Verfügbarkeit des physikalischen Dienstes
- Übertragungsrate
- Übertragungsverzögerung

Bild: Dienste der physikalischen Schicht



PH: Physical Layer
PDU: Protocol Data Unit
SDU: Service Data Unit
SAP: Service Access Point

Bild: Bitübertragungsdienst



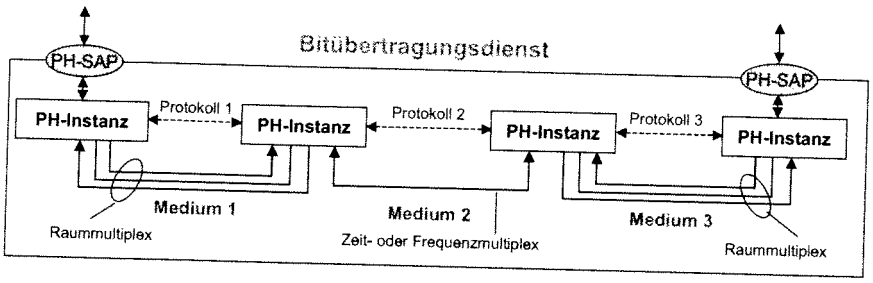
Dienstelemente

PH-activate (request, indication)
PH-deactivate (request, indication)
PH-data (request, indication)

Bild: Bitübertragungsdienst

Die beiden Funktionen ermöglichen eine Reihe von Diensten, wobei hier speziell auf die Bereitstellung von Gütemerkmalen (QoS) hingewiesen wird:

- Verbindungsbetrieb zwischen Sicherungsinstanzen über PH-SAPs (Service Access Points),
- Übertragung von PH-SDUs in serieller oder paralleler Form mit Halbduplex- oder Duplexbetrieb,
- Einrichtung von mehreren physikalischen Endpunkten,
- Einhaltung der Bitreihenfolge, auch bei paralleler Übertragung,
- Festlegung einer physikalischen Übertragungsverbindung mittels Güteparameter.



Dienst	request	indication	response	confirmation	Parameter
activate	x	x	x	x	Dienstgüteparameter
data	x	x			Bit: 0 oder 1 (oder Bitblock)
abort		x			Ursache(n)
deactivate	x	x	x	x	

SAP: Service Access Point

Bild: Bitübertragungsdienst

Die Bitübertragungsdienst kann auch mehrere Übertragungsstrecken mit verschiedenen Multiplextechniken enthalten. Die Bitströme (PH-PDUs) werden streckenweise zwischen PH-Instanzen übertragen. Sie überwachen unter anderen die Qualität der Übertragung. Die gesammelten Daten sind die Basis für Netzmanagement-Entscheidungen.

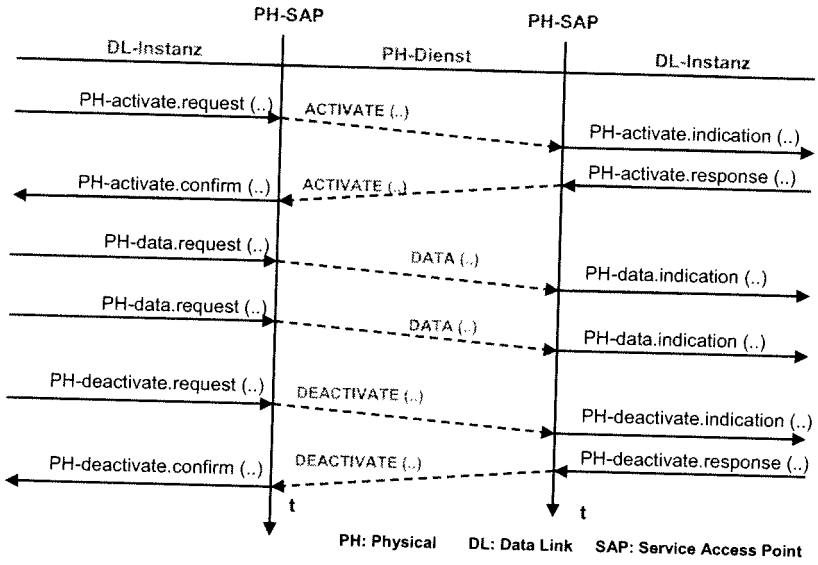


Bild: Zeitfolgediagramm der PH-Dienst

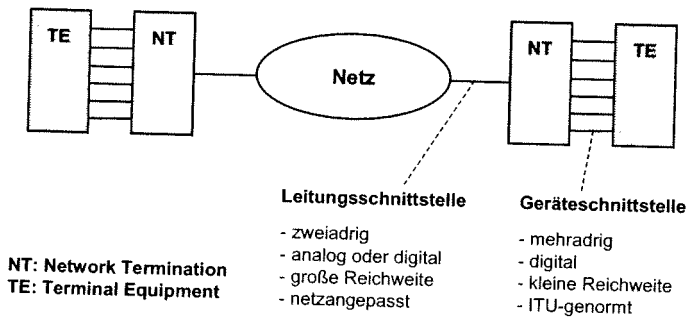
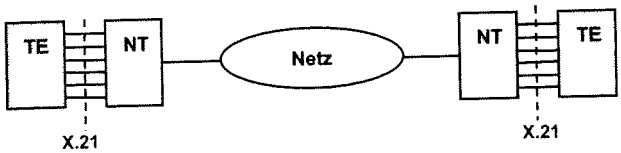


Bild: Datenübertragung

Wichtige Standards der Schicht 1 sind:

- **X.21:** Schnittstelle für synchrone Datenübertragung über öffentliche Datennetze. Dabei wird die DTE aus dem Netz getaktet.
- **X.21bis:** Schnittstelle zwischen DTE und synchronen Modems der V-Serie in öffentlichen Datennetzen.
- **V.24:** Schnittstelle für asynchrone Datenübertragung über Telefonleitungen.
- **RS-232-C:** Ein amerikanischer Standard, die sehr ähnlich zu V.24 ist.



Benutzerklasse	Datenübertragungsrate (netto)	Signalisierung - IA 5
3	600 bit/s	600 bit/s
4	2,4 kbit/s	2,4 kbit/s
5	4,8 kbit/s	4,8 kbit/s
6	9,6 kbit/s	9,6 kbit/s
7	48 kbit/s	48 kbit/s
19	64 kbit/s	64 kbit/s

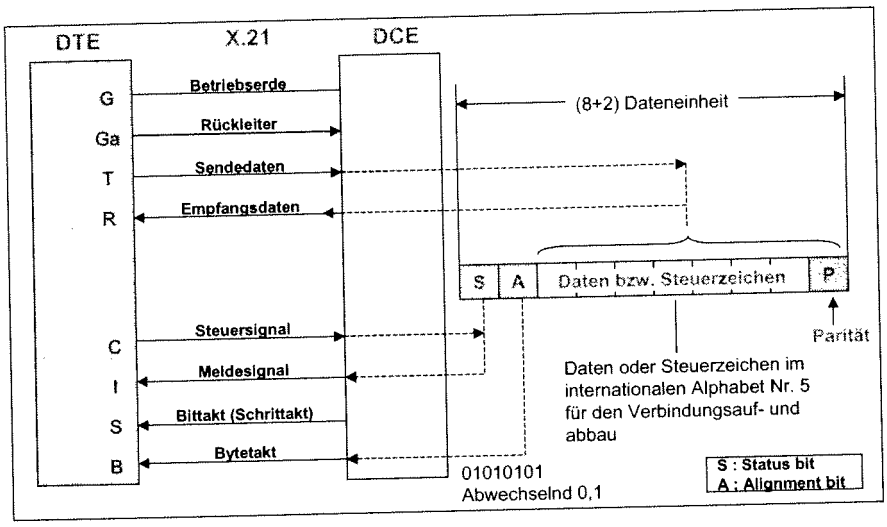
X.1: Benutzerklasse für Synchronbetrieb

IA 5 - International Alphabet Number 5

X.21, X.21 bis

Leitungsvermittelte Datennetze besitzen keine große Bedeutung mehr. X.21 beschreibt eine Verbindungs-Schnittstelle für DTE-DCE für die synchrone Übertragung in solchen Netzen, wird aber auch in Paketnetzen wie X.25 eingesetzt. Die vorgesehenen Schnittstellenleitungen ermöglichen den Verbindungsauf- und -abbau sowie die eigentliche Datenübertragung. Die Wählzeichen werden nach dem IA5 Code (International Alphabet Number 5) übertragen. Nach Aufbau der Verbindung ist eine transparente Übertragung möglich. X.21bis erlaubt den Einsatz von DTE mit V.24-Schnittstellen in digitalen Netzen mit Paket- oder Leitungsvermittlung.

Bild: Synchrone Datenübertragung: X.21



Über die X.21-Schnittstelle werden Daten in Rahmen von 10 Bits ausgetauscht. Sie bestehend aus Zustandsbit, Synchronisationsbit, 7-Bit Daten oder Steuerzeichen sowie einem Paritätsbit. Erdleiter, Rückleiter, Bit- und Bytetakt werden parallel übertragen.

Bild: X.21 Schnittstelle

7 6 5	4 3 2 1								
		0	0	0	0	1	1	1	1
		0	0	1	1	0	0	1	1
		0	1	0	1	0	1	0	1
0 0 0	0 0 0 0	NUL	(TC7) DLE	Sp	0	@	P	`	p
0 0 0	0 0 0 1	(TC1) SOH	DC1	!	1	A	Q	a	q
0 0 1	0 0 1 0	(TC2) STX	DC2	"	2	B	R	b	r
0 0 1	0 0 1 1	(TC3) ETX	DC3	#	3	C	S	c	s
0 1 0	0 1 0 0	(TC4) EOT	DC4	(S)	4	D	T	d	t
0 1 0	0 1 0 1	(TC5) ENQ	(TC8) NAK	%	5	E	U	e	u
0 1 1	0 1 1 0	(TC3) ACK	(TC9) SYN	&	6	F	V	f	v
0 1 1	0 1 1 1	BEL	(TC10) ETB	'	7	G	W	g	w
1 0 0	1 0 0 0	FE0 (BS)	CAN	(	8	H	X	h	x
1 0 0	1 0 0 1	FE1 (HT)	EM	)	9	I	Y	i	y
1 0 1	1 0 1 0	FE2 (LF)	SUB	*	:	J	Z	j	z
1 0 1	1 0 1 1	FE3 (VT)	ESC	+	;	K	Ä	k	ä
1 1 0	1 1 0 0	FE4 (FF)	IS4 (FS)	,	<	L	Ö	l	ö
1 1 0	1 1 0 1	FE5 (CR	IS3 (GS)	-	=	M	Ü	m	ü
1 1 1	1 1 1 0	SO	IS2 (RS)	.	>	N	^	n	ß
1 1 1	1 1 1 1	SI)	IS1 (US)	/	?	O	_	o	DEL

Das Internationales Alphabet Nr. 5 besteht aus 7 Bits und enthält Nutz- und Steuerzeichen.

Bild: Internationales Alphabet Nr. 5

Kurzzeichen	Benennung	Übersetzung
Übertragungszeichen		
SOH	Start of Header	Kopf-Anfang
STX	Start of Text	Text-Anfang
ETX	End of Text	Text-Ende
EOT	End of Transmission	Ende der Übertragung
ENQ	Enquiry	Stationsaufforderung
ACK	Acknowledge	Positive Rückmeldung
DLE	Data Link Escape	Übertragungsumschaltung
NAK	Negative Acknowledgment	Negative Rückmeldung
SYN	Synchronisation, IDLE	Synchronisierung, Leerzeichen
ETB	End of Transmission Block	Ende des Übertragungsblockes
Formatsteuerzeichen		
BS	Backspace	Rückwärtsschritt
HT	Horizontal Tabulation	Horizontaler Tabulator
LF	Line Feed	Zeilenvorschub
VT	Vertical Tabulation	Vertikaler Tabulator
FF	Form Feed	Formularvorschub
CR	Carriage Return	Wagenrücklauf

Bild: Bedeutung einiger Zeichen

Der zeitliche Ablauf der Datenübertragung über der X.21 wird gesteuert über den parallelen Steuerleitungen (Control der DTE und Indication der DCE). Ein Duplexdatenaustausch kann nur stattfinden, wenn die C- und I-Signale auf logisch 0 liegen. Die Auslösung

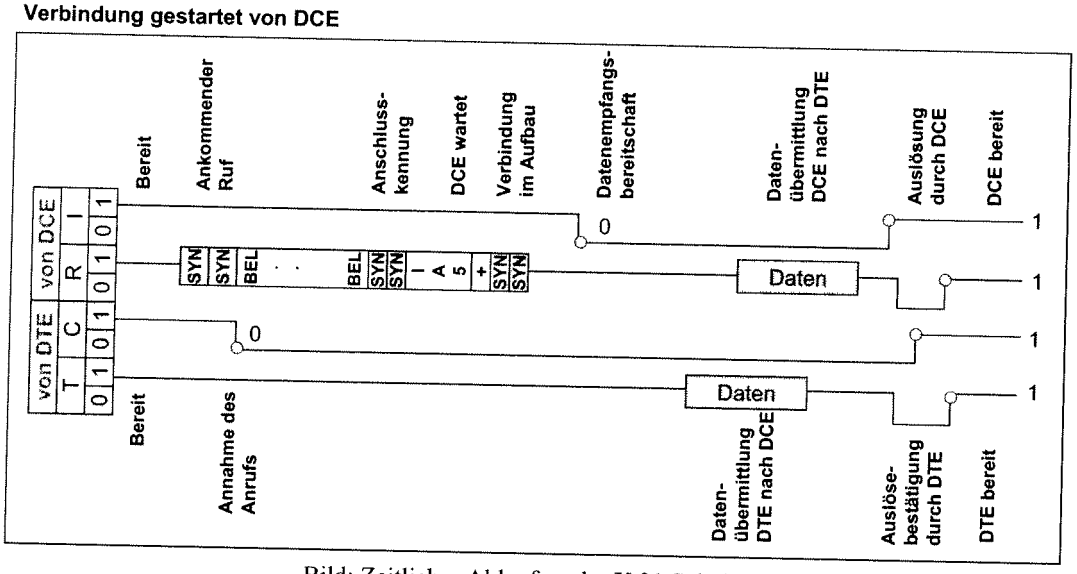
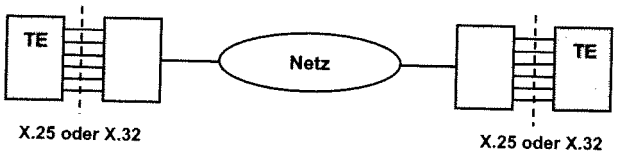


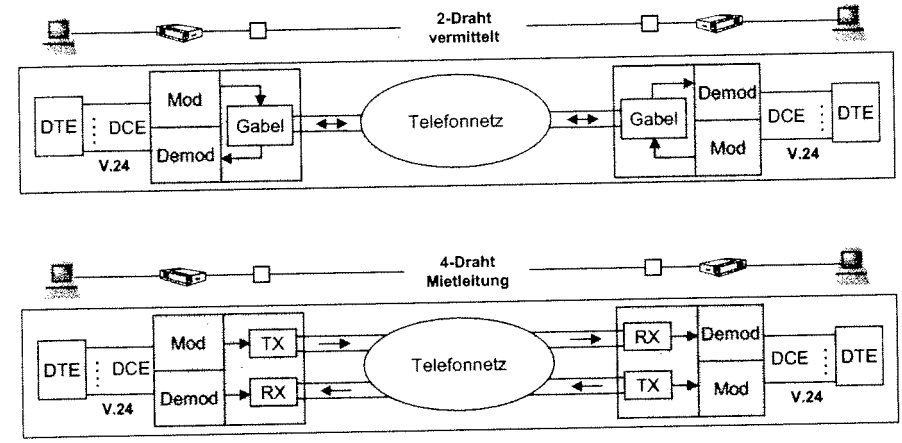
Bild: Zeitlicher Ablauf an der X.21 Schnittstelle



Benutzerklasse	Datenübertragungsrate	Signalisierung
8	2,4 kbit/s	2,4 kbit/s
9	4,8 kbit/s	4,8 kbit/s
10	9,6 kbit/s	9,6 kbit/s
11	48 kbit/s	48 kbit/s
12	1,2 kbit/s	1,2 kbit/s
13	64 kbit/s	64 kbit/s

X.1 Benutzerklasse für Paketbetrieb

Bild: Asynchrone Datenübertragung: X.25 oder X.32



DCE Data Circuit Equipment
DTE Data Terminal Equipment

TX Transmit
RX Receive

Bild: Modem-Verbindungen

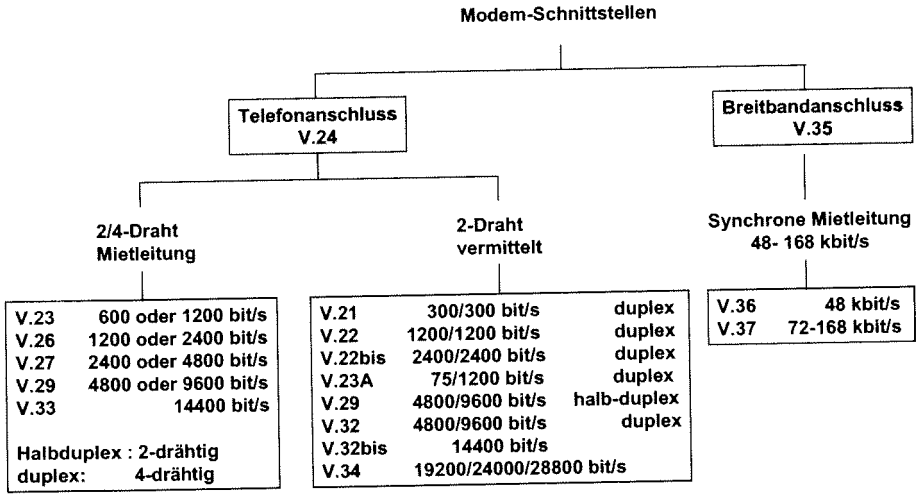


Bild: Modem-Schnittstellen: V.Serie

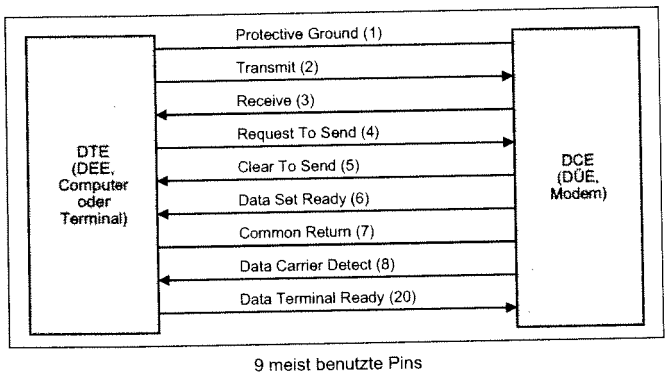


Bild: V.24 / RS-232 C: Pinbelegung

V.24 und RS-232-C

Die Schnittstelle (Interface) nach V.24 entspricht im wesentlichen RS-232-C. Sie ist sehr weit verbreitet, erlaubt jedoch nur eine maximale Datenrate von 20 kbit/s bei einer maximalen Distanz von 15 m. Bei kleineren Distanzen erreicht man jedoch wesentlich höhere Datenraten.

V.24 beschreibt nur die logische Definition der Schnittstellenleitungen und die darauf ablaufenden Vorgänge. Die elektrischen und mechanischen Eigenschaften sind in V.28 festgelegt. Eine logische Null wird durch eine Spannung von weniger als -3V repräsentiert, eine logische Eins durch mindestens + 4V. Maximal bzw. minimal sind + 15 V bzw. - 15 V zulässig. Alle Leitungen werden unsymmetrisch gegen Masse betrieben. Die standardisierte Steckverbindung ist 25-polig. Die Leitungen der Pins 1 bis 8 und 20 werden praktisch immer benötigt, während die anderen weniger wichtige Funktionen repräsentieren und deshalb oft weggelassen werden. Dann kann auch eine kleinere 9-polige Steckverbindung eingesetzt werden.

Die Pins 1 bzw. 7 werden als Schutzerde (protective ground) bzw. Betriebserde (signal ground) genutzt. Sendedaten (TxD: Transmit Data) verwenden Pin 2, Empfangsdaten (RxD: Receive Data) Pin 3. Mit Pin 4 (RTS: Request To Send) wird von der DTE das Einschalten des Senders verlangt, die Sendebereitschaft wird über Pin 5 (CTS: Clear To Send) gemeldet. Pin 6 zeigt an, dass die DTE betriebsbereit ist (DSR: Data Set Ready), Pin 20 meldet dasselbe für die DCE (DTR: Data Terminal Ready). Pin 22 (RI: Ring Indicator) meldet einen ankommenden Ruf. Pin 8 (RLSD/CD: Received Line Signal Detector, Carrier Detector; auch DCD: Data Carrier Detect) zeigt einen ausreichenden Pegel des empfangenen Signals an.

Takte werden auf den Pins 24, 15 und 17 übertragen. Auf Pin 24 (TC: Transmitter Clock) gibt die DTE der DCE den Sendeschritttakt vor. Über Pin 15 (TxC: Transmitter Clock) taktet ein synchrones Modern die DTE beim Senden. Pin 17 (RxC: Receive Clock) übernimmt dieselbe Funktion beim Empfangen.

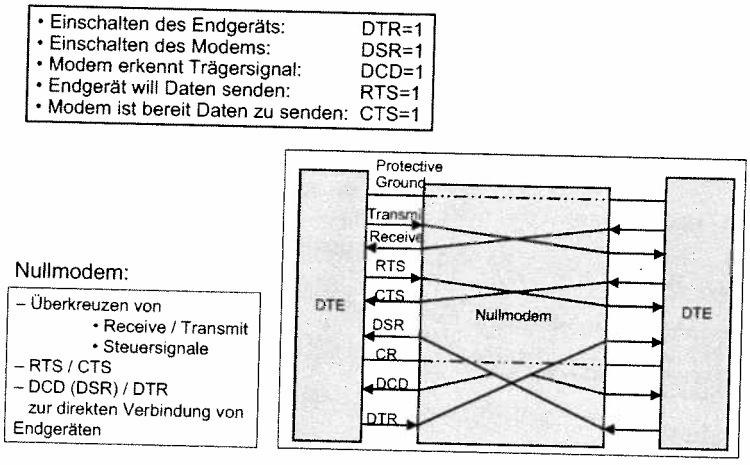


Bild: RS-232 C Schnittstelle und Nullmodem

Die Pins 14, 16, 19, 13 und 12 beziehen sich auf einen Hilfskanal. Die Signale TxD, RxD, RTS, CTS und DCD sind sinngemäß wie die entsprechenden Signale des Hauptkanals zu interpretieren. Die Pins 9 und 10 sind für Testzwecke reserviert. Pin 18 (LL: Local Loopback) aktiviert einen Test, bei dem das gesendete Signal die lokale DCE durchläuft und von dieser dann zum Sender zurückgegeben wird. Pin 21 verlangt einen Remote Loopback, sofern das Signal vom DTE gesendet wird. Der Loopback wird dann vom entfernten Modern ausgeführt, wodurch beide Modems und die Übertragungsstrecke getestet werden. Die entfernte DTE wird über Pin 25 (TM: Test Mode) informiert, dass ein Test stattfindet.

V.35, V.36, V.37

Die Verbindungsschnittstellen V.35, V.36 und V.37 verwenden im Gegensatz zu V.24 erdsymmetrische Takt- und Datenleitungen. Dadurch werden höhere Datenraten erreicht (in derselben Reihenfolge: 48 kbit/s, 72 kbit/s und 144 kbit/s). Steuer- und Meldeleitungen bleiben unsymmetrisch. Die elektrischen Eigenschaften für unsymmetrische Leitungen werden (mit Ausnahme von V.35) in V.10 (bzw. in RS-423-A) spezifiziert, diejenigen für symmetrische Leitungen in V.11 (bzw. RS-422-A). Die Funktion der Leitungen in V.35 bis V.37 entspricht der in V.24.

V.10, V.11, RS-449

Für die erdsymmetrischen Takt- und Datenleitungen der Schnittstellen V.35 bis V.37 sind Stecker mit mehr Pins erforderlich. Der Stecker für V.35 weist 34 Pins auf, als Spannungspegel werden - 0,55 V (logische 1) bzw. + 0,55 V (logische 0) verwendet. Für V.36 werden 15-polige Stecker für Datennetze bzw. 37-polige Stecker für Telefonnetze) eingesetzt. Für V.10 wird eine Datenrate von 20 kbit/ s über eine Distanz von maximal 50 m bzw. 100 kbit/s über 19 m spezifiziert. Bei V.11 werden 100 kbit/s über maximal 1000 m, 2 Mbit/s über 50 m und 10 Mbit/s über 10 m erreicht, sofern die Leitungen mit dem Wellenwiderstand abgeschlossenen sind.

Weitere Schnittstellen mit höherer Geschwindigkeit

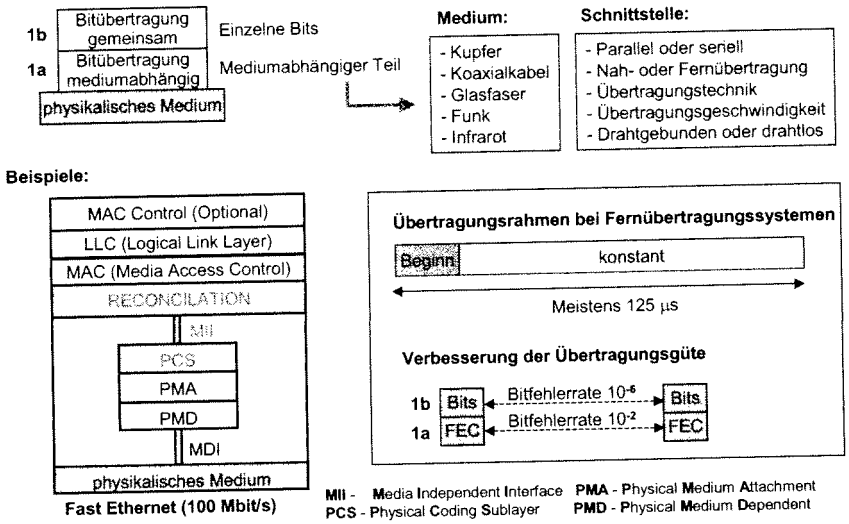
Die oben behandelten Schnittstellen sind Geräteschnittstellen (externe Schnittstellen) und stellen primär Punkt-zu-Punkt Verbindungen bereit. Als Schnittstellen zu DCE können auch (geräteinterne) parallele Systembusse (PCI: Peripheral Component Interconnect) oder externe, serielle Busse (USB, Firewire) genutzt werden.

Einige weitere Schnittstellen für höhere Geschwindigkeiten sind:

- **Ethernet:** 10/100 Mbit/s (Fast Ethernet, FE), GbE, 10GbE
- **ATM25:** Eine vom ATM-Forum spezifizierte Schnittstelle für ADSL-Netzanschlüsse mit 25,6 Mbit/s. Sie ermöglicht den durchgängigen Transport von ATM-Zellen zwischen Dienstanbieter und Teilnehmer. Funktionen dieser Schnittstelle sind die Segmentierung und Reassemblierung von Datenpaketen in ATM-Zellen, die Erzeugung und Überprüfung der Zellen-Header und Leitungscodierung für das verwendete Übertragungsmedium.
- **ATM50:** Von der FSAN-Initiative (Full Service Access Network) erarbeitete Spezifikation für eine VDSL-Schnittstelle mit 50 Mbit/s.
- **UTOPIA, UTOPIA-2** (Universal Test and Operations Physical Interface for ATM): Vom ATM-Forum definierte Schnittstellen zwischen ATM-Bausteinen für die Schichten 1 und 2. UTOPIA-1 verwendet einen bidirektionalen Datenbus mit der Breite von 8 Bits mit einer Taktfrequenz 7 bis 25 MHz und ATM-Datenraten bis 155 Mbit/s. Bei UTOPIA-2 kann der Bus 8 oder 16 Bits breit sein und kann mit bis zu 50 MHz getaktet werden.

Zudem kann mehr als ein Baustein der Schicht 1 angesprochen werden:

- **TAXI** (Transparent Asynchronous Receive Transnit Interface) steht für eine optische Schnittstelle, mit der Endgeräte oder FDDI-Netze an einen ATM-Switch angeschlossen werden können. Die Datenrate ist 100 Mbit/s, als Leitungscode wird eine 4B5B-Codierung genutzt.



Zur Erhöhung der Flexibilität wird heute die Bitübertragungsschicht aufgeteilt in einen gemeinsamen und einen mediumabhängigen Teil.

Die diversen Medien sind: Kupfer, Koaxialkabel, Glasfaser, Funk und Infrarot.

Ferner sind die Eigenschaften der Schnittstelle zu betrachten:

- parallel oder seriell,
- Nah- oder Fernübertragung,
- Übertragungstechnik,
- Übertragungsgeschwindigkeit,
- drahtgebunden oder drahtlos.

Bild: Unterteilung der Bitübertragungsschicht

Wichtige Beispiele sind auch:
Die Aufteilung bei den Ethernet-Standards (10 Mbit/s, 100 Mbit/s, 1 Gbit/s und 10 Gbit/s).

- Die Verbesserung der Bitfehlerrate durch Forward Error Coding (FEC) bei schlechten Übertragungsmedien.

Synchronisation bei bitserieller Übertragung

- **Asynchrone Übertragung**
  - Übertragung eines Datenblocks kann zu jedem Zeitpunkt erfolgen
  - Anfang und Ende müssen vom Sender speziell markiert werden
    - Start/Stop-Verfahren
    - Präambel mit 0/1-Folge
  - Sender und Empfängertakt können voneinander abweichen dadurch beschränkte Datenrate und Rahmengröße
- **Synchrone Übertragung**
  - Übertragung der Daten nur zu festen Zeitpunkten
  - Permanente Synchronisation auch wenn keine Nutzdaten gesendet werden
    - gemeinsames Taktsignal
    - Leitungscodes mit Bittaktrückgewinnung (eventuell mit Verwürfeln (Scrambling) der Daten)

Bild: Bitsynchronisation

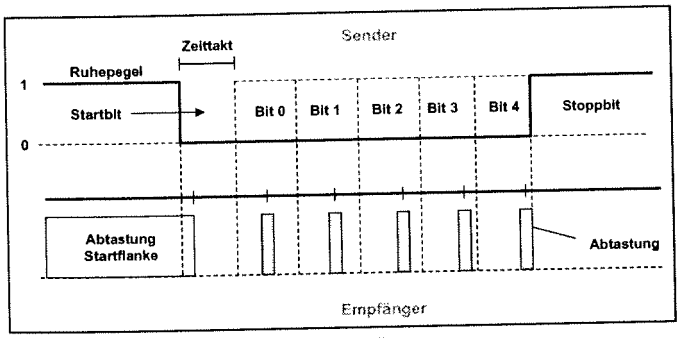


Bild: Asynchrone Übertragung

Asynchrone Übertragung

Bei der asynchronen Übertragung werden einzelne Zeichen übertragen. Jedes Zeichen wird als Rahmen dargestellt, der ein **Startbit,** n Datenbits und ein (oder mehr) **Stoppbits** enthält. Die Taktgeber im Sender und Empfänger liefern nominal dieselbe Frequenz, sind aber unabhängig voneinander. Dadurch ist eine (geringe) Frequenzdifferenz unvermeidlich. Für die Übertragungsdauer eines Zeichens wird durch das Startbit bzw. durch dessen Startflanke eine hinreichende Synchronisation hergestellt. Damit kann der Empfänger die zeitliche Lage der empfangenen Bits bestimmen und das empfangene Signal in der Bitmitte abtasten.

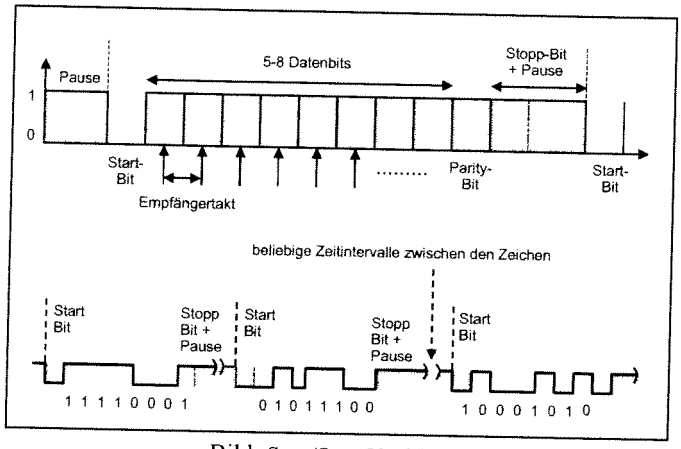


Bild: Start/Stop-Verfahren

Zwischen zwei Zeichen liegt eine Pause, deren Dauer mindestens die Länge des Stoppbits beträgt. Bei der asynchronen Übertragung wird ein bestimmter Zeichencode (häufig der ASCII-Code) zugrunde gelegt, der (auf dem Bildschirm und Drucker) darstellbare Zeichen und Steuerzeichen enthält. Damit ist die Übertragung nicht transparent, d. h., es können nicht beliebige Bitkombinationen übertragen werden. Zur Interpretation eines Steuerzeichens als normales Zeichen kann das Escape-Zeichnen vorangestellt werden.

Die asynchrone Übertragung ist einfach, die Zahl der pro Zeichen übertragbaren Nutzbits in der Praxis maximal acht und der Zusatzaufwand zur Übertragung von Start- und Stoppbits ist hoch.

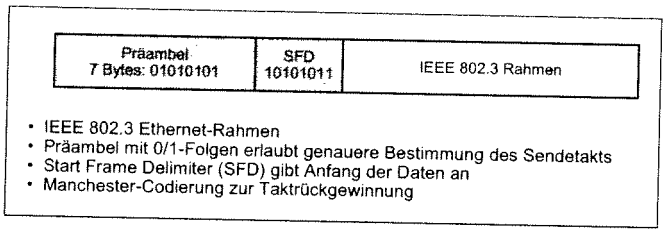


Bild: Bitsynchronisation bei IEEE 802.3 Ethernet

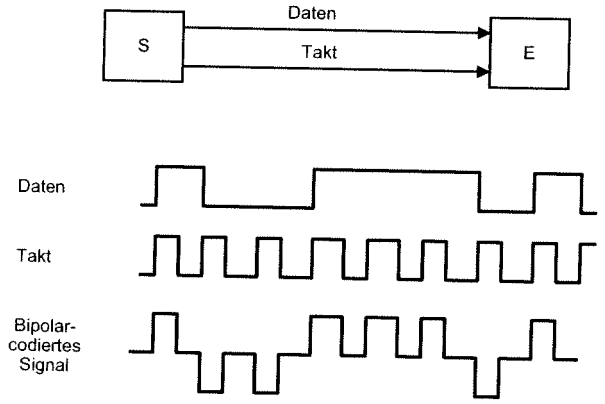


Bild: Synchrone Übertragung

Synchrone Übertragung

Im Gegensatz zur asynchronen Übertragung werden die Taktgeber von Sender und Empfänger aufeinander synchronisiert. Dies erfolgt zu Beginn eines Rahmens durch Synchronisationsbits. Die Synchronisation wird während der Übertragung aufrechterhalten. Da man den Takt des Senders in der Regel nicht auf einer eigenen Leitung übertragen möchte, muss der Leitungscode genügend Taktinformation beinhalten.

Die synchrone Übertragung kann bitorientiert oder zeichenorientiert durchgeführt:

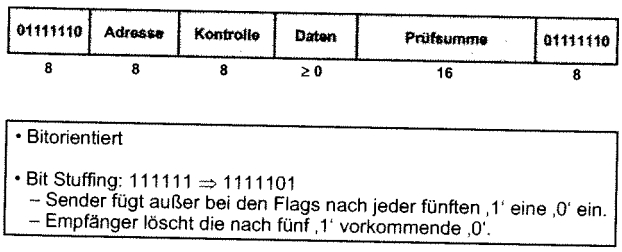
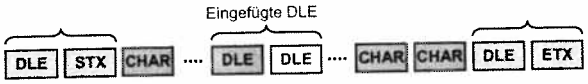


Bild: High-Level Data Link Control (HDLC)

Bei der bitorientierten Variante wird ein festes Bitmuster gewählt, häufig 01111110 als Rahmenbegrenzung (flag). Als Nutzdaten sollen beliebige Bitmuster mit beliebiger Länge übertragen werden. Damit eine Folge von sechs Einsen in den Nutzdaten nicht als Rahmenbegrenzung interpretiert wird, wird das Bitstopfen (bit stuffing) angewendet. Dabei wird nach jeweils fünf Einsen vom Sender eine Null eingefügt und vom Empfänger wieder entfernt. Somit kann die Bitfolge für die Rahmenbegrenzung in den Nutzdaten nicht auftreten.



- DLE (data link escape)
  - zeigt Steuerzeichen an
- Steuerzeichen
  - zeigen Anfang und Ende eines Datenpakets an
  - STX (start of text)
  - ETX (end of text)
- Character Stuffing

Bild: Zeichenorientierte Protokolle

Bei der zeichenorientierten Variante werden - wie bei der asynchronen Übertragung - Zeichen eines bestimmten Codes übertragen, allerdings ohne Start- und Stoppbits. Escape-Zeichen werden wie bei der asynchronen Übertragung verwendet.

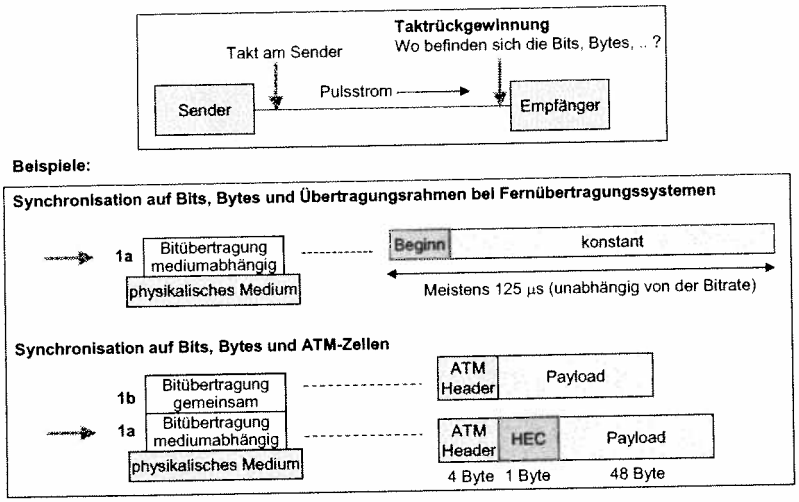


Bild: Synchronisation bei serieller Übertragung

Eine Hauptaufgabe bei der seriellen Übertragung ist die Taktrückgewinnung beim Empfänger. Sie besteht aus der Synchronisation auf einzelne Bits, Bytes, Worte als Puffergrößen (z.B. 32 oder 64 Bits) sowie die Synchronisation auf Übertragungsrahmen.

Bei der Zellvermittlungstechnik ATM wird in der Schicht 1a die Header-Prüfsumme (HEC, Header Error Code) beim Senden generiert und nach Empfang vernichtet.

Aufgaben der HEC-Prüfsumme:
- Fehlererkennung der Header-Information,
- Synchronisation auf ATM-Zellen.

Synchronisation
- Neusynchronisation bei asynchroner Übertragung,
- Dauersynchronisation bei synchroner Übertragung (2 Mbit/s und 1.5 Mbit/s),
- Nachsynchronisation bei synchroner Übertragung (GSM),
- Nachsynchronisation bei synchroner Übertragung (Satellitenfunk),
- Nachsynchronisation bei synchroner Übertragung (PDH- und SDH-Systeme).

Weiteres Thema: Kontinuierliche Bitstrom bei synchroner Übertragung.

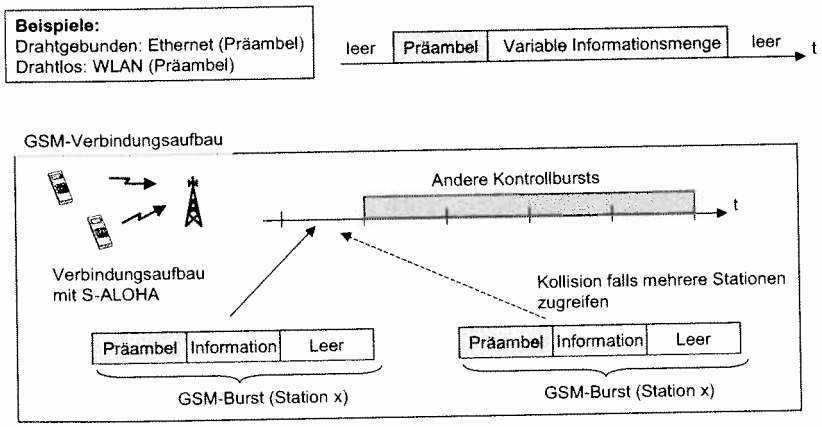


Bild: Neusynchronisation bei asynchroner Übertragung

Bei Ethernet und IEEE 802.11 WLAN muss der Empfängerstation sich auf den eintreffenden Rahmen mit Hilfe einer Präambel aufsynchronisieren.

Eine Aufsynchronisierung ist auch bei GSM während der Einbuchungsphase oder bei Anfrage zu einem Verbindungsaufbau, beide mit dem S-ALOHA Protokoll, notwendig.

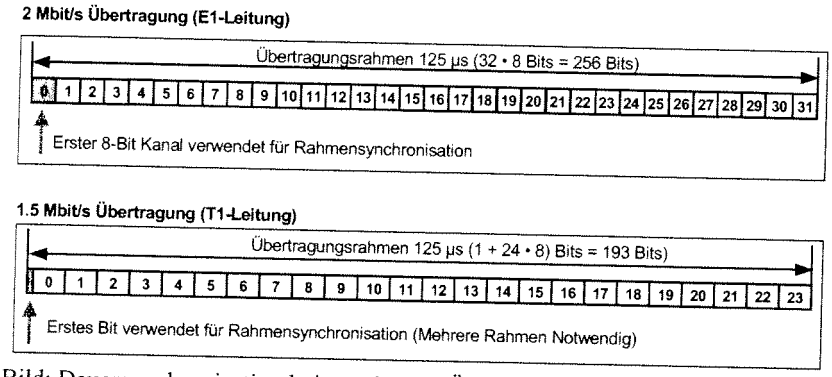
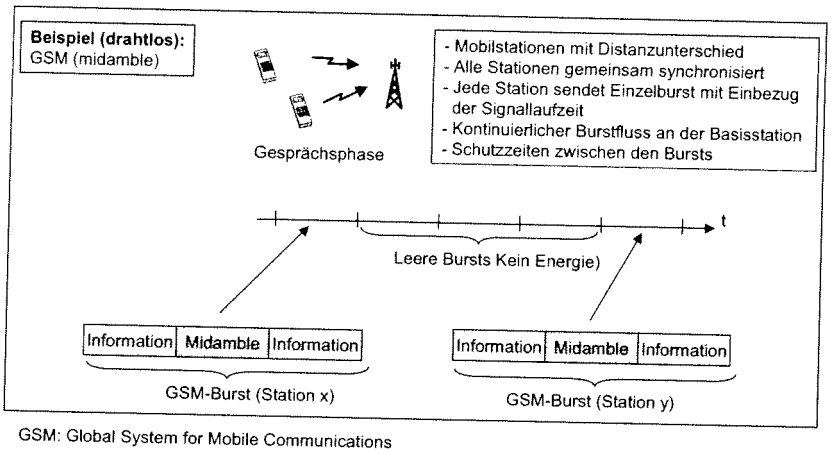


Bild: Dauersynchronisation bei synchroner Übertragung (2 Mbit/s und 1.5 Mbit/s)

Bei den Übertragungssystemen E1 (2 Mbit/s) und T1 (1,5 Mbit/s) ist dauerhaft ein Übertragungsrahmen mit einer Periode von 125 µs vorhanden. Synchronisiert erfolgt auf die Rahmenerkennung am Anfang der Übertragungsrahmen.



GSM: Global System for Mobile Communications

Bild: Nachsynchronisation bei synchroner Übertragung (GSM)

Im allgemeinen muss eine bestehende Synchronisation dauernd nachsynchronisiert werden. Bei GSM-Bursts geschieht dies über sogenannte Midambles.

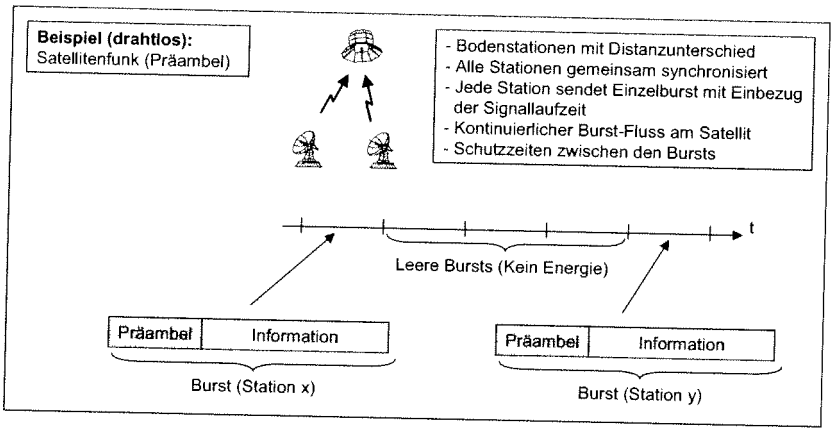
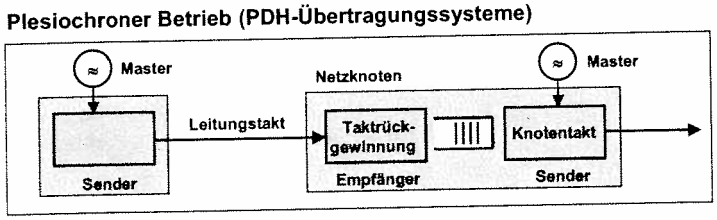


Bild: Nachsynchronisation bei synchroner Übertragung (Satellitenfunk)

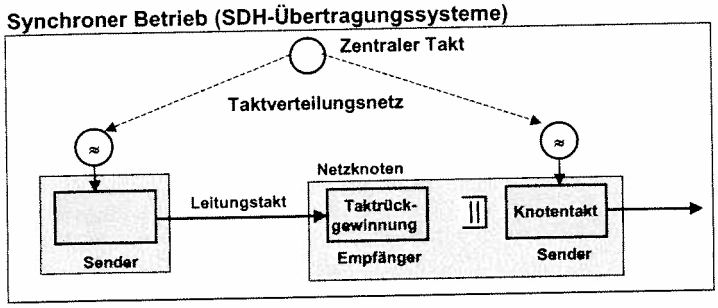
Bei Satellitensystemen geschieht dies über eine Präambel.

Plesiochroner Betrieb (PDH-Übertragungssysteme)



PDH: jeder Netzknoten hat seinen eigenen Taktgenerator

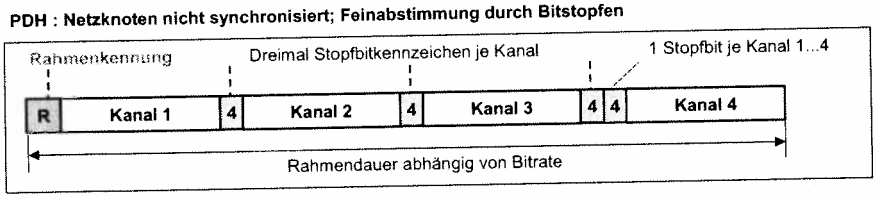
Synchroner Betrieb (SDH-Übertragungssysteme)



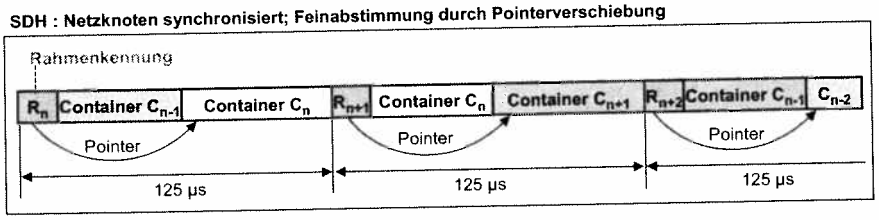
SDH: alle Netzknoten sind synchron über einem Taktverteilungsnetz miteinander gekoppelt. Dadurch ist die Taktdifferenz zwischen Empfänger und Sender eines Knotens bei SDH äußerst gering.

Bild: Nachsynchronisation bei synchroner Übertragung (PDH- und SDH-Systeme)

PDH : Netzknoten nicht synchronisiert; Feinabstimmung durch Bitstopfen



SDH : Netzknoten synchronisiert; Feinabstimmung durch Pointerverschiebung



Auch bei den PDH- und SDH-Übertragungssystemen muss der Taktunterschied zwischen benachbarten Netzelementen dauernd ausgeglichen werden.

Bei PDH (Plesiochronous Digital Hierarchy) sind die Netzelementen nicht untereinander synchronisiert. Deshalb muss regelmäßig gestopft werden, um einen Verlust von Datenbits zu vermeiden.

Bild: Nachsynchronisation bei synchroner Übertragung (PDH- und SDH-Systeme)

Stopfen bei PDH heißt das bei zu hohem Sendetakt Stopfbits eingeschoben werden und bei zu niedrigerem Takt Stopfbits entfernt werden. Für ein Zeitmultiplex-System mit vier gemultiplexten Kanälen sind vier Stopfbits vorgesehen. Falls im Rahmen Stopfbits vorhandenen sind, werden sie vorher im gleichen Rahmen dreimal in den Stopfbitkennzeichenfeldern angekündigt.

Bei SDH (Synchronous Digital Hierarchy) sind die Netzelementen über ein getrenntes Taktverteilungsnetz untereinander synchronisiert. Hier genügend die sporadische Verschiebung eines Pointers, der anzeigt, wo ein beliebig positionierbarer Container mit den Informationsdaten anfängt. Ein Container befindet sich mindestens in zwei SDH-Rahmen. Je nach Pointerwert kann ein Container sich auch über drei SDH-Rahmen erstrecken.

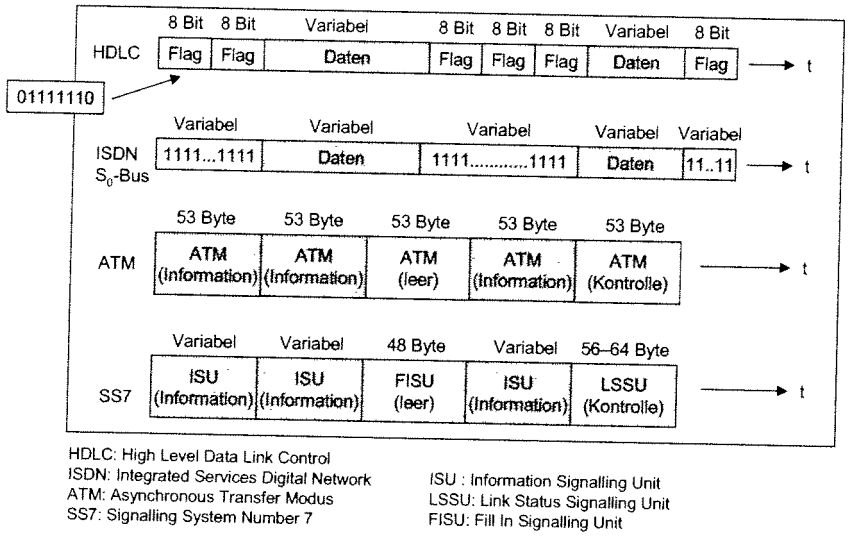


Bild: Synchrone Übertragung (kontinuierlicher Bitstrom)

Für die seriell synchronisierte Übertragung ist es wesentlich, dass auf der Bitübertragungsschicht ein kontinuierlicher Bitstrom vorhanden ist.

Bei **HDLC** wird auf der Sicherungsschicht Flags von 8 Bits eingefügt, wenn nichts zu übertragen ist.

Bei **ISDN** werden auf dem S_0-Bus von den Stationen dauernd Einsen gesendet, wenn nichts zu übertragen ist.

Bei **ATM** sind dauernd ATM-Zellen vorhanden: Information-, Kontroll- oder Leerzelle.

Auch beim Signalisierungsnetz **SS7** (Signalling System Number 7) werden Informations-, Kontroll- oder Leer-Einheiten gesendet.

Es wird jedoch darauf hingewiesen, dass dieser kontinuierliche Bitstrom ein logischer Bitstrom ist und zur eigentlichen Übertragung durch die Leitungscodierung entsprechend umgewandelt wird.

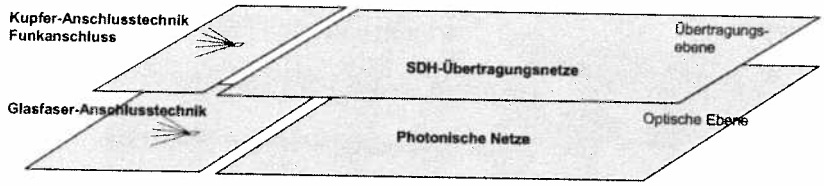
2.1 OSI-Referenzmodell: Schicht 1 – Übertragungssysteme

Version: Dez. 2003

Inhalt

- Plesiochrone Digitale Hierarchie (PDH)
- Synchrone Digitale Hierarchie (SDH)
- Photonische Übertragungssysteme
- Taktrückgewinnung
- Synchronisation von Netzknoten
- Struktur von Übertragungsrahmen
- ADSL- und HDSL-Übertragungssysteme

Die Übertragungseinrichtungen können in zwei Übertragungsebenen eingeteilt werden: eine elektrische und eine optische Ebene. Die Anschlusstechnik wird getrennt betrachtet. Hier gehören die Kupferleitungen sowie die verschiedenen Funkzugangstechniken zur elektrischen und die Glasfasersysteme zur optischen Ebene.



Anschlusstechnik

PDH	Plesiochronous Digital Hierarchy
ADSL	Asynchronous Digital Subscriber Line
HSDL	High Bit Rate Digital Subscriber Line
WLL	Wireless Local Loop
FTTC	Fiber-to-the Cabinet
FTTB	Fiber-to-the Building
FTTH	Fiber-to-the Home
PON	Passive Optical Network

SDH-Übertragungsnetze

SDH	Synchronous Digital Hierarchy
DXC	Digital Cross Connect
ADM	Add/Drop Multiplexer

Photonische Übertragungsnetze

OXC	Optical Cross Connect
OADM	Optical Add/Drop Multiplexer

Bild: Netztechnologien: Übertragung

Abgesehen von Richtfunk- und Satellitenstrecken erfolgt die Übertragung im Netz selbst immer optisch. Die Endgeräte gehören zur elektrischen Ebene. Die Glasfaser mit Sender (Laser) und Empfänger (Photodiode)bilden die optische Ebene. Können im optischen Bereich auch Glasfasern oder einzelne Wellenlängen in optischen Koppelfeldern durchgeschaltet werden, so ist man im Bereich der optischen oder photonischen Netze. Dabei handelt es sich um Durchschaltevermittlung. Die optische Paketvermittlung ist derzeit im Forschungsstadium.

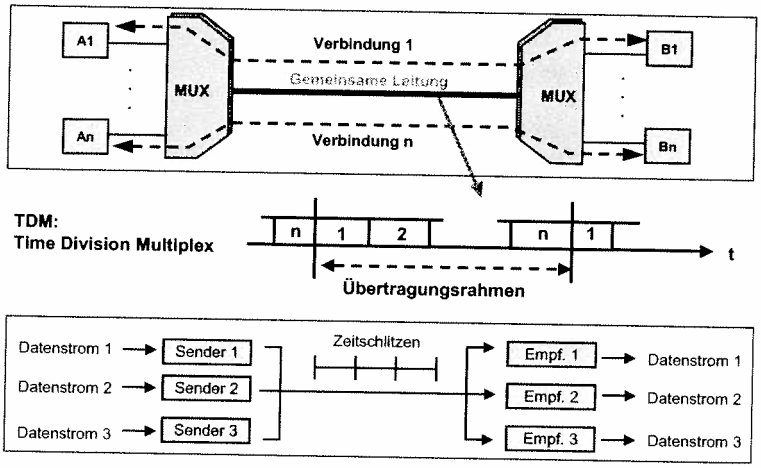


Bild: Zeitmultiplexausnutzung einer Leitung

Die elektronischen Übertragungssysteme verwenden Zeitmultiplextechnik, um die Leitungen bis zu hohen Bitraten auszunützen. Heute werden Zeitmultplex-Bitströme bis zu 40 Gbit/s erzeugt.

Im Einsatz sind plesiochrone und synchrone Übertragungssysteme.

In modernen Telekommunikationsnetzen verwendet man die Systeme der Plesiochrone Digital Hierarchie (PDH) heute hauptsächlich als Zugangsleitungen. Die Netzknoten werden durch Übertragungssysteme der Synchrone Digital Hierarchie (SDH) Technik verbunden.

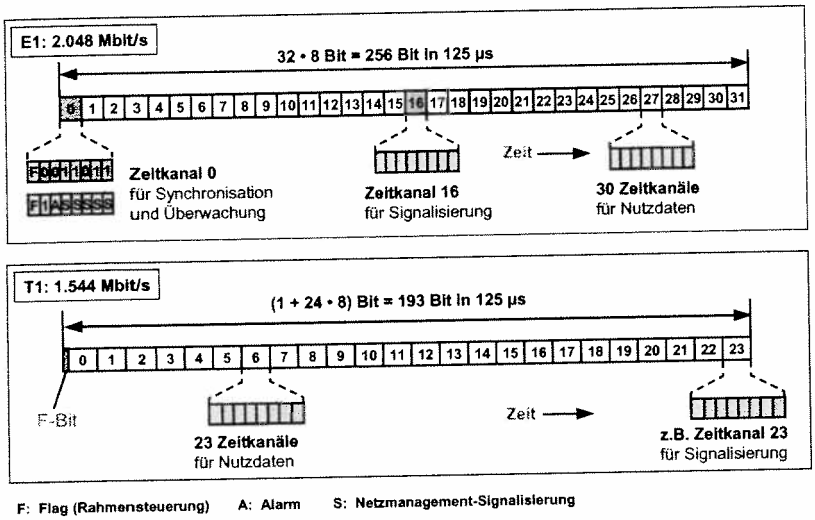


Bild: Übertragungsrahmen E1 und T1

Plesiochrone Digitale Hierarchie (PDH)

Alle PDH-Systeme zur Daten- und Sprachübertragung basieren auf der Grundbitrate von 64 kbit/s.

In **Europa** werden 30 Nutzkanäle und 2 Zusatzkanäle zu einem Bitstrom von 2 Mbit/s zusammengefasst. Man spricht von einem PCM30-System oder E1 System (European Transmission Level 1).

In **Nordamerika und Japan** werden 24 Nutzkanäle plus 1 Bit zur Kennung des Übertragungsrahmens zu einem Bitstrom von 1.5 Mbit/s zusammengefügt. Für die Signalisierung kann 1 Nutzkanal zugewiesen werden. Das PCM24-System bezeichnet man auch als T1 System (Transmission Level 1)

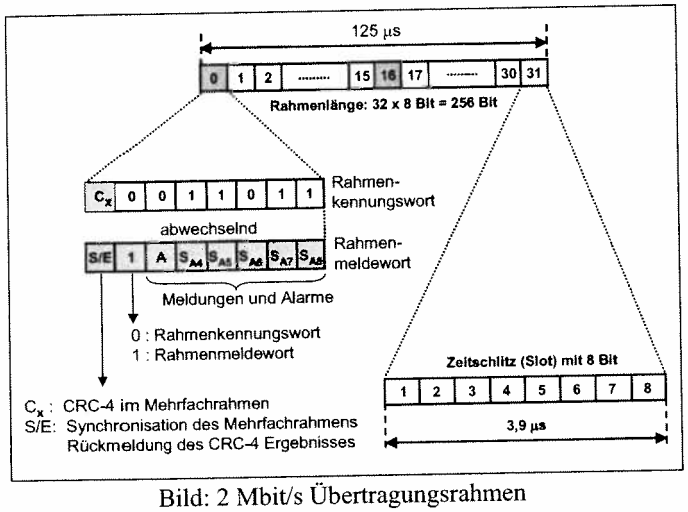


Bild: 2 Mbit/s Übertragungsrahmen

Der 2 Mbit/s Übertragungs- oder Pulsrahmen mit 30 Zeitabschnitten mit Nutzdaten zu je 64 kbit/s hat zusätzlich zwei Hilfskanälen für die Synchronisierungs- und Signalisierungsinformation (Zeitkanal 0 bzw. 16).

Die Bitrate pro Zeitkanal von 64 kbit/s (8 Bit alle 125 µsec) basiert auf einer Sprachabtastung mit 8 kHz und einer Sprachcodierung von 8 Bit.

Der Rahmen ist 32 x 8 = 256 Bit lang und wiederholt sich im Rhythmus von 125 µs. Die Übertragungsdauer eines Kanals beträgt jeweils 125 µs /32 = 3,906 µs.

Zeitkanal 0 enthält abwechselnd:

1) Das **Rahmenkennungswort** zur Kennzeichnung des Rahmenbeginns (Bitfolge 0011011).
2) Das **Rahmenmeldewort** mit zwei wichtigen Funktionen: Fehlerüberwachung und Fehlermeldung.

Mit Hilfe des A-Bit und der S_A-Bit werden Alarme und Meldungen zwischen Sende- und Empfangseinheit ausgetauscht. Das erste Bit des Zeitkanals 0 wird in einen Mehrfachrahmen aus 16 Übertragungsrahmen verwendet. Das zweite Bit ist abwechselnd 0 und 1 und gibt damit an, ob es sich um ein Rahmenkennungswort bzw. Rahmenmeldewort handelt.

Überwachung der 2 Mbit/s Übertragungsqualität mit einem CRC-4-Verfahren

Die Datenübertragungsqualität der bittransparenten Datenkanäle werden durch eine zyklische Redundanzprüfung (Cyclic Redundancy Check, CRC-4) sichergestellt. Für die Qualitätsüberwachung der 2 Mbit/s Bitstrom werden 16 aufeinander folgende Übertragungsrahmen als Mehrfachrahmen betrachtet, der in zwei Hälften (I und II) zu je 8 Rahmen unterteilt ist. Der resultierende CRC-Rahmen hat somit eine zeitliche Dauer von 16 x 125 µs = 2 ms.

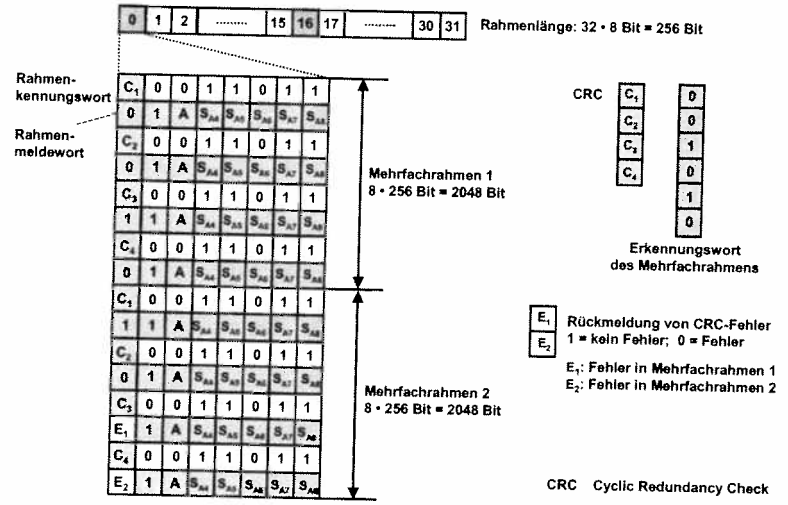


Bild: 2 Mbit/s Mehrfach-Übertragungsrahmen

Zur Bildung der CRC-Worte werden acht aufeinanderfolgende Rahmen durch ein Polynom vierten Grades ($x^4 + x + 1$) binär dividiert.Der 4 Bit breite Divisionsrest wird in den C_1 bis C_4 Bits im Rahmenkennungswort übertragen. Der Empfänger überprüft die CRC-Übertragung. Ist das Resultat unterschiedlich, wurde mindestens ein Bit des Mehrfachrahmens (insgesamt 8 x 256 Bit = 2048 Bit) verfälscht. Es kann nicht erkannt werden, ob nur ein Bit oder mehrere Bits während der Übertragung verfälscht wurden.

Mit der E-Bits (E_1, E_2) im Meldewort wird das Ergebnis der CRC-Überprüfung an den Sender zurückgemeldet.

Ob der Empfänger sich auf die richtigen 16 Rahmen auf synchronisiert hat, wird erkannt durch das vertikalverteilte Erkennungswort des Mehrfachrahmens (001010). Die einzelnen Bit werden in den Meldeworten übertragen.

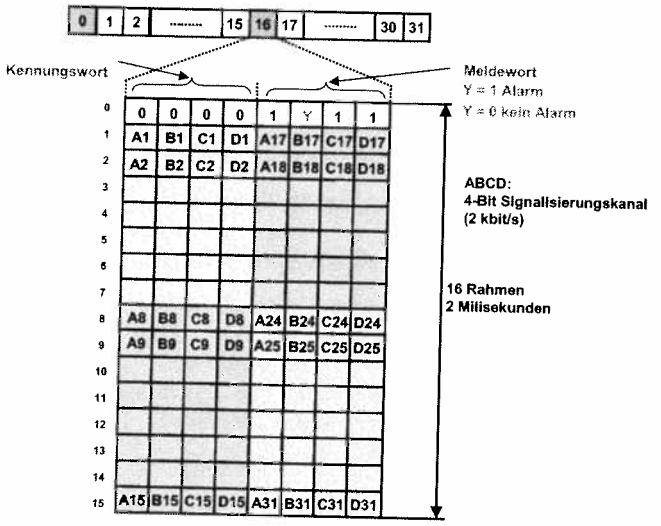


Bild: 2 Mbit/s Übertragung: Signalisierungskanal

Kanalgebundene Signalisierung

Bei der kanalgebundenen Signalisierung steht jedem Nutzkanal eine fest zugeordnete Signalisierungskapazität zur Verfügung, unabhängig davon, ob aktuell gerade Signalisierungsinformation übertragen werden muss oder nicht.

Bei der 2 Mbit/s Übertragung werden sämtliche Signalisierungsinformationen mit Hilfe von ABCD-Bits übertragen. Jeder der Signalisierungskanäle hat eine Wortbreite von 4 Bit und wird nur in jedem sechzehnten Übertragungsrahmen einmal übertragen, d.h. mit 8000 [1/s] x (1/16) x 4 bit = 2 kbit/s.

Zwei zusätzliche 2-kbit/s-Kanäle dienen zur Synchronisation (Kennungswort) und zur Übertragung von Signalisierungsalarmen (Meldewort).

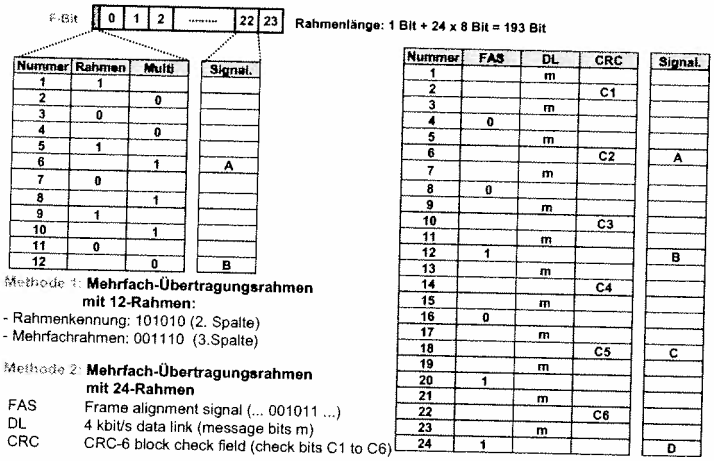


Bild: 1,5Mbit/s Mehrfach-Übertragungsrahmen

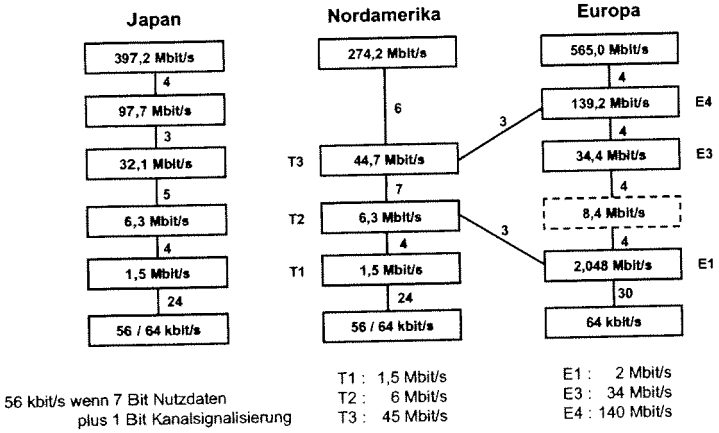


Bild: Plesiochrone Digitale Hierarchie (PDH)

Aus dem PCM-30-Grundsystem hat sich schrittweise die Plesiochrone Digitale Hierarchie (PDH) entwickelt. Je vier Untersysteme werden zu einem Obersystem vereinigt (E2, E3 und E4 mit 8, 34 bzw. 140 Mbit/s). 16 Kanäle zu je 2 Mbit/s werden heute direkt zu einem 34 Mbit/s Bitstrom zusammengeführt.

Die nordamerikanische Hierarchie basierend auf 24 Basiskanäle zu 64 kbit/s verwendet Bitraten von 1,5 Mbit/s, 6,3 und 45 Mbit/s (T1, T2, T3). Die japanische Hierarchie basiert ebenfalls auf 24 Basiskanäle und benutzt teilweise andere Bitraten.

Die höchsten Bitraten kommen in älteren transozeanischen Übertragungssystemen vor.

Während im 2-Mbit/s-PCM-Grundsystem die Datenworte **byteweise** verschachtelt werden, fassen Multiplexer der höheren Hierarchie die Zubringerdaten **bitweise** zusammen. Alle Grundsysteme und Multiplexer höherer Ordnung haben ihre eigenen und unabhängigen Taktversorgungen. Taktunterschiede der einzelnen Multiplexzubringer werden durch sogenannte Stopftechniken ausgeglichen.

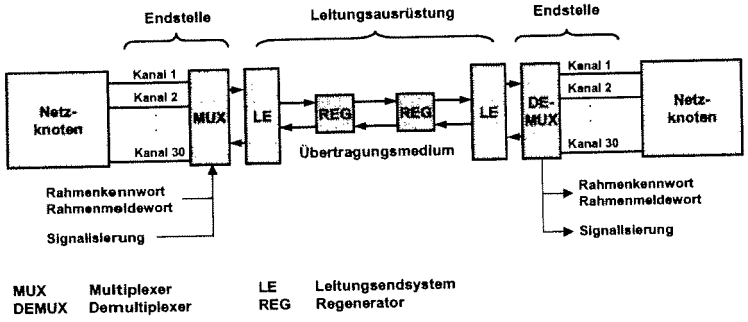


Bild: PCM-30 Übertragungssystem

Ein PCM-30 Übertragungssystem besteht aus einem Multiplexer, der die 30 Nutzkanäle, den Synchronisations- und Überwachungskanal 0 und den Signalisierungskanal 16 gemäß der PCM-Rahmenstruktur byteweise zu einem Bitstrom von 2 Mbit/s verschachtelt.

Das Empfängerendsystem verwendet einen Demultiplexer, um Nutz- und Zusatzkanäle dem Netzknoten einzelnen zu Verfügung zu stellen.

Die Leitungsausrüstungen enthalten die Sender- und Empfängerkomponenten. Falls die Übertragungsdistanz zu groß ist, können die pulsförmige Signale in Regeneratoren wiederhergestellt werden (3R-Regeneration: Amplitude, Pulsform und zeitliche Pulslage).

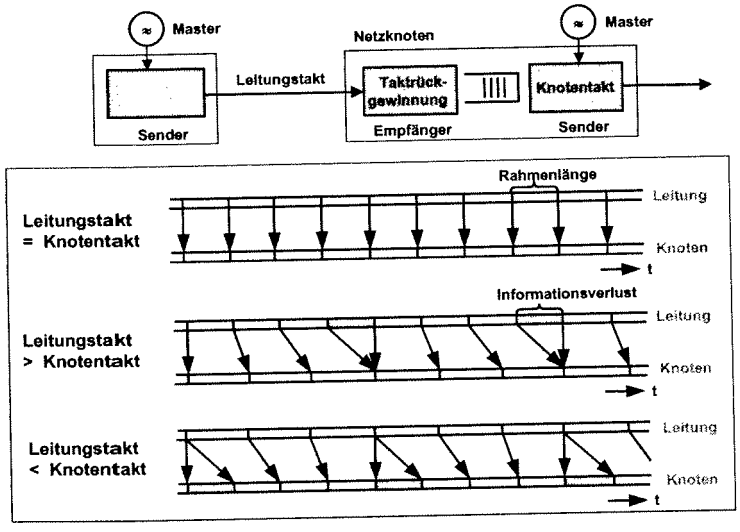


Bild: Plesiochroner Betrieb

Die Taktgeneration in beiden Endsystemen einer PDH-Übertragungsstrecke ist nicht synchronisiert. Da der Bittakt durch die Taktrückgewinnungselektronik aus dem empfangenen Bitstrom abgeleitet wird, arbeitet der Empfänger mit dem Leitungstakt und die weitere Elektronik im Knoten mit dem Knotentakt.

Es sind drei Fälle zu betrachten:

1) Leitungstakt = Knotentakt: in diesem Fall fließt der Eingangsbitstrom mit der gleichen Taktrate ab. Es geht keine Information verloren.

2) Leitungstakt > Knotentakt: es kommen hier mehr Datenbits an als abfließen können , so dass bei vollem Ausgangspuffer am Empfänger Datenbits regelmäßig verloren gehen.

3) Leitungstakt < Knotentakt: hier werden weniger Bits gesendet als im betrachteten Knoten abgenommen werden. Deshalb ist der Empfangspuffer regelmäßig leer, wenn Datenbits ausgelesen werden sollen.

Zum Ausgleich der Taktunterschiede zwischen Unter- und Obersystem wird bei PDH die sogenannte **Positiv-Stopftechnik** angewendet. Ob gestopft wird, also Leerinformation übertragen wird, oder das entsprechende Bit als Träger von Information anzusehen ist, wird dem Empfänger mit Hilfe der Stopfindikatoren mitgeteilt. Diese werden über den Rahmen verteilt in ungerader Anzahl mehrfach gesendet. Wenn während der Übertragung die Stopfindikatoren gestört werden, so führt ein Mehrheitsentscheid immer noch mit hoher Wahrscheinlichkeit zu einer korrekten Erkennung des Stopfbits. Eine Fehlinterpretation würde sofort zum Synchronverlust im Untersystem führen.
In den Multiplexrahmen der 8 und 34 Mbit/s Bitraten sind dreimal ein Stopfbitindikator für jeden der vier gemultiplexten Kanäle vorhanden. Sie zeigen an, ob sich ein Leer- oder Informationsbit in Stopffeld befindet. In einem 140 Mbit/s Übertragungssystem gibt es fünfmal eine Voranzeige.
Der Aufbau der Übertragungsrahmen basiert für alle Hierarchiestufen auf dem gleichen Prinzip: die Zubringersignale werden **bitweise verschachtelt** und die jeweiligen hierarchiespezifischen Rahmenkennungswörter, Betriebssignale, Stopfkennungen und Stopbits hinzugefügt. Jeder der Rahmen ist in gleich lange Blöcke unterteilt. Für jedes Untersystem wird jeweils zu Beginn eines Blocks ein Bit zur Stopfkennung eingefügt.

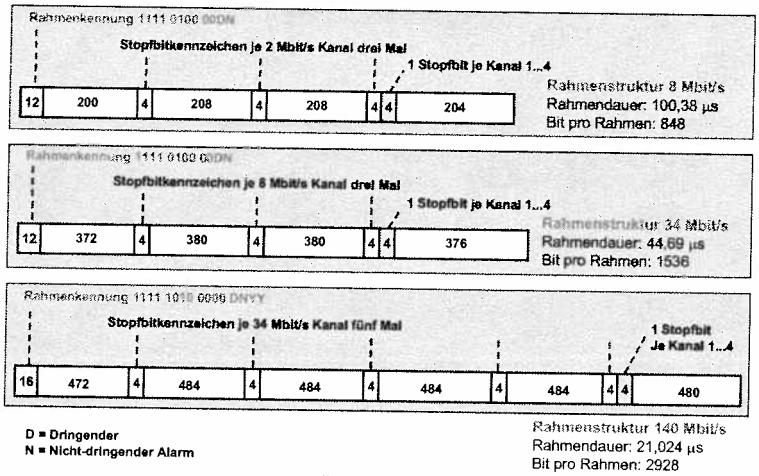


Bild: PDH-Übertragungsrahmen

Die PDH-Multiplexrahmen haben
- unterschiedliche Strukturen,
- unterschiedlich lange Rahmenerkennungsworte,
- unterschiedliche Rahmendauer,
  - Die Anzahl Bit pro Rahmen ist nicht ein Vielfaches der anderen Rahmen der PDH-Hierarchie.

Ein 64 kbit/s-Kanal in einem Multiplex-Rahmen kann nur zugegriffen werden, wenn bis zu einem E1-System (2 Mbit/s) demultiplext wird.

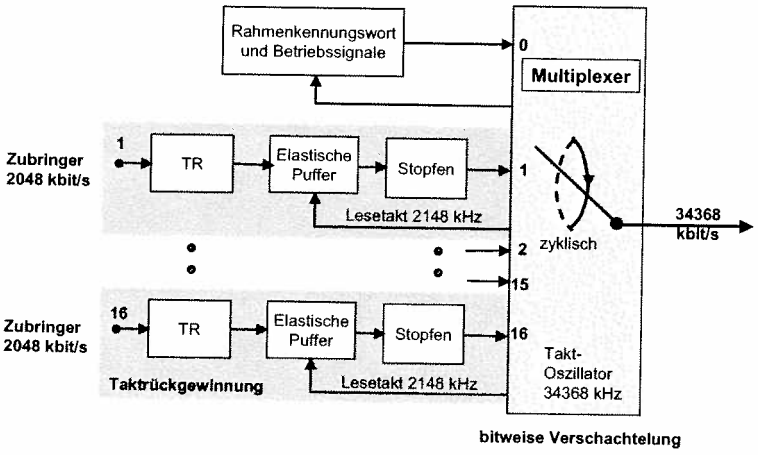


Bild: Funktionsprinzip eines PDH-Multiplexers für 34 Mbit/s

In einem PDH-Multiplexer für 34 Mbit/s wird zuerst für jedes ankommende 2-Mbit/s-Signal der Takt abgeleitet und den Bitstrom in einen elastischen Pufferspeicher eingeschrieben. Aus diesem Puffer werden die Daten mit einem Takt von 2148 kHz ausgelesen, der über die Teilung durch den Faktor sechzehn aus dem Takt des Ausgangssignals erzeugt wird. Durch den schnelleren Auslesetakt von 2148 kHz gegenüber dem Einschreibtakt von 2048 kHz würde der Pufferspeicher ohne Gegenmaßnahmen leerlaufen. Der Auslesevorgang wird zyklisch immer wieder angehalten, um die Daten der anderen Zubringer, das Rahmenkennungswort und die Alarmmeldung dem Bitstrom hinzuzufügen. Wird die Taktdifferenz zwischen Lese- und Schreibtakt zu groß, wird ein zusätzliches Bit eingefügt, das als Stopfbit bezeichnet wird.

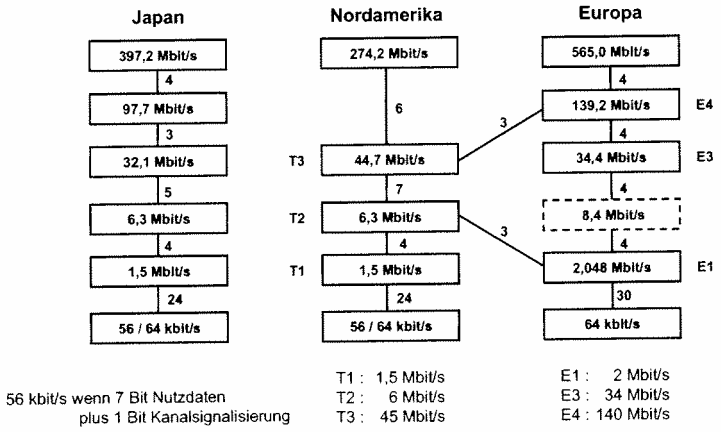


Bild: Plesiochrone Digitale Hierarchie (PDH)

Aus dem PCM-30-Grundsystem hat sich schrittweise die Plesiochrone Digitale Hierarchie (PDH) entwickelt. Je vier Untersysteme werden zu einem Obersystem vereinigt (E2, E3 und E4 mit 8, 34 bzw. 140 Mbit/s). 16 Kanäle zu je 2 Mbit/s werden heute direkt zu einem 34 Mbit/s Bitstrom zusammengeführt.

Die nordamerikanische Hierarchie basierend auf 24 Basiskanäle zu 64 kbit/s verwendet Bitraten von 1,5 Mbit/s, 6,3 und 45 Mbit/s (T1, T2, T3). Die japanische Hierarchie basiert ebenfalls auf 24 Basiskanäle und benutzt teilweise andere Bitraten.

Die höchsten Bitraten kommen in älteren transozeanischen Übertragungssystemen vor.

Während im 2-Mbit/s-PCM-Grundsystem die Datenworte **byteweise** verschachtelt werden, fassen Multiplexer der höheren Hierarchie die Zubringerdaten **bitweise** zusammen. Alle Grundsysteme und Multiplexer höherer Ordnung haben ihre eigenen und unabhängigen Taktversorgungen. Taktunterschiede der einzelnen Multiplexzubringer werden durch sogenannte Stopftechniken ausgeglichen.

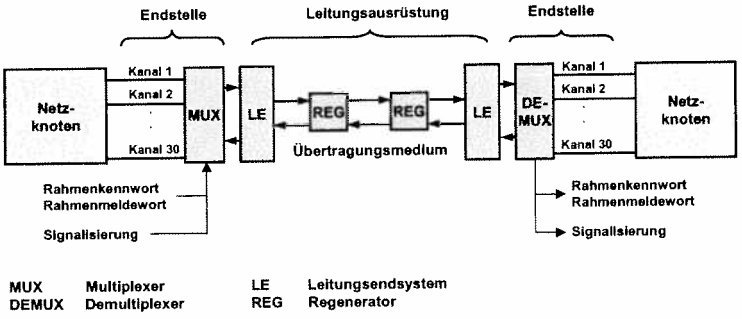


Bild: PCM-30 Übertragungssystem

Ein PCM-30 Übertragungssystem besteht aus einem Multiplexer, der die 30 Nutzkanäle, den Synchronisations- und Überwachungskanal 0 und den Signalisierungskanal 16 gemäß der PCM-Rahmenstruktur byteweise zu einem Bitstrom von 2 Mbit/s verschachtelt.

Das Empfängerendsystem verwendet einen Demultiplexer, um Nutz- und Zusatzkanäle dem Netzknoten einzelnen zu Verfügung zu stellen.

Die Leitungsausrüstungen enthalten die Sender- und Empfängerkomponenten. Falls die Übertragungsdistanz zu groß ist, können die pulsförmige Signale in Regeneratoren wiederhergestellt werden (3R-Regeneration: Amplitude, Pulsform und zeitliche Pulslage).

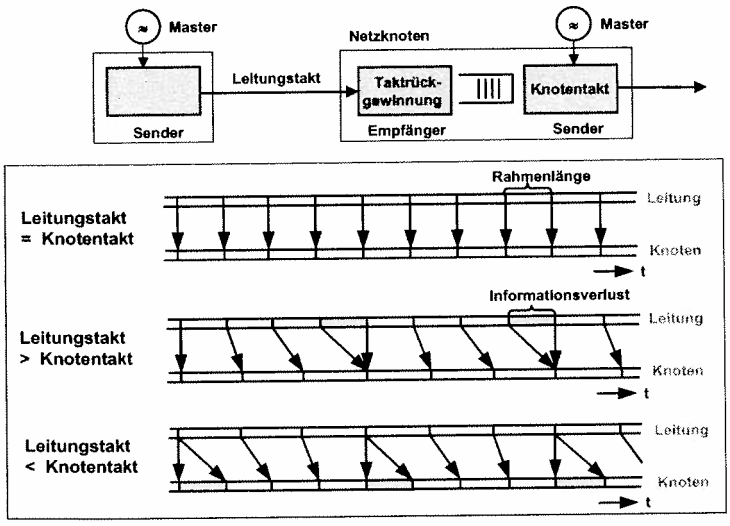


Bild: Plesiochroner Betrieb

Die Taktgeneration in beiden Endsystemen einer PDH-Übertragungsstrecke ist nicht synchronisiert. Da der Bittakt durch die Taktrückgewinnungselektronik aus dem empfangenen Bitstrom abgeleitet wird, arbeitet der Empfänger mit dem Leitungstakt und die weitere Elektronik im Knoten mit dem Knotentakt.

Es sind drei Fälle zu betrachten:

1) Leitungstakt = Knotentakt: in diesem Fall fließt der Eingangsbitstrom mit der gleichen Taktrate ab. Es geht keine Information verloren.

2) Leitungstakt > Knotentakt: es kommen hier mehr Datenbits an als abfließen können , so dass bei vollem Ausgangspuffer am Empfänger Datenbits regelmäßig verloren gehen.

3) Leitungstakt < Knotentakt: hier werden weniger Bits gesendet als im betrachteten Knoten abgenommen werden. Deshalb ist der Empfangspuffer regelmäßig leer, wenn Datenbits ausgelesen werden sollen.

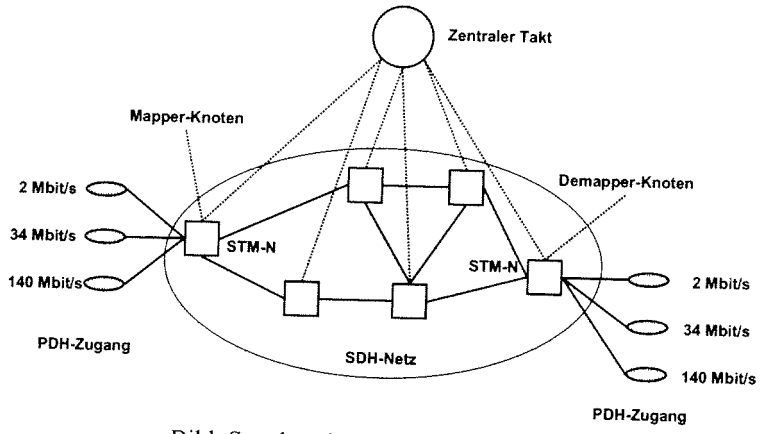


Bild: Synchronisation eines SDH-Netzes

SDH-Knoten werden über eine eigenständige hierarchische Taktverteilung synchronisiert. Eine Haupttaktquelle (PRS = Primary Reference Source) muss eine Frequenzgenauigkeit besser als 1.10^{-11} aufweisen. Sie ist als ein frei schwingender Generator definiert und wird nicht von einem anderen Takt synchronisiert. Üblicherweise wird dazu eine Anordnung von zwei oder mehr Cäsium-Atomnormale verwendet. Die Genauigkeit eines Cäsium-Normales beträgt 1.10^{-12}. Es werden auch GPS-Taktquellen (GPS = Global Positioning System) eingesetzt. Diese Systeme verwenden meistens einen Rubidium-Generator, welcher vom GPS synchronisiert wird und erreicht eine Genauigkeit von circa 1.10^{-12}.

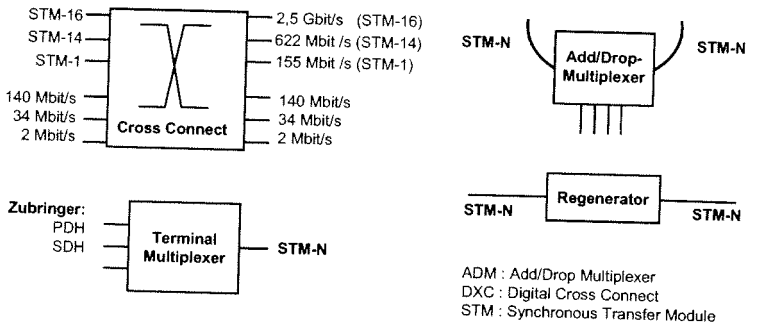


Bild: SDH-Netzelemente

Vier Typen von SDH-Netzelementen sind zu unterscheiden: Digital-Crossconnect (DXC), Add-and-Drop Multiplexer (ADM), Terminal-Multiplexer und elektronische Regeneratoren.

Alle Netzelementen führen eine 3R-Verstärkung (Amplitude, Pulsform und zeitliche Lage des Pulses) durch. Abgesehen vom Regenerator multiplexen die Netzelemente PDH- und SDH-Kanäle auf verschiedene Weise.

Zu beachten ist, dass es sich hier immer um Durchschaltevermittlung von PDH- und SDH-Kanälen handelt.

Aufgaben der multiplexfähigen Netzelemente:
- **DXC:** Durchschalten von PDH- und SDH-Bitströmen verschiedener Bitraten.
- **ADM:** Hauptteil der Bitströme bleibt auf dem Ring. Eingefügt bzw. herausgenommen werden terminierend Bitströme.
- **Terminal Multiplexer:** Konzentration/Expansion von PDH-Bitströmen.

Besonders in den Netzen privater Netzbetreiber ist der digitale Richtfunk das Rückgrat digitaler Kommunikation. Bei niedrigem Verkehrsaufkommen sind die 155 Mbit/s des SDH-Standards deutlich überdimensioniert. Um hier eine wirtschaftliche Lösung zu ermöglichen, bieten die Richtfunk- Systemhersteller auch Übertragungssysteme an, die bei 51 Mbit/s arbeiten und auf dem SONET-Standard basieren (STS-1).

Add/Drop-Multiplexer (ADM) erlauben im Ortsnetz neue Netzstrukturen in Form synchroner Ringe. Ein solcher Ring ist bei geschickter Auslegung selbstheilend, d.h. bei Unterbrechung einer Richtung ist er auch ohne Eingriff des Netzmanagements in der Lage, die Übertragung aufrechtzuerhalten (automatische Ersatzschaltung).

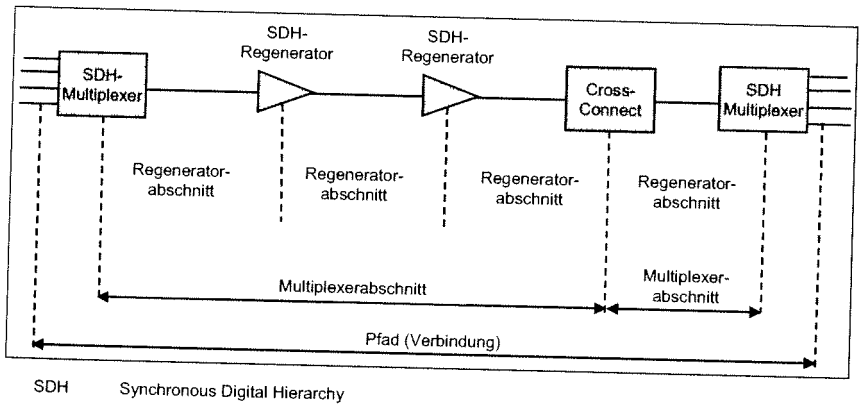


Bild: SDH-Übertragungsstrecke

Eine typische SDH-Übertragungsstrecke umfasst zwei Arten von Transportabschnitten:

Regenerator Section (Regeneratorabschnitt): zwischen allen Netzelementen.
Multiplexer Section (Multiplexer abschnitt): zwischen Multiplexern, Cross-Connects und Add/Drops.

Die Qualität der Abschnitte können durch sogenannte B-Bytes im STM1-Rahmenoverhead überwacht werden.

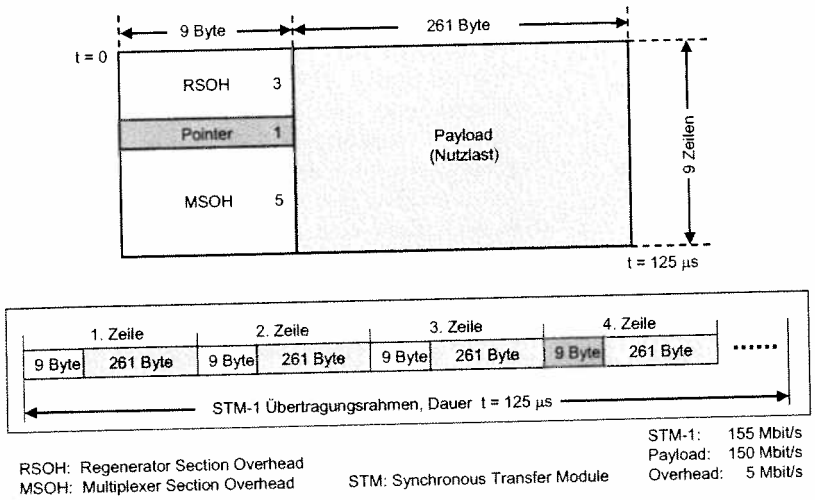


Bild: STM-1 Rahmen

Der STM-1-Rahmen wird üblicherweise in der bildlichen Darstellung mit 9 Zeilen zu je 270 Byte strukturiert. Die zeitlich Reihenfolge der Übertragung der einzelnen Bitzustände erfolgt pro Zeile von links nach rechts. Die Übertragungsgeschwindigkeit berechnet sich zu (270 x 9 x 8 Bit) /125 µs = 155,52 Mbit/s.

Die Rahmenwiederholfrequenz berechnet sich aus der Rahmendauer zu 8000 Hz. An jedem Kreuzungspunkt von Zeile und Spalte, der ein Byte symbolisiert, findet sich ein Kanal mit 64 kbit/s (8 Bit · 8000 /s)

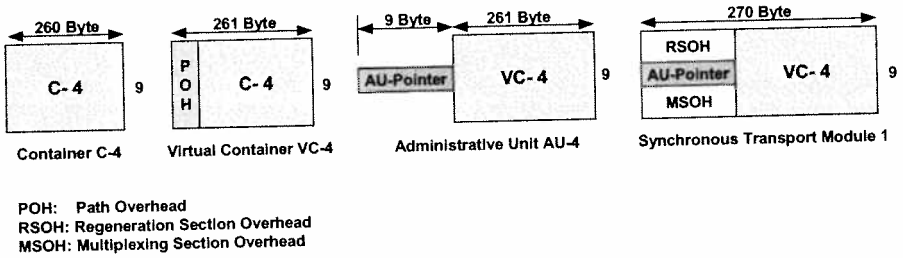


Bild: Terminologie in SDH

In der SDH-Terminologie betrachtet man als Payload-Einheit für den STM-1 Übertragungsrahmen ein sogenannter **Container C-4**. Dies ist der Byte-Bereich, wo die Bitraten der PDH-Bitströme durch einen Abbildungsvorschrift eingefügt werden können bzw. der 150 Mbit/s Nutz-Bitstrom eines STM-1 übertragen wird.

Durch Zufügen einer Byte-Spalte, der Pfad-overhead (POH, Pfadoverhead) entsteht ein **virtueller Container VC-4**. Durch Hinzufügung eines Zeigers (Pointer) entsteht eine Einheit, die man in einem Netz einsetzen kann: eine administrative Einheit (administrative Unit AU-4). Zusammen mit dem Regeneration- bzw. Multiplex-Section erhält man den STM-1 Übertragungsrahmen.

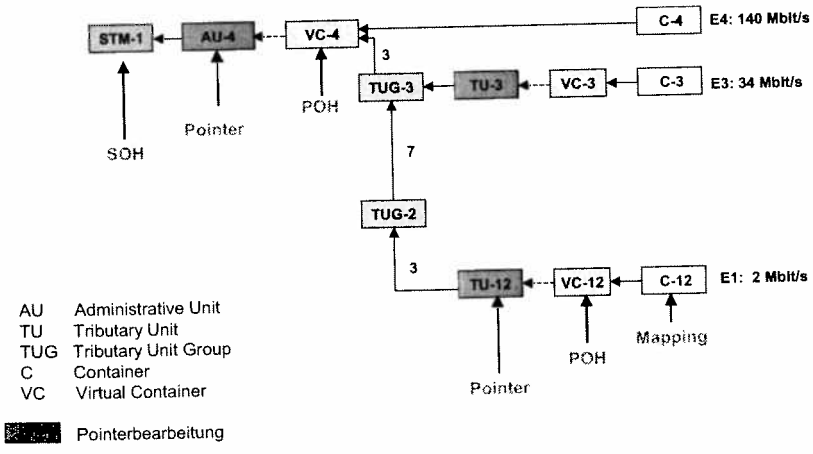


Bild: Abbildung von E-Systemen in SDH

Zur Abbildung von E1- bzw. E3-Bitströmen gilt eine ähnliche Termologie. Ein C-12 Container mit 2 Mbit/s wird zum V-12 durch den Path-Overhead, danach zu Tributary Unit durch Zufügen eines Pointers, und durch Verschachtelung von drei Tributary Units zu einem Tributary Unit Group 2. Durch Verschachtelung von weiteren sieben solchen Einheiten entsteht einen Tributary Unit Group 3. Drei solche Gruppen passen in einem VC-4. Es können somit 3 x 7 x 3 = 63 PCM-30 Bitströme in einem 155 Mbit/s STM-1 Rahmen übertragen werden.
Für einen 34 Mbit/s Anschluss ginilt ähnliches. Mögliche Mischungen: 63 xE1, 42xE1 + 1xE3 , 21xE1 + 2xE3 oder 3xE3.

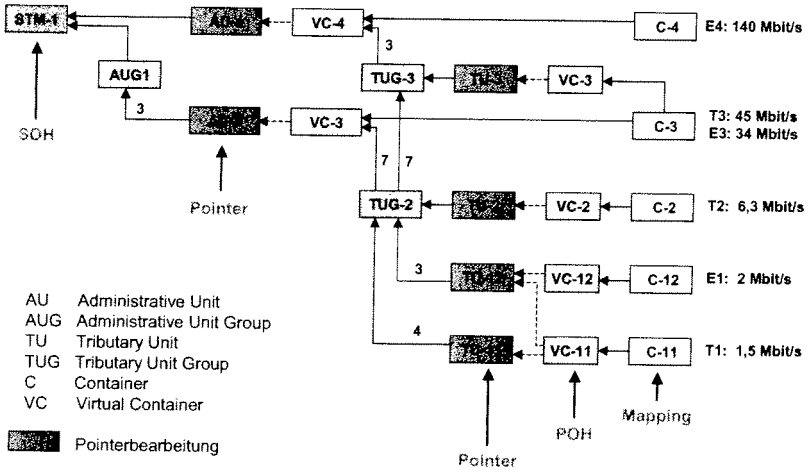


Bild: Abbildung von PDH-Bitströmen in SDH

Betrachtet man auch die nordamerikanischen Bitraten, so entsteht ein umfangreicheres Schema, wobei allerdings die Abbildungsstruktur erhalten bleibt.

Die einzelnen Zubringersignale werden somit in speziell für sie vorgesehene Containertypen abgebildet. Die Größe der Container ist einerseits so standardisiert, dass Schwankungen der plesiochronen Zubringersignale genügend Raum finden und andererseits die Containerverschachtelung innerhalb des Rahmens optimiert erfolgen kann. Deshalb sind die Container deutlich größer, als es aufgrund der maximalen Zubringerschwankungen erforderlich wäre. Ständig oder zu bestimmtem Zeitpunkt nicht mit Nutzinformation belegter Raum innerhalb der Container wird gestopft.

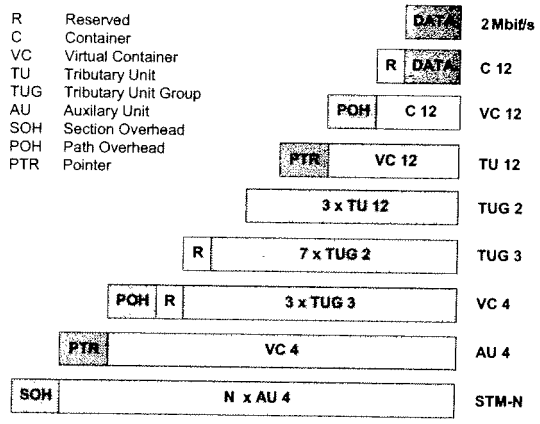


Bild: Abbildungsprinzip in SDH

Im Bild ist die Abbildungsprozedur von 63xE1 Bitraten zu einem STM-N anders dargestellt. Dabei ist N = 4, 16, 64, 96 mit den Bitraten 622 Mbit/s, 2,5 Gbit/s, 10 Gbit/s und 40 Gbit/s. Der Multiplexvorgang von einem STM-4 Rahmen entsteht durch byteweise Verschachtelung von vier STM-1 Rahmen.

Die Rahmendauer ist immer 125 µs, nur die Anzahl Byte pro Rahmen wird entsprechend größer.

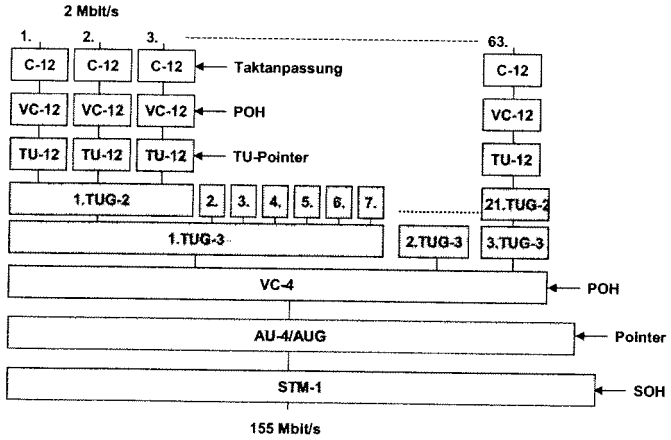
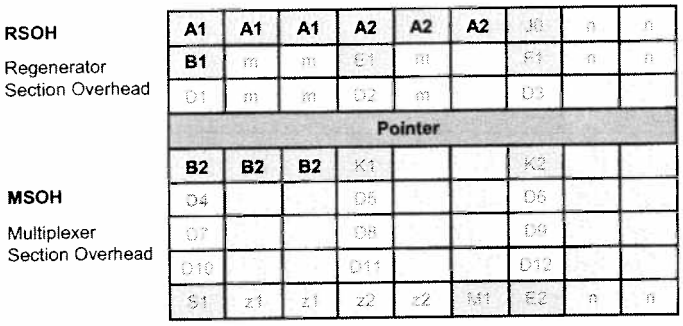


Bild: Abbildung von 2 Mbit/s Signalen auf STM-1 Rahmen



A1, A2	**Rahmensynchronisation**
B1, B2	**Qualitätsüberwachung (Paritätsvergleich)**
D1...D3	RSOH-Netzmanagement (192 kbit/s)
D4...D12	MSOH-Netzmanagement (576 kbit/s)
E1, E2	Sprechverbindung
F1	Wartung
J0	Regenerator Section Trace (Kennzeichnung Sender)
K1, K2	Steuerung für Ersatzschaltung / Alarmmeldungen
S1	Kennzeichnung Taktqualität
M1	Rückmeldung Übertragungsfehler (BIP)
z1, z2	Reserve
m	Mediumabhängig (z.B. Richtfunk, Satellit)
n	Nationale Anwendung

Bild: Aufbau des Section Overhead (SOH)

Section Overhead (SOH)

Der SOH nimmt mit einer Kapazität von 5,1 Mbit/s kaum mehr als 3% des Übertragungsvolumens in Anspruch. Der SOH kann als Block der Größe 9 x 9 Byte betrachtet werden. Die Übertragungskapazität beträgt 9 x 9 x 64 kbit/s = 5,184 Mbit/s.

Der obere Teil des SOH wird als RSOH (Regenerator-SOH), der untere als MSOH (Multiplexer-SOH) bezeichnet. Der RSOH ist allen Netzelementen zugänglich. Er kann von einem dazu berechtigten Netzelement ausgelesen und verändert werden. Der MSOH wird über den gesamten Multiplexabschnitt - von Anfang bis Ende -unverändert übertragen und darf somit nur von Cross-Connects; Add/Drops und Terminal Multiplexer verändert werden.

Die **Synchronisationsinformation A1 und A2** wird dreifach wiederholt. Dies dient weniger der Synchronisationssicherheit, sondern ist auf die Evolution der SDH aus dem amerikanischen SONET-Standard zurückzuführen.

B-Bytes überwachen die Qualität der Übertragung:
- B1 auf Regeneratorabschnitten,
- B2 auf Multiplexabschnitten.

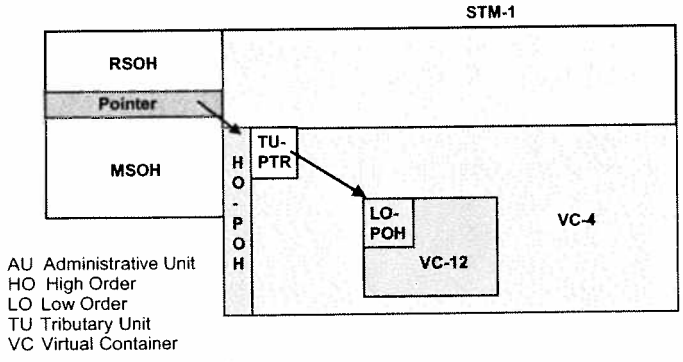


Bild: Arten der Pointer

Arten der Pointer

Damit das Zubringersignal auf den Takt des SDH Netzelements, in dem der STM-1 erzeugt wird, angepasst werden kann, wird ein Pointer (PTR) verwendet, der gewährleistet, dass das Zubringersignal innerhalb des STM-1 gleiten kann.

VC-12 und VC-3 werden mit einem TU-PTR versehen, so dass sie innerhalb der TUG-2 bzw. TUG-3 gleiten können. Der TU-PTR des VC-12 hat einen fixen Platz am Anfang der TUG-2, und der TU-PTR des VC-3 hat einen fixen Platz am Anfang der TUG-3. Beide TU-PTR zeigen auf den Beginn des POH des VC-12 oder VC-3.

Der VC-4 wird hingegen mit einem AU-PTR versehen, so dass er innerhalb des STM (präziser: innerhalb der AUG, die den Payload Teil des STM komplett ausfüllt und daher einen fixen Platz hat) gleiten kann. Der AU-PTR steht in der vierten Zeile des SOH, zwischen RSOH und MSOH. Er zeigt auf den Beginn des POH des VC-4.

Mit zwei Pointerzugriffen kann somit auf einen VC-12 (2 Mbit/s) oder einen VC-3 (34 Mbit/s) zugegriffen werden.

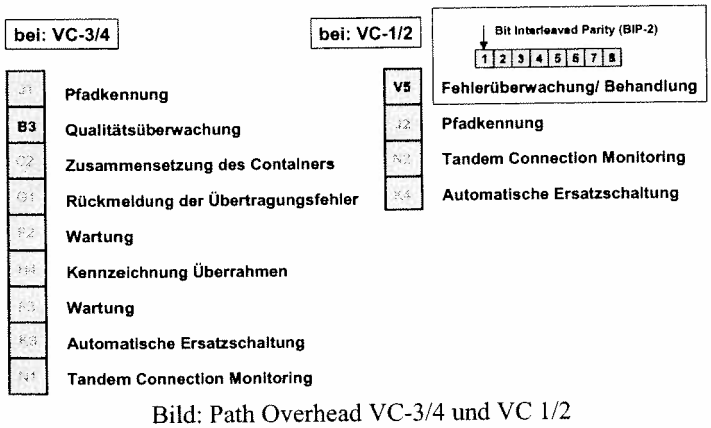
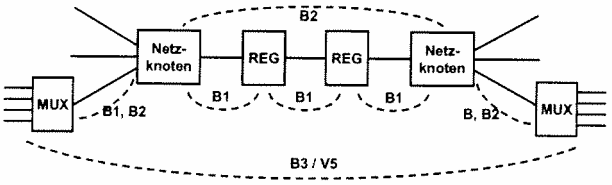


Bild: Path Overhead VC-3/4 und VC 1/2

Der Path-Overhead (POH) dient der Qualitätskontrolle der Containerübertragung selbst. Er begleitet den Container bis zu seinem Ziel.

Zur Qualitätsüberwachung eines Pfades dient das Byte B3 in einem VC-4 bzw. VC-3 Container.

Eine Qualitätsüberwachung eines 2 Mbit/s Signals wird mit einem V5 Byte ermöglicht.



Byte	Rahmenabschnitt	Länge	Überwachungsabschnitt
B1	RSOH	BIP-8	STM-1 (2430 Bytes)
B2	MSOH	BIP-24	STM-1 ohne RSOH
B3	POH VC-3/4	BIP-8	VC-3/4
V5	POH VC-1/2	BIP-2	VC-1/2

Bild: Übertragungsqualität: Paritätsüberwachung

Die Fehlerüberwachung während des Betriebs ist in SDH einfacher gestaltet als der CRC-Vergleich in PDH, ermöglicht trotzdem bei niedrigen Fehlerhäufigkeiten mit befriedigender Zuverlässigkeit eine Aussage über die aktuelle Übertragungsqualität des gesamten Rahmens und der einzelnen Container.

In der SDH wird das Verfahren der bitverschachtelten Parität (Bit Interleaved Parity, BIP) verwendet. Dabei wird die Parität eines bestimmten Rahmenteils jeweils innerhalb einer Gruppen von 2, 8 ode 24 Bits gebildet (BIP-2, BIP-8 oder BIP-24). Diese Bitgruppen werden spaltenweise angeordnet und die Parität jedes einzelnen Bits in vertikaler Richtung berechnet. Ist die Gesamtzahl der l-Zustände innerhalb einer vertikalen Reihe ungerade, wird auf gerade Parität ergänzt, d.h. im entsprechenden Paritätswort eine l gesetzt

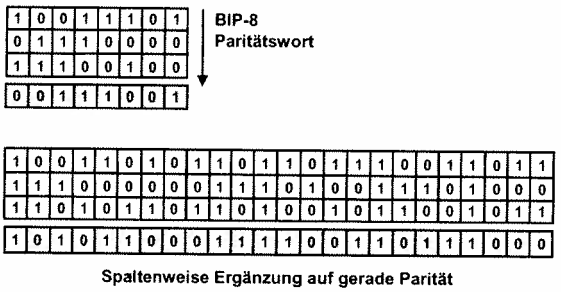


Bild: Bildung der Paritätsworte

Der Empfänger vergleicht das empfangene Paritätswort mit dem selbst berechneten Wert. Da für jedes Übertragungselement auch nur bestimmte Rahmenteile zugänglich sind, ist die abschnittsweise Überprüfung einer Übertragungsstrecke möglich.
Bas Bild zeigt die Erzeugung von BIP-8 und BIP 24. Mit dem BIP-Verfahren ist nicht die exakte Zahl von Übertragungsfehlern ermittelbar, da innerhalb einer vertikalen Reihe ein Doppelfehler nicht erkannt wird.

Wertebereich des Pointers

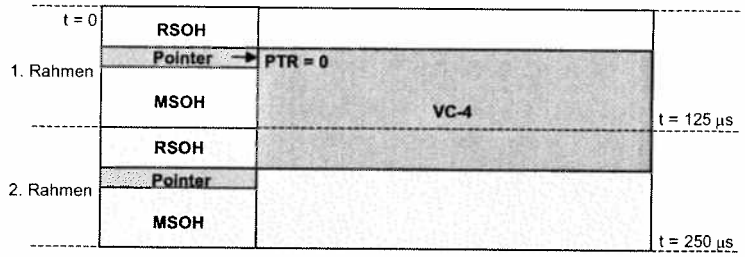
Der Pointer des VC-4 gibt den Ort an, wo der VC-4 beginnt. Er gibt dabei den Offset zwischen dem Ende des Pointer-Feldes und dem Beginn des VC-4 in 3-Byte Schritten an. Das bedeutet, dass ein VC-4 nicht an jeder beliebigen Stelle innerhalb des Payloadbereiches anfangen kann, sondern nur bei jedem dritten Byte. Der Pointer kann keine negativen Werte annehmen.

Der kleinste Wert des Pointers (PTR = 0) entsteht dann, wenn der VC-4 unmittelbar nach dem PTR anfängt. Die Lage dieses VC-4 liegt dann mit genau drei Zeilen im nächsten STM-Rahmen.

Der größte Wert des Pointers (PTR = 782) wird dann erreicht, wenn der VC-4 genau 3 Bytes vor dem Beginn des Pointer-Feldes des nächsten STM anfängt. Der Wert errechnet sich durch: (261 Bytes x 9 Zeilen) / 3 -1 = 782. Der dazugehörige VC-4 liegt dann fast drei Zeilen im übernächsten STM-Rahmen.

Abhängig vom Pointerbeginn kann sich ein VC-4 über drei STM-1 Rahmen erstrecken.

Pointerminimum



Pointermaximum

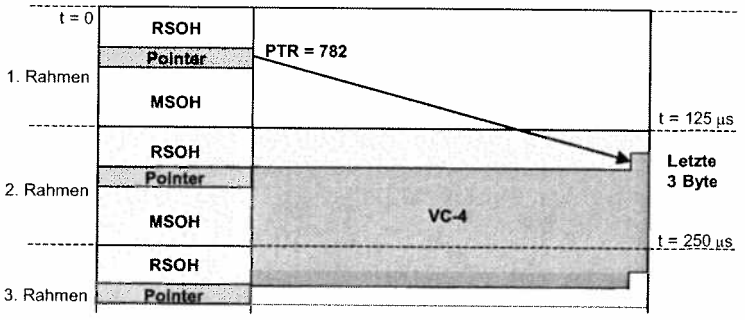


Bild: Pointerminimum und Pointermaximum

In den Quellen der Zubringersignale und beim Übergang zwischen verschiedenen SDH Netzen treten Taktschwankungen auf. Sie sind darauf zurückzuführen, dass es für die unterschiedlichen Netzelemente und in den einzelnen SDH Netze verschiedene Taktquellen gibt. Diese geringe Taktschwankungen werden durch Pointeradjustierung ausgeglichen.

Pointeradjustierung

Tritt nun eine Taktschwankung auf, die größer ist als 3 Byte, so kann sie durch Verschieben des VC-4 im Payloadfeld ausgeglichen werden. Gleichzeitig wird der Wert des Pointers inkrementiert oder dekrementiert. Nach einer solchen Pointeraktion bleibt der Pointer mindestens drei STM-Rahmen lang unverändert.

Im ersten Beispiel ist die Taktquelle des Signals zu langsam, das heißt, es kommen zu wenig Daten in den SDH Knoten, um den VC-4 vollständig zu füllen. Daher wird zwischen dem n-1-ten VC-4 und dem n-ten VC-4 eine 3 Byte große Lücke gelassen und der Pointer um 1 inkrementiert. Der n-te VC-4 fängt um 3 Byte später an als der n-1-te VC-4 im vorigen STM-Rahmen.

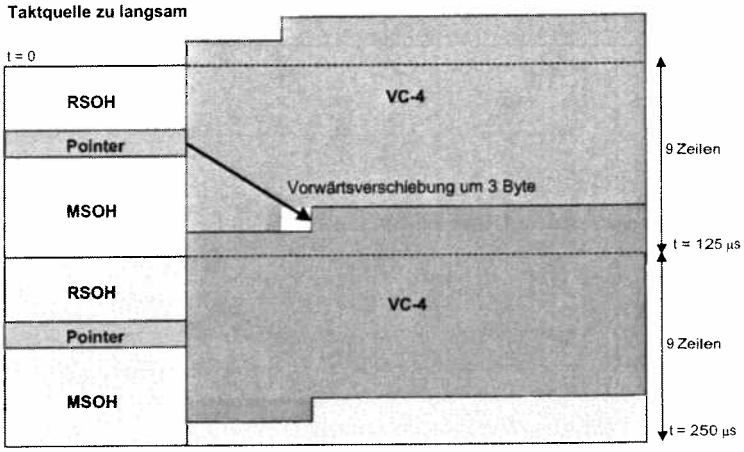


Bild: Positive Pointeradjustierung

Im zweiten Beispiel ist die Taktquelle des Signals zu schnell, das heißt, es kommen zu viele Daten in den SDH Knoten, und der VC-4 läuft über. Der Beginn des n-ten VC-4 wird um 3 Byte nach vorne verlegt und der Pointer um 1 dekrementiert. Da aber an der Stelle, an der der n-te VC-4 anfangen sollte, noch Daten des n-1-ten VC-4 stehen, muss irgendwo Platz für die übergelaufenen Daten geschaffen werden. Dazu sind 3 Byte am Ende des Pointer-Feldes reserviert, in die jene 3 Bytes eingetragen werden, die am Anfang des n-ten VC-4 stehen sollten. Der n-te VC-4 ist daher um 3 Byte kürzer und kann früher enden. So wurde Platz für die zu rasch ankommenden Daten geschaffen.

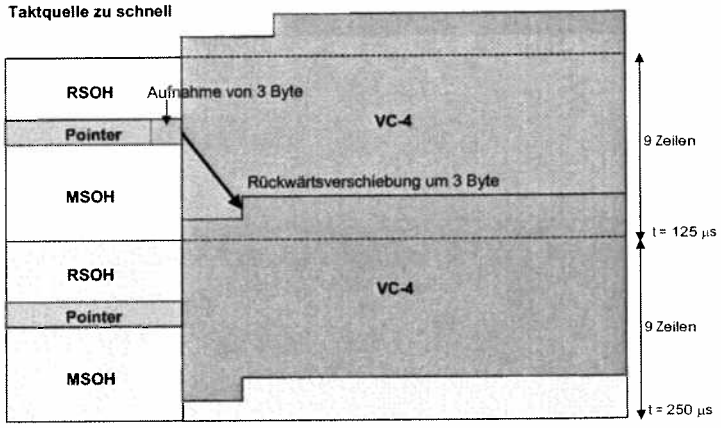


Bild: Negative Pointeradjustierung

Transportmodule STM-N

In PDH verfügt jede Hierarchieebene über eine eigene Rahmenstruktur. Die Bitrate BR der europäischen Hierarchie n+1 ergibt sich zu:

$BR_{n+1} = m \times BR_n + A_{n+1}$ (m = 4)

In A ist zusätzliche Übertragungskapazität für Stopfprozesse und hierarchiespezifische Betriebs- und Synchroninformationen enthalten.

Bei der Bildung der oberen SDH-Hierarchien entfällt jeglicher zusätzlicher Overhead. Jeweils 4, 16, 64 und 256 STM-1-Module werden byteweise gemultiplext. Dabei entstehen die Bitraten: 622 Mbit/s, 2,5 Gbit/s, 10 Gbit/s und 40 Gbit/s.

Zur Information sind die exakten Werte ebenfalls angegeben:

155,052	Mbit/s	(STM-1)
622,080	Mbit/s	(STM-4)
2 488,320	Mbit/s	(STM-16)
9 953,280	Mbit/s	(STM-64)
39 813,120	Mbit/s	(STM-256)

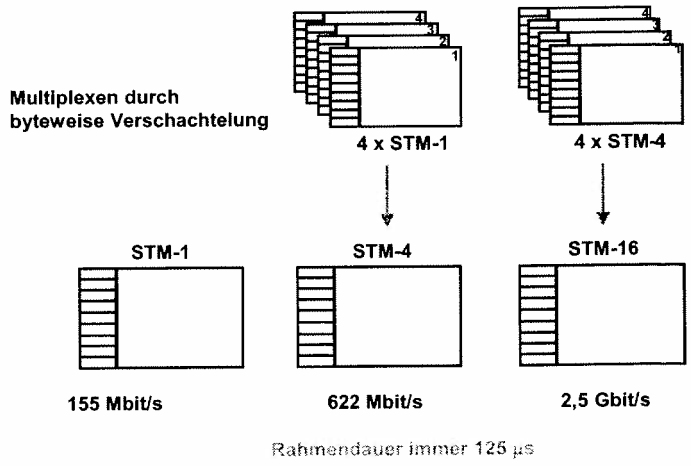


Bild: Bildung der SDH Hierarchie

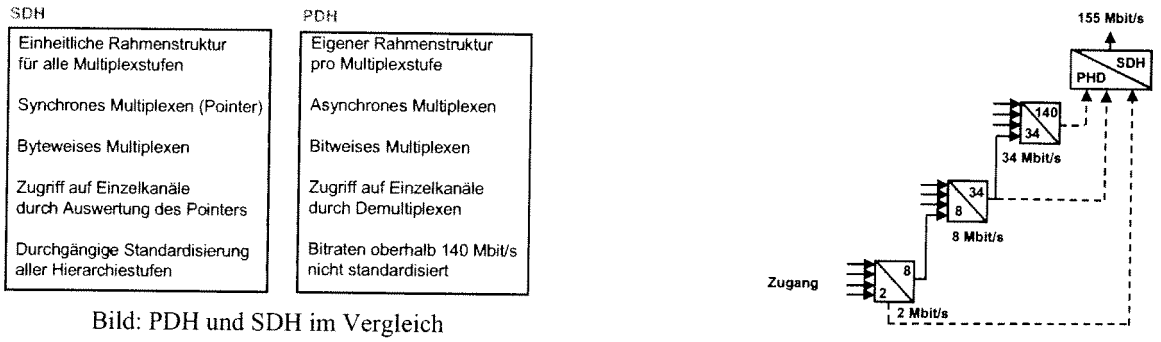


Bild: PDH und SDH im Vergleich

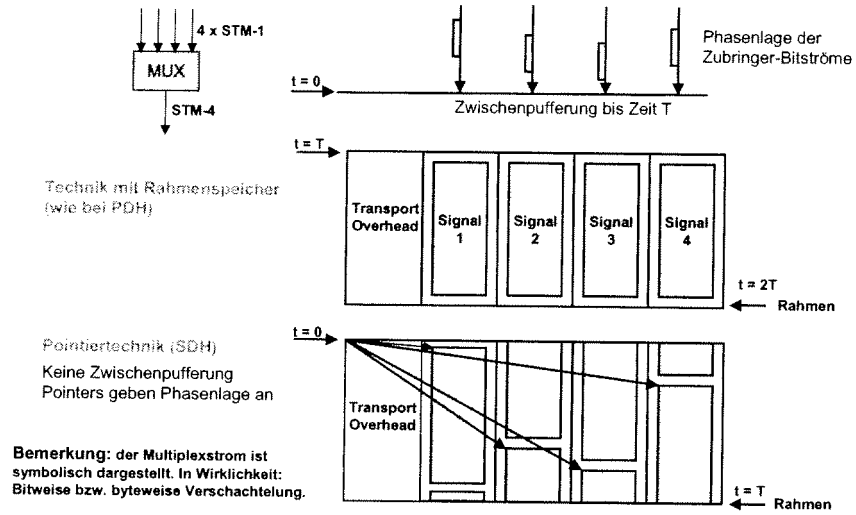


Bild: Unterschiede in der Transporttechnik

Das Pointer-Feld des übergeordneten Container VC-4 bezogen auf den Rahmenbeginn ist immer an fester Stelle. Durch Auswertung des Pointerwertes ist der Beginn des VC-4 bekannt. Innerhalb des VC-4 kann der Nutzlastbereich in ihren untergeordneten Virtuellen Containern frei gleiten. Die Lage der Pointer von untergeordneten Einheiten ist in bezug auf den Beginn des VC-4 festgelegt und somit durch Abzählen von Bits auffindbar.

In der PDH müssen die Zubringer innerhalb des gesamten Bitstroms durch Auswertung der Synchronisationssignale gesucht werden, in der SDH ist die Lage der Zubringer durch Auswertung von maximal zwei Pointern sofort bekannt.

Vorteil: Aufwendige Pufferspeicher zur Synchronisation der Nutzlast auf den Rahmenbeginn entfallen ebenso wie zeitliche Verzögerungen bei der Multiplexbildung.

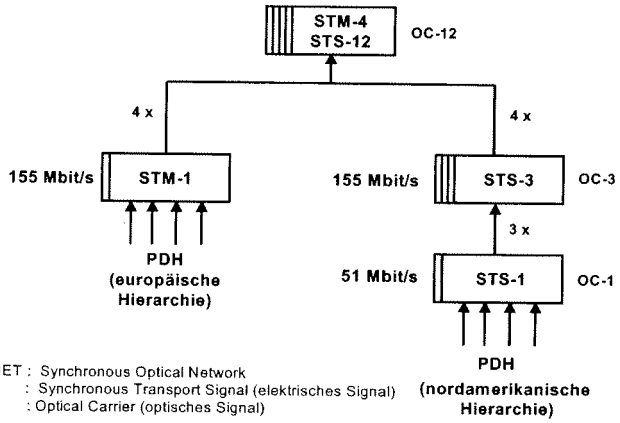


Bild: SDH und SONET

SONET- (Synchronous Optical Network)
Die ersten Impulse für die neue Netztechnologie eines synchron optischen Netzes (Synchronous Optical Network, SONET) kamen Mitte der achtziger Jahre von führenden Telekommunikationsunternehmen in den USA. Oberstes Ziel bei der Standardisierung der SDH in Europa war es, einen weltweit gültigen, zu SONET kompatible Standard zu schaffen.

Die Grundbitrate von SONET ist 51 Mbit/s. Ein Multiplex von drei solchen Einheiten bildet ein STM-1.

Das nordamerikanische System unterscheidet zwischen elektrischen (STS) und optischen Signal (OC).

Auch für SDH-Übertragungssysteme wurden SONET-Schnittstellen entwickelt. Sie finden ihren Einsatz in internationalen SDH/SONET-Verbindungen und in der Übertragung von europäischen PDH-Richtfunkzubringern bei 51 Mbit/s. Häufig wird für dieses Übertragungsprinzip auch die Bezeichnung STM-0 oder Sub-STM verwendet.

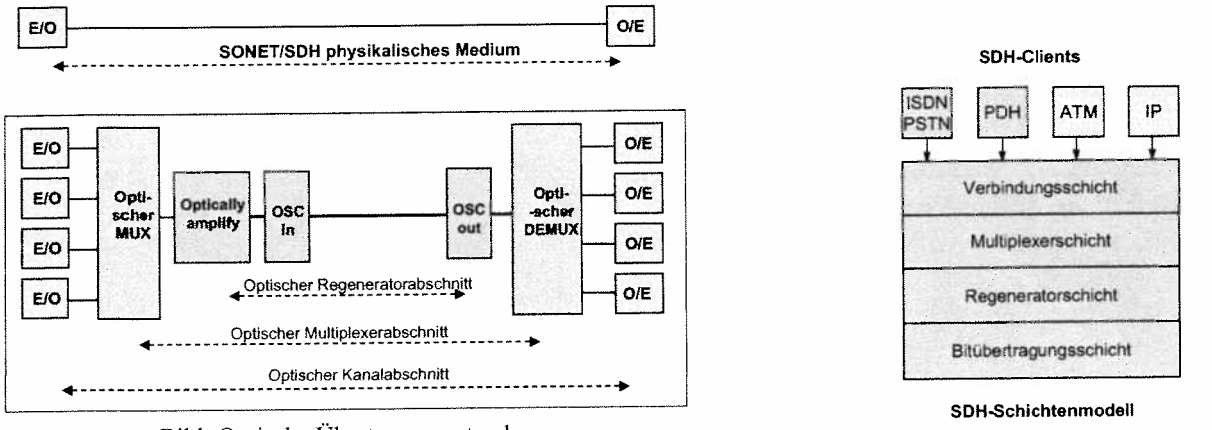


Bild: Optische Übertragungsstrecke

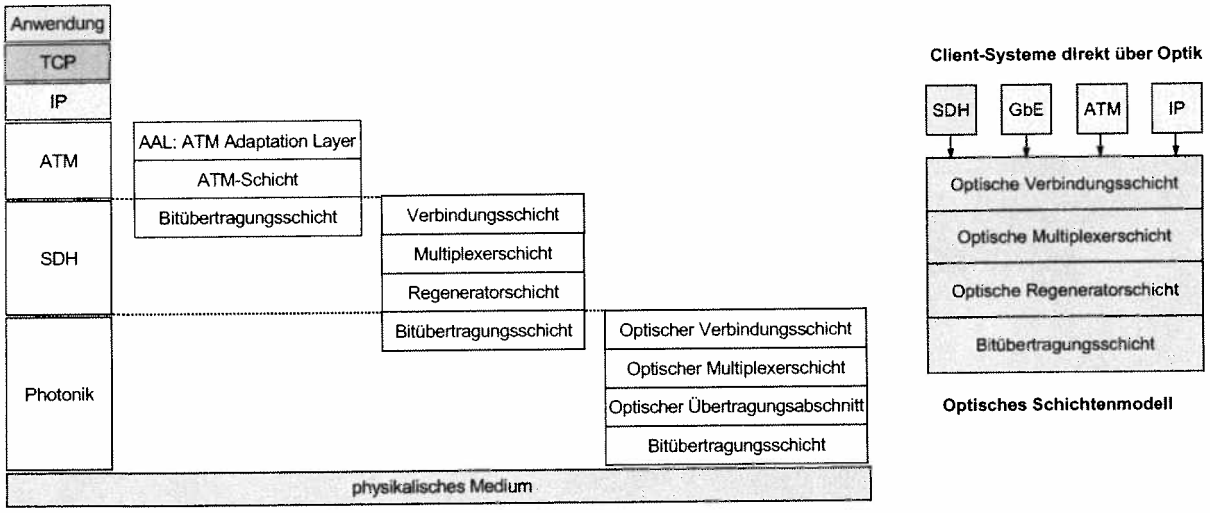


Bild: Stratum-Protokollschichtung

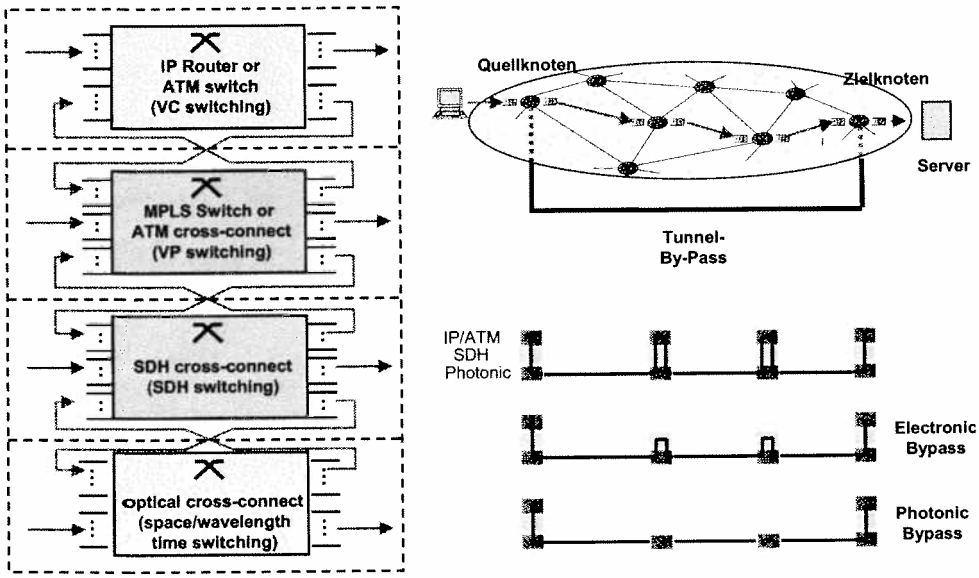
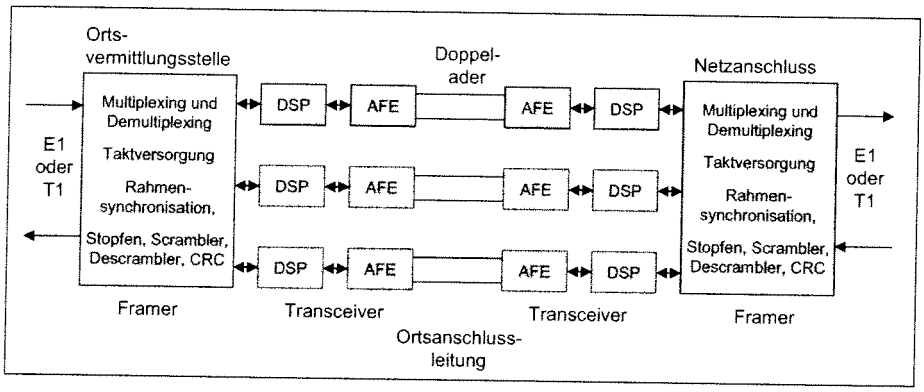
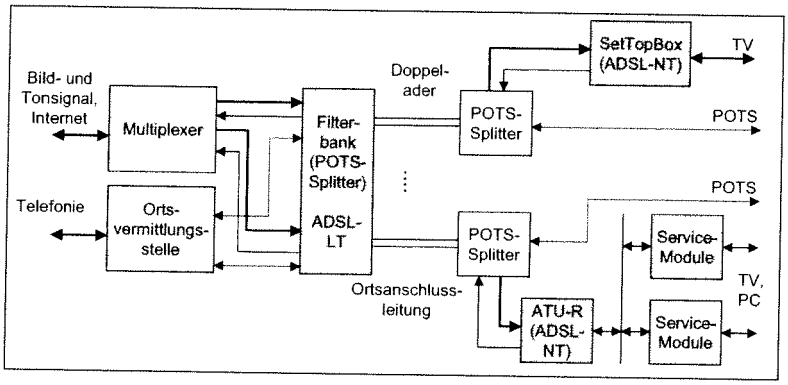


Bild: Vermittlungsknoten für Tunnel By-Passing



AFE:
DSP: Digital Signal Processor

Bild: HDSL-Übertragungssystem



LT: Line Termination
NT: Network Termination

Bild: ADSL-Übertragungssystem

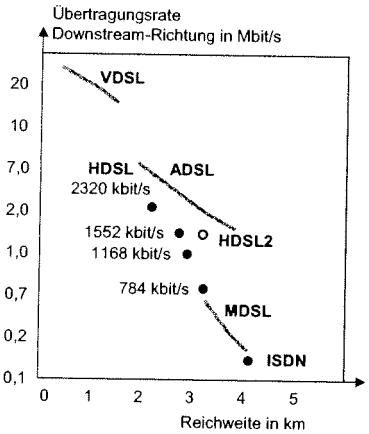
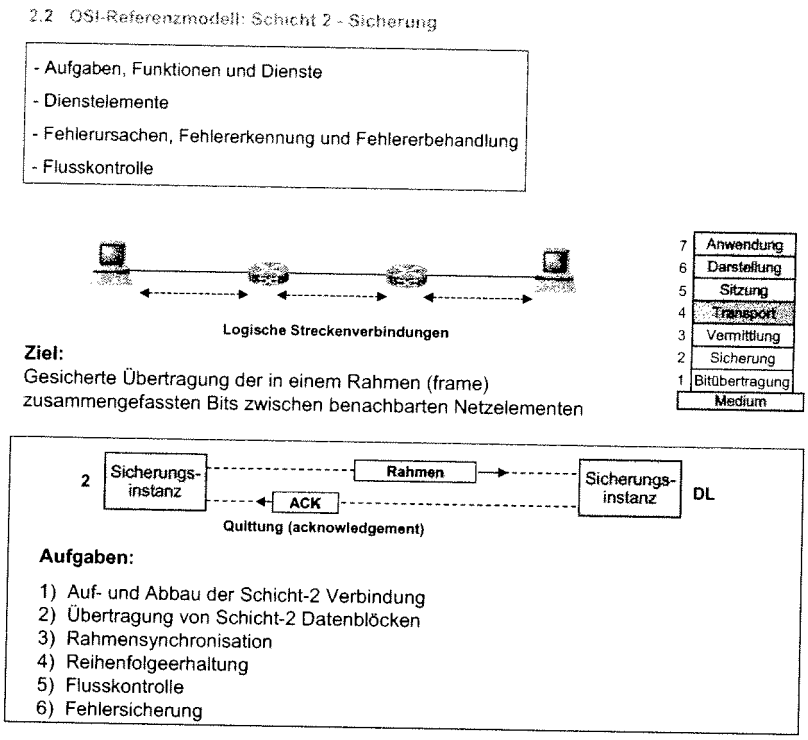


Bild: Reichweiten von xDSL-Verfahren

2.2 OSI-Referenzmodell: Schicht 2 - Sicherungsschicht

Version: Dez. 2003

Inhalt:



Schicht 2: Sicherungsschicht (DL: Data Link)
Die Sicherungsschicht macht die ungesicherten Übertragungen zu gesicherten Systemverbindungen. Dazu wird zuerst eine logische Schicht-2 Verbindung zwischen den benachbarten Netzknoten aufgebaut. Allgemein gilt, dass abgesehen von Schicht 1, wo eine physikalische Verbindung bestehen muss, auf allen anderen Schichten jeweils logische Verbindungen aufzubauen sind. Die logischen Verbindungen der Schichten 2 und 3 sind abschnittsweise, also von Netzsystem zu Netzsystem. Die logischen Verbindungen ab Schicht 4 hinauf sind Ende-zu-Ende.

Bild: Schicht 2: Sicherungsschicht

Allgemein sind die ersten zwei Aufgaben jeder Schicht, der Auf- und Abbau der logischen Verbindung und der Austausch von Datenblöcken. Zu beachten ist, dass je nach Schicht die Datenblöcke verschieden bezeichnet werden.

Die **Sicherungsschicht** überträgt ganze **Rahmen** (frames) über eine Teilstrecke (link). Die Rahmen müssen fehlerfrei übertragen werden. Da Übertragungsfehler grundsätzlich nicht vermeidbar sind, müssen Möglichkeiten zur Fehlererkennung und -beseitigung bestehen. Die Bitübertragungsschicht hingegen ist nur für die Übertragung einzelner Bits über eine Teilstrecke (link) zuständig.

Im Einzelnen erledigt die Sicherungsschicht die folgenden Aufgaben:

- Rahmensynchronisation (Frame Synchronisation): Anfang und Ende eines Rahmens müssen erkannt werden.
- Flusssteuerung (Flow Control): Der Sender darf den Empfänger nicht mit Rahmen überschwemmen, er muss die Empfangsbereitschaft des Empfängers berücksichtigen.
- Fehlersicherung (Error Control): Bei der Übertragung aufgetretene Fehler müssen behoben werden.
- Unterscheidung von Nutzdaten und Steuerinformation: Der Empfänger muss zwischen Nutzdaten und Steuerinformation unterscheiden können, da beide auf dem selben Übertragungsweg übertragen werden sollen.
- Übertragungssteuerung (Link Management): Eine geordnete, fehlerfreie Übertragung muss durch geeignete Mechanismen für Koordination und Kooperation sichergestellt werden.

Vielfachzugriffsverfahren gehören ebenfalls zur Sicherungsschicht.

Wenn man die Funktionen der Bitübertragungsschicht hinzunimmt, lässt sich der gesamte Aufbau einer Teilstrecke in einer Übersicht darstellen. In einzelnen Anwendungen sind nicht alle Funktionsblöcke erforderlich. Dies betrifft z. B. die **Verwürfelung** (scrambling, bezweckt das Aufbrechen von langen Null- und Eins-Folgen zur spektralen Formung des Leitungssignals) und die Modulation (falls keine Breitbandübertragung verlangt wird).

(1) **Auf- und Abbau von Sicherungsverbindungen**

Physikalische Verbindungen mit mehreren Endpunkten (Mehrpunkt-Verbindung, *Multipoint Connection*) benötigen zusätzliche Funktionalität der Sicherungsschicht, um Sicherungsverbindungen zu identifizieren und um die physikalische Verbindung zu nutzen.

- Die Adressierungsmöglichkeit für mehrere Verbindungsendpunkte muss vorhanden sein
- Eine Verbindung der Sicherungsschicht kann mehrere unterschiedliche physikalische Verbindungen nutzen, um der Durchsatz zu verbessern.

(2) **Abbildung der Sicherungs-Dienstdateneinheiten**

Dienstdateneinheiten müssen eindeutig auf Protokolldateneinheiten abgebildet werden

(3) **Rahmensynchronisation** (Framing)

Zusammenfassung physikalischer Dienst-Dateneinheiten zu Sicherungsprotokoll-dateneinheiten

(4) **Reihenfolgeerhaltung** (Sequencing)

Korrekte Reihenfolge der DL-SDUs wird über Sicherungsverbindung aufrecht erhalten

(5) **Flusskontrolle** (Flow Control)

Kontrolle der Flussrate mit der Rahmen gesendet und empfangen werden können.

(6) **Fehlersicherung**

- **Fehlererkennung** (Error Detection)

  Erkennung von Übertragungsfehlern, Formatfehlern oder operationellen Fehlern (auf physikalischer Verbindung oder als Ergebnis einer Fehlfunktion der entfernten Instanz)

- **Fehlerbehebung** (Error Recovery)

  Oft durch Aufforderung an entfernte Instanz, den als fehlerhaft erkannte Rahmen nochmals zu senden

Bild: Aufgaben der Sicherungsschicht

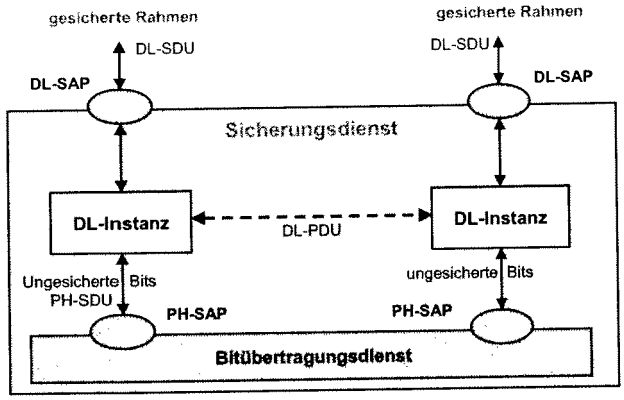
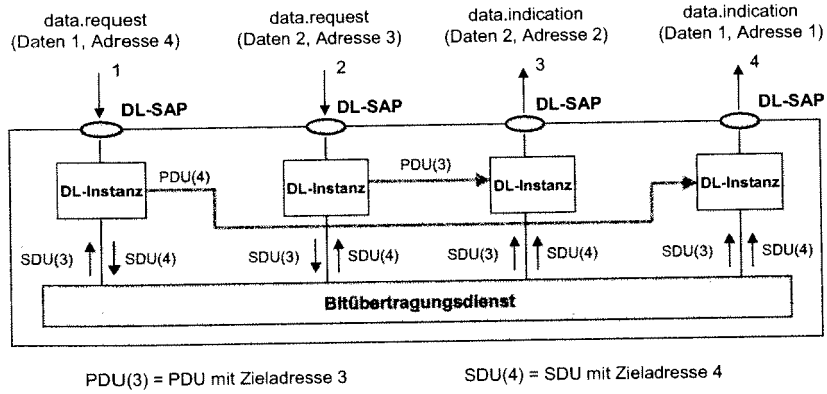


Bild: Sicherungsdienst



PDU(3) = PDU mit Zieladresse 3 SDU(4) = SDU mit Zieladresse 4

Bild: Mehrpunkt-Übertragung

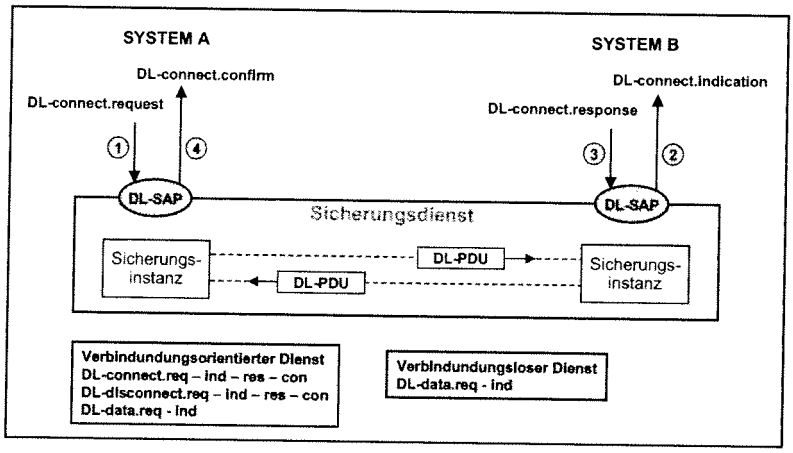


Bild: Sicherungsdienst: Primitive

(1a) Betrieb von Sicherungsverbindungen
Zwischen zwei Instanzen können mehrere Sicherungsverbindungen betrieben werden, Auf- und Abbau dieser Verbindungen geschieht dynamisch.

(1b) Einrichtung von Verbindungsendpunkt-Identifikatoren
Jeder Verbindung werden lokal eindeutige Verbindungsendpunkt-Identifikatoren zugeordnet, um eintreffende Daten einer dieser Verbindungen zuzuordnen.

(1c) Auswahl der Dienstqualitätsparameter (Quality-of-Service)
Sicherungsschicht wählt für die Dauer einer Sicherungsverbindung die Dienstqualität in Abhängigkeit der Dienstqualität auf der Vermittlungsschicht aus.

Dienstgüte-Parameter beinhalten:
- mittlere Zeit zwischen erkannten aber nicht behebbaren Fehlern
- Restfehlerrate durch duplizierte oder verlorengegangene DL-SDUs (Pakete)
- Verfügbarkeit des Dienstes, abhängig von Zuverlässigkeit der Knoten
- Übertragungsverzögerung
- Durchsatz pro Zeiteinheit von korrekt übertragenen DL-SDUs

(2/3) Übertragung von Sicherungs-Dienstdateneinheiten (DL-SDU)
Die maximal erlaubte Länge der DL-SDUs kann begrenzt sein. Dies ist abhängig von der Fehlercharakteristik der physikalischen Verbindung und der Fähigkeit der Sicherungsschicht, Übertragungsfehler zu erkennen und zu korrigieren

(4) Reihenfolgeerhaltung (Sequencing)
Weiterleitung aller empfangenen DL-SDUs in der korrekten Reihenfolge

(5) Flusskontrolle (Flow Control)
Empfangsinstanzen kontrollieren die Rate, mit der sie DL-SDUs von der Vermittlungsschicht empfangen können.

(6) Benachrichtigung über Fehler (Error Notification)
Mitteilung von Fehlern (z. B. Zusammenbruch der Sicherungsverbindung), die von Sicherungsschicht entdeckt, aber nicht behoben werden können, an der Instanz der Vermittlungsschicht

Bild: Dienste der Sicherungsschicht

Dienst	req.	ind.	res.	con.	Parameter
Verbindungsaufbau:					
DL-connect	x	x	x	x	Adressen, Dienstgüteparameter
DL-activate	x			x	Adressen
DL-acquire	x			x	welche Übertragungsstrecken
DL-negotiate	x	x	x	x	Dienstgüteparameter
Transferphase:					
DL-data	x	x	x	x	Information, Adressen
DL-expedited_data	x	x	x	x	Information, Adressen
DL-flow control	x	x			on, off
DL-reset	x	x	x	x	Adressen der Verbindung
DL-notify	x	x		x	Adressen
DL-abort	x	x			Adressen der Verbindung
Verbindungsabbau:					
DL-disconnect	x	x	x	x	Adressen
DL-deactivate	x			x	Adressen

Primitive (x = vorhanden)

Bild: Dienstprimitive der Sicherungsschicht

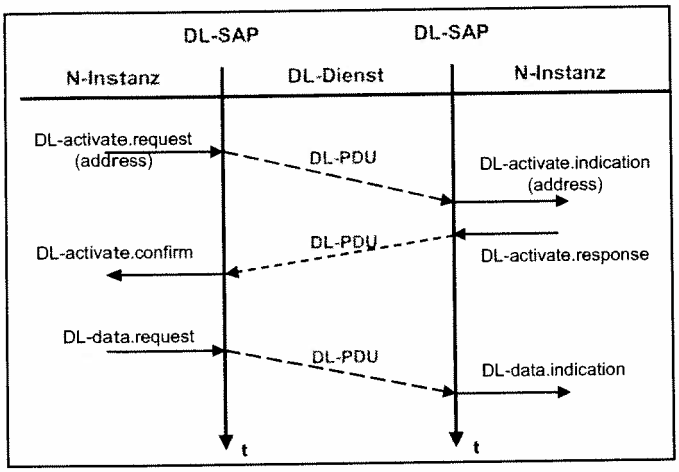


Bild: Benutzung des Activate-Dienstes

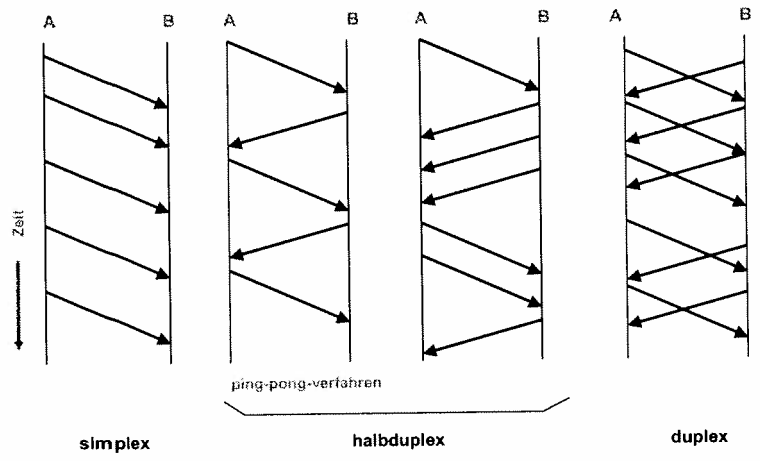
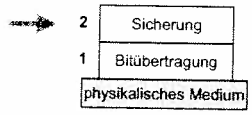


Bild: Betriebsarten der Übertragung

Uni- und bidirektionale Übertragung

Eine unidirektionale Übertragung von A nach B lässt in der Gegenrichtung (B nach A) keine Kommunikation zu. Fast immer ist eine bidirektionale Übertragung gewünscht, bei der beide Übertragungsrichtungen nutzbar sind.

Eine Teilstrecke kann uni- oder bidirektional genutzt werden. Der Begriff Simplex bezeichnet eine unidirektionale Übertragung, Duplex eine bidirektionale Übertragung. Im Halbduplex-Betrieb werden die beiden Übertragungsrichtungen abwechselnd genutzt, im Vollduplex-Betrieb gleichzeitig. Bei einer bidirektionalen Übertragung werden in der Gegenrichtung nicht nur Nutzdaten übertragen, sondern auch Quittungen (acknowledgment). Eine Quittung kann auch einem Nutzdatenpaket mitgegeben werden, diese wird als Piggyback-Quittung bezeichnet.



Erkennung der Rahmen aus Bitstrom

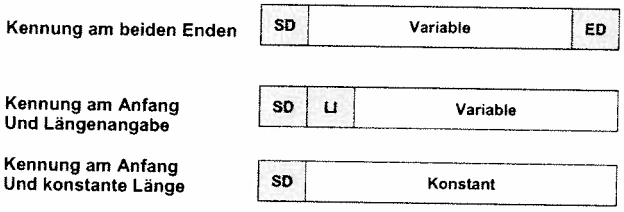


Bild: Rahmenerkennung

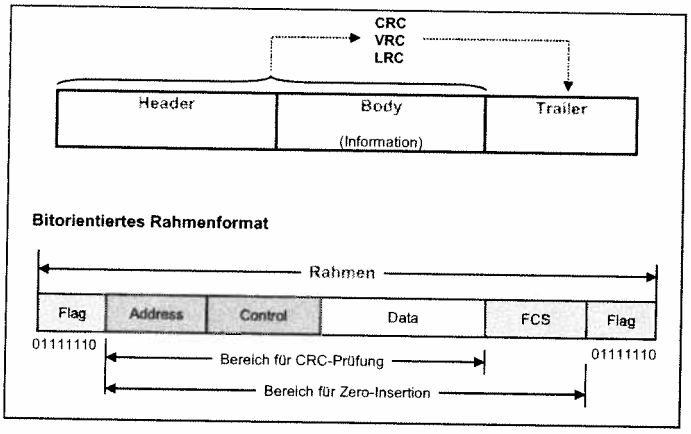
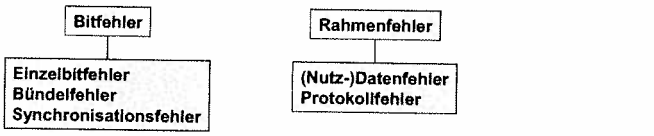


Bild: Allgemeines Format einer DL-PDU



Eine Störung von 20 ms führt
- bei Telex (50 bit/s, Signaldauer: 20 ms) zu einem Fehler von 1 Bit ⇒ **Einzelbitfehler**
- bei ISDN (64 kbit/s, Signaldauer: 15,625 µs) zu einem Fehler von 1280 Bit ⇒ **Bündelfehler**
- bei Breitband-ISDN (mit 155 Mbit/s, Signaldauer: 6,45 ns) zu einem Fehler von ca. 3,1 Mbit

- Ein zuverlässiger Kommunikationsdienst erfordert Fehlererkennung und Fehlerbehebung.
- Diese Mechanismen tragen erheblich zur Komplexität von Protokollen bei.
- Kommunikationsprotokolle unter der Annahme fehlerfreie Übertragungen, sind sehr einfach

Bild: Fehler - Typen, Unsachen und Auswirkungen

Rahmenbildung und Rahmensynchronisation

Die Bildung von Rahmen soll sicherstellen, dass die übertragenen Signale einer Kommunikationsbeziehung zugeordnet und korrekt interpretiert werden können. Die **Rahmensynchronisation** ermöglicht die eindeutige Erkennung von Rahmenanfang und -ende.

Dafür gibt es drei Möglichkeiten:

- Rahmenanfang und -ende werden durch eine festgelegte Markierung (flag) gekennzeichnet.
- Der Rahmenanfang wird markiert, die Rahmenlänge wird explizit im Header angegeben.
- Die Rahmenlänge ist konstant und fest vereinbart. Damit muss nur der Rahmenanfang markiert werden. Die Rahmensynchronisation setzt eine zuverlässige Bitsynchronisation (Taktregenerierung) voraus.

Fehlersicherung

In Datennetzen ist meist eine fehlerfreie Übertragung erforderlich, beispielsweise für Daten oder Programme. Ein falsch empfangenes Bit kann bereits die Übertragung völlig nutzlos machen. Da Übertragungsfehler physikalisch unvermeidlich sind, werden Verfahren zu ihrer Beseitigung benötigt.

Prinzipiell können Fehler behoben werden durch:

- Übertragungswiederholung (automatic repeat)
- Fehlerkorrektur (error correction, FEC: Forward Error Correction).

Verfälschung von Bits bei der Übertragung – Bitfehler

Beispiel: - Null-Bit werde durch 0 Volt repräsentiert; Eins-Bit durch 5 Volt
- Entscheidungsschwelle sei 2,5 Volt
- Übertragungsstrecke ist nicht optimal: Rauschen, Signaldämpfung

Ergebnis: Empfänger empfängt Signalwert von 3 Volt, obwohl ursprünglich 0 Volt gesendet wurde. ⇒ Bitfehler.

Fehlerursachen
- Rauschen
- Schaltvorgängen in benachbarten Stromkabel
- Verlust der Bit-Synchronisation

Verfälschung von Dateneinheiten – Rahmenfehler

Fehlerarten
- Verlust/Duplizierung einer Dateneinheit
- Abweichung der Empfangsreihenfolge von Dateneinheiten

Fehlerursachen
- Bitfehler im Rahmen
- verfrühte Datenwiederholung

Bild: Fehlertypen und Fehlerursachen

Unterschieden wird nach:
- Bitfehler,
- Rahmenfehler.

Einzelbitfehler
z.B. Rauschspitzen, die die Detektionsschwelle bei digitaler Signalerfassung überschreiten

Bündelfehler
Länger anhaltende Störung durch Überspannung, Starkstromschaltprozesse, etc.

Synchronisationsfehler
- Alle Bits bzw. Zeichen werden falsch erkannt
- Auswirkung einer Störung ist abhängig von der Übertragungsgeschwindigkeit

Rechenbeispiel

Eine Störung von 20 ms führt
- bei Telex (50 bit/s, Signaldauer: 20 ms) zu einem Fehler von 1 Bit ⇒ Einzelbitfehler
- bei ISDN (64 kbit/s, Signaldauer: 15,625 µs) zu einem Fehler von 1280 Bit ⇒ Bündelfehler
- bei Breitband-ISDN (mit 155 Mbit/s, Signaldauer: 6,45 ns) zu einem Fehler von ca. 3,1 Mbit

Bild: Fehlertypen

Übertragungsfehler können durch **Rauschen** oder durch **Störungen** verursacht werden. Der Empfänger ist dann nicht mehr in der Lage, aus dem empfangenen Signal das gesendete Symbol/Bit korrekt zu decodieren. Bitfehler können isoliert **(Einzelbitfehler)** oder in Gruppen **(Bündelfehler,** burst error) auftreten.

Ein Maß für den Umfang der Übertragungsfehler ist die **Bitfehlerrate** (Anzahl falscher Bits bezogen auf die Anzahl insgesamt gesendeter Bits), die als Mittelwert über einen längeren Zeitraum gemessen wird. Durch die Fehlerbeseitigung können nicht alle Fehler behoben werden, so dass eine **Restfehlerwahrscheinlichkeit** zurück bleibt. Deshalb wird die Fehlerbeseitigung so ausgelegt, dass die Restfehlerrate akzeptabel ist.

- Die Fehlerwirkungen gestörter Bits können sehr unterschiedlich sein.
- Dies ist abhängig davon welche Bits einer Dateneinheit betroffen sind.

(Nutz-)Datenfehler
Bits innerhalb der Nutzdaten werden gestört.

Protokollfehler
Störungen können Protokollkontrolldaten, Steuerzeichen, Adressen oder sonstige protokollrelevante Daten verfälschen oder vernichten.

Für einen zuverlässigen Kommunikationsdienst sind Mechanismen zur Fehlererkennung und –behebung erforderlich.

Diese Mechanismen tragen erheblich zur Komplexität von Protokollen bei, die einen zuverlässigen Dienst anbieten, falls sie diesen nicht bereits von unterliegenden Schichten bereitgestellt bekommen.

Kommunikationsprotokolle, die von der Annahme fehlerfreier Übertragung ausgehen, sind sehr einfach.

Bild: Fehlerwirkungen

Fehlerwirkungen:
- Datenfehler,
- Protokollfehler.

Bezüglich Bitfehlern
- Fehlererkennende Codes
- Fehlerkorrigierende Codes

Bezüglich kompletter Dateneinheiten
- Sequenznummern
- Zeitüberwachung
- Quittungen
- Sendewiederholungen

Redundanz
- Fehlererkennung von Datenfehlern beim Empfänger durch Hinzufügung von Redundanz beim Sender.

Bild: Fehlererkennung und -behebung

Codierung zur Fehlererkennung

Zur Fehlererkennung wird zusätzliche, redundante Information übertragen, durch deren Auswertung der Empfänger Übertragungsfehler feststellen kann. Die Fehlerbehebung geschieht dann durch Anforderung einer Übertragungswiederholung beim Sender.

Zu einer vorbestimmter Einheit wird jeweils ein redundantes Bit hinzugefügt
- **Gerade Parität** : es wird auf **gerade** Anzahl von 1-Bit ergänzt
- **Ungerade Parität**: es wird auf **ungerade** Anzahl von 1-Bit ergänzt

Folgende Varianten werden unterschieden

Vertikale Parität
- An jedes einzelne Zeichen (bestehend aus n Bits) wird ein Paritätsbit angefügt (d.h. ein Paritätsbit pro Reihe)
- Erkennung von Bitfehlern ungerader Anzahl (1-Bitfehler, 3-Bitfehler etc.)

Längsparität
- An eine Folge von Zeichen wird ein dediziertes Prüfzeichen angefügt. Dieses enthält jeweils ein Paritätsbit pro Spalte (d.h. pro n-tem Bit aller Zeichen)

Matrixparität
- Vertikale Parität und Längsparität werden kombiniert. Jeweils 1 Paritätsbit pro Spalte und pro Reihe eines aus mehreren Zeichen bestehenden Blocks
- Auch als Block Check Character (BCC) bezeichnet.
- Falls Störungen weniger als 8 Bit betreffen (bei einer Zeichenlänge von 8 Bit), wird der Fehler gefunden.

Bild: Paritätsbits

Fehlererkennung durch Paritätsbits

Die **Parität** einer Bitkette (Wort) der Länge n ist die Anzahl der Einsen in diesem Wort. Ein Code, dessen Worte alle eine gerade Anzahl von Einsen aufweisen, besitzt eine gerade Parität. Bei einer ungeraden Parität ist die Anzahl der Einsen immer ungerade.

Paritätsverfahren:
- Gerade/ungerade Parität.
- Vertikale Parität,
- Längsparität,
- Matrixparität.

Aus einem Code mit Wörtern der Länge n - 1 entsteht durch Anhängen eines Paritätsbits ein Code mit gerader bzw. ungerader Parität. Codes dieser Art, bei denen die Nutzbits unverändert als Block übertragen und die Prüfbits dann angehängt werden, heißen **systematische Blockcodes.** Paritätsbits können sehr einfach durch Exklusiv-Oder-Verknüpfungen berechnet werden.

Allgemein wird eine ungerade Anzahl von Bitfehlern erkannt, eine gerade Anzahl nicht. Diese Erkenntnis hilft aber in der Praxis nicht weiter. Die Distanz zweier Codewörter ist die Anzahl der Bitpositionen, in denen sich diese Codewörter unterscheiden. Die Hamming-Distanz eines Codes ist der Minimalwert der Distanzen zwischen allen möglichen Paaren von Codewörtern. Allgemein gilt: Ein Code mit der Hamming-Distanz d kann d - 1 Fehler erkennen.

Paritätsbits können auf einzelne Zeichen oder auf längere Datenblöcke angewendet werden. Bei Datenblöcken kann die Wahrscheinlichkeit unerkannter Fehler zu hoch werden, wenn nur ein Paritätsbit verwendet wird. Deshalb verwendet man **mehrfache Paritätsprüfungen** und ordnet dazu die Bits mehrerer Zeichen in einer Matrix an. Für jede Zeile wird eine Längsparität und für jede Spalte eine Querparität ermittelt. Damit können alle 2-Bit-Fehler, alle 3-Bit-Fehler und ein Teil der möglichen 4-Bit-Fehler erkannt werden. Die Anwendung eines Paritätsbits auf ein Zeichen verringert dessen Fehlerrate ungefähr um den Faktor 10^{-2}. Bei der kombinierten Paritätsprüfung mit Längs- und Querparität sinkt die Fehlerrate auf ca. 10^{-4}.

Fehlererkennung durch Prüfsummen

Die durch Bitfolgen dargestellten Zeichen werden als numerische Werte aufgefasst. Zeichen werden zu Blöcken zusammengefasst und die Summe aller numerischen Werte wird berechnet. Die Summe kann verkürzt mit einer Bitanzahl entsprechend ein oder zwei Zeichen dargestellt werden. Die so ermittelte Prüfsumme wird bei der Übertragung an die Nutzdaten angehängt. Prüfsummen werden bei IP verwendet.

Anstelle eines einzigen Paritätsbits wird hier eine Sicherungssequenz an die zu übertragende Dateneinheit angefügt.

- Wird auch als FCS (Frame Check Sequence) bezeichnet
- Basiert auf Division in Modulo-2-Binärarithmetik; wobei keine Überträge stattfindet

Entspricht bitweiser XOR-Operation: 1+1 = 0+0 = 0, 1+0 = 0+1 = 1

Beispiele für bitweise XOR-Operation

10011011	00110011	11110000	01010101
11001010	11001101	10100110	10101111
01010001	11111110	01010110	11111010

Bitstrings als Repräsentation von Polynomen, z.B. Dateneinheit 10011010 entspricht Polynom $M(x) = x^7 + x^4 + x^3 + x$

- Dateneinheit wird als unstrukturierte Bitfolge aufgefasst, d.h. auch die Anzahl der zu prüfenden Bit ist beliebig (oberhalb einer Mindestlänge).
- Es werden auch keine ganzzahligen Vielfache von 8 Bit gefordert.

Bild: Cyclic Redundancy Check (CRC)

Fehlererkennung durch CRC

Das CRC-Verfahren (Cyclic Redundancy Check) verwendet zyklische Blockcodes.

Ein systematischer Blockcode (Nutz- und Prüfbits sind in zwei Blöcken angeordnet) wird **als zyklisch bezeichnet,** wenn die zyklische Vertauschung der Bits eines Codewortes wieder ein gültiges Codewort ergibt.

Zyklische Codes lassen sich auf einfache Weise mit rückgekoppelten Schieberegistern erzeugen und prüfen. Die redundante Information wird als Blockprüffolge (FCS: Frame Check Sequence) berechnet und an die Nutzdaten angehängt.

- Gleiches Generatorpolynom G(x) für Sender und Empfänger
- Höchstes und niederwertigstes Bit von G(x) müssen 1 sein

Dazu werden die Bits der Nutzinformation als Koeffizienten eines Polynoms aufgefasst.

Prüfsumme (Checksum) wird berechnet
- Dateneinheit mit m Bits entspricht D(x)
- Dateneinheit muss länger sein als Generatorpolynom
- Prüfsumme entspricht Rest R der Division $(x^r D(x)) / G(x)$
  - r: Grad des Generatorpolynoms
  - $x^r D(x)$ fügt r Nullstellen an das Ende der Dateneinheit

Prüfsumme wird an die zu sendenden Daten angehängt
- Entspricht der Addition des Restes: $x^r D(x) + R$

Empfänger überprüft Dateneinheit
- Division der empfangenen Dateneinheit durch G(x)
  - Ist der Rest der Division Null, dann wurde kein Fehler erkannt
  - Ist der Rest der Division ungleich Null, dann ist die empfangene Dateneinheit fehlerhaft

Dieses Polynom wird durch ein festgelegtes **Generatorpolynom** dividiert, der Divisionsrest bildet die Blockprüfsumme. Sender und Empfänger berechnen die Blockprüfsumme in gleicher Weise.

Wenn nun der Empfänger zwischen der empfangenen und der von ihm selbst berechneten Blockprüfsumme einen Unterschied feststellt, weiß er, dass die Übertragung fehlerhaft war.

Bild: Berechnung des CRC

Folgende Fehler werden durch CRC erkannt
- sämtliche Einzelbitfehler
- sämtliche Doppelfehler, wenn $(x^k + 1)$ nicht durch das Prüfpolynom teilbar ist, für $k \leq$ Rahmenlänge
- sämtliche Fehler ungerader Anzahl, wenn (x+1) Faktor des Prüfpolynoms ist
- sämtliche Fehlerbursts der Länge $\leq$ Grad des Prüfpolynoms

International genormt sind u.a. folgende Prüfpolynome

CRC-12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$

CRC-16 = $x^{16} + x^{15} + x^2 + 1$

CRC-ITU = $x^{16} + x^{12} + x^5 + 1$

CRC-32 = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Erkennen aller Einzelbitfehler
x^k und x^0 dürfen nicht gleich Null sein

Nahezu alle Doppelbitfehler
G(x) muss mindestens drei Terme besitzen

Jede ungerade Anzahl an Bitfehlern
G(x) muss den Faktor x+1 enthalten

Alle Bursts mit bis zu m Bitfehlern
G(x) hat den Grad m

Bild: Erkennen von Bitfehlern mit CRC

CRC-16 und CRC-ITU entdecken
- alle Einzel- und Doppelfehler
- alle Fehler ungerader Anzahl
- alle Fehlerbursts mit der Länge $\leq$ 16
- 99,997 % aller Fehlerbursts mit der Länge 17
- 99,998 % aller Fehlerbursts mit der Länge 18 und mehr

Bild: Leistungsfähigkeit von CRC

Realisierung in Hardware
Benutzung von rückgekoppelten Schieberegistern.
CRC kann während des Durchschiebens durch das Schieberegister berechnet werden.

Prinzip
Dateneinheit durchläuft bitweise das Schieberegister.
Rückkopplung erfolgt an den Stellen, an denen das Generatorpolynom auf 1 gesetzt ist.

Beispiel

Schieberegister mit Generatorpolynom $G(x) = x^{16} + x^{12} + x^5 + 1$

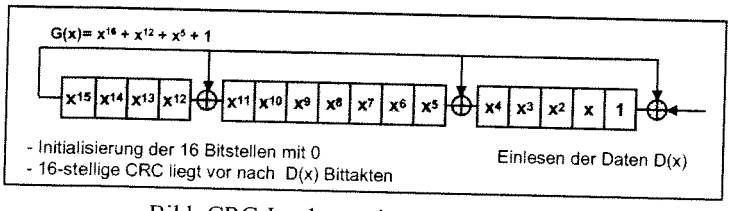


Bild: CRC-Implementierung in Hardware

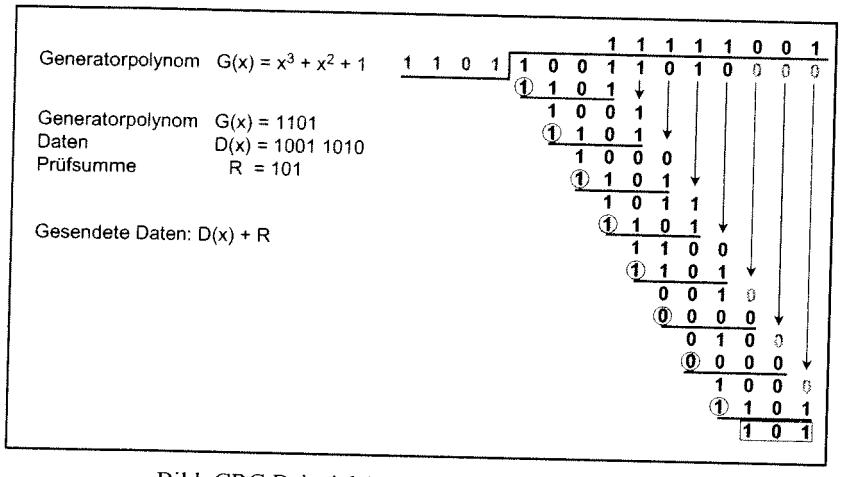


Bild: CRC Beispiel 1: Berechnung der Prüfsumme

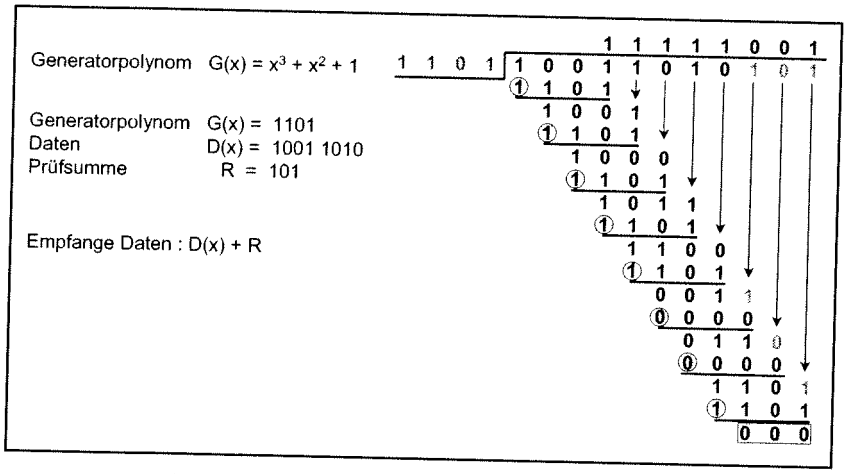


Bild: CRC Beispiel 1: Überprüfung der Prüfsumme

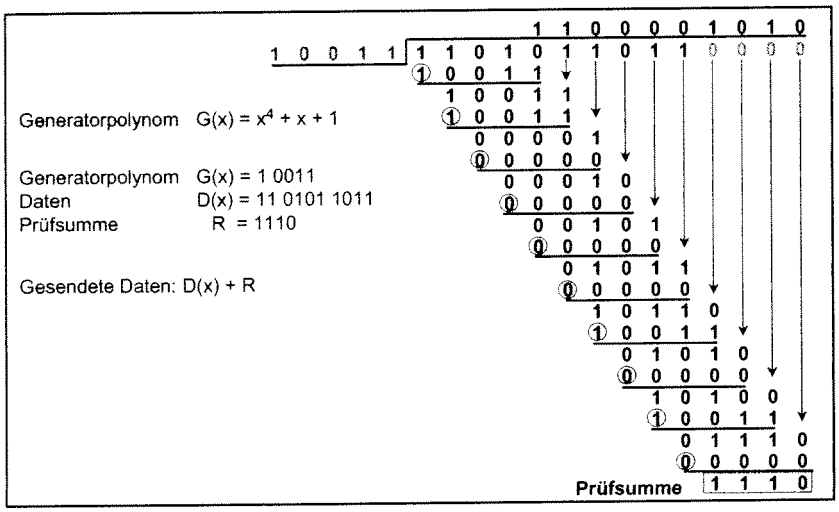


Bild: CRC Beispiel 2: Berechnung der Prüfsumme

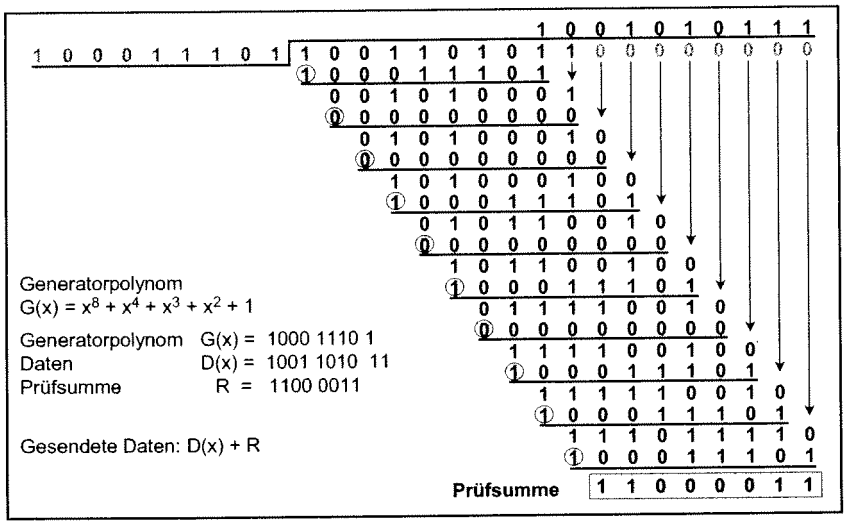


Bild: CRC Beispiel 3: Berechnung der Prüfsumme

Bislang war die Redundanz nur zur Überprüfung der Daten mitgeliefert worden, jetzt soll sie dazu dienen, verloren gegangene Dateneinheiten zu rekonstruieren.

Beispiel:
Zu senden sind die Dateneinheiten
0101 - D1
1111 - D2
0000 - D3

Dazu wird über XOR eine weitere Dateneinheit berechnet:

1010 - D4

Diese vier Dateneinheiten werden jetzt an den Empfänger gesendet.

Bild: Vorwärtsfehlerkorrektur

Codierung zur Fehlerkorrektur

Codeworte der Länge n werden durch Hinzufügen redundanter Information auf die Länge m vergrößert. Der Quotient n/m wird als Coderate bezeichnet. Gebräuchliche Werte sind 1/2, -1/4 und 7/8. Man unterscheidet Block- und Faltungscodes (block code, convolutional code). Bei Blockcodes wird die redundante Information - wie bei der Verwendung von Paritätsbits - aus Blöcken von Nutzinformationen berechnet. Bei Faltungscodes wird die Redundanz fortlaufend aus aufeinander folgenden Bits berechnet.

Der Empfänger muss nur drei der vier Dateneinheiten korrekt empfangen, um die fehlende Dateneinheit rekonstruieren zu können.

Er verknüpft einfach die korrekt empfangenen Dateneinheiten mit XOR und erhält so die fehlende:

D1 geht verloren: 1111
0000
1010
0101 - D1

D2 geht verloren: 0101
0000
1010
1111 - D2

D3 geht verloren: 0101
1111
1010
0000 - D3

Empfänger muss aber wissen, welche Dateneinheit verloren gegangen ist .

Bild: Vorwärtsfehlerkorrektur — Ablauf

Die Fehlerkorrektur ist gekennzeichnet durch einen relativ hohen Verarbeitungsaufwand und eine niedrige Coderate, die zu einer schlechten Kanalausnutzung führt. Deshalb wird sie in der Regel nur dort eingesetzt, wo eine Übertragungswiederholung nicht praktikabel ist.

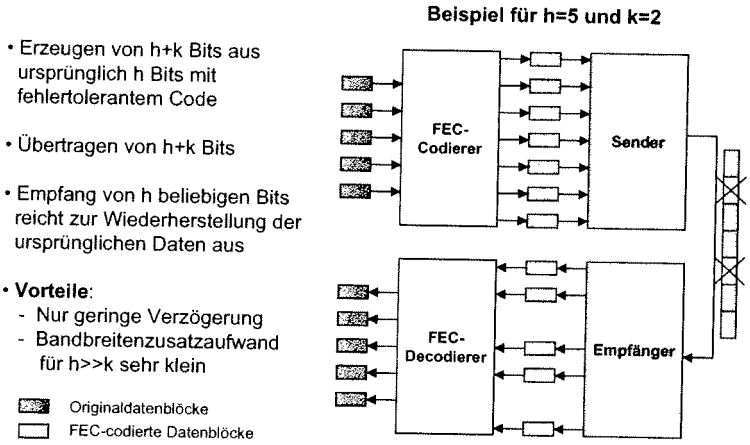


Bild: Vorwartsfehlerkorrektur

Anwendungsbeispiele sind:

- Terrestrische Funksysteme (GSM: Global System for Mobile Communications),
- Stark bandbegrenzte, leitungsgebundene Übertragungssysteme (trellis coded modulation bei Modems),
- Fernseh-Verteilnetze und die Kommunikation über Satelliten,
- Fehlerkorrektur in digitalen Speichern (Arbeitsspeicher und Massenspeicher, z. B. CD-ROM).

Fehlerbehebung, ARQ-Verfahren

ARQ-Verfahren (Automatic Repeat Request) leisten die Behebung erkannter Fehler, indem verfälscht empfangene oder verlorene Pakete vom Sender nochmals gesendet werden.

Die Erkennung von Übertragungsfehlem wird durch fehlererkennende bzw. fehlerkorrigierende Codes geleistet. Zusätzlich treten andere Probleme auf. Die Verzögerung eines Rahmens auf der Übertragungsstrecke kann schwanken und unter Umständen große Werte annehmen. Rahmen können ganz verloren gehen, wenn ein Rahmen so stark verfälscht ist, dass der Empfänger ihn nicht mehr als solchen erkennen kann. Deshalb ist über die Flusssteuerung hinaus ein Mechanismus erforderlich, der sich um die Beseitigung dieser Fehler kümmert.

Da fehlende und fehlerhafte Rahmen nochmals übertragen werden (dies so oft wie nötig, allerdings wird bei Erreichen einer vorher festgelegten Anzahl Wiederholungen die Kommunikation mit einer Fehlermeldung abgebrochen), bezeichnet man diese Mechanismen als ARQ (Automatic Repeat Request). Korrekt empfangene Rahmen werden durch **positive Quittungen** (acknowledgment) quittiert, falsch empfangene Rahmen können durch **negative Quittungen** (reject) nochmals angefordert werden. Nicht empfangene Rahmen stellt der Sender dadurch fest, dass er innerhalb einer festgelegten Zeit (timeout) keine Quittung für einen gesendeten Rahmen erhält. Er führt daraufhin von sich aus eine Wiederholung der Übertragung durch.

Beachte:

- Eine positive Quittung enthält die Sequenznummer des nächsten erwarteten Blocks.
- Eine negative Quittung enthält die Sequenznummer eines fehlerhaften Blocks.

Die Bedeutung (Semantik) von Quittungen kann also positiv oder negativ sein und sich auf einzelne Rahmen oder eine Folge von Rahmen (Summenquittung) beziehen. Quittungen werden ausgelöst durch den Empfang eines Rahmens oder den Ablauf eines Zeitgebers (timeout).

Mit Paritätsbits und Prüfsummen können Bitfehler erkannt werden.

Erkennung

Zur Erkennung von Fehlern bezüglich kompletter Dateneinheiten (Rahmenfehler) sind zusätzliche Mechanismen erforderlich.

- Sequenznummern (Sequence number)
- Zeitgeber (Timer)

Auch wenn alle Dateneinheiten empfangen wurden, können die genannten Mechanismen erforderlich sein.

Behebung

Zur Behebung der Fehler werden die folgenden Mechanismen verwendet
- Quittungen (Acknowledgements)
- Sendewiederholungen (Retransmissions)

Bild: Fehlerkontrolle bei Rahmenfehlern

Problemstellung
- Woher weiß der Empfänger, ob die Dateneinheiten in der richtigen Reihenfolge ankommen?
- keine Duplikate enthalten sind?
- keine Dateneinheiten fehlen?

Mechanismus
- Die Dateneinheiten (oder die Bytes) werden durchnummeriert.
- Eine entsprechende Kennung wird mit jeder Dateneinheit übertragen.
- Diese Kennung wird als *Sequenznummer* bezeichnet.

Fehlerszenarien
Sequenznummern helfen, wenn Dateneinheiten nicht ausgeliefert werden.

Bild: Sequenznummern

Problemstellung
Wann entscheidet ein Empfänger, dass eine Dateneinheit nicht angekommen ist?

Mechanismus
In Abhängigkeit einer zeitlichen Obergrenze wird *vermutet*, dass eine Dateneinheit nicht mehr beim Empfänger eintrifft.

Der Empfänger startet einen Zeitgeber jeweils dann, wenn er eine korrekte Dateneinheit empfangen hat. Wird die nächste nicht innerhalb dieses so Vorgegebenen Zeitintervalls empfangen, so wird vermutet, dass sie im Netz verloren ging.

Bild: Zeitgeber

Problemstellung
Wie erfährt der Sender, dass eine Dateneinheit überhaupt nicht bzw. nicht korrekt beim Empfänger angekommen ist?

Mechanismus
- Der Empfänger teilt dem Sender mit, ob er eine Dateneinheit empfangen hat oder nicht.
- Hierzu werden spezielle Dateneinheiten, sogenannte Quittungen, versendet (ACK: Acknowledgement).

Varianten
Positive Quittung
Empfänger teilt dem Sender mit, dass er die entsprechenden Daten erhalten hat.

Negative Quittung
- Empfänger meldet dem Sender, dass er die entsprechenden Daten nicht erhalten hat (z.B. bei falscher Reihenfolge).

NACK: Negative Acknowledgement

Quittungen werden oftmals in Kombination mit Zeitgebern verwendet.

Bild: Quittungen

Weitere Varianten

Selektive Quittungen
Die Quittung bezieht sich auf eine einzelne Dateneinheit.

Beispiel
– Negative selektive Quittung, falls der Verlust einer Dateneinheit vom Empfänger vermutet wird (NACK).
– Lässt sich mit NACKs ein zuverlässiger Dienst bereitstellen?
SACK: Selective Acknowledgement

Kumulative Quittungen
Die Quittung bezieht sich auf eine Menge von Dateneinheiten, die in der Regel durch eine obere Sequenznummer beschränkt ist.

Beispiel
– Positive kumulative Quittung, die besagt, dass alle Dateneinheiten bis zur angegebenen Sequenznummer korrekt empfangen wurden.

Bild: Quittungen

Grundlegende Variante zur Sendewiederholung
- Sender erhält positive Quittungen über den Erhalt einer Dateneinheit.
- Sender kann Sendewiederholungen ausführen.

Varianten
- Wann werden Quittungen versendet?
- Wann werden Sendewiederholungen veranlasst?

Situation
Eine Reihe verschiedener ARQ-Mechnismen ist verfügbar, wobei zwischen grundlegenden Unterschieden und Implementierungsfeinheiten differenziert werden muss. Im folgenden werden grundlegende Varianten diskutiert.

Bild: Automatic Repeat Request: ARQ

Grundlegendes einfaches ARQ-Verfahren
Sender wartet auf die Quittung zu einer gesendeten Dateneinheit, bevor er eine neue Dateneinheit senden darf.

- Falls keine Quittung empfangen wird, erfolgt die Wiederholung der Dateneinheit nach dem Ablauf des Zeitgebers.
- Es können Duplikate von Dateneinheiten entstehen.

Sequenznummern
- Wie viele Bits werden bei Stop-and-Wait für die Sequenznummer benötigt?
- Annahme: Sequenznummern identifizieren Dateneinheiten.

Nachteil
Stets nur eine nicht quittierte Dateneinheit beim Sender

Bild: Einfachstes ARQ-Verfahren: Send-and-Wait

Die Flusskontrolle (flow control, auch Flusskontrolle) hat die Aufgabe zu verhindern, dass ein schneller Sender einen langsamen Empfänger mit Daten überschwemmt.

Der Empfänger besitzt einen Pufferspeicher, der eine bestimmte Anzahl empfangener Rahmen zwischenspeichern kann, bevor der Protokollstapel diese übernimmt. Große Pufferspeicher sind vorteilhaft, aber teuer. Folglich benötigt der Empfänger einen Mechanismus, mit dem er den Sender veranlassen kann, eine bestimmte Zeit zu warten. Hierzu sendet der empfangsbereite Empfänger dem Sender eine Quittung, die ihm erlaubt, bis zu n Blöcke zu senden.

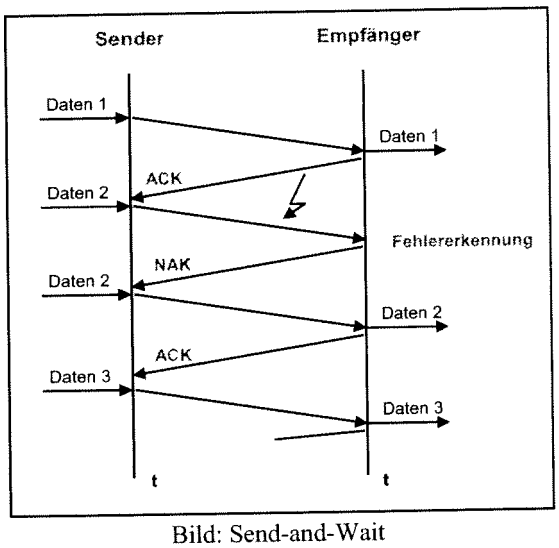


Bild: Send-and-Wait

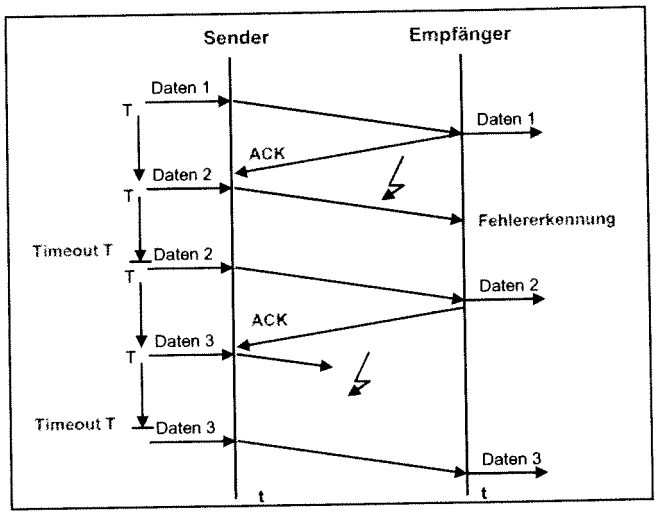


Bild: Send-and-Wait

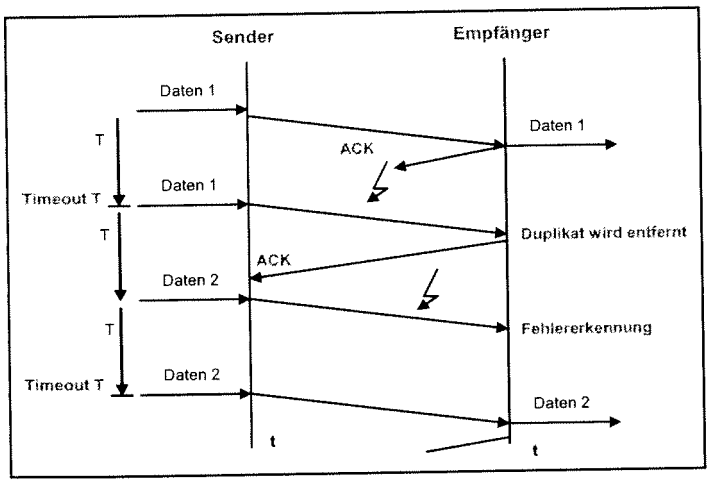


Bild: Send-and-Wait

Stop-and-Wait
Bei diesem Verfahren sendet der Sender genau einen Rahmen. Danach wartet er auf eine Quittung (Empfangsbestätigung) des Empfängers, nach deren Erhalt er einen weiteren Rahmen sendet. Abläufe dieser Art werden in Zeitdiagrammen dargestellt In diesem sehr einfachen Fall ist angenommen, dass alle Rahmen in der Reihenfolge des Absendens unverfälscht beim Empfänger eintreffen. Vorteil des Stop-and-Wait-Verfahrens ist der geringe Aufwand für das Protokoll. Nachteil ist ein geringer Durchsatz, insbesondere auf Übertragungsstrecken mit langer Laufzeit, auf denen kurze Rahmen übertragen werden. Grund dafür ist, dass die Übertragungsstrecke nur während kurzer Zeit mit einer Übertragung beschäftigt ist und dann relativ lange auf eine Quittung (ACK: Acknowledgment) wartet.

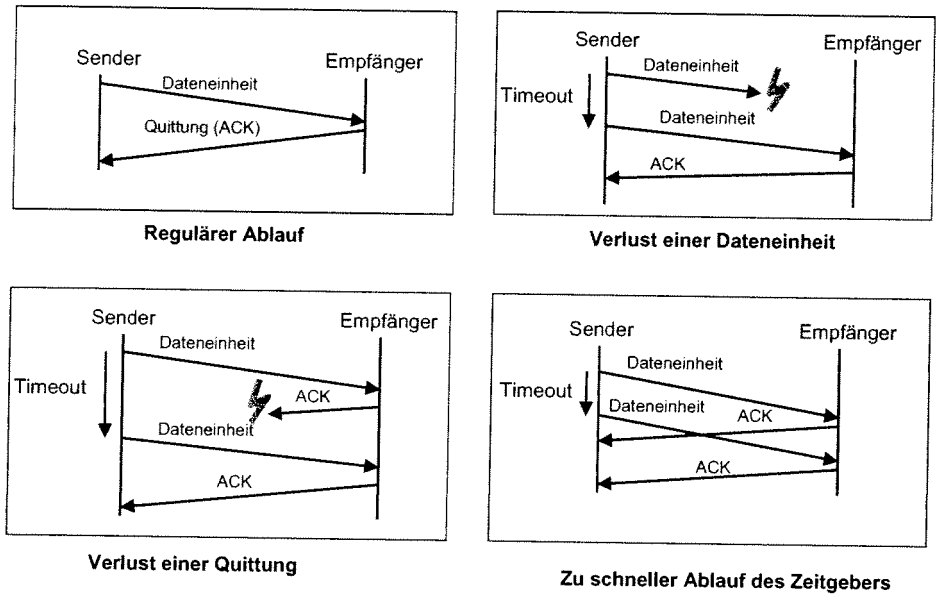


Bild: Send-and-Wait : Szenarien

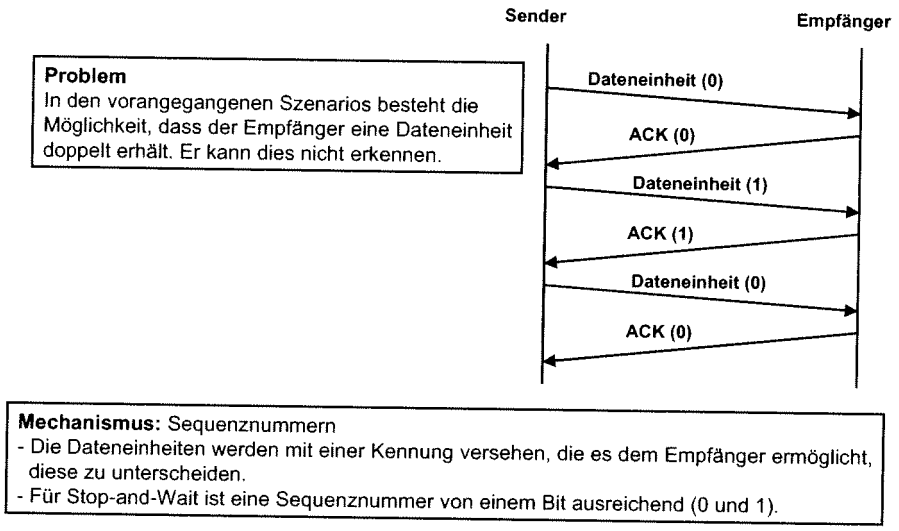


Bild: Send-and-Wait : Sequenznummern

Fenstermechanismus (Sliding Window)

Eine höhere Auslastung der Übertragungsstrecke lässt sich erreichen, wenn mehrere Rahmen nacheinander gesendet werden, bevor eine Quittung erwartet wird. Dies wird als **(Schiebe-)Fensterverfahren** (sliding window) bezeichnet. Dabei darf der Sender eine Anzahl w (Fenstergröße) Rahmen senden, ohne eine Quittung zu erhalten. Wenn diese Anzahl ausgeschöpft ist, muss der Sender warten, bis eine Quittung eintrifft. Die maximale Fenstergröße ist ein vordefinierter Parameter. Die Rahmen haben zur eindeutigen Kennzeichnung Sequenznummern. Rahmen links des Sendefensters wurden bereits gesendet, Rahmen im Sendefenster dürfen noch ohne Quittungseingang gesendet werden.

Beim Senden eines Rahmens verschiebt sich die linke Fenstergrenze um einen Block nach rechts, das Fenster schrumpft. Bei Erhalt einer Quittung verschiebt sich die rechte Fenstergrenze um einen Rahmen nach rechts, das Fenster dehnt sich (aber nur bis maximale Fenstergröße). Bei w = 0 darf nichts weiter gesendet werden.

Für die Nummerierung der Rahmen sollen k Bit (k möglichst klein) verwendet werden, d. h., die Rahmennummern sind modulo k dargestellt. Damit lässt sich eine maximale Fenstergröße von 2^{k-1} darstellen. Nach Erreichen der größten Rahmennummer folgt die 0 als nächste Nummer (wrap around). Bei kleinen k kann dies zu Problemen führen, indem die Sequenznummer unter Umständen nicht mehr eindeutig einen Rahmen benennt.

Ziel

Erhöhung des Durchsatzes im Vergleich zu Stop-and-Wait. Das Warten auf eine Quittung vor dem Senden der nächsten Dateneinheit soll vermieden werden.

Verfahren

Der Sender kann mehrere Dateneinheiten senden bis er eine Quittung erhalten muss. Die maximale Anzahl der nicht quittierten Dateneinheiten ist begrenzt (typischerweise durch ein sogenanntes Sliding Window).

Variante 1
- Empfänger quittiert korrekt empfangene Dateneinheiten wie bei Stop-and-Wait.
- Die Quittung kann allerdings kumulativ erfolgen, d.h. für mehrere Dateneinheiten auf einmal kumulative Sequenznummer gibt an, bis wohin die Daten korrekt empfangen wurden, d.h. es handelt sich um positive Quittungen.
- Alle noch nicht quittierten aber gesendeten Daten werden vom Sender wiederholt (Go-Back-N, wobei N die kumulative Sequenznummer ist)

Variante 2
- Nicht korrekt empfangene Dateneinheiten werden mit einer negativen Quittung (NACK) bestätigt
- Sender wiederholt daraufhin ab dieser Sequenznummer alle gesendeten Dateneinheiten (Go-Back N, wobei N die Sequenznummer in der negativen Quittung ist).

Bild: Go-Back-N ARQ

Ziel

Erhöhung der Datenrate im Vergleich zu Stop-and-Wait. Reduzierung des Datenaufkommens im Vergleich zu Go-Back-N.

Verfahren
- Der Sender kann mehrere Dateneinheiten senden, bis er eine Quittung erhalten muss.
- Die maximale Anzahl der nicht quittierten Dateneinheiten ist begrenzt. (wie bei Go-Back-N)
- Der Empfänger sendet eine negative Quittung, wenn er einen Fehler erkennt.
- Diese Quittung bezieht sich auf eine einzelne Dateneinheit.
- Empfänger wiederholt genau die Dateneinheit mit der bei der negativen Quittung angegebenen Sequenznummer.
- Nur die nicht korrekt empfangenen Dateneinheiten werden vom Senderwiederholt.

Bild: Selective Reject ARQ

Einfachste Methode
Sender-Empfänger-Flusskontrolle

Meldungen
– Halt
– Weiter

Kann der Empfänger nicht mehr Schritt halten, schickt er dem Sender eine Halt-Meldung.

Ist ein Empfang wieder möglich, gibt der Empfänger die Weiter-Meldung.

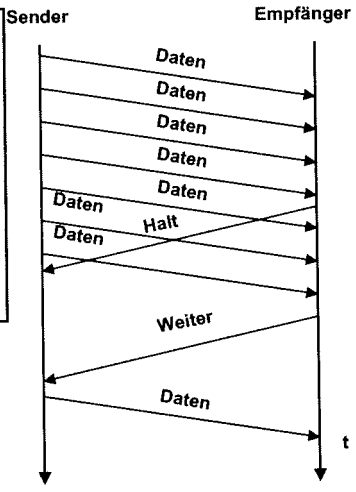


Bild: Flusskontrolle mit Halt-/Weiter-Meldungen

Funktionsweise
Durch Zurückhalten der Quittung (z.B. ACK/NACK) kann der Sender gebremst werden.

Das bedeutet, dass ein Verfahren zur Fehlererkennung für die Flusskontrolle mitbenutzt wird.

Problem
Der Sender kann nicht mehr unterscheiden, ob seine Dateneinheit völlig verloren ging ob der Empfänger die Quittung wegen Überlast zurückgehalten hat.

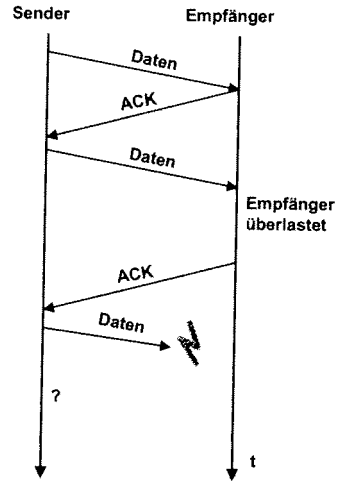


Bild: Implizite Flusskontrolle

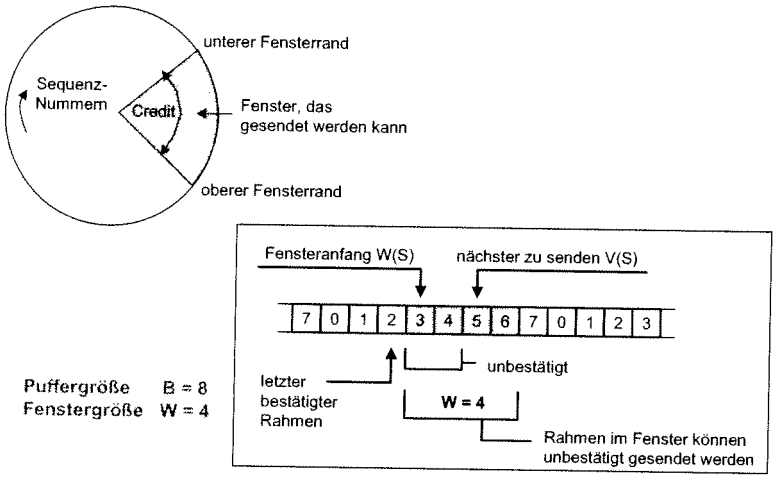


Bild: Fenstermechanismus

Sender

SWS: Send Window Size
(max. Anzahl ausstehender Dateneinheiten)

LAR: Last ACK Received
(Sequenznummer der letzten quittierten Dateneinheit)

LFS: Last Frame Sent
(Sequenznummer der letzten gesendeten Dateneinheit)

SWS = LFS - LAR + 1

Empfänger

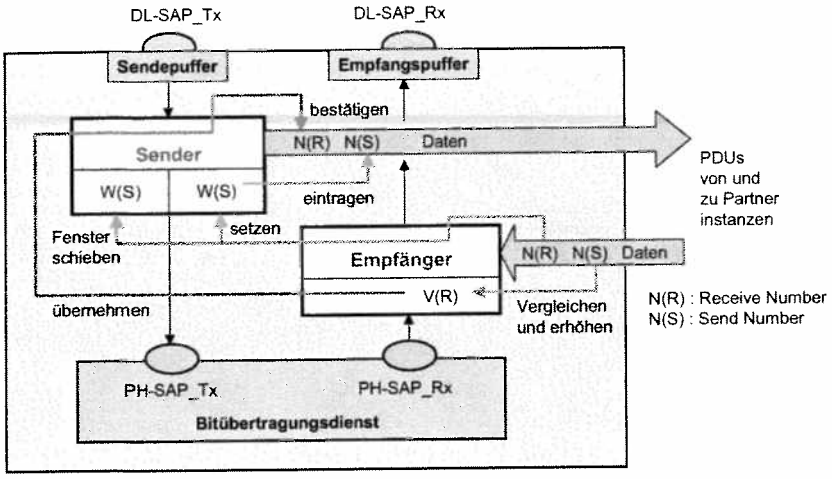
RWS: Receiver Window Size
(max. Anzahl nicht in Reihenfolge empfangener Dateneinheiten)

LFA: Last Frame Accepted
(Sequenznummer der letzten empfangbaren Dateneinheit)

NFE: Next Frame Expected
(Sequenznummer der nächste in Reihenfolge erwartete Dateneinheit)

RWS = LFA - NFE + 1

Bild: Flusskontrolle mit Sliding Window



W(S) = Window (Sender)
W(R) = Window (Receiver)
N(S) = Sequence number (Sender)
N(R) = Sequence number (Receiver)

Bild: Automaten der Sicherungsinstanz

2.2a OSI-Referenzmodell: Schicht 2a – Mediumzugriff

Version: Dez. 2003

- Aufgaben und Funktionen
- ALOHA, S-ALOHA, CSMA, CSMA/CD
- CSMA/CA im lokalen Funknetz IEEE 802.11
- Token Ring, Token Bus
- FDDI (Fiber Distributed Data Interface)
- Reservierungsverfahren, Schedulingverfahren, Kreditverfahren
- Slotted Ring, Buffer-Insertion Ring
- CSMA/CA beim ISDN-Mehrfachanschluss

S-ALOHA = Slotted ALOHA
CSMA = Carrier Sense Multiple Access
CSMA/CD = CSMA with Collision Detection
CSMA/CA = CSMA with Collision Avoidance

S-ALOHA = Slotted ALOHA
CSMA = Carrier Sense Multiple Access
CSMA/CD = CSMA with Collision Detection
CSMA/CA = CSMA with Collision Avoidance

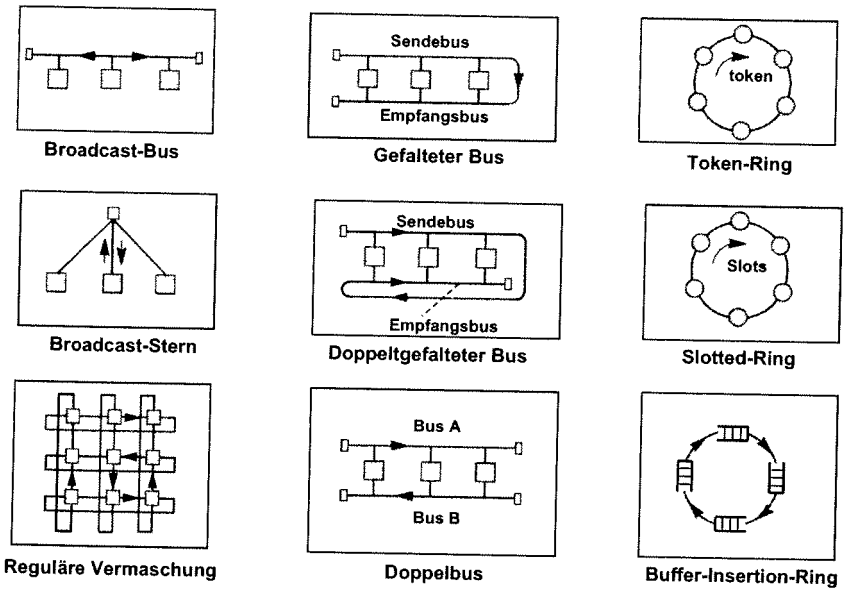


Bild: Topologien in lokalen Netzen

Bei einem **Broacastnetz** wird das Signal eines Senders von allen angeschlossenen Empfängern unmittelbar (jedoch um die Signallaufzeit verzögert) empfangen. Jeder Empfänger muss selbst feststellen, ob er das Signal aufnimmt oder nicht.

Bei einem **Teilstreckennetz** läuft das Signal des Senders über (genau) eine Teilstrecke, an deren Ende ein Empfänger das Signal aufnimmt und (falls erforderlich) auf einer anderen Teilstrecke wieder aussendet.

Beispiele dazu sind:

- **Bussysteme:** gefalteter Bus, doppelt-gefalteter Bus, Dualbus.
- **Ringnetze:** Token Ring, Slotted Ring, Buffer-Insertion Ring.
- **Vermaschte Netze:** Reguläre und irreguläre Vermaschung.

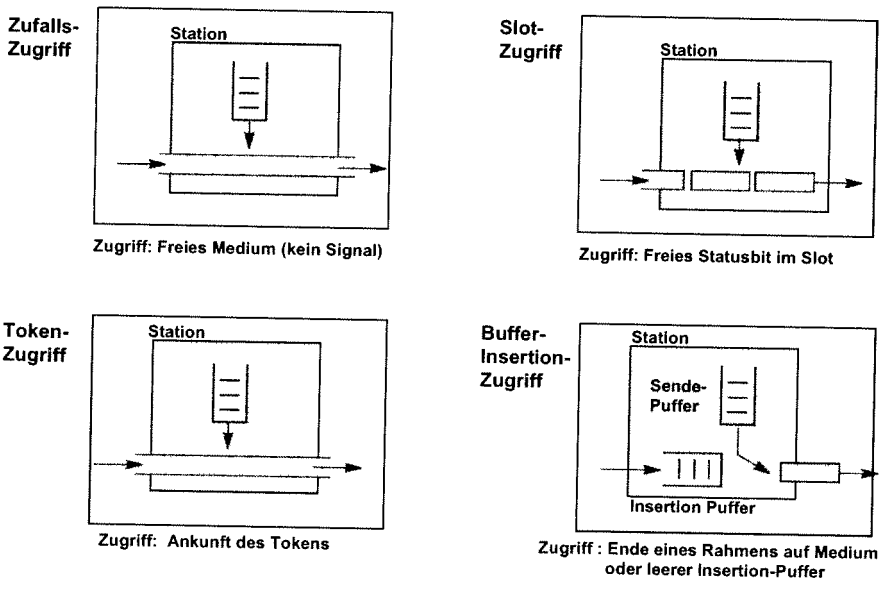


Bild: Basiszugriffsmechanismen auf ein gemeinsames Medium

Medienzugriffsprotokolle

Zur Abwicklung eines geordneten Zugriffs auf ein gemeinsames Übertragungsmedium sind Medienzugriffsprotokolle notwendig. Man spricht von einem MAC-Protokoll (Medium Access Control).

Wichtige Zugriffsverfahren sind:

- Zufälliger Zugriff (Aloha, Slotted Aloha, Ethernet),
- Token Zugriff (Token Ring, Token Bus, FDDI),
- Slotted Zugriff (ATM-Ring),
- Insertion-Buffer-Zugriff (Insertion Ring, IEEE 802.17 RPR, Resilient Packet Ring).

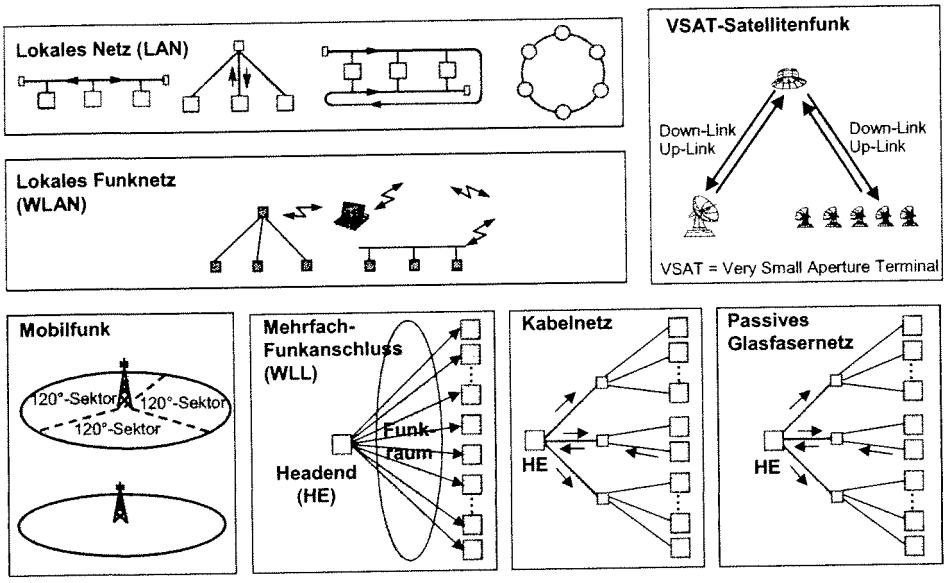


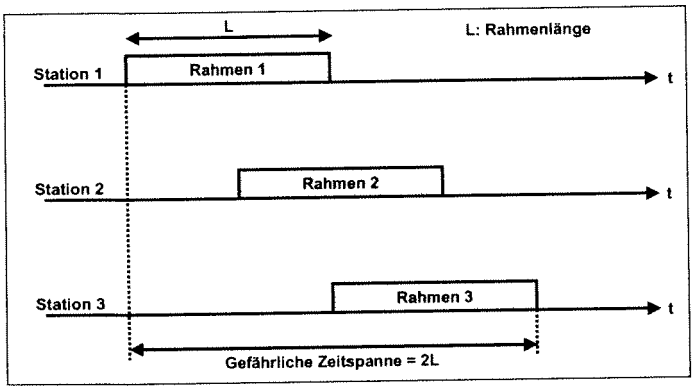
Bild: Bereiche mit einem gemeinsamen Medium

Gemeinsame Medien findet man

- in lokalen Netzen (LAN, Local Area Network),
- in lokalen Funknetzen (WLAN, Wireless Local Area Networks),
- in Mobilfunknetzen (gemeinsame Funkschnittstelle),
- in Satellitennetzen,
- bei einem Mehrfachfunkanschluss (Multipoint WLL, Multipoint Wireless Local Loop,
- in Kabelnetzen (CATV, Cable TV Networks),
- in passiven Glasfasernetzen (PON, Passive Optical Network).

Ausgehend von Ethernet und Token Ring als den bekanntesten Vertretern der ersten LAN-Generation hat sich eine Vielzahl von Medienzugriffsprotokollen entwickelt. Demnach finden in nahezu allen Protokollen Modifikationen oder Kombinationen folgende Basismechanismen Verwendung:

- zufälligen Zugriff (Aloha, Slotted Aloha, Ethernet, WLAN),
- Tokenverfahren (Token Ring, Token Bus, FDDI),
- Reservierungsverfahren,
- Schedulingverfahren,
- Creditverfahren (ATMR für Slotted Ring oder Buffer-Insertion Ring).



Max. Durchsatz 18%
Kollision: alle 3 Rahmen

Bild: ALOHA

Reines ALOHA

Das grundlegende Konzept eines ALOHA-Systems ist einfach: Benutzer können jederzeit übertragen, wenn sie Daten senden müssen. Es treten dadurch Kollisionen auf, und die kollidierenden Rahmen werden zerstört. Aber durch die Bestätigungsmöglichkeit der Broadcast-Technik kann ein Absender immer herausfinden, ob sein Rahmen zerstört wurde, indem er die Meldungen des Mediums abhört. Bei einem LAN folgt diese Bestätigung unmittelbar. Bei Satelliten ergibt sich eine Verzögerung von 270 ms, bis der Absender weiß, ob die Übertragung erfolgreich war. Falls der Rahmen zerstört wurde, wartet der Absender eine zufällig gewählte Zeitspanne und sendet dann nochmals.

Die Wartezeit muss zufällig sein, sonst kollidieren die gleichen Rahmen immer wieder. Systeme, in denen Benutzer eines gemeinsamen Medium so benutzen, dass es zu Problemen kommen kann, sind allgemein als Konkurrenzsysteme (Contention Systems) bekannt. Jedes Mal, wenn zwei Rahmen zur gleichen Zeit versuchen, das Übertragungsmedium zu besetzen, entsteht eine Kollision, und beide werden verstümmelt. Falls auch nur das erste Bit eines neuen Rahmens das letzte Bit eines fast beendeten Rahmens überschneidet, werden beide Rahmen völlig zerstört, und beide müssen später erneut übertragen werden. Die gefährliche Zeitspanne beträgt zweimal die mittlere Rahmenlänge L. Unter der Annahme, dass der Datenverkehr homogen ist, erhält man einen Durchsatz von 18%. Der Rest der Übertragungskapazität geht durch Kollisionen und Wiederholungen verloren.

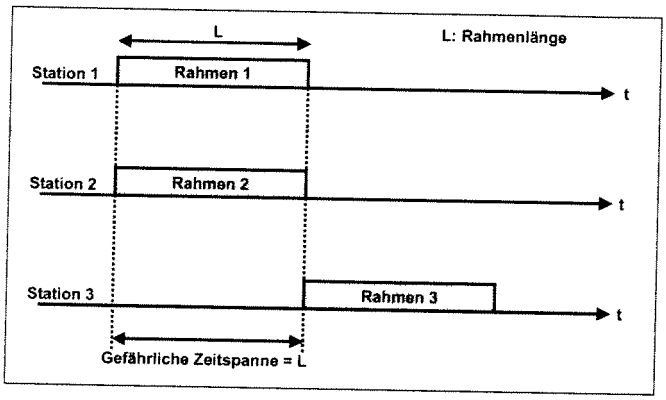


Bild: Slotted-ALOHA

Bei Slotted-ALOHA (S-ALOHA) wird die Zeit in einzelne Intervalle eingeteilt, wobei jedes Intervall einem Rahmen entspricht. Im Gegensatz zu reinem ALOHA darf eine Station nicht sofort senden, sobald ein Rahmen vorliegt. Statt dessen muss auf den nächsten Slot gewartet werden. So wird das stetige reine ALOHA in eine getakte Variante abgewandelt. Da die gefährliche Zeitspanne um die Hälfte gekürzt wurde, ist die Kollisionswahrscheinlichkeit auch um die Hälfte kleiner. Es finden keine Teilüberlappungen der Rahmen statt.
Der Durchsatz steigt auf 36%.

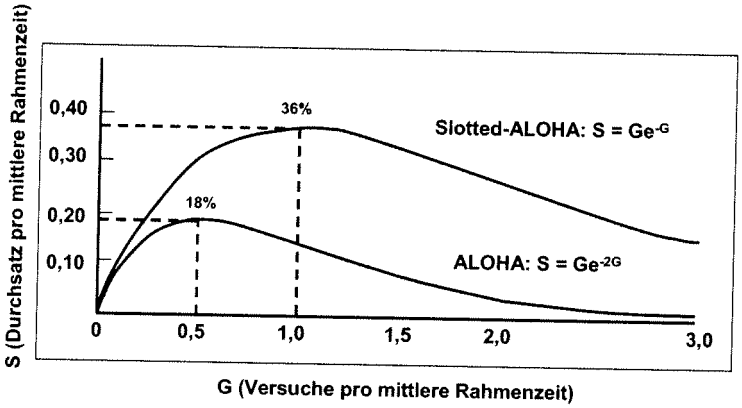


Bild: Durchsatz bei ALOHA und S-ALOHA

Beim zufälligen Zugriff mit den Protokollen ALOHA und Slotted-ALOHA senden die Stationen ihre Rahmen unkoordiniert weg. Bei diesem unkontrollierten Medienzugriff können mehrere Stationen gleichzeitig senden. Die Übertragungssignale der Rahmen werden sich dann überlagern und die Rahmen werden dadurch zerstört. Es finden Kollisionen statt. Deshalb müssen das MAC-Protokoll oder Instanzen auf höheren Protokollschichten Mechanismen zur Erkennung und Behebung möglicher Datenverluste beinhalten.

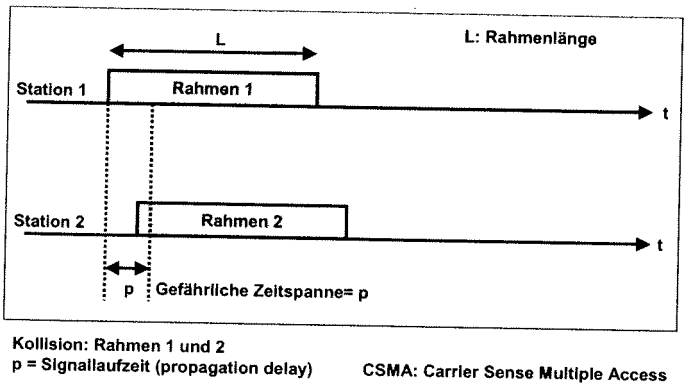


Bild: Zufällig mit Rahmen-Kollision: CSMA

CSMA (Carrier Sense Multiple Access)

Zuerst wird das Zugriffsprotokoll **1-Persistent CSMA** betrachtet. Wenn eine Station Daten zu übertragen hat, hört sie erst das Medium ab, ob bereits eine Station übermittelt. Ist das Medium besetzt, wartet sie, bis das Übertragungsmedium frei wird. Wenn die Station ein freies Medium vorfindet, wird ein Rahmen übertragen. Falls eine Kollision auftritt, wartet die Station eine zufällige Zeitspanne und beginnt von vorn. Dieses Protokoll heißt 1-Persistent, weil die Station bei einem freien Medium mit einer Wahrscheinlichkeit von eins sendet.

Die Ausbreitungsverzögerung hat einen großen Einfluss auf die Leistungsfähigkeit des Protokolls. Durch die Signalausbreitungsverzögerung ist es unvermeidlich, dass kurz nachdem eine Station zu senden begonnen hat, eine andere Station auch senden will und das Übertragungsmedium überprüft. Wenn das Signal der ersten Station die zweite noch nicht erreicht hat, findet die zweite ein freies Medium vor und beginnt auch zu senden, was zu einer Kollision führt. Je größer die Ausbreitungsverzögerung ist, desto wichtiger wird dieser Effekt und desto geringer wird die Leistungsfähigkeit des Protokolls.

Eine zweite Variante ist **non-Persistent CSMA**. Bei diesem Zugriffsprotokoll wird der Zugriff bewusst verzögert, falls das Medium frei ist. Vor dem Senden überprüft eine Station das Medium. Falls keine Station sendet, fängt die Station selbst an. Ist allerdings das Medium bereits belegt, überprüft die Station das Medium nicht andauernd, um sofort auf das Medium zuzugreifen, sobald das Ende der vorherigen Übertragung erkannt wird. Statt dessen wird eine zufällige Zeitspanne gewartet und dann der Vorgang wiederholt. Dieser Algorithmus führt zu einer besseren Auslastung des Mediums, aber auch zu längeren Wartezeiten als beim 1-Persistent CSMA.

Eine weitere Variante ist **p-Persistent CSMA**. Es wird ein getakteten Mediumzugriff vorausgesetzt und arbeitet folgendermaßen: Wenn eine Station senden will, überprüft sie das Medium. Ist es frei, sendet die Station mit einer Wahrscheinlichkeit p. Mit einer Wahrscheinlichkeit von q = 1 – p wartet sie bis zum nächsten Zeitschlitz. Ist dieser Slot auch frei, wird entweder gesendet oder gewartet, wiederum mir den Wahrscheinlichkeiten p und q. Dieser Vorgang wird wiederholt, bis entweder der Rahmen übertragen worden ist oder eine andere Station zu senden begonnen hat. Im letzteren Fall wird reagiert, als ob eine Kollision stattgefunden hat (d.h. eine zufällige Zeitspanne warten und dann alles von vorn beginnen). Wenn die Station das Medium von vornherein belegt vorfindet, wartet sie auf den nächsten Slot und beginnt die obige Prozedur.

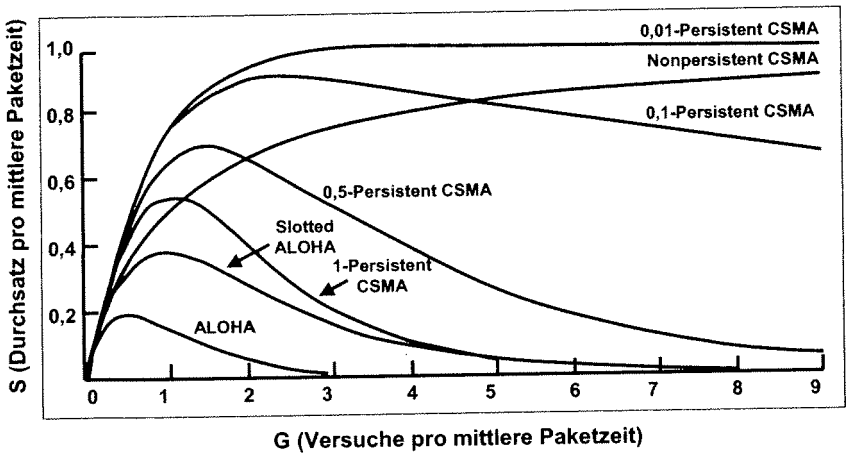
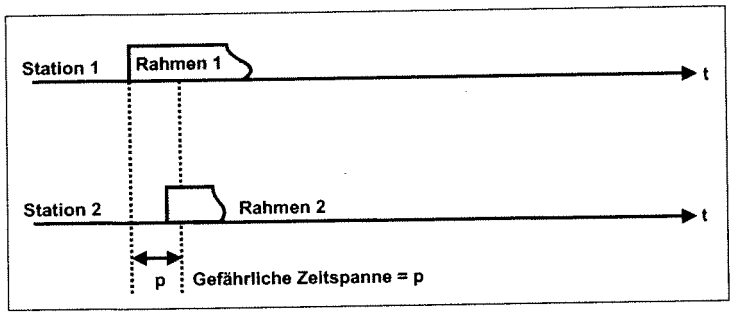


Bild: Zufallsgesteuerte Protokolle: Durchsatz

Das Bild zeigt den Durchsatz gegenüber dem Verkehrsangebot für alle drei Protokolle sowie das reine und getaktetes ALOHA.



Kollision: Rahmen 1 und 2 mit sofortigem Abbruch
p = Signallaufzeit (propagation delay)

Bild: Zufällig mit Kollisionserkennung: CSMA/CD

CSMA/CD: CSMA with Collision Detection
Die CSMA-Protokolle sind zweifellos gegenüber ALOHA eine Verbesserung, da sie sicherstellen, dass keine Station sendet, wenn sie das Medium als belegt erkennt. Eine weitere Verbesserung ist der Abbruch einer Übertragung, wenn eine Kollision erkannt wird. Dies bedeutet, wenn zwei Stationen das Medium als frei erkennen und beide gleichzeitig zu senden beginnen, werden beide fast sofort eine Kollision erkennen. Die Übertragung wird in CSMA/CD sofort abgebrochen, sobald eine Kollision erkannt wird.

Dieses Protokoll heisst CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Dieses Zugriffsprotokoll benutzt genau wie viele andere LAN-Protokolle das folgende Konzept. Zu einem bestimmten Zeitpunkt hat eine Station die Übertragung ihres Rahmens beendet. Jede andere Station, die einen Rahmen zu senden hat, kann das jetzt versuchen. Wenn sich zwei oder mehr Stationen gleichzeitig zum Senden entschließen, kommt es zu einer Kollision. Kollisionen können erkannt werden, indem die Leistung oder Impulsbreite des empfangenen Signals mit dem übertragenen Signal verglichen wird. Jede Station erkennt die Kollision, unterbricht ihre Übertragung, wartet eine zufällige Zeitspanne und versucht es dann erneut, unter der Annahme, dass inzwischen keine andere Station zu übertragen begonnen hat. Deshalb besteht das CSMA/CD-Modell aus abwechselnden Konkurrenz- und Übertragungsperioden, wobei Leerlauf entsteht, sobald keine Station sendet.

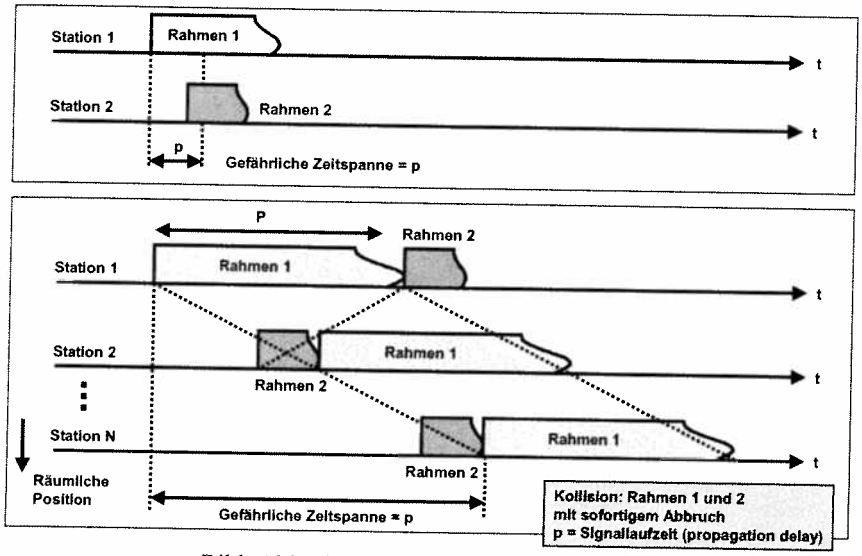


Bild: Ablauf einer Kollision bei CSMA/CD

Die sofortige Beendigung der Übertragung bei beschädigten Rahmen spart Zeit und Übertragungskapazität.

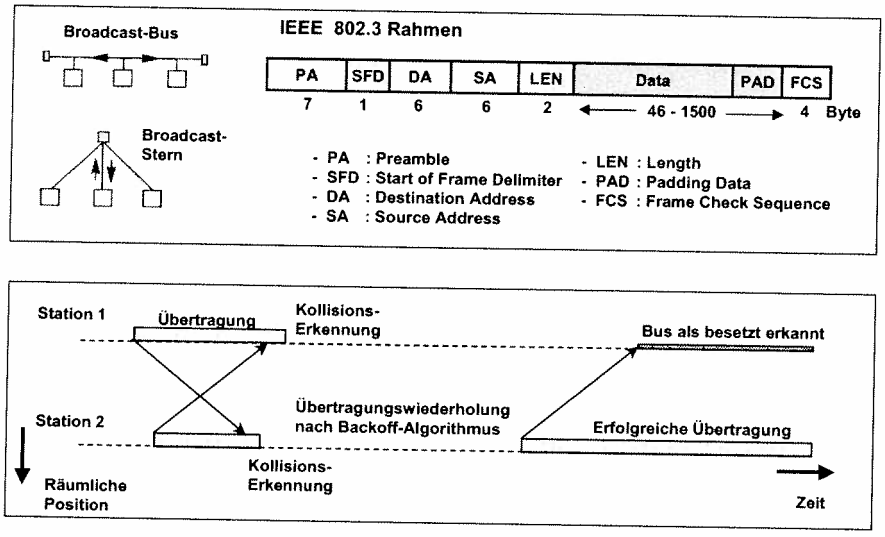


Bild: IEEE 802.3 Standard CSMA/CD

Mediumzugriffsverfahren CSMA/CD

Das Prinzip setzt viele beteiligte Sender voraus (Multiple Access), die vor dem Senden das Medium abzuhören (Carrier Sense) und auch während der Datenübertragung das Medium überprüfen (Collision Detection). Entdeckt eine Station eine Kollision bzw. einen Fehler, so sendet sie ein sogenanntes Jamming-Signal (JAM), das sich in seiner Bitkombination deutlich von allen anderen unterscheidet und den Fehler dadurch noch verstärkt.

Wenn die gleichzeitig sendenden Stationen abgebrochen haben, müssen alle einen Moment warten, damit sich das Medium beruhigt (Interframe Gap). Dann wählt jede sendebereite Station mit Hilfe des Backoff-Algorithmus eine zufällige Zeitspanne, nach der sie ihren Sendevorgang wiederholt. Die Station mit der kürzesten Verzögerung beginnt die Übertragung erneut. Die restlichen Stationen hören diese Station und warten ihren Sendeversuch ab. Sollten zufällig zwei Stationen gleichzeitig begonnen haben, so tritt erneut eine Kollision auf und das beschriebene Verfahren beginnt von Neuem.

Die notwendigen Informationen des CSMA/CD-Zugriffsverfahrens befinden sich in dem MAC-Rahmen. Im IEEE 802.3 standardisierten CSMA/CD besteht der Rahmen aus den folgenden Feldern:

PA	Präambel	Hierbei handelt es sich um eine Folge von 0 und 1 über 7 Byte. Sie dient zur Bitsynchronisation.
SFD	Start Rahmen Delimiter	Das SFD-Feld kennzeichnet den Rahmenbeginn und hat das Format 10101011.
DA	Destination Address	Zieladresse
SA	Source Address	Quelladresse
LEN	Length	Dieses 2-Byte große Feld enthält die Länge des Rahmens.
Daten		Hier stehen die Daten, die innerhalb der LLC-Schicht erzeugt und an die MAC-Schicht übergeben wurden.
PAD	Padding	PAD ist ein Füllfeld. Wenn die Rahmenlänge kleiner als für einen CSMA/CD-Betrieb notwendig ist, wird der Rahmen mit einer entsprechenden Anzahl Bytes bis zum Erreichen der Rahmenmindestgröße (512 Bit) aufgefüllt.
FCS	Rahmen Check Sequence	Das 4-Byte große Rahmenprüffeld beinhaltet eine Rahmen-Prüfsequenz, die mittels zyklischem Codierungsverfahren gebildet werden. Abgesichert werden Adressen, Länge, LLC-Daten und die Füllzeichen. Ein Rahmen wird als fehlerhaft erkannt, wenn die Rahmenlänge nicht mit der im Length-Field angegebenen Länge übereinstimmt, die Rahmenlänge nicht ein Vielfaches von 8 Bit ist oder die FCS-Prüfung negativ verläuft.

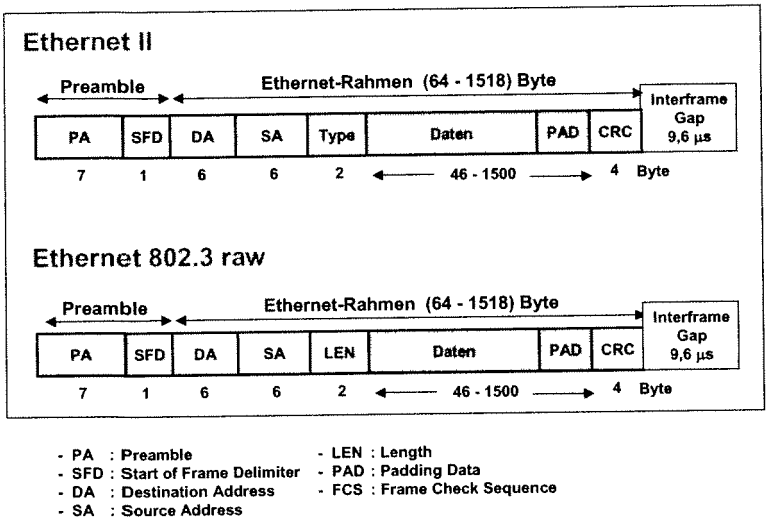


Bild: Rahmenformate in Ethernet

Neben dem IEEE 802.3-Standard existiert auch die Vorgängerversion Ethernet (V.2). Im Ethernet wird ein anderer MAC-Rahmen spezifiziert. Es ist bei Ethernet keine Längenangabe vorgesehen, ferner ist keine Unterstützung bzw. eine Schnittstelle zur LLC-Schicht festgelegt. Dafür bietet Ethernet ein Typ-Feld, das Umsetzungsmechanismus (SNAP) in die LLC-Struktur erforderlich macht.

- Die MAC-Subschicht regelt den Medienzugriff und die vom Zugriffsverfahren abhängige Block- oder Rahmenbildung
- Datenendgerät (Data Terminal Equipment, DTE) ist jedes an einem lokalen Netz angeschlossene Station oder Netzkomponente, die mit einer MAC-Funktion ausgestattet ist.
- Die für das Absenden eines Rahmens minimaler Länge benötigte Zeit wird als Slot Time bezeichnet.

$$Slot\ Time = \frac{Minimale\ Rahmenlänge}{Übertragungsrate}$$

Übertragunsrate	Minimale Rahmenlänge	Slot Time
10 Mbit/s	512 bit	51.2 µs
100 Mbit/s	512 bit	5.12 µs
1 Gbit/s	4096 bit	4.096 µs

Bild: Zugriffsprotokoll und Slotgröße in CSMA/CD

Der IEEE 802.3-Standard sieht eine minimale Rahmenlänge von 512 Bits vor, daraus resultiert die im Standard festgeschriebene maximale Signallaufzeit (Slot-Time) von 51,2 µs. Die Signallaufzeit - auch Kollisionsfenster genannt - gibt die Zeit an, die maximal vergehen darf, bis ein Datenrahmen von einer Station an einem Ende des LANs zu einer Station am anderen Ende des LANs und wieder zurückgewandert ist. Nur so können entstandene Kollisionen von den einzelnen Stationen entdeckt werden. Das Kollisionssignal muss ankommen, bevor das letzte Rahmen-Bit gesendet wird.

Es ergibt sich also ein Kollisionsfenster von 51,2 µs. Dieses wird benötigt, um den sogenannten Konfliktparameter K auf einem Wert kleiner eins zu halten. Steigt K auf einen Wert größer eins, könnte ein Sender seinen gesamten Rahmen über das Medium übertragen, ohne dass ein Konflikt erkennbar würde.

Der Parameter K berechnet sich aus der Gleichung:

K = maximale Signallaufzeit / Rahmenübertragungszeit = (Mediumlänge/Signallaufzeit) / (Rahmenlänge/Mediumbitrate)

Die Grenzen für CSMA/CD liegen also u.a. in der Distanz, in der Bitrate und in der minimalen Rahmenlänge.

Carrier Sense
bedeutet, dass eine sendewillige Station das Medium erst abhört, ob schon Datenverkehr auf ihm abläuft (listen before talking).

Multiple Access
bedeutet, dass alle Stationen gleichberechtigt auf das Übertragungsmedium jederzeit zugreifen können.

Collision Detect
Falls zwei Stationen in einer Kollisionsdomäne gleichzeitig senden, wird der Sendevorgang sofort abgebrochen.
Nach einer durch den Backoff-Algorithmus bestimmten Wartezeit versuchen die Stationen ihre Rahmen erneut zu senden.

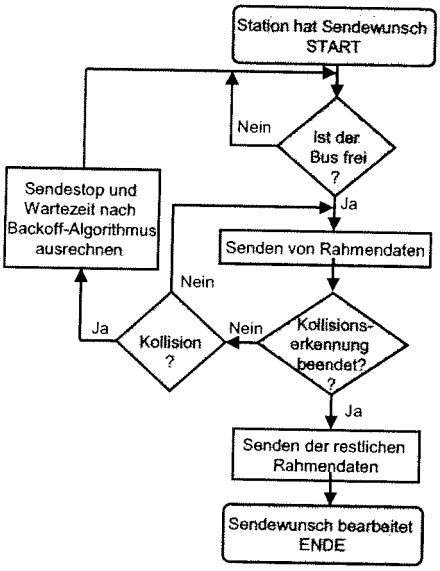


Bild: Zugriffsprotokoll CSMA/CD

- Kollision tritt nur im Ethernet mit Halbduplex-Verfahren ein.
- Slot Time ist die Länge des kleinsten Rahmens (64 Byte) im Medium (512 Bitzeiten).
- Kollisionserkennung wird nur während der Übertragung der ersten 576 Bitzeiten durchgeführt (ergibt sich aus dem kleinstmöglichen Frame von 64 Byte = 512 Bit, plus einer Sperrzeit für die Kollisionserkennung).
- Daraus ergibt sich die maximale Ausdehnung einer Kollisionsdomäne (aus der halben Signallaufzeit der kleinsten Rahmengröße).
- Die erkannten Kollisionen werden durch ein Störsignal (JAM-Signal) anderen Stationen mitgeteilt.
- Das JAM-Signal besteht aus einer 32 Bit langen Folge von 1 und 0.

Bild: Jamming-Signal in CSMA/CD

Um die Kollisionserkennung sicherzustellen, muss die minimale MAC-Rahmendauer mindestens doppelt so groß sein wie die Signalausbreitungszeit zwischen zwei Stationen mit der maximalen Entfernung. Hierbei entsteht ein Zielkonflikt zwischen möglichst großer Buslänge, hoher Datenrate und der Möglichkeit, auch kurze Rahmen zu senden.

Bei einer Bitrate von 10 Mbit/s ist die Bitdauer 0,1 µs. Dies entspricht einer Kabellänge von 20 Metern.

Es soll vermieden werden, dass die Stationen nach dem Auftreten einer Kollision wieder gleichzeitig versuchen, ihre Rahmen auszusenden.

- Jede Station in einer Kollisionsdomäne ermittelt die ganze Zahl r nach dem Zufallsprinzip innerhalb folgendes Wertbereichs:

$$0 \le r < 2^k ,$$

wobei $k = 1,2...n$ und n stellt die Anzahl der Wiederholungsversuche dar.

- Die Wartezeit wird dann als $w = r \cdot (Slot\ Time)$ ermittelt.
- Falls es wieder zur Kollision kommt wird die Variable n um eins erhöht.
- Nach dem zehnten gescheiterten Versuch bleibt die Variable k konstant (k = 10).

Bild: Backoff-Algorithmus in CSMA/CD

Nach einer erkannten Kollision muss die sendende Station den Sende—Prozess unterbrechen und eine Pause einlegen. Die Pausendauer wird nach dem Backoff-Algorithmus, der für alle Stationen gültig ist, ermittelt. Die Pausendauer ist immer ein Vielfaches eines Slots. Weil das Kollisionsfenster 51,2 µs groß ist, muss ein Slot eine Länge von 512 Bits haben.

Um den Algorithmus an einem Beispiel zu erklären, nehmen wir k als Parameter an. Der Parameter k ist die Anzahl der Kollisionen bezüglich eines Rahmens. Der nächste Übertragungsversuch ist über die nächsten 2^k Slots gleichverteilt.

Nach der 1. Kollision: k = 1; 2^k = 2: Der Übertragungsversuch findet im nächsten oder übernächsten Slot statt.
Nach der 2. Kollision: k = 2; 2^k = 4: Der Übertragungsversuch findet innerhalb der nächsten vier Slots statt.

Der Parameter k darf maximal den Wert 10 annehmen, d.h. dass k nach der 10. Kollision nicht mehr erhöht wird (Backoff limit). Insgesamt sind nur 16 Kollisionen (attempt limit) innerhalb der Übertragung eines Rahmens erlaubt. Bei mehr als 16 Kollisionen wird ein Excessive Collision Error ausgegeben.

Falls:
- die maximale Ausdehnung des Netzes zu groß ist oder
- über Repeater/Hubs zu viele Netzsegmente gekoppelt wurden,

kann es zu einer nicht erkannten Kollision kommen.

- Solche Kollisionen nennt man „Late Collisions" und können nur von höheren Protokollebenen (z.B. Schicht 4 eines verbindungsorientierten Protokolls) erkannt und korrigiert werden.

Zusätzlich gibt es sogenannte späte Kollisionen, die entstehen, wenn die maximale Netzausdehnung zu groß ist oder der Übertragungspfad zu viele Netzelemente enthält.

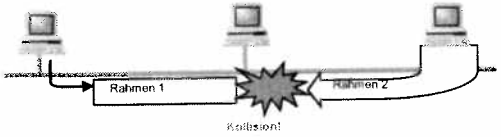
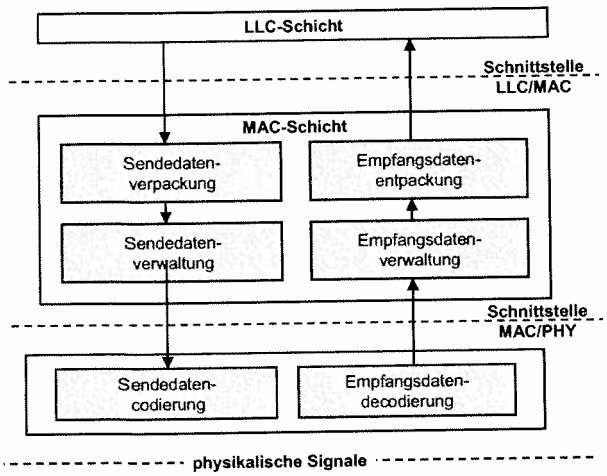


Bild: Späte Kollisionen in CSMA/CD



Die Protokoll-Funktionen teilen sich in fünf Gruppen auf:

- Sendedaten-Verpackung (transmit data encapsulation),
- Sendedaten-Verwaltung (transmit link management),
- Sendedaten-Codierung (transmit data encoding),
- Empfangsdaten-Decodierer (receive data decoding),
- Empfangsdaten-Verwaltung (receive data management).

Bild: IEEE 802.3 Protokoll-Funktionen

Die Funktion der Sendedatenverpackung besteht darin, einen Rahmen zu erzeugen, in den sie die von der LLC-Schicht erhaltenen Informationen aufnimmt.

Die Sendedatenverwaltung stellt fest, ob das Medium frei ist, und veranlasst die Übertragung. Im Anschluss an eine Übertragung muss ein Interframe Gap (Interframe Delay = 9,6 µs) eingelegt werden, um den Rahmen zu schützen und um ein garantiert störungsfreies Medium für die nächste Übertragung zur Verfügung zu haben. Ferner veranlasst sie bei auftretenden Kollisionen die Aussendung eines Störsignals (JAM).

Die Sendedatencodierung übernimmt den Bitstrom und codiert ihn nach dem Manchester-II-Verfahren. Der Empfangsdatendecodierer decodiert den empfangenen Bitstrom und übergibt ihn an die Empfangsdatenverwaltung. Bei der Empfangsdatenverwaltung wird die Prüfung auf Korrektheit und Vollständigkeit des empfangenen Rahmens durchgeführt.

IEEE 802.11 WLAN (Wireless LAN), Lokales Funknetz

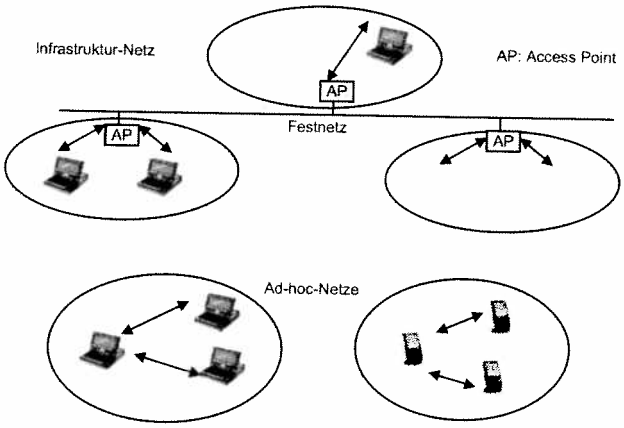


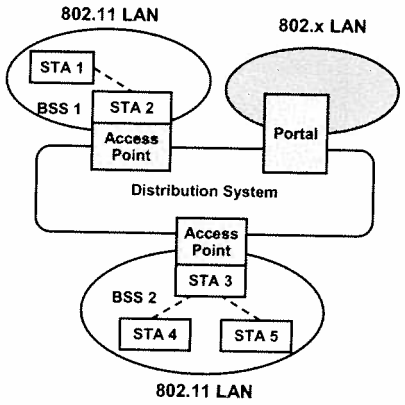
Bild: IEEE 802.11 Wireless LAN Architektur

Netzarchitektur und Schichtenmodell

Für drahtlose, lokale Netze (WLAN) ist IEEE 802.11 gegenwärtig der wichtigste Standard. Netze nach IEEE 802.11 werden primär als Infrastrukturnetze aufgebaut, können aber auch Ad-hoc-Netze sein. Die mobilen Stationen (Endgeräte) sind in Gruppen eingeteilt, die über denselben, festen Zugangspunkt (AP, Access Point) kommunizieren und als BSS (Basic Service Set) bezeichnet werden. Mehrere Zugangspunkte können über ein festes Netz, das DS (Distribution System) verbunden sein. Dieses erlaubt über ein Portal auch den Zugang zu übergeordneten Netzen. Das ESS (Extended Service Set) umfasst die verkabelte Infrastruktur (DS, Distribution System) und alle Basic Service Sets (BSS). Bei Ad-Hoc-Netzen spricht man von IBSS (Independent Basic Service Set). Falls das WLAN QoS-Eigenschaften aufweist, spricht man von QBSS (QoS Basic Service Set).

- **Station (STA)**
  - Rechner mit Zugriffsfunktion auf drahtloses Medium und Funkkontakt zum Access Point
- **Basic Service Set (BSS)**
  - Gruppe von Stationen, welche dieselbe Funkfrequenz nutzen
- **Access Point (AP)**
  - Station, die in Funk-LAN und das verbindende Festnetz (Distribution System) integriert ist
- **Portal**
  - Übergang in anderes Festnetz

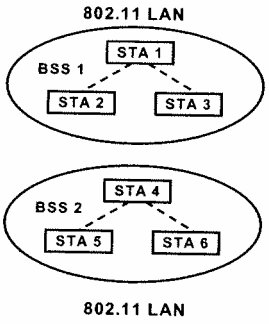
Bild: IEEE 802.11-Infrastrukturnetze



Netzvarianten:
BSS (Basic Service Set)
IBSS (Independent Basic Service Set)
ESS (Extended Service Set)
QBSS (QoS Basic Service Set)

- direkte Kommunikation mit begrenzter Reichweite
- **Station (STA)**
  - Rechner mit Zugriffsfunktion auf das drahtlose Medium
- **Independent Basic Service Set (IBSS)**
  - Gruppe von Stationen, welche die selbe Funkfrequenz nutzen

Bild: IEEE 802.11 Ad-hoc-Netze



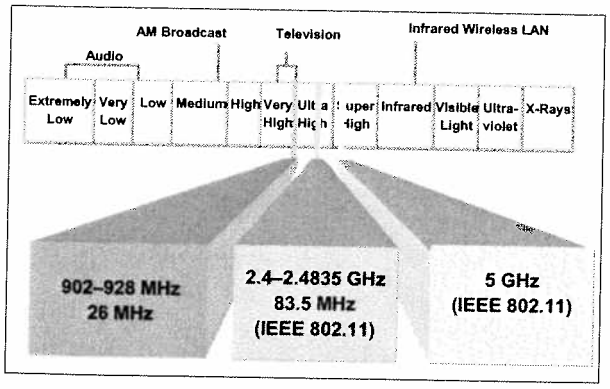


Bild: Lizenzfreie ISM-Frequenzbänder

ISM-Bands: Industrial-Scientific-Medical Frequency Bands

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
Maximale bit rate	1 oder 2 Mbit/s	11 Mbit/s	54 Mbit/s	54 Mbit/s
Benutzer-rate	0.5 - 1 Mbit/s	5.5 Mbit/s	22-26 Mbit/s	17-22 Mbit/s
Frequenzband	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz
Reichweite	80 m	57 m	12 m	19 m
Gleichzeitige Kanäle	3	3	8	3

Bild: IEEE 802.11 Standards

Heute: IEEE 802.11b (11 Mbit/s, 2,4 GHz).
Neu: - IEEE 802.11g (bis 54 Mbit/s, 2,4 GHz).
- IEEE 802.11d (bis 54 Mbit/s, 5 GHz).

Die 802.11d-Standard enthält Ergänzungen, um die 802.11a Standard in Europe anzuwenden.

Das Schichtenmodell nach IEEE 802.11 spezifiziert die physikalische Schicht PHY und die Medienzugriffsschicht MAC. Die PHY-Schicht wird unterteilt in PMD (Physical Medium Dependent) und PLCP (Phycal Layer Convergence Protocol). PMD ist für die Codierung der Daten zuständig, PLCP überprüft den Kanalzustand (carrier sense) und stellt der MAC-Schicht eine vom Übertragungsmedium unabhängige Schnittstelle zur Verfügung.

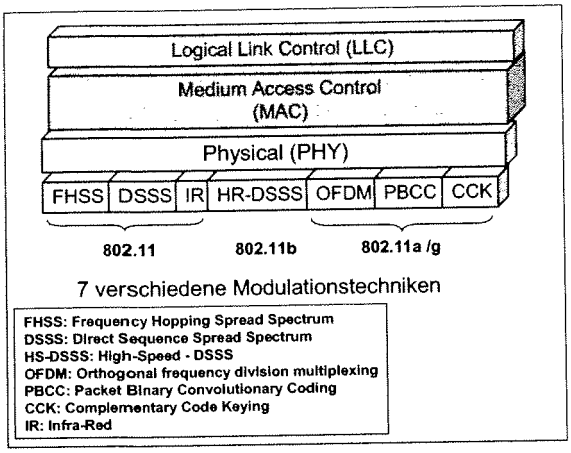


Bild: IEEE 802.11 Protokollstruktur

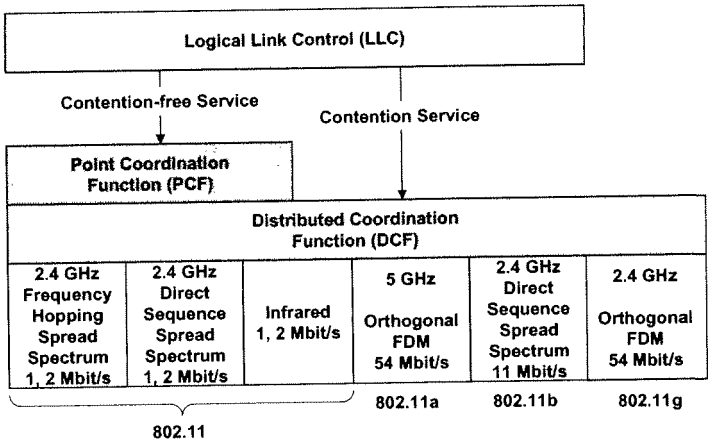


Bild: IEEE 802.11 Protokollstruktur

Die MAC-Schicht ist wie üblich für den Medienzugriff verantwortlich und bietet zusätzliche Funktionen wie Verschlüsselung und Fragmentierung. Bei drahtloser Übertragung soll die Verschlüsselung die Vertraulichkeit gewährleisten. Die Fragmentierung kann bei hohen Bitfehlerraten eingesetzt werden um die Rahmenfehlerrate zu begrenzen. Dadurch lassen sich Wiederholungen fehlerhaft empfangener Pakete begrenzen.

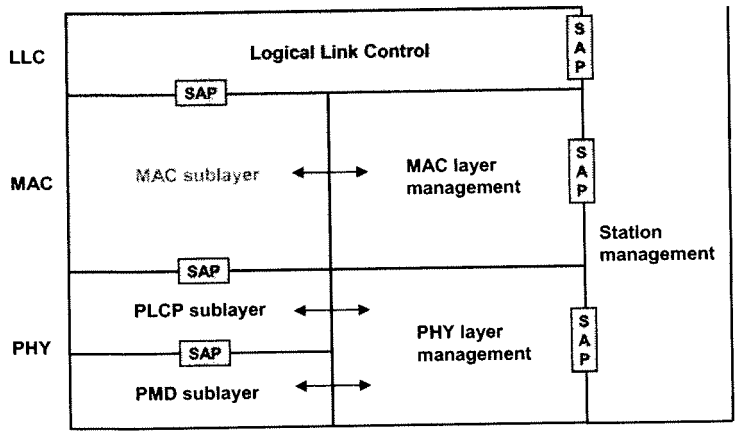
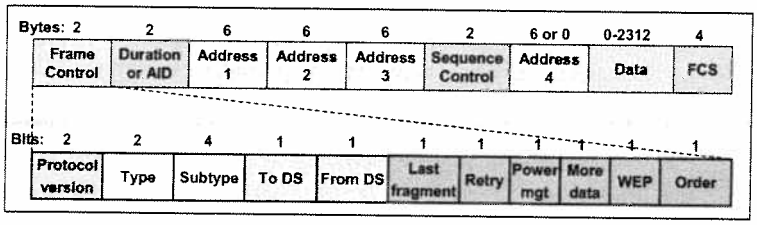


Bild: IEEE 802.11 Protokollstruktur

Das PHY-Management kümmert sich primär um die Wahl des zu verwendenden Sendekanals, während das MAC-Management den Wechsel zwischen verschiedenen Access Points (das so genannte roaming) steuert. Das Station-Management koordiniert alle anderen Funktionen.



		addr 1	addr 2	addr 3	addr 4
Ad-Hoc	0 0	DA	SA	BSSID	-
From AP	0 1	DA	BSSID	SA	-
To AP	1 0	BSSID	SA	DA	-
Within DS	1 1	RA	TA	DA	SA

AP: Access Point
AID: Association Identification
BSSID: Basic Service Set Identifier
FCS: Frame Check Sequence
DS: Distribution System
DA: Destination Address
RA: Receiver Address
SA: Source Address
TA: Transmitter Address
WEP: Wired Equivalent Privalency

Bild: IEEE 802.11 MAC-Rahmenformat

Der MAC-Rahmen besteht einerseits aus einer nicht abgebildeten Präambel, die von der verwendeten Modulationstechnik auf dem Medium abhängt und somit zur physikalischen Schicht gehört und anderseits den eigentlichen MAC-Informationen. Dadurch wird auch die Erkennung von Rahmenbeginn in der physikalischen Schicht gemacht. Die Rahmenlänge wird durch das Duration-Feld (Belegungszeit des Mediums) bestimmt.

Der Rahmen enthält vier Adressen, die je nach Kommunikationsszenario verwendet werden. Die vier Verwendungsarten sind durch die beiden To/From DS Bits gekennzeichnet.

Im Sequence-Control-Feld werden die Rahmen durchnummeriert.

Die einzelnen Bits im Rahmen-Kontroll-Feld haben die folgende Bedeutung:

- **Protocol Version:** Protokollversion (derzeit gleich Null).
- **Type:** Rahmentyp (Daten, Kontrolle oder Verwaltung).
- **Subtype:** Einzelne Kommandos oder Antworten.
- **To/From DS:** Adressierung.
- **Last Fragment:** Mit Wert 1 wird angezeigt, dass noch Fragmente folgen.
- **Retry:** Mit Wert 1 wird angezeigt, dass es sich um eine Wiederholung handelt.
- **Power Management:** Mit Wert 1 wird angezeigt, dass die sendende Station in Power-Saving Modus geht.
- **More Data:** Mit Wert 1 wird angezeigt, dass die sendende Station noch weitere Daten für die Empfangsstation hat.
- **WEP:** Mit Wert 1 wird angezeigt, dass der Wired Equivalent Privacy Sicherheitsmechanismus verwendet wird.
- **Order:** Mit Wert 1 wird angezeigt, dass die empfangenen Rahmen in strikter Reihenfolge behandelt werden müssen.

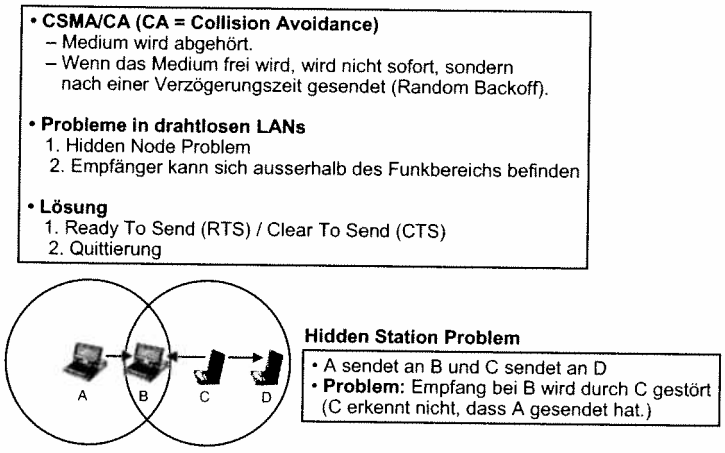
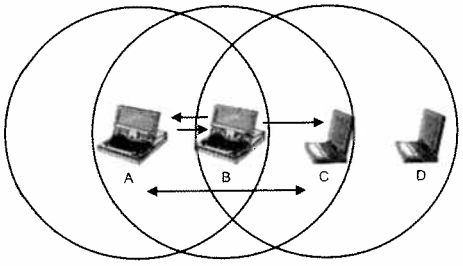


Bild: IEEE 802.11 Wireless LANs

Das Hidden-Station-Problem

Zu großen Performance-Einbußen kann es bei einem drahtlosen Netz durch das so genannte Hidden-Station-Problem kommen. Darunter versteht man das fälschliche Erkennen eines freien Mediums, obwohl dieses bereits belegt ist. Dies tritt genau dann ein, wenn die sendende Station außerhalb der Reichweite der prüfenden Station liegt. Station A kann Station B erreichen, jedoch nicht Station C. Station C wiederum kann nur Station B erreichen, jedoch nicht Station A.

Dies bedeutet, die Stationen A und C können Rahmen von Station B empfangen, jedoch wegen der fehlenden Reichweite keine Rahmen untereinander austauschen. Probleme treten in diesem Fall auf, wenn die Stationen A und C mehr oder weniger zeitgleich versuchen, ein Rahmen an Station B zu übertragen. Dies kann auftreten, da Station C nicht erkennen kann, dass Station A bereits ein Rahmen an Station B sendet und das Medium bereits belegt ist.



1. Ready To Send (RTS) durch A
2. Clear To Send (CTS) durch B, C erkennt folgende Übertragung
3. A sendet Daten
4. B quittiert

Bild: Das Hidden-Station-Problem

Zur Vermeidung dieses Effekts sieht der IEEE-802.11-Standard den RTS/CTS-Mechanismus (Ready To Send und Clear To Send) vor. Dabei schickt der Sender A nach Erkennen eines freien Mediums zuerst ein RTS-Rahmen zum Empfänger B, das den gewünschten Umfang der Sendung über das Duration-ID-Feld des Headers ankündigt. Danach überträgt der Empfänger ein CTS-Rahmen, wenn das Medium frei ist, wobei er ebenfalls über das Duration-ID-Feld die Sendedauer bestätigt. Dieses CTS-Rahmen hören alle Stationen innerhalb der Funkzelle der Empfängerstation (auch Station C, die A nicht hören kann) und wissen Bescheid, dass das Übertragungsmedium nun für eine bestimmte Dauer belegt ist. Über den Empfang des CTS-Rahmens können alle Stationen ihren sogenannten NAV-Wert entsprechend setzen, wodurch für die benötigte Dauer der vollständigen Datenübertragung keine weitere Station mehr versuchen wird, auf das Medium zuzugreifen.

Damit ist gewährleistet, dass bei der empfangenden Station keine Kollision auf dem Medium auftritt. Der Network Allocation Vector (NAV) ist ein Timer zur Vermeidung von Kollisionen. Über den NAV-Wert wird bestimmt, wie lange das Medium voraussichtlich für die Übertragung der Daten belegt ist. Jede Station verwaltet den NAV-Wert. Erst wenn der NAV-Wert abgelaufen ist, versucht sie gegebenenfalls auf das Medium zuzugreifen (Collision Avoidance).

Auf diese Weise können zwar immer noch Rahmen auf dem Funkmedium kollidieren, jedoch handelt es sich dann dabei nur um die RTS/CTS-Rahmen, deren Länge gegenüber den Datenrahmens relativ kurz ist (20 Byte für ein RTS-Rahmen und 14 Byte für ein CTS-Rahmen). Tritt eine Kollision hingegen beim Übertragen eines Datenrahmens auf, so ist das Medium relativ lange belegt, da die sendende Station die Kollision nicht erkennen kann und den Rahmen bis zum Ende aussendet. Beim RTS/CTS-Mechanismus wird hingegen bei einer eventuellen Kollision das Medium nur kurzzeitig unnötig belegt, was zu einer besseren Haushaltung der verfügbaren Bandbreite führt.

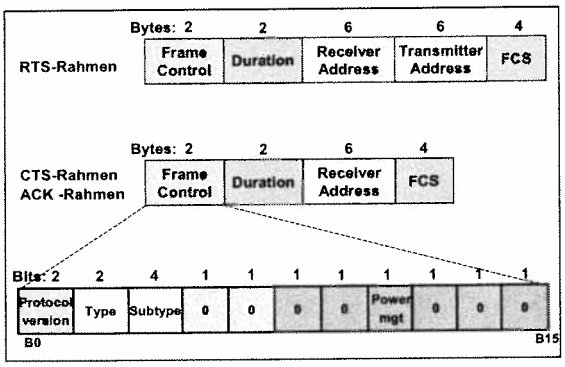
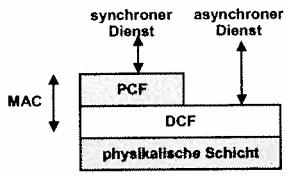


Bild: IEEE 802.11 Kontrollrahmen

In der Praxis wird der RTS/CTS-Mechanismus über eine Schwelle aktiviert. Die Schwelle entspricht dabei der Länge des zu übertragenden Datenrahmens. Ist diese Länge größer als die festgelegte Schwelle, so wird vor der Aussendung des Datenrahmens das RTS-Rahmen ausgesendet und auf den Empfang des CTS-Rahmens gewartet. Dies soll verhindern, dass das Übertragungsmedium durch RTS/CTS-Rahmen unnötig belastet wird, obwohl nur kurze Datenrahmens übertragen werden sollen. Dadurch wird der Tatsache Rechnung getragen, dass für die Übertragung von kurzen Rahmen eine geringere Zeit benötigt wird, somit die Wahrscheinlichkeit für eine eventuell auftretende Kollision geringer ist und auf RTS/CTS-Mechanismus ohneweiteres verzichtet werden kann.



- **Distributed Coordination Function (DCF)**
  - asynchroner Datenverkehr mit einer auf die Stationen verteilten Zugriffsfunktion
  - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
  - MAC-Schicht-Quittierung für alle nicht-Broadcast-Rahmen mit eventueller Übertragungswiederholung
- **Point Coordination Function (PCF)**
  - synchroner Datenverkehr unter der Kontrolle des Access Point
  - Stationen senden nur nach Polling durch PCF
  - Aufbau einer Polling-Liste
  - optionaler Modus

Bild: 802.11-Zugriffsverfahren

Da das Funkmedium ein gemeinsames Medium (Shared Medium) darstellt, können bei einem zeitgleichen Zugriff von zwei oder mehreren Stationen Kollisionen auftreten, die zu einer unvollständigen Datenübertragung führen können. Deshalb muss über ein geeignetes Zugriffsverfahren dafür gesorgt werden, dass Kollisionen vermieden und verlorene Daten wiederholt ausgesendet werden. Diese Funktion übernimmt der IEEE.802.11-MAC-Layer als primäre Aufgabe. Zudem stellt die MAC-Schicht typische Funktionen bereit, die sonst auf höheren Schichten angesiedelt sind: Fragmentierung, Rahmenwiederholungen (Frame Retransmissions) und die Empfangsbestätigung der Rahmen (Acknowledgements).

Distribution Coordination Function

Innerhalb des IEEE 802.11-MAC unterscheidet man zwischen zwei Methoden:

- **Distribution Coordination Function (DCF):** Dies ist der Basiszugriffsmethode und ist ein dezentraler Ansatz,
- **Point Coordination Function (PCF):** Eine zentrale Methode.

In Anlehnung an Ethernet (IEEE 802.3) benutzt das IEEE 802.11-MAC-Protokoll als Basiszugriffsmethode Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).

Im Gegensatz zu IEEE 802.3 verzichtet die Definition allerdings aufgrund der Eigenschaften der drahtlosen Datenübertragung auf eine Kollisionserkennung (Collision Detection, CD). Denn aus technischen Gründen (entweder kann eine Station nur Daten senden oder Daten empfangen) ist eine Kollisionserkennung während der Aussendung der Daten nicht möglich. Zudem lassen sich Kollisionen auf dem drahtlosen Medium nicht von anderen Störungen unterscheiden. Aus diesem Grund setzt man eine Kollisionsvermeidung (Collision Avoidance, CA) ein. Durch das Verfahren der Kollisionsvermeidung soll die Wahrscheinlichkeit für das Auftreten einer Kollision klein gehalten und eine vollständige Datenübertragung sichergestellt werden.

Möchte eine Station Daten aussenden, so prüft sie, ob das Medium frei ist (Carrier Sense). Ist das der Fall, beginnt sie mit der Aussendung der Daten. Da jedoch mehrere Stationen mehr oder weniger zeitgleich versuchen können, auf das Medium zuzugreifen, besteht die Gefahr, dass sie zu der Ansicht gelangen können, dass das Medium frei ist (Multiple Access) und deshalb ebenfalls mit der Aussendung der Daten beginnen. In diesem Fall tritt zwangsläufig eine Kollision auf, wodurch die übertragenen Daten verloren gehen. Weil bei CSMA/CA Kollisionen nicht ausgeschlossen werden können, spricht man von der Contention Period (CP), also von der Zeitspanne, bei der CSMA/CA den Medienzugriff regelt. Das ist eine Phase, in der mehrere Stationen untereinander in Konkurrenz um den Medienzugriff stehen. Die zentralistische Verwaltung des Medienzugriffs PCF stellt hingegen eine Methode bereit, mit der Kollisionen vermieden werden können. Man spricht deshalb von der Contention Free Period (CFP), als der Zeitspanne, in der das Medium zentral verwaltet wird. CFP ist für zeitkritische Anwendungen gedacht, wo der Medienzugriff innerhalb einer bestimmten Zeit gewährleistet sein muss, z. B. für die Übertragung von Sprachdaten. Die Implementierung von CFP ist laut Standard optional und baut auf das CSMA/CA-Verfahren auf.

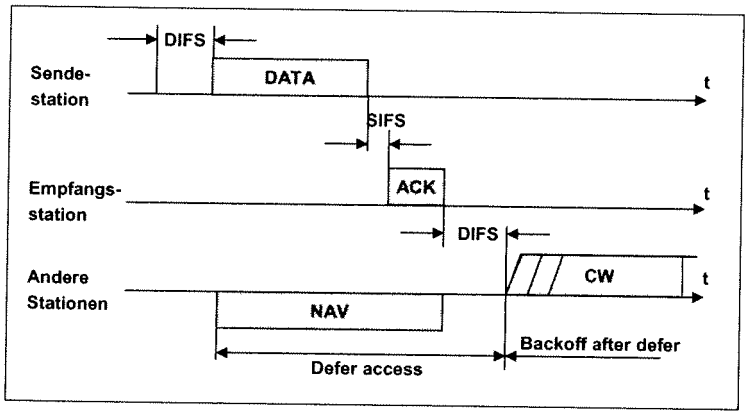


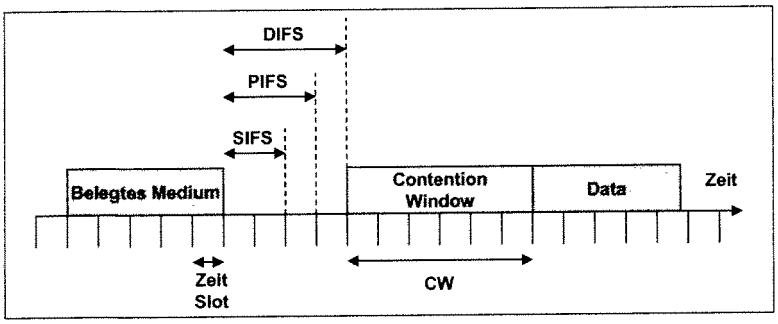
Bild: IEEE 802.11: Medium Access Control

Der entscheidende Unterschied beim CSMA/CA zum CSMA/CD besteht in der Funktion der Kollisionsvermeidung. Sie basiert auf dem so genannten NAV-Wert. Der NAV-Wert wird auf jeder Station verwaltet und über eine Angabe im Rahmen-Header, das Duration-ID-Feld, gebildet. In jedem ausgesendeten Rahmen wird über das Duration-ID-Feld angegeben, wie lange das Medium für die vollständige Übertragung der Daten belegt sein muss.

Da alle Stationen diese Information empfangen, können sie ständig ihren NAV-Wert aktualisieren, und die sendende Station kann auf diese Weise das Medium für die benötigte Zeit der Datenübertragung reservieren. Erst wenn der NAV-Wert abgelaufen ist, werden andere Stationen versuchen, auf das Medium zuzugreifen; Kollisionen werden so vermieden.

Da jedoch Kollisionen nicht ausgeschlossen werden können und andere Störeinflüsse die Datenübertragung nachhaltig beeinflussen können, wird der erfolgreiche Empfang der Daten dem Sender vom Empfänger durch eine Empfangsbestätigung (Acknowledgement) mitgeteilt. Bleibt die Empfangsbestätigung aus, so werden die Daten vom Sender nach einer bestimmten Wartezeit erneut ausgesendet. Die Wartezeit wird über einen Backoff-Algorithmus gebildet, wobei die Wartezeit über eine Zufallszeit bestimmt wird und bei jedem erneuten Versuch bis zu einer bestimmten Grenze ansteigt.

Die Empfangsbestätigung basiert auf einem 14 Byte langen Rahmen, in dem kein Datenteil enthalten ist und der nur aus einem verkürzten Header besteht. Nur Unicast-Rahmen werden über die Aussendung einer Empfangsbestätigung bestätigt, Broadcast- und Multicast-Rahmen werden nicht bestätigt. Dies lässt sich damit begründen, dass es nicht sinnvoll ist, wenn jeder Empfänger den Empfang bestätigen würde. Zudem kennt der Sender gar nicht alle potenziellen Empfänger und kann somit nicht wissen, mit welchen Empfangsbestätigungen er zu rechnen hat.



DIFS : DCF interframe space
PIFS : PCF interframe space
SIFS : Small interframe space
CW: Collsion Window

Bild: CSMA/CA access mechanism

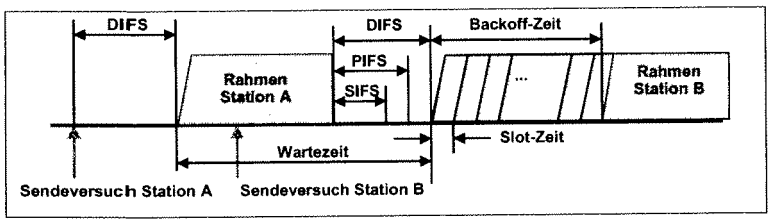
Nachdem eine Station Daten ausgesendet hat, erwartet sie innerhalb eines bestimmten Zeitraums eine Empfangsbestätigung. Damit die Empfangsbestätigung vom Empfänger ausgesendet werden kann, ohne dass eine andere Station bereits das Medium für die Übertragung ihrer Daten belegt hat, haben die Empfangsbestätigungen bei dem Medienzugriff eine höhere Priorität. Die Sicherstellung der Prioritäten wird über verschiedene Abstände zwischen zwei aufeinander folgenden Rahmen realisiert, die als Interframe Space (IFS) bezeichnet werden.

Der Standard sieht vier verschiedene IFS vor, die bei der Sicherstellung der Prioritäten folgende Funktion haben:

- **SIFS (Short Interframe Space)** definiert einen Mindestabstand für ACK-Rahmen, Clear-to-Send-Rahmen (Bestätigung eines Request-to-Send-Rahmen beim CTS/RTS-Mechanismus), Folgerahmens, die von einem Burst einer fragmentierten Nachricht stammen oder als Reaktion auf ein Polling-Rahmen im PCF. SIFS entspricht der Zeit zwischen dem letzten Symbol einer vorherigen Rahmen und dem ersten Symbol, der Präambel, des neu ausgesendeten Rahmens.
- **PIFS (Point Interframe Space)** wird nur von Stationen verwendet, die im PCF-Modus arbeiten. Über PIFS wird während der PCF sichergestellt, dass ein bevorzugter Medienzugriff von PCF-Stationen ermöglicht wird. In der Standard IEEE 802.11q ist dieser Wert noch mit 8 Intervallen erweitert worden, um ein prioritärer Zugriff mit 8 Prioritäten zu ermöglichen.
- **DIFS (Distributed Interframe Space)** wird von Stationen genutzt, die im DCF-Modus arbeiten. Der Mindestabstand laut DIFS wird für die Aussendung des Daten- und Managementrahmens verwendet.
- **EIFS (Extended Interframe Space)** wird bei Stationen angewendet, die im DCF-Modus arbeiten. Sollte der PHY bei der Aussendung eines Rahmens über die FCS (Rahmen Check Sequence) festgestellt haben, dass der Inhalt des Rahmens nicht korrekt ist, so wird die Aussendung des Rahmen abgebrochen. In diesem Fall wird der Zugriff auf das Medium nach dem Ablauf des EIFS erlaubt und die Stationen müssen nicht die Zeit abwarten, die ursprünglich über das Duration-ID-Feld als NAV-Wert definiert wurde.

Da der SIFS kürzer als der DIFS ist, haben Rahmentypen, die nach dem Ablauf des SIFS gesendet werden dürfen, beim Medienzugriff eine höhere Priorität als die Rahmen, die erst nach Ablauf des DIFS gesendet werden dürfen. Auf diese Weise wird auf jeden Fall sichergestellt, dass ACK-Rahmen vor Datenrahmens bevorzugt ausgesendet werden dürfen und eine Station eine Chance hat, nach dem fehlerfreien Empfang der Daten den ACK-Rahmen auszusenden.

Damit sichergestellt ist, dass nicht alle Stationen nach dem Ablauf des DIFS zeitgleich auf das Medium zugreifen und ihre Daten aussenden, wartet jede Station für sich eine bestimmte Zeit ab, bevor sie eventuell mit der Aussendung der Daten beginnt.



- Sendebereite Station hört Medium ab
- Senden bei freiem Medium der Dauer eines Inter-Frame Space (IFS)
- Verzögerung um IFS + eine zufällige Backoff-Zeit bei belegtem Medium
  ⇒ Kollisionsvermeidung
- Wird das Medium während der Backoff-Zeit von einer anderen Station belegt, bleibt der Backoff-Timer so lange stehen.
- Prioritätsklassen durch unterschiedlich lange IFS
  1. short IFS (SIFS): CTS, ACK, poll response
  2. PCF IFS: poll
  3. DCF IFS (DIFS): RTS, Daten

Bild: IEEE 802.11: CSMA/CA-Verfahren

Die Wartezeit wird auf jeder Station nach dem Zufallsprinzip über den Backoff-Algorithmus erstellt. Die Station mit der kleinsten Wartezeit greift als erste auf das Medium zu und sendet ihre Daten über das Medium aus, wodurch für alle anderen Stationen das Medium als belegt gilt. Die anderen Stationen setzen ihren NAV-Wert anhand des Duration-ID-Felds auf den Zeitwert, der für die Übertragung des Rahmen benötigt wird. Die Zeit, die im Duration-ID-Feld angegeben wird, entspricht der Zeit, die für die Übertragung des aktuellen Rahmens und für den darauf erwartete ACK-Rahmen benötigt wird. Nach Ablauf des NAV-Werts und einer weiteren DIFS versuchen die anderen Stationen wieder auf das Medium zuzugreifen.

- Backoff-Zeit = Int [CW * R] * Slotzeit
  - CW (contention window, z.B. CW_{min}= 31) wird bei jedem erfolglosem Versuch verdoppelt bis Cw_{max} (z.B. = 255) erreicht ist
  - R: Zufallszahl zwischen 0 und 1
  - Slotzeit
    - = Verzögerung zum Anschalten des Senders
    - + Signallaufzeit
    - + Verzögerung um belegtes Medium zu erkennen
- Dekrementieren des Backoff-Timers bei freiem Medium

Bild: Berechnung der Backoff-Zeit

Die Wartezeit ermittelt sich über die Formel:
Backoff Time = CW x Random x Slot Time.

Die Slot Time ist vom jeweiligen PHY abhängig und wird von diesem vorgegeben. CW steht für Contention Window und stellt eine Integer Zahl dar, die über das Zufallsprinzip aus der Menge $CW_{min} \leq CW \leq CW_{max}$ gebildet wird. Der minimale und maximale Werten CW_{min} und CW_{max} sind wie die Slot Time vom verwendeten PHY-Typ abhängig.

Bei der ersten Aussendung ist z.B. beim DSSS-PHY CW_{min} mit 31 und CW_{max} mit 255 festgelegt. Für CW ergibt sich somit ein Wert zwischen diesen beiden Werten.

Die Slot Time ist beispielsweise beim DSSS-PHY auf 20 µs festgelegt. Bei jedem erfolglosen Versuch der Datenaussendung wird der nächste Bereich für den CW-Wert zugrunde gelegt. Der CW-Wert wird wieder zurückgesetzt, sobald Daten erfolgreich übertragen wurden und dies durch einen ACK-Rahmen bestätigt wurde oder wenn nach einem ausgesendeten RTS-Rahmen ein CTS-Rahmen empfangen wurde.

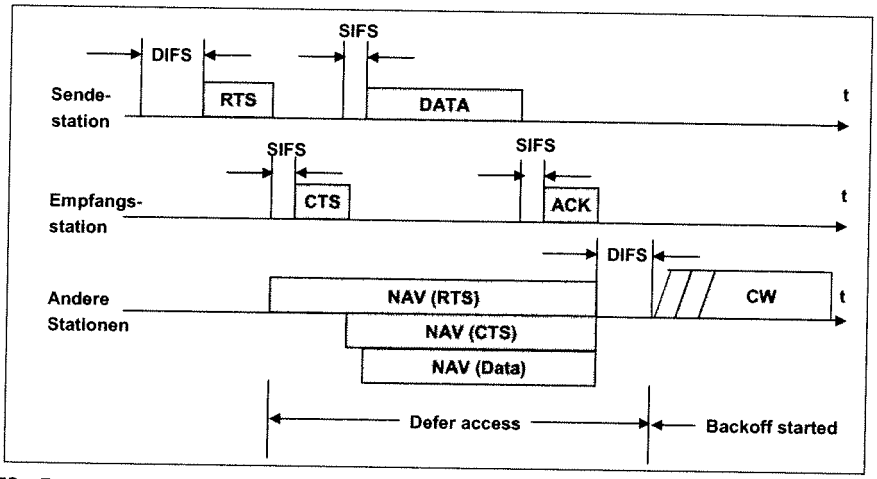


Bild: IEEE 802.11: Medium Access Control

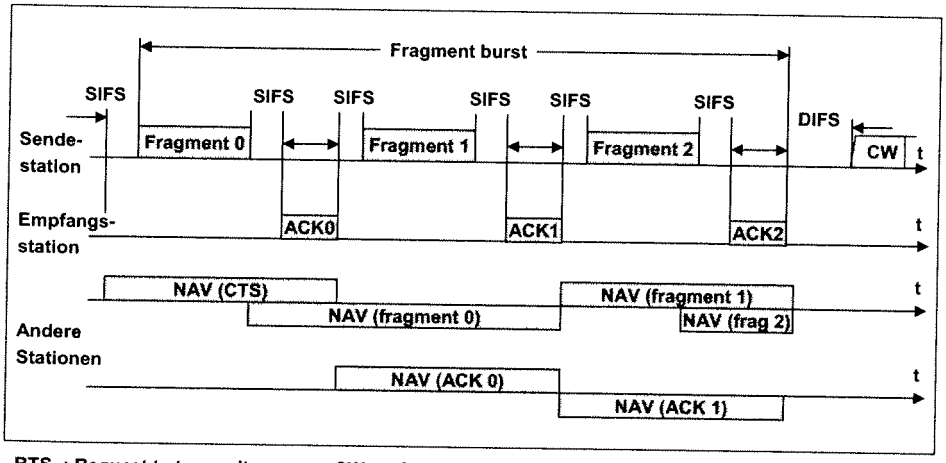


Bild: IEEE 802.11: Medium Access Control

Fragmentierung
Müssen längere zusammenhängende Daten übertragen werden, so werden diese unterteilt und in die Datenteile mehrere Rahmen gepackt, wobei man von einer Fragmentierung spricht. Die einzelnen Rahmen, die zu einem Datenteil gehören, werden als Fragmente bezeichnet. Auf der Seite des Empfängers werden die Fragmente wieder zusammengesetzt, so dass das ursprüngliche Datenteil wieder vorliegt.

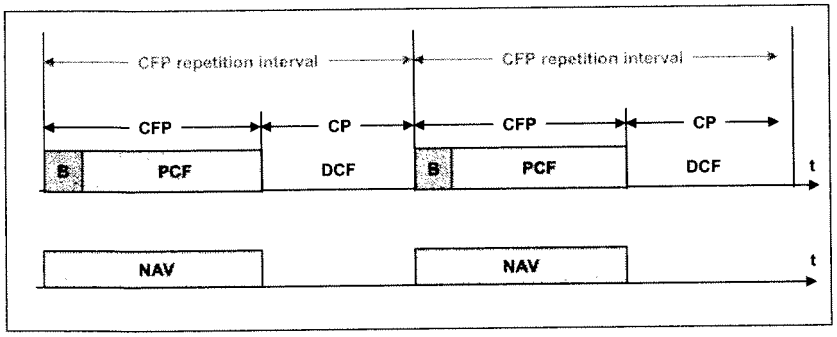
Für die Kontrolle der Fragmentierung wird das Sequence-Control-Feld des Rahmen-Headers genutzt. Das Sequence-Control-Feld gibt die Fragmentnummer und die Sequenznummer an. Die Sequenznummer ist bei allen Fragmenten gleich, die zu einem Datenteil gehören. Über diese werden sie als zusammenhängende Daten identifiziert. Über die Fragmentnummer werden die einzelnen Fragmente durchnummeriert, so dass auf Seiten des Empfängers die Daten wieder in der richtigen Reihenfolge zusammengesetzt werden können. Bei allen Fragmenten, mit der Ausnahme des letzten, ist im Control-Feld des Rahmen-Headers das More-Fragment-Bit gesetzt. Über das More-Fragment-Bit wird dem Empfänger angezeigt, dass weitere Fragmente folgen werden. Wird ein Fragment empfangen, in dem das More-Fragment-Bit nicht gesetzt ist, so erkennt der Empfänger, dass es sich um das letzte Fragment handelt und die Daten vollständig übertragen wurden.

Der fehlerfreie Empfang jedes einzelnen Fragments wird über ein Acknowledgement vom Empfänger bestätigt. Sollte das Acknowledgement beim Sender ausbleiben, so kann dies daran liegen, dass das Fragment oder das dazugehörende Acknowledgement nicht fehlerfrei übertragen werden konnte. In diesem Fall sendet der Sender das Fragment erneut aus und wartet mit der Aussendung des nächsten Fragmentes, bis er das Acknowledgement des vorherigen Rahmens empfangen hat. In diesem Fall wird über ein Retry-Bit des Rahmen-Headers angezeigt, dass es sich um eine wiederholte Aussendung eines Rahmens handelt. Über das gesetzte Retry-Bit kann der Empfänger das wiederholt ausgesendete Fragment erkennen. Falls er das Fragment jedoch bereits empfangen hat, kann er das doppelte Fragment verwerfen. Dadurch wird dessen Dateninhalt nicht an die höheren Schichten weitergeleitet. Somit wird vermieden, dass bei einem verlorengegangenen Acknowledgement dieselben Daten wiederholt an die höheren Schichten weitergereicht werden. In diesem Fall wird der Empfänger trotzdem den Empfang des Fragments über ein Acknowledgement bestätigen, damit der Sender das nächste Fragment aussendet.

Bei einer fragmentierten Datenübertragung, findet also ein ständiger Wechsel zwischen einem Fragment und einem dazugehörigen Acknowledgement statt, bis das zusammenhängende Datenteil übertragen worden ist. Grundsätzlich folgt das Acknowledgement nach dem letzten Bit des Fragments und einem SIFS. Dadurch hat das Acknowledgement die höchste Priorität beim Medienzugriff und es ist gewährleistet, dass die Empfangsbestätigung übertragen werden kann. Für die Übertragung eines Fragments gilt dieselbe Wartezeit, d. h., das Fragment wird nach dem letzten Bit des Acknowledgement und eines SIFS übertragen. Demnach braucht ein Sender von fragmentierten Daten nach dem Medienzugriff nur das Acknowledgement des letzten Fragments und ein SIFS abzuwarten, bevor das nächste Fragment aussendet wird. Auf diese Weise wird fortlaufend für alle Fragmente ein vorrangiger Medienzugriff gewährleistet.

Da der bevorzugte Medienzugriff sichergestellt ist, ist es bei einer fragmentierten Datenaussendung nicht notwendig, den NAV-Wert für die gesamte Datenlänge zu setzen. Würde man den NAV-Wert für die gesamte Datenlänge setzen, so würde dies bei einem Abbruch der Datenaussendung dazu führen, dass das Übertragungsmedium unnötig lange reserviert und somit für andere Stationen nicht zugänglich wäre. Der NAV-Wert wird demnach für jedes Fragment und das dazugehörige Acknowledgement über das Duration-ID-Feld des Rahmen-Headers neu gesetzt. Die einleitenden RTS- und CTS-Rahmen setzen den NAV-Wert für ihre Übertragungsdauer, das erste Fragment und das dazugehörige Acknowledgement.

Die fragmentierte Datenübertragung wird nicht nur bei langen Daten angewendet, deren Länge die maximal zulässige Datenlänge eines Rahmens überschreitet, sondern auch bei kürzeren Daten. Die Fragmentierung wird in der Praxis über einen Parameter eingestellt, mit dem festgelegt wird, ab welcher Datenlänge eine Fragmentierung durchgeführt werden soll. So können lange Rahmen vermieden werden und eine Datenübertragung bei einer kritischen Umgebung sicherer und zuverlässiger gestaltet werden, da längere Rahmen eher gestört und bei kürzeren Rahmen die Wahrscheinlichkeit einer Störung geringer ist. Auf diese Weise kann eine notwendige wiederholte Aussendung von verloren gegangenen Rahmen vermieden werden. In der Gesamtbetrachtung kann somit die Performance gesteigert werden. Die Fragmentierung kann jedoch nur bei Unicast-Rahmen angewendet werden, bei Broadcast- oder Multicast-Rahmen ist eine Fragmentierung nicht möglich.



B : Beacon
CFP : Collision free period
CP : Collision period
NAV : Network allocation vector
DCF : Distributed coordination function
PCF : Point coordination function

Bild: IEEE 802.11: Medium Access Control

Point Coordination Function

Die PCF (Point Coordination Function) ist im 802.11-Standard neben der DCF eine optionale Methode des MAC-Layers, die ein Zugriffsverfahren definiert. Bei der dezentralen Verwaltung des Übertragungsmediums spricht man von der Contention Free Period (CFP).

In der CP werden zwar Kollisionen vermieden, jedoch können diese nicht ausgeschlossen werden. Dies wirkt sich für zeitkritische Anwendungen negativ aus, da innerhalb eines bestimmten Zeitraums keine fehlerfreie Datenübertragung garantiert und somit die Verzögerungszeit nicht kalkuliert werden kann.

PCF stellt funktionell eine Erweiterung des DCF dar. Wird das Übertragungsmedium über PCF verwaltet, so spricht man bei der Zeitspanne dieser Verwaltungsmethode von der Contention Free Period (CFP). Während der CFP wird der Zugriff auf das Übertragungsmedium von einer zentralen Stelle verwaltet, die als Point Coordinator (PC) bezeichnet wird. Der PC erteilt den einzelnen Stationen einer Zelle über so genannte CF-Poll-Rahmen die Berechtigung für den Zugriff auf das Übertragungsmedium. Auf diese Weise werden Kollisionen ausgeschlossen, und innerhalb eines bestimmten Zeitraums kann ein Zugriff auf das Übertragungsmedium garantiert werden. Zeitkritische Anwendungen, wie beispielsweise die Übertragung von Sprachdaten, werden somit ermöglicht.

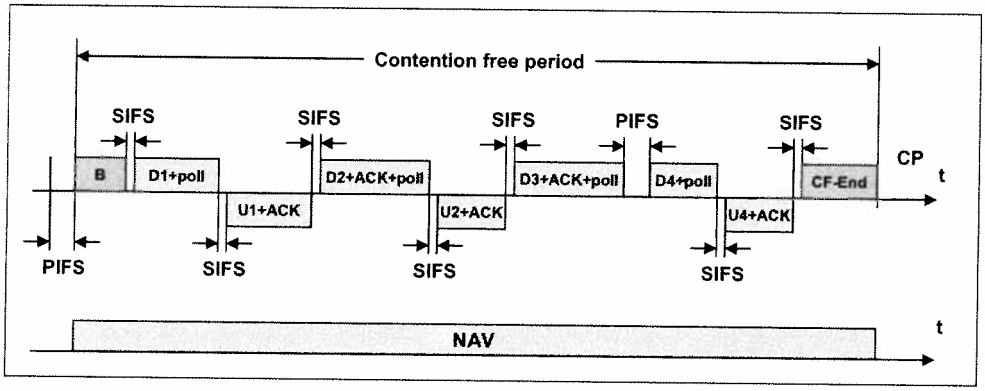


Bild: IEEE 802.11: Medium Access Control

Die Funktion des Point Coordinators wird von dem Access Point einer Zelle wahrgenommen. Der Access Point hat somit nicht nur die Aufgabe, einen Datenaustausch zwischen den Stationen einer Zelle und dem Verteilungssystem zu realisieren, sondern kann auch den Einsatz von zeitkritischen Anwendungen ermöglichen.

Leitet ein Access Point die Contention Free Period (CFP) ein, so findet ein Wechsel zwischen der CFP und der Contention Period (CP) auf dem Übertragungsmedium statt. Die Zeitspanne der CFP und der CP wird dabei vom Access Point bestimmt. Der Wechsel soll sicherstellen, dass Stationen einer Zelle, die kein PCF unterstützen, ebenfalls auf das Medium zugreifen können. Diesen Stationen wird während der CP gewährleistet, auf das Medium zuzugreifen.

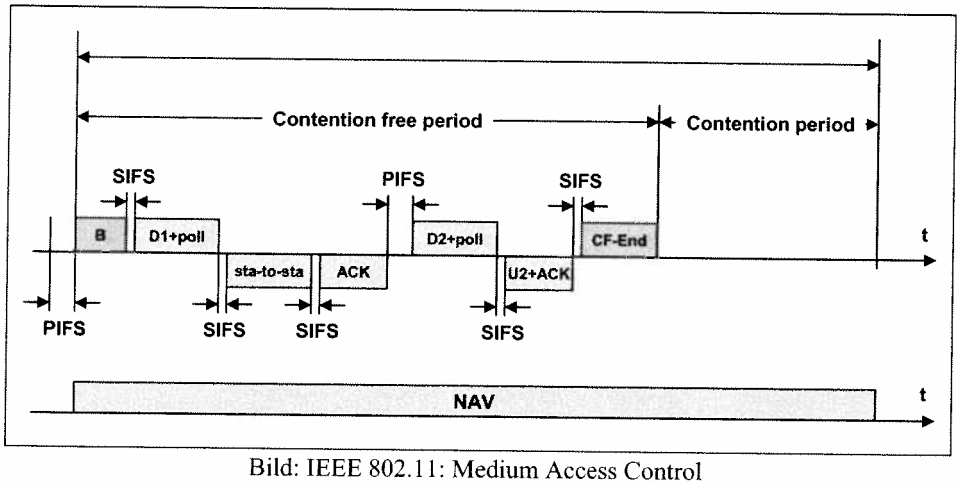


Bild: IEEE 802.11: Medium Access Control

Der Access Point leitet die CFP über die Aussendung eines so genannten Beacon-Rahmen ein, das in regelmäßigen Zeitabständen als Broadcast wiederholt ausgesendet wird. Die zeitlichen Abstände werden als Beacon-Intervall bezeichnet. Über die regelmäßige Aussendung von Beacon-Rahmen werden die Stationen, die innerhalb der Reichweite eines Access Point stehen, über Attribute der Zelle informiert.

Der Zeitabstand zwischen dem Beginn einer CFP und der darauf folgenden CFP wird als CFP-Intervall bezeichnet und stellt ein Vielfaches des Beacon-Intervalls dar. Die wichtigste Information des Beacon-Rahmen stellt für die Verwaltung des Medienzugriffs das Duration-ID-Feld dar. Über das Duration-ID-Feld wird der NAV-Wert der Stationen für die Dauer der CFP gesetzt. Dies stellt sicher, dass Stationen, die kein PCF unterstützen, während der CFP nicht auf das Medium zugreifen. Innerhalb eines CFP-Intervalls findet ein Wechsel von PCF nach CP statt, wobei sichergestellt wird, dass während der Dauer der CP mindestens ein Rahmen übertragen werden kann

Letztendlich ist die Dauer der kollisionsfreien Periode (CFP) variabel und liegt unter der Kontrolle des Access Points. Falls keine Daten mehr anstehen, die während der PCF übertragen werden sollen, kann der Access Point die CFP durch Aussendung eines CF-End-Rahmen beenden. In diesem Fall bleibt der CFP-Intervall unberührt, und die CP wird entsprechend der eingesparten Zeit verlängert. Die Stationen, die kein PCF unterstützen, setzen aufgrund des CF-End-Rahmen ihren NAV-Wert zurück und können somit versuchen, während der CP auf das Übertragungsmedium zuzugreifen.

Die Zuteilung des Übertragungsmediums erfolgt für die PCF-Stationen mittels einer Reservierung des Übertragungsmediums, die durch die Vergabe eines Senderechts vom Access Point an die mobilen Stationen erfolgt. Diesen Vorgang bezeichnet man als Polling, da der Access Point die einzelnen Stationen in seiner Zelle nacheinander abfragt, ob sie Daten zu versenden haben. Die Stationen dürfen dabei erst Daten versenden, nachdem sie vom Access Point ein CF-Poll-Rahmen erhalten

haben. Der Access Point erhält auf diese Weise die Kontrolle über das Übertragungsmedium und kann somit vermeiden, dass Kollisionen auftreten. Damit der Access Point weiß, welche Stationen er über ein Poll-Rahmen abfragen muss, geben die Stationen während ihrer Anmeldung beim Access Point bekannt, dass sie PCF unterstützen und eventuell während der CFP Daten übertragen möchten. Der Access Point trägt, basierend auf dieser Information, die PCF-Stationen in eine Polling-Liste ein. Der Access Point arbeitet während der CFP die Polling-Liste ab und schickt an die entsprechenden Stationen ein CF-Poll-Rahmen. Hat die gefragte Station Daten anstehen, die sie während der CFP übertragen möchte, so überträgt sie diese Daten.

Da DCF und PCF sich parallel einsetzen lassen, ist eine Kompatibilität zu Stationen gewährleistet, die kein PCF unterstützen. Durch die Unterstützung von PCF sind zeitkritische Anwendungen möglich, so lassen sich z. B. Sprachdaten zwischen mobilen Stationen austauschen. Natürlich muss man hierbei einkalkuliert, dass die Verzögerungen auch bei einer Datenrate von 11 Mbit/s relativ groß werden können.

Bluetooth

Bluetooth ist ein Funknetz sehr geringer Ausdehnung (Piconetz), das zum Ersatz von Kabelverbindungen zwischen Geräten wie Notebooks, Organizern, Peripheriegeräten, Mobiltelefonen dient. Bluetooth ist ein Ad-hoc-Netz und benötigt also keine eigene Infrastruktur. Mehrere Piconetze können dadurch zu einem Scatternet verbunden werden, dass ein Knoten abwechselnd Teilnehmer in mehreren Piconetzen sein kann. Jedes Piconetz nutzt eine andere Hüpfsequenz. Ein Knoten wird Teilnehmer eines Piconetzes, indem er sich auf die Hüpfsequenz dieses Netzes synchronisiert. Dabei wird die Mitgliedschaft im bisherigen Piconetz beendet. Der Knoten muss die Hüpfsequenz des Masters des Piconetzes kennen, dem er sich anschließen will.

Die **IrDA-Schnittstelle** (Infrared Data Association) wurde ebenfalls als Ersatz für Kabelverbindungen konzipiert. Auf Grund der Übertragung mit infrarotem Licht ist jedoch eine Sichtverbindung zwischen den Teilnehmein erforderlich. IrDA bietet lediglich eine Schnittstelle zwischen zwei Teilnehmern, die Distanz ist auf 2 m und die Datenrate auf 115 kbit/s begrenzt.

Bluetooth bietet Distanzen von ca. 10 m bei Datenraten von ca. 700 kbit/s. Das Konzept nutzt das lizenzfreie 2,4-GHz-Band. Es ist auf geringstmögliche Kosten (Einchip-Realisierung der Netzwerkschnittstelle) und niedrigen Energieverbrauch (Batteriebetrieb) ausgelegt. Die hochfrequente Sendeleistung beträgt maximal 100 mW.

Eine Picozelle enthält einen Master und maximal sieben Slaves. Auf der physischen Schicht wird ein Frequenzhüpfverfahren mit Zeitmultiplex zur Trennung der Übertragungsrichtungen TDD (Time Division Display) verwendet. Jeder Bluetooth-Knoten kann Master oder Slave sein. Zu jedem Zeitpunkt darf nur ein Master existieren. Der Knoten, der ein Piconetz einrichtet, wird automatisch dessen Master. Alle Knoten eines Piconetzes verwenden denselben Hüpfcode mit derselben Phasenlage. Das Frequenzhüpfverfahren liefert 1600 Frequenzwechsel pro Sekunde. Die Zeitspanne zwischen zwei Frequenzwechseln heißt Slot und dauert 625 µs. In Ländern, die eine Bandbreite von mindestens 80 MHz zulassen. werden 79 Hüpffrequenzen im Abstand von jeweils 1 MHz verwendet. Im statistischen Mittel kommen alle Frequenzen in einer Hüpfsequenz gleich häufig vor. Der Master bestimmt die Hüpfsequenz aufgrund seiner eindeutigen Kennung, so dass die Eindeutigkeit einer Hüpfsequenz garantiert ist. Somit werden Picozellen durch Codemultiplex (CDMA) entkoppelt. Innerhalb einer Picozelle steuert der Master den Medienzugriff durch Abfrage (Polling) und Reservation.

Bluetooth bietet zwei verschiedene Dienste:

- **Synchroner, verbindungsorientierter Dienst** (SCO: Synchronous Connection-Oriented Link): Für die Übertragung von Sprachsignalen reserviert der Master zwei aufeinander folgende Slots in festen Zeitintervallen.
- **Asynchroner, verbindungsloser Dienst** (ACL: Asynchronous Connectionless Link): Der Master steuert das Piconetz durch Polling.

Bluetooth kann wahlweise folgende Verbindungen betreiben:

- Ein Asynchronous Connectionless Link (ACL),
- Drei Synchronous Connection-Oriented Links (SCO),
- Ein Asynchronous Connectionless Link (ACL) und gleichzeitig ein Synchronous Connection-Oriented Link (SCO).

Jeder synchrone, verbindungsorientierte Link weist eine Datenrate von 64 kbit/s auf. Asynchrone, verbindungslose Links können symmetrisch mit bis zu 432 kbit/s und asymmetrisch mit 721 kbit/s bzw. 57 kbit/s in der Gegenrichtung konfiguriert werden. Ein Bluetooth-Rahmen wird in einem Slot gesendet. Der Access Code wird aus der eindeutigen Kennung des Masters abgeleitet und jedem Rahmen mitgegeben. Er dient auch zur Synchronisation der Slaves.

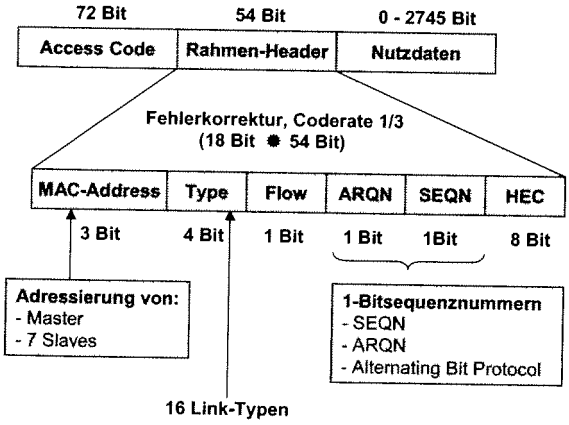


Bild: Bluetooth: Rahmenformat

Die MAC-Adresse des Headers erlaubt die Adressierung des Masters und der maximal 7 Slaves. 16 Link-Typen können unterschieden werden. Falls Quittungen erforderlich sind, werden diese im nächsten Slot im Zeitduplex (TDD) übertragen. Dafür werden 1-Bit-Sequenznummern (SEQN) und Quittungsnummern (ARQN) - das so genannte Alternating Bit Protocol - verwendet. Das HEC-Feld (Header Error Control) ist für die Fehlersicherung des Headers zuständig. Der Header wird zusätzlich mit einem fehlerkorrigierenden Code der Rate 1/3 gesichert, so dass statt 18 Headerbits insgesamt 54 übertragen werden. Für höhere Datenraten können Multi-Slot-Rahmen (bestehend aus 3 oder 5 aufeinander folgenden Slots) übertragen werden.

Für SCO-Verbindungen existieren weitere Ein-Slot-Rahmen mit unterschiedlich starker Fehlersicherung der Header. Damit kann die Übertragung an die Fehlerrate des Kanals angepasst werden. Sprachdaten über SCO werden bei Übertragungsfehlern nicht wiederholt. Stattdessen wird eine besonders robuste Art der Sprachcodierung genutzt.

IEEE 802.5: Token-Ring

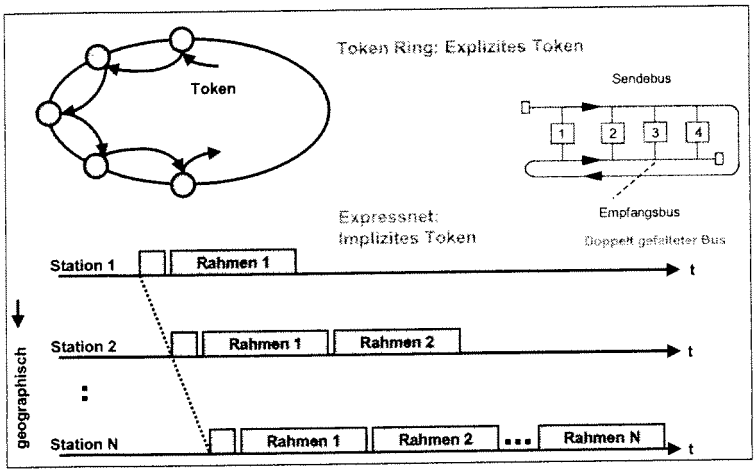


Bild: Token Passing – Explizites und Implizites Token

Token-Verfahren vergeben das Senderecht in zyklischer Reihenfolge an alle Stationen. Dabei kann das Token explizit als Bitmuster von einer Station zur nächsten weitergereicht oder ein vordefinierter Netzzustand als virtuelles Token interpretiert werden.

Aus verschiedenen Servicekonzepten (Single-, Multiple- oder Exhaustive Service) und abweichenden Zeitpunkten der Weiterleitung des Token (Single Rahmen-, Single Token- oder Multiple Token-Verfahren) resultiert für das Token-Verfahren eine Vielzahl von Protokollvarianten.

Token-Ring Mediumzugriff

Die Betriebsweise des MAC-Protokolls ist grundsätzlich unkompliziert. Wenn kein Datenverkehr vorliegt, kreist ständig ein 3-Byte-Token und wartet, dass es von einer Station dadurch übernommen wird, dass diese ein bestimmtes 0-Bit im zweiten Byte auf 1 setzt. Dieser Vorgang ändert die ersten beiden Byte in eine Rahmenstartfolge ab. Dann gibt die Station den Rest eines normalen Datenrahmens aus.

Unter normalen Bedingungen umkreist das erste Bit des Rahmens den Ring und kehrt zum Absender zurück, bevor der ganze Rahmen übertragen worden ist. Höchstens ein sehr langer Ring kann eventuell einen kleinen Rahmen als ganzen enthalten. Deshalb muss die übertragende Station den Ring leeren, während sie weitersendet. Das heißt, dass die Bits, die ihre Rundreise um den Ring beendet haben, zurückkommen und vom Absender entfernt werden.

Eine Station darf das Token höchstens für die Dauer der Token-Haltezeit behalten, die normalerweise bei 10 ms liegt, wenn nicht ein anderer Wert eingestellt wurde. Falls nach der Übertragung des ersten Rahmens noch genug Zeit bleibt, können weitere Rahmen gesendet werden. Nachdem alle anstehenden Rahmen übertragen wurden oder die Übertragung eines weiteren Rahmens die Token-Haltezeit überschreiten würde, baut die Station den 3-Byte großen Token-Rahmen wieder auf und gibt ihn auf den Ring aus.
Beim Token Ring wird zwischen zwei Stationstypen unterschieden: normale Stationen und die Monitorstation. Die Station, die sich als erste aktiv an den Ring koppelt, wird zur Monitorstation. Sie hat die besondere Aufgabe der Tokenverwaltung, d.h. sie generiert das Token, das auf dem Ring kreist.

Empfängt eine zum Senden bereite Station dieses Token, dann wandelt sie es in ein Datenrahmen um und versendet ihre Daten mit diesem Rahmen. Diese Daten werden dann von jeder Station empfangen, überprüft und falls die Daten nicht für sie bestimmt sind, regeneriert und auf dem Ring weitergeleitet. Sind die Daten an der Zielstation angelangt, werden sie von dieser Station kopiert, als kopiert gekennzeichnet und wieder auf den Ring weitergeleitet. Die Quellstation muss ihre eigenen Daten wieder entfernen sowie ein neues Token generieren und absenden. Mit diesem Verfahren hat die Quellstation eine einfache Kontrolle über die korrekte Rahmenübertragung.

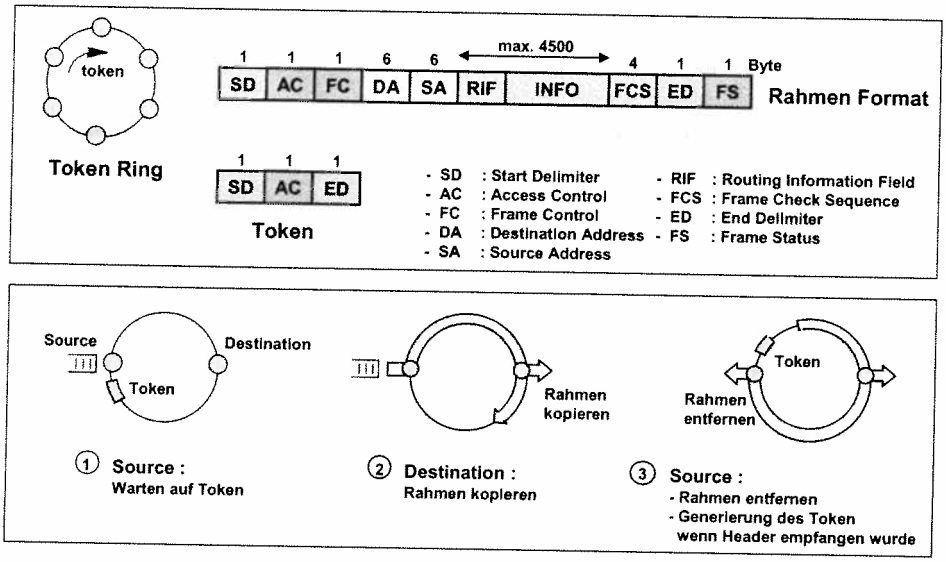


Bild: IEEE 802.5 Standard: Token Ring

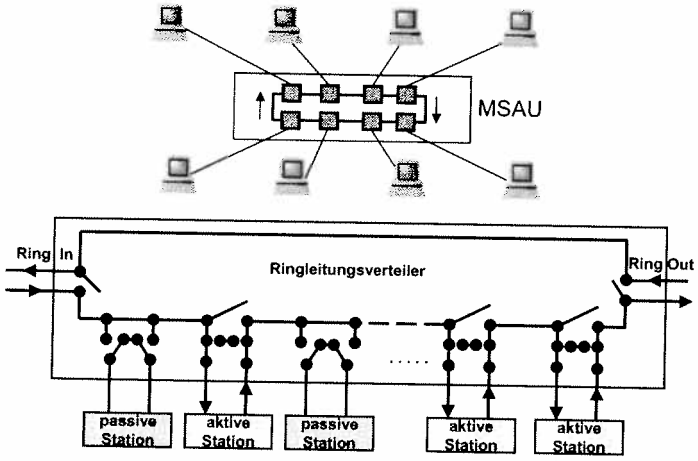


Bild: Multi-Station Access Unit (MSAU)

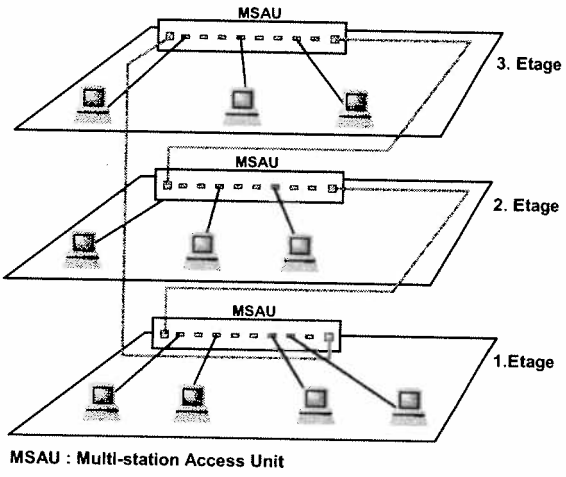


Bild: IEEE 802.5 - Gebäude-Ring

Die Topologie von Token Ring ist ein Ring mit einer teilweisen sternförmigen Verkabelungstechnik. Der Ringleitungsverteiler ist dabei die zentrale Komponente, an der die einzelnen Stationen angeschlossen werden. Der Ringleitungsverteiler wird auch oft als Ring Hub bezeichnet. Als Übertragungsmedien können entweder STP-, UTP- oder Koaxial-Kabel oder Glasfaser eingesetzt werden

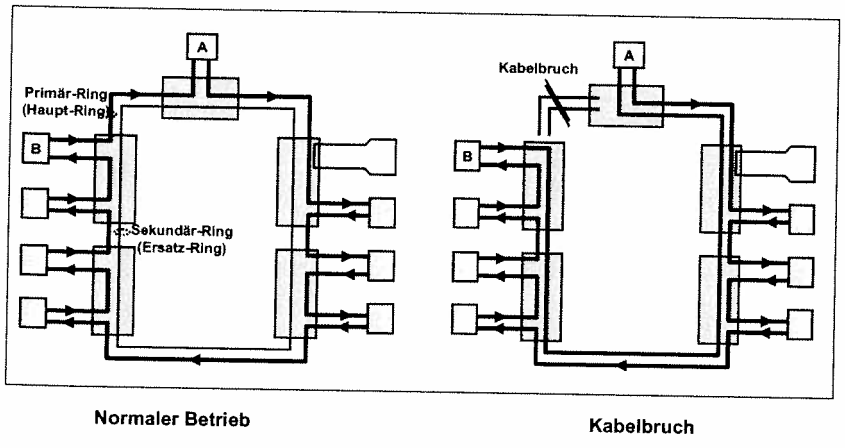
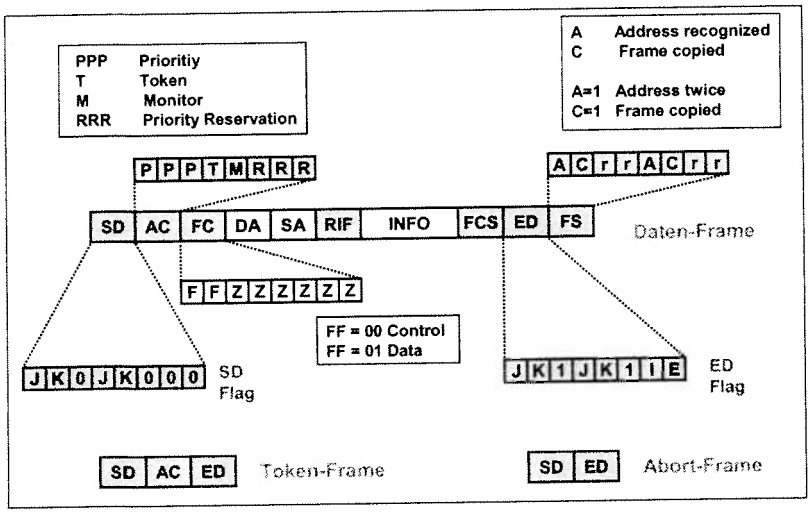


Bild: IEEE 802.5 Netztopologie

Durch die Verwendung eines Primär- und eines Sekundär-Ringes kann die Verfügbarkeit des LANs erhöht werden, d.h. bei Ausfall einer Station oder bei einem Kabelbruch umgehen die Ringverteiler die Fehlerstelle. Bei Änderung der Anzahl der angeschlossenen Stationen rekonfiguriert das LAN sich selbständig.



J, K, I, E : Spezialsymbole im Differential Manchester Code

Bild: IEEE 802.5 - MAC-Rahmen

Man unterscheidet folgende MAC-Rahmen:

- Token-Rahmen,
- Abort-Rahmen,
- Daten-Rahmen.

Ein Abort-Rahmen wird generiert, wenn eine Station ein fehlerhaftes Token oder einen sonstigen nicht behebbaren Fehler erkennt.
Der eigentliche Datenrahmen beinhaltet, wie auch der Token-Rahmen, den Starting Delimiter (SD), das Zugriffskontrollfeld (AC) und den Ending Delimiter (ED). Weiterhin werden zusätzliche Felder benötigt, um den Datenrahmen korrekt zum Empfänger zu leiten.

SD Starting Delimiter	Das erste Feld beinhaltet die Startsequenz des Rahmens mit der statische Bitkombination JK0JK000. Dadurch kann eine Präambel zur Bitsynchronisation entfallen.
AC Access Control	Das Zugriffskontrollfeld beinhaltet die Bitkombination PPPTMRRR (PPP – Zugriffspriorität, T – Token, M – Monitor, RRR – Prioritäten-Reservierung)
	Das Token wird durch das gesetzte Tokenbit (T = 1) gekennzeichnet, das bedeutet, dass als nächstes nur noch das 1 Byte große Ending Delimiter-Feld (ED) folgen kann. Ist das T-Bit nicht gesetzt, so handelt es sich um ein Datenrahmen. Mit Hilfe der P-Bits können Zugriffsprioritäten vergeben werden. Das M-Bit kann nur von der aktiven Monitorstation gesetzt werden. Die R-Bits dienen der Reservierung von Zugriffsprioritäten.
FC Frame Control	Das Rahmen-Kontrollfeld hat die Bitkombination FFZZZZZZ - FF = 00 MAC-Rahmen mit Kontrollinformationen - FF = 01 LLC-Rahmen mit Daten - Z-Bits: Kontroll-Bits für Token-Ring Protokoll und dessen Management
DA Destination Address	Entspricht dem Aufbau einer MAC-Adresse
SA Source Address	Der Aufbau der Quelladresse entspricht im wesentlichen dem Aufbau der Zieladresse, nur mit dem Unterschied, dass das Null-Bit nicht zur Unterscheidung zwischen Individual- und Gruppenadresse herangezogen wird. Wird das Null-Bit auf eins gesetzt, bedeutet das, dass sich Routing-Informationen (RIF-Feld) im Rahmen befinden.
Info Information	Das Info-Feld beinhaltet entweder Daten oder Steuerinformationen der MAC-Schicht
FCS Frame Check Sequence	Die Prüfsumme bezieht sich alle Felder bis auf das FS-Feld und das ED-Feld alle Rahmenfelder ab.
ED Ending Delimiter	Das ED-Feld beinhaltet die Bit-Kombination JK1JK1IE I-Bit (Intermediate-Bit): I = 1: Rahmen gehört zu einer Gruppe von aufeinander folgenden Rahmen I = 0: der letzte Rahmen oder einzelner Rahmen E-Bit (Error-Bit) wird gesetzt bei Erkennung eines Fehlers im Rahmen.
FS Frame Status	Das Rahmen-Statusfeld hat die Bitkombination ACrrACrr A-Bit (Address-Recognized-Bit), C-Bit (Rahmen-Copied-Bit) Die einzelnen Bits werden doppelt aufgeführt, weil das FCS-Prüffeld das FS-Feld nicht absichert. A = 1 falls eine Adresse in einem Netz doppelt vorkommt C = 1 falls eine Station die an sie adressierten Daten empfangen (kopiert) hat r-Bits für zukünftige Erweiterungen reserviert

Token Ring-Management

Die Überwachung des Token-Zugriffsverfahrens wird von einer Station im Token Ring übernommen, die als sogenannter aktiver Monitor eingesetzt wird. Die restlichen Stationen im Ring werden als Standby-Monitore (d.h. Reservemonitore) bezeichnet. Die Standby-Monitore kontrollieren die Funktionsfähigkeit des aktiven Monitors mit Hilfe spezieller Timer.

Der aktive Monitor muss:	- eine minimale Pufferkapazität im Ring sicherstellen, - ein fehlerhaftes Token oder Rahmen erkennen, - Mehrfachumkreisungen eines Rahmens verhindern, - sicherstellen, dass nur ein aktiver Monitor im Ring vorhanden ist.

Minimale Pufferkapazität

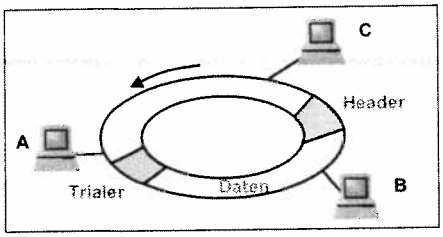
Bei Übertragungsrate von 4 Mbit/s ist ein Bit ca. 50 m lang. Weil das Token 24 Bit lang ist, müsste der Ring 1200 m lang sein. Da diese Länge in der Praxis nicht immer realisierbar ist, muss der aktive Monitor dafür sorgen, dass die Speicherfähigkeit des Ringes so groß ist wie das Token selbst, weil das Token ja die grundlegende Basis für das Token-Protokoll ist. Der Monitor stellt dazu ausreichend Pufferplatz bereit.

Es gilt: Länge des Bits = Signalausbreitungsgeschwindigkeit auf dem Medium / Bitrate

Standardmäßig wird jeder Station eine maximal mögliche Übertragungszeit von 10 ms eingeräumt. Durch die vorgegebene Übertragungszeit ergibt sich die im Token Ring maximale Rahmengröße von 4000 Byte (4 Mbit/s) bzw. 18000 Byte (16 Mbit/s). Wird nun diese zur Übertragung bereitgestellte Zeit von einer Station überschritten, so wird der Token- bzw. Daten-Rahmen von der Monitorstation als Verlust angesehen. Treten des weiteren unvorhergesehene Fehlersituationen und damit Störungen des Token oder eines Rahmens auf (z.B. durch Signalverletzungen im Medium), dann wird ein neues Frei-Token generiert. Mehrfachumkreisungen eines Rahmens, die dann zustande kommen, wenn eine Quellstation ihren Rahmen nicht vom Ring nimmt, werden vom aktiven Monitor entfernt. Hierzu setzt der Monitor das M-Bit im AC-Feld jedes Rahmens und erkennt somit, dass ein Rahmen schon zum zweiten Mal den Ring umkreist. Erhält der Monitor nun ein solcher Rahmen, bei dem das M-Bit gesetzt wurde, dann wurde dieser Rahmen nicht gelöscht. Der Monitor nimmt den Rahmen vom Ring und generiert ein neues Frei-Token.

Active Monitor Present Rahmen (AMP-Rahmen)	Mit Hilfe des Active-Monitor-Present-Rahmens, das in bestimmten Zeitintervallen vom aktiven Monitor ausgesendet wird, können die Standby-Monitore erkennen, dass immer noch ein aktiver Monitor vorhanden ist. Bleiben diese Rahmen aus, gehen die Stationen davon aus, dass der aktive Monitor nicht mehr funktionsfähig ist. Ist dies der Fall, dann wird der Claim-Prozess gestartet.
Claim-Token-Rahmen	Sollte eine Station im Ring, die nicht gerade aktiver Monitor ist, anhand Unfähigkeit eines ihrer Timer oder aufgrund fehlender AMP-Rahmen bemerken, dass der aktive Monitor nicht mehr korrekt funktioniert, beginnt sie, ein Claim-Token-Rahmen auszusenden. Nach seiner Aussendung wird das Claim-Token von Station zu Station weitergeleitet. Die einzelnen Stationen setzen als Quell-MAC-Adresse (SA-Feld) ihre eigene MAC-Adresse ein, sofern sie numerisch größer als die im Claim-Token eingetragene Adresse ist. Mit dieser Vorgehensweise wird die Station mit der numerisch größten MAC-Adresse zum neuen aktiven Monitor im Ring.
Purge-Rahmen	Zur Initialisierung des Rings wird vom aktiven Monitor ein Purge-Rahmen versendet. Dies veranlasst die Stationen, ihre Sendevorgänge abzubrechen und ihre Timer neu zu initialisieren.
SMP-Rahmen Standby Monitor Present Rahmen	Ein SMP-Rahmen (Standby Monitor Present Rahmen) wird von einem Standby-Monitor in bestimmten Zeitabständen ausgesendet. Dies dient dazu, die MAC-Adresse der Station ausfindig zu machen, die sich vor der Station befindet, welche den SMP-Rahmen aussendet. Mit der Aussendung von SMP-Rahmen kennt somit jede Station im Ring ihre Vorgängerstation. Das Wissen darüber, welche Station die Vorgängerstation ist, ist für den nachfolgend beschriebenen Beacon-Prozess besonders wichtig.
	Das SMP-Rahmen wird als Broadcast ausgesendet, d.h. jede Station schaut sich das SMP-Rahmen an. Da üblicherweise die A-Bits (Address Recognized) und C-Bits (Rahmen Copied) im Rahmen-Status Feld (FS-Feld) von den Stationen gesetzt werden, weiß die Station, die ein solches Broadcast-Rahmen mit nicht gesetztem A-Bit und C-Bit empfangen hat, dass die eingetragene Quell-MAC-Adresse die Adresse ihrer Vorgängerstation sein muss. Diese Adresse wird abgespeichert und das SMP-Rahmen neu ausgesendet, und so weiter.
Beacon-Rahmen	Der Beacon-Prozess wird nach Erkennung bzw. Lokalisierung von Netzfehlern gestartet. Fehler treten entweder in einer Station oder im Übertragungsmedium zwischen zwei Stationen A und B auf. Der Beacon-Prozess wird dann gestartet, wenn Station B innerhalb einer bestimmten Zeitspanne keinerlei Token bzw. Rahmens erhalten hat. Ist dies der Fall, nimmt Station B an, dass ein Versagen in der Vorgängerstation A oder im Übertragungsmedium dazwischen aufgetreten ist. Station B sendet daraufhin ein Beacon-Rahmen. In diesem Rahmen stehen die MAC-Adresse der Station B und die MAC-Adresse ihrer Vorgängerstation A. Die angeschlossenen Stationen, die den Beacon-Rahmen erhalten, senden diesen unverändert weiter und stoppen das Token Ring-Protokoll. Der Datentransport wird somit eingestellt und es wird innerhalb kürzester Zeit bekannt, dass zwischen Stationen A und B ein Fehler aufgetreten ist. Als mögliche Fehlerbehebungsmaßnahme wird die fehlerhafte Station vom Ring getrennt oder der Sekundär-Ring mit dem Primär-Ring verbunden, um so den einwandfreien Ablauf des Token-Ring-Protokolls bis zur Behebung des Fehlers zu gewährleisten.

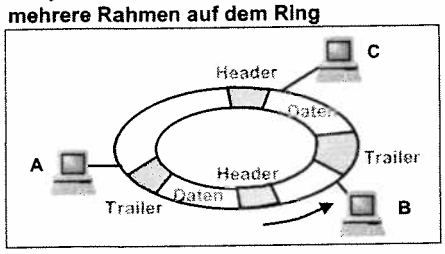
Single Token-Verfahren
nur ein Rahmen auf dem Ring



Beim 4 Mbit/s-Ring befindet sich nur jeweils ein MAC-Rahmen auf dem Ring, während beim 16 Mbit/s-Ring gleichzeitig mehrere Rahmen auf dem Ring sein können (bessere Ringauslastung).

Der Unterschied zwischen den beiden Verfahren besteht darin, wann ein neues Token generiert wird und ob mehr als ein Rahmen gleichzeitig auf dem Ring übertragen werden darf.

Early Token-Release
mehrere Rahmen auf dem Ring



Beim 16 Mbit/s-Ring spricht man vom Early Token Release. Zwischen den einzelnen Rahmen werden Idle-Zeichen (Füllzeichen) generiert. Das ganze Verfahren ist nur wirksam bei großen Netzen ab 2 km (Backbone-, Campusnetze), bei kleineren Netzen macht sich das Early-Token-Release nicht bemerkbar.

Bild: IEEE 802.5 - Tokenverfahren

Prioritäten im Token Ring

Im Token-Ring besteht die Möglichkeit, dass einzelne Stationen für Daten, die sie versenden wollen, Prioritätsstufen angeben. Diese Prioritätsstufen liegen im Bereich von 0 bis 7, wobei die 7 die höchste Priorität darstellt. Damit lässt sich die Zugriffsmöglichkeit jeder Station auf den Ring festlegen. Das bedeutet, dass eine Station nur dann auf den Ring zugreifen kann, wenn die Priorität des empfangenen Tokens kleiner oder gleich der Stationspriorität ist. Die Priorität eines Tokens wird mit Hilfe der drei P-Bits im AC-Feld des Tokens festgelegt.

Das IEEE 802.5-Protokoll enthält ausführliche Beschreibungen für die Behandlung von Rahmen mehrerer Prioritäten. Der 3-Byte große Token-Rahmen enthält ein Feld im mittleren Byte, das die Priorität des Tokens angibt. Will eine Station einen Rahmen der Priorität n übermitteln, muss sie warten, bis sie ein Token mit einer Priorität kleiner oder gleich n erlangt. Weiterhin kann eine Station versuchen, sich das nächste Token zu reservieren, indem sie in die Reservierungsbits eines passierenden Datenrahmens die Priorität des zu sendenden Rahmens einträgt. Wenn dort bereits eine höhere Priorität vorgemerkt ist, kann die Station keine Reservierung durchführen. Nach Beendigung des aktuellen Tokens wird das nächste Token mit der reservierten Priorität erstellt.

Durch diesen Vorgang wird die Reservierungspriorität immer höher geschraubt. Das Protokoll enthält mehrere komplexe Regeln, um dieses Problem zu eliminieren. Der Grundgedanke ist, dass eine Station, welche die Reservierungspriorität erhöht, dafür verantwortlich ist, die Priorität nach Erledigung auch wieder herabzusetzen.

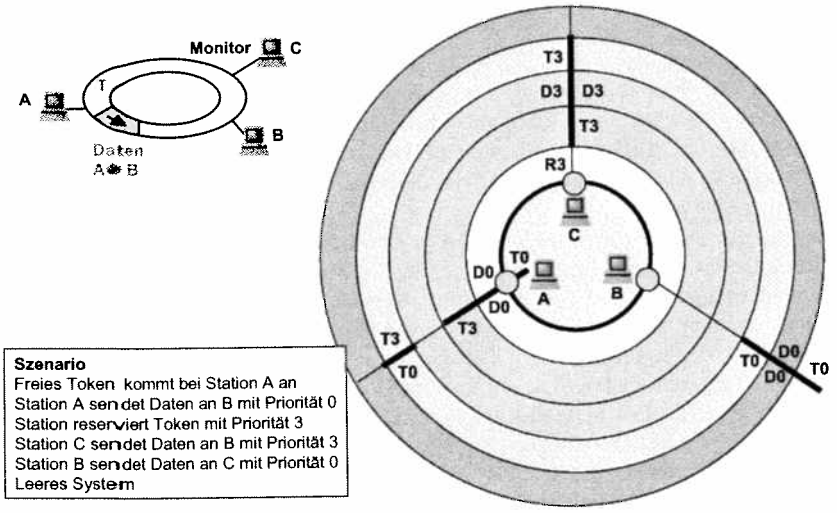


Bild: IEEE 802.5 - Prioritätsmechanismus

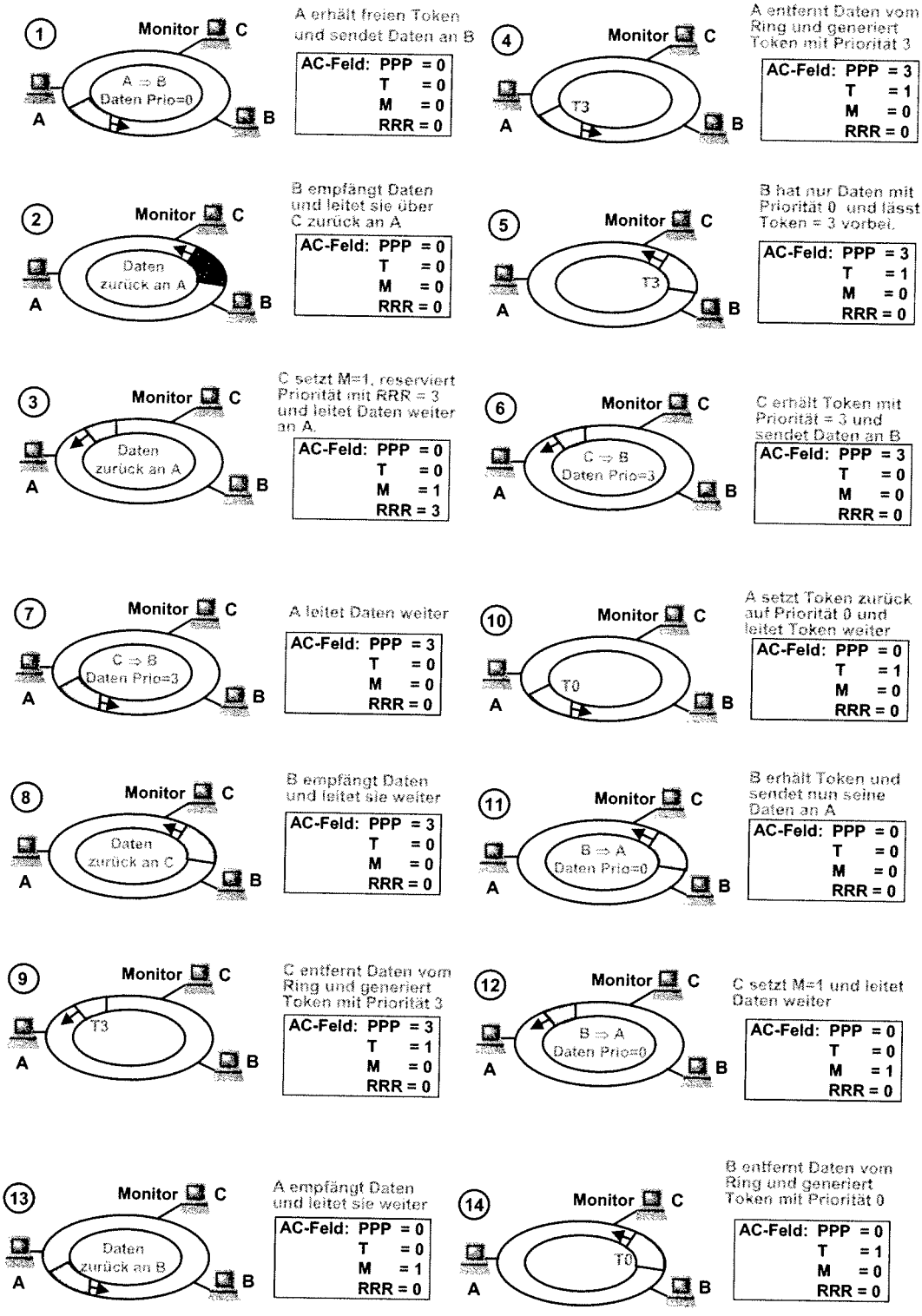


Bild: IEEE 802.5: Prioritätszugriff

Ringmanagement (Ringwartung)

Jeder Token-Ring hat eine Überwachungsstation (Monitor Station), die den ganzen Ring überblicken kann. Fällt die Überwachungsstation aus, stellt ein Konkurrenzprotokoll sicher, dass sofort irgendeine andere Station als Überwachungsstation ausgewählt wird (jede Station kann potentiell als Überwachungsstation fungieren). Solange die Überwachungsstation ordnungsgemäß funktioniert, ist sie allein dafür verantwortlich, den korrekten Betrieb des Rings zu überwachen.

Wenn der Ring gerade ausgebaut wird oder eine Station feststellt, dass keine Überwachungsstation vorhanden ist, kann ein Claim-Token-Kontrollrahmen gesendet werden. Falls dieser Rahmen den Ring ganz umkreist, bevor ein anderer Claim-Token-Kontrollrahmen gesendet wird, übernimmt der Sender die Aufgabe der Überwachungsstation (jede Station hat integrierte Überwachungsfunktionen).

Zu den Aufgaben der Überwachungsstation gehört auch, dafür zu sorgen, dass das Token nicht verloren geht, im Fall eines Ringzusammenbruchs Maßnahmen zu ergreifen, den Ring von Rahmenbruchstücken zu säubern und auf kreisende Rahmen zu achten. Solche Rahmen entstehen, wenn eine Station einen kurzen Rahmen ganz auf einen langen Ring überträgt und dann aussteigt oder ausgeschaltet wird, bevor der Rahmen wieder abgezogen wird. Wird nichts unternommen, kreist der Rahmen unendlich.

Sechs Kontrollrahmen:

Duplicate_address_test	Purge
Beacon	Active_monitor_present
Claim_Token	Standby_monitor_present

Test, ob zwei Stationen die gleiche Adresse haben, dient zum Auffinden von Brüchen im Ring Versuch, die Überwachungsstation zu werden erneute Initialisierung des Rings Periodische Ausgabe von der Überwachungsstation Ankündigung, das potentielle Überwachungsstationen vorhanden sind

Um verlorene Token aufzuspüren, besitzt die Überwachungsstation einen Timer, der auf das größtmögliche tokenlose Zeitintervall (jede Station übermittelt während der ganzen möglichen Token-Haltezeit) eingestellt ist. Wenn dieser Timer abläuft, leert die Überwachungsstation den Ring und bringt ein neues Token in Umlauf.

Tritt ein verstümmelter Rahmen auf, kann er von der Überwachungsstation durch ein ungültiges Rahmenformat oder eine falsche Prüfsumme entdeckt werden. Der Ring wird zur Entleerung geöffnet und im jetzt leeren Ring wird ein neues Token gestartet. Verwaiste Rahmen werden von der Überwachungsstation entdeckt, indem bei jedem durchlautenden Rahmen das Überwachungsbit im Byte Zugriffsteuerung gesetzt wird. Wenn bei einem ankommenden Rahmen dieses Bit bereits gesetzt ist, stimmt etwas nicht, weil dieser Rahmen dann bereits zum zweiten Mal vorbeikommt und nicht entfernt wurde; das führt dann die Überwachungsstation durch.

Eine weitere Funktion der Überwachungsstation betrifft die Länge des Rings. Das Token ist 24 Bit lang, also muss der Ring entsprechend lang sein, um 24 Bit aufzunehmen. Wenn sich die 1-Bit-Verzögerungen der Stationen und die Kabellänge zu weniger als 24 Bit summieren, fügt die Überwachungsstation weitere Bits ein, so dass das Token kreisen kann.

Eine Wartungsfunktion, die eine Überwachungsstation nicht durchführen kann, ist das Aufspüren von Unterbrechungen im Ring. Falls eine Station feststellt, dass einer seiner Nachbarn tot zu sein scheint, übermittelt sie einen Beacon-Kontrollrahmen, der die Adresse der eventuell ausgefallenen Station enthält. Hat sich der Beacon-Kontrollrahmen so weit wie möglich vorwärtsbewegt, ist ersichtlich, wie viele Stationen ausgefallen sind. Diese Stationen können durch Verwendung von Bypass-Relais aus dem Ring genommen werden.

Es muss damit gerechnet werden, dass eine Überwachungsstation durchdreht, trotzdem aber weiterhin periodisch die Steuerrahmen Active-Monitor-Present erzeugt.

Weiterentwicklungen
Der ursprüngliche Token Ring wurde durch drei Konzepte weiterentwickelt:

- **Switched Token Ring.** Sein Ansatz entspricht dem des Switched Ethernet: von jedem Port des Switch zu genau einem Teilnehmer besteht eine dedizierte Verbindung mit 16 Mbit/s. An den Ports eines Switches können Teilnehmer mit 4 Mbit/s und auch mit 16 Mbit/s angeschlossen werden, was zu einer erhöhten Flexibilität führt. Damit ist das Prinzip des gemeinsamen Mediums, wie es beim konventionellen Token Ring besteht, ergänzt durch dedicated media zwischen dem Switch und den einzelnen Teilnehmern. Mit Token Ring Switches können auch Backbones aufgebaut werden. Backbones sind Netze höherer Leistung, die einzelne Netze (Teilnetze) zu einem gesamten Netz zusammenfügen.
- **Full-Duplex Token Ring** (auch als **DTR:** Dedicated Token Ring bezeichnet). Dieser Vorschlag ist in IEEE 802.5r standardisiert. Er ist analog zum Vollduplex Ethernet und sieht auf jeder dedizierten Verbindung zwischen Switch-Port und Teilnehmer eine Vollduplex-Übertragung vor. Damit steigt die effektive Datenrate auf 32 Mbit/s.
- **HSTR** (High-Speed Token Ring), standardisiert in IEEE 802.5t. Er ist analog zum Fast-Ethernet, indem einfach die Datenrate von 16 Mbit/s auf 100 Mbit/s erhöht wird. Auf der physischen Schicht des HSTR werden die Vorgaben der physischen Schicht von Fast-Ethernet übernommen. Da Fast Ethernet durch starken Wettbewerb preisgünstig ist, kann HSTR davon profitieren.

Weitere Konzepte für den Token Ring sind in Entwicklung. Dazu gehören eine Gbit/s-Variante (IEEE 802.5v), ein Konzept zur Realisierung von VLAN (Virtual LAN) und das Konzept der Link Aggregation. Link Aggregation bedeutet die Verbindung zweier Switches durch parallele Links zur Erhöhung der Bandbreite.

IEEE 802.4: Token-Bus -Protokoll

Bei der Initialisierung des Rings werden die Stationen in der Reihenfolge ihrer Stationsadressen eingefügt, von der höchsten zur niedrigsten. Die Übergabe des Tokens erfolgt ebenfalls von oben nach unten. Jedes Mal, wenn eine Station das Token erhält, darf sie für eine bestimmte Zeitspanne Rahmen übertragen. Dann muss sie das Token weitergeben. Erhält eine Station das Token, hat aber nichts zu senden, gibt sie es sofort weiter.

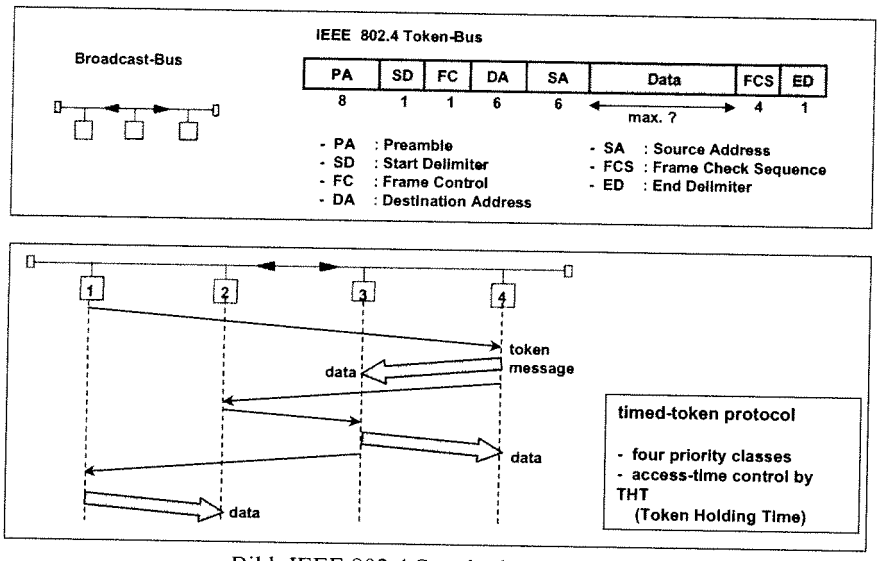


Bild: IEEE 802.4 Standard: Token Bus

Der Token-Bus definiert die vier Prioritätsklassen 0, 2, 4 und 6. Für Datenverkehr; 0 ist die niedrigste und 6 die höchste Klasse.

Am einfachsten kann man sich vorstellen, dass jede Station intern in vier Unterstationen entsprechend den vier Prioritätsklassen aufgeteilt wird.

Wenn die MAC-Teilschicht Daten schickt, werden sie auf ihre Priorität geprüft und zu einer der vier Unterstationen weitergeleitet. Dadurch enthält jede Unterstation ihre eigene Warteschlange von zu übertragenden Rahmen.

Wenn eine Station über das Kabel das Token erhält, wird es intern an die Unterstation der Priorität 6 weitergeleitet, die nun Rahmen übertragen kann, wenn welche vorhanden sind. Wenn sie fertig ist (oder der Timer abläuft), wird das Token intern an die Unterstation der Priorität 4 weitergegeben. Dieser Vorgang wird wiederholt, bis entweder die Unterstation der Priorität 0 alle eigenen Rahmen übertragen hat oder der Timer abgelaufen ist. In jedem Fall wird das Token an die nächste Station im Ring weitergegeben. Durch genaues Setzen der Timer kann ein Mindestanteil der gesamten Token-Zeit für Datenverkehr der Priorität 6 garantiert werden. Die niedrigeren Prioritäten müssen sich mit dem zufriedengeben, was übrigbleibt. Wenn die Unterstationen mit den höheren Prioritäten ihren Anteil der verfügbaren Zeit nicht brauchen, wird er nicht verschwendet, sondern kann durch die Stationen der niedrigeren Priorität verwendet werden. Dieses Prioritätsschema, das dem Datenverkehr der Priorität 6 einen festen Anteil der Netzkapazität garantiert, kann für die Übertragung von Sprache und Datenverkehr in Echtzeit benutzt werden.

Das Rahmenformat vom Token-Bus ist im Bild dargestellt. Die Präambel wird wie bei IEEE 802.3 benutzt, um den Takt des Empfängers zu synchronisieren, allerdings kann sie 1 Byte kurz sein. Die Felder Startbegrenzer und Endbegrenzer werden benutzt, um die Rahmengrenzen zu kennzeichnen. Beide Felder beinhalten analoge Codierungen, die anderen Symbolen als 0 oder I entsprechen. Folglich können sie nicht zufällig in normalen Daten vorkommen, so dass kein Längenfeld nötig ist.

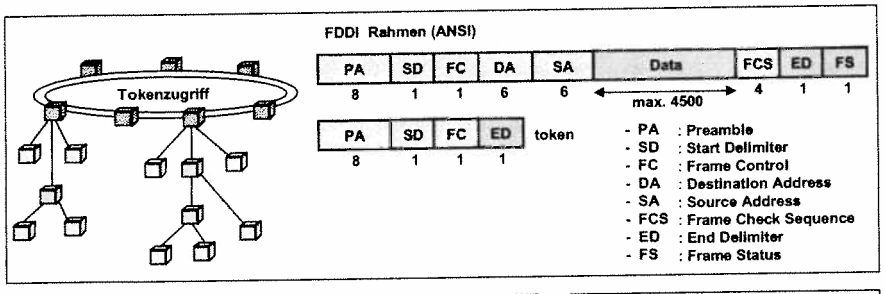
Das Feld Rahmenkontrolle unterscheidet Datenrahmen von Kontrollrahmen. Im Fall eines Datenrahmens enthält es auch noch die Rahmenpriorität. Es kann auch einen Indikator enthalten, der vom Empfänger eine Bestätigung über den korrekten oder fehlerhaften Empfang eines Rahmens fordert. Ohne diesen Indikator durfte der Empfänger nichts mehr senden, da er ja nicht über das Token verfügt.

Bei Kontrollrahmen wird durch das Feld Rahmenkontrolle die Art des Rahmens festgelegt. Darunter fallen die Tokenweitergabe und verschiedene Wartungsrahmen, die z.B. die Eingliederung neuer Stationen bewerkstelligen oder einer Station ermöglichen, den Ring zu verlassen.

Fiber Distributed Data Interface (FDDI) – ANSI Standard

Das FDDI (Fiber Distributed Data Interface) ist ein Ring-LAN mit einem gemeinsamen Übertragungsmedium von 100 Mbit/s, wobei die FDDI-Spezifikation die untersten zwei Schichten im logischen LAN-Modell betrifft. Hier ist das Übertragungsmedium, die Bitübertragung und das Zugriffsverfahren festgelegt. Für das FDDI-Management wurde die Komponente SMT (Station Management) spezifiziert.

Das FDDI ist ein rekonfigurationsfähiges LAN, so dass ein Betrieb mit reduzierter Leistung nach Ausfall einiger Komponenten oder nach einer Unterbrechung der Ringleitung garantiert werden kann. Damit ist FDDI ein fehlertolerantes LAN.



- ANSI-Standard
- 100 Mbit/s Datenrate (125 Mbit/s auf Medium)
- 4B/5B Codierung
- Physikalischer Ring mit Ring/Baum Verkabelung
- Bis zu 500 Stationen, bis zu 100 km totale Ringlänge
- Gegenläufiger Doppelring (zweiter Ring nur Redundanz)
- Zeitkontrolliertes Token-Protokoll
- Synchrone (Echtzeit) und asynchrone Verkehrsklassen
- Acht Prioritätsklassen für den asynchronen Verkehr

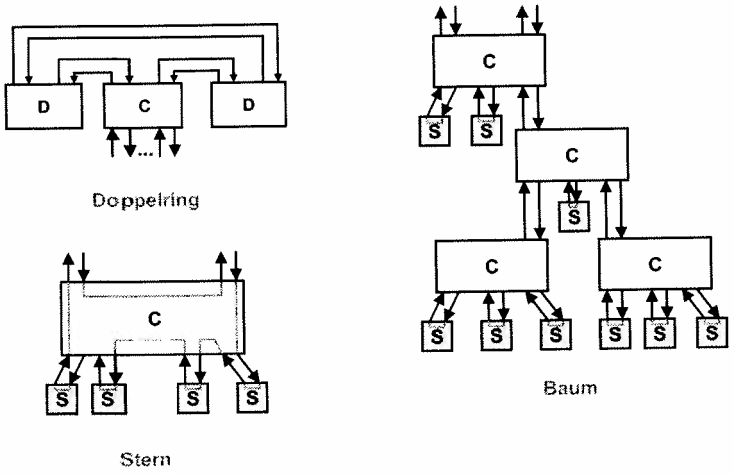
Zeitkontrolliertes Token-Protokoll

Zugriff kontrolliert durch
- **THT**
  (Token Hoding Time)
- **TTRT**
  (Target Token Rotation Time)

FDDI spezifiziert eine Netztopologie, die in einen Ringbereich (Trunk) und einen Baumbereich (Tree) zerfällt.

Der Ringbereich besteht aus einem gegenläufigen Glasfaser-Doppelring (Primär- und Sekundärring), an dem die FDDI-Stationen angeschlossen sind. Zwischen den Stationen existiert jeweils eine Punkt-zu-Punkt-Verbindung. Falls das Netz fehlerfrei arbeitet, wird nur der Primärring für die Datenübertragung genutzt, der Sekundärring dient als Backup-Medium im Störungsfall (z.B. Glasfaser-Unterbrechung).

Bild: Fiber Distributed Data Interface (FDDI)



FDDI-Stationstypen

In FDDI werden vier Stationstypen definiert:

- DAS: Doppelanschluss-Station
  (Dual Attached Station)
- SAS: Einzelanschluss-Station
  (Single Attached Station)
- DAC: Doppelanschluss-Konzentrator
  (Dual Attached Concentrator)
- SAC: Einzelanschluss-Konzentrator
  (Single Attached Concentrator)

Bild: FDDI: Netztopologien

Stationstypen

- **Doppelanschlusstation, DAS (Dual Attachment Station)**
- **Einzelanschlusstation, SAS (Single Attachment Station)**
- **Doppelanschlusskonzentrator, DAC (Dual Attachment Concentrator)**
- **Einzelanschlusskonzentrator, SAC (Single Attachment Concentrator)**

Porttypen

- **Port A und Port B für den Anschluss an den Doppelring**
- **Port M für die Eröffnung eines Baumbereiches;**
- **Port S für den Anschluss an einen Konzentrator.**

Bild: Stations- und Porttypen

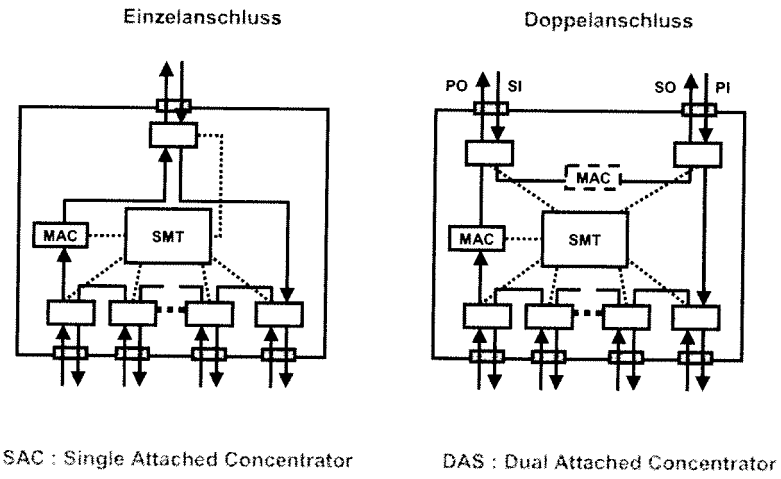


Bild: FDDI: Konzentratortypen

- **Synchroner Verkehr**
  Länge und Häufigkeit von synchronen Rahmen werden im Claim-Prozess ausgehandelt
- **Asynchroner Verkehr**
  Zeitabstände zwischen Sendevorgängen sind unbestimmt
  - **Restricted**
    nur für zwei Stationen zugänglich, z.B. für schnellen Dateitransfer
  - **Non-Restricted**
    für alle stationen zugänglich, bietet 8 Prioritätsstufen.

Bild: FDDI: Verkehrsarten

- **TRT (Token Rotation Time)**
  - Jede Station misst die aktuelle Rotationszeit des Tokens
- **TTRT (Target Token Rotation Time)**
  - Die Sollzeit für eine Token-Umlauf; sie wird im Claim-Prozess ausgehandelt
- **THT (Token Holding Time)**
  - Maximale Zeit, die ein Token zum Senden asynchroner Daten gehalten werden darf
    - THT = TTRT - TRT
- **LC (Late Counter)**
  - Erfasst, ob ein Token später als TTRT angekommen ist;
  - bei Wiederholung (d.h. LC = 2) wird der Claim-Prozess gestartet.

Bild: FDDI Mediumzugriffsparameter

MAC-Frame-Typen:

- Token-Rahmen zur dezentralen Erteilung der Sendeberechtigung,
- Daten-Rahmen zur Datenübertragung,
- Claim-Rahmen zur Festlegung der sog. Target Token Rotation Time (TTRT) in der sogenannten Bidding-Phase und zur Erstellung des logischen Ringes (Ringinitialisierungs-Phase),
- Beacon-Rahmen für die Ringüberwachung.

Wie beim Token Ring darf eine Station nur dann senden, wenn sie sich im Besitz des Token befindet.

Es gibt aber einige Besonderheiten, wie:

- Die Sendezeit in jeder Station ist variabel und ist durch den Parameter THT (Token Holding Time) bestimmt.
- Der maximale THT-Wert ist begrenzt.
- Innerhalb der THT-Zeit kann eine Station mehrere MAC-Rahmen senden.
- Die maximale Rahmenlänge ist auf 4500 Bytes festgelegt.

Hat eine Station Daten zum Senden, so wartet sie auf das Token. Kommt das Token an die sendebereite Station an, erhält sie mit dem Eintreffen des Tokens die Sendeberechtigung. Sie nimmt das Token vom Ring und sendet ihre Rahmen. Unmittelbar nach dem Aussenden des letzten Rahmens reicht die sendeberechtigte Station das Token an ihre Nachbarstation weiter. Das direkte Absenden des Token nach allen Rahmen ist ein wesentliches Merkmal des FDDI-Zugriffsverfahrens und wird als Early Token Release bezeichnet. Damit besteht die Möglichkeit, mehrere Rahmen von verschiedenen Stationen auf dem Ring

gleichzeitig zu übertragen, wodurch der Ring bei starkem Datenverkehr voll belegt (ausgelastet) sein kann. Die Zielstation (MAC-Zieladresse) erkennt ihre eigene MAC-Adresse, kopiert ihre Rahmen und leitet sie weiter. Die Quellstation (MAC-Quelladresse) erkennt schließlich ihre eigene MAC-Adresse im Rahmen wieder und ist damit verpflichtet den MAC-Rahmen vom Ring zu nehmen. Stationen, die nicht sendeberechtigt sind, prüfen die vorbeilaufenden Rahmen auf Fehler, die im FS-Feld eingetragen werden können und leiten sie auf den Ring weiter

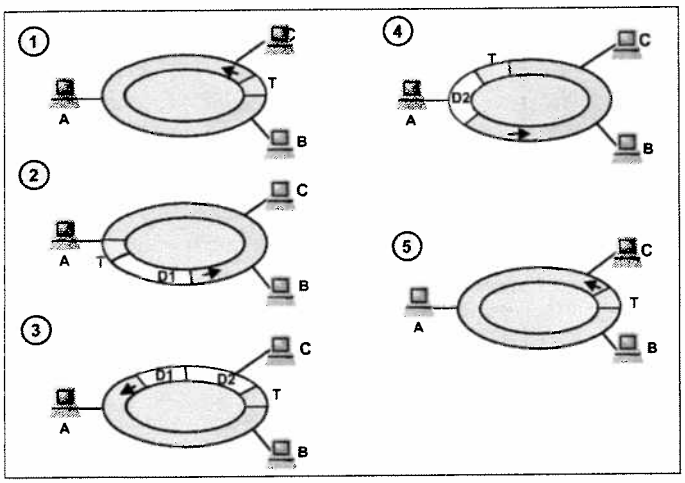


Bild: FDDI Mediumzugriffsmechanismus

Hat eine Station Daten zum Senden, so wartet sie auf das Token.

Kommt das Token an die sendebereite Station an, erhält sie mit dem Eintreffen des Token die Sendeberechtigung.

Sie nimmt das Token vom Ring und sendet ihre Rahmen. Unmittelbar nach dem Aussenden der letzten Rahmen reicht die sendeberechtigte Station das Token an ihre Nachbarstation weiter.

Das direkte Absenden des Token nach den Rahmen ist ein wesentliches Merkmal des Zugriffsverfahrens und wird als Early Token Release bezeichnet.

Damit besteht die Möglichkeit, mehrere Rahmen von verschiedenen Stationen auf dem Ring gleichzeitig zu übertragen, wodurch der Ring bei starkem Rahmen-Verkehr voll belegt (ausgelastet) sein kann. Die Zielstation (MAC-Zieladresse) erkennt ihre eigene MAC-Adresse, kopiert ihre Rahmen und leitet sie weiter. Die Quellstation (MAC-Quelladresse) erkennt schließlich ihre eigene MAC-Adresse im Frame wieder und ist damit verpflichtet den MAC-Rahmen vom Ring zu nehmen. Stationen, die nicht sendeberechtigt sind, prüfen die vorbeilaufenden Rahmen auf Fehler, die im FS-Feld eingetragen werden können und leiten sie auf den Ring weiter.

Synchroner und asynchroner Verkehr

Im FDDI darf jede Station nur dann senden, wenn sie im Besitz des Token ist. Grundsätzlich sind dann zwei Arten des Rahmen-Verkehrs möglich:

- synchroner Verkehr,
- asynchroner Verkehr.

Nach dem FDDI-Zugriffsverfahren kann mit Hilfe des Claim-Prozesses zwischen den Stationen ausgehandelt werden, dass einige Stationen das Token in quasi konstanten Zeitabständen erhalten, um ihre Rahmen senden zu dürfen. Beim asynchronen Verkehr gibt es keine Vereinbarungen hinsichtlich der Token-Rotation, so dass die Stationen eine zufällige Zeit auf das Token warten müssen, um ihre Rahmen senden zu dürfen. Die Zeitabstände, die sich hierbei zwischen den von einer Station gesendeten Rahmen ergeben, sind unbestimmt, so dass man vom asynchronen Verkehr spricht. Die im synchronen Verkehr gesendeten Daten werden im folgenden als Synchron-Daten (SD) bezeichnet. Die in Form von asynchronen Rahmengesendeten Daten werden Asynchron-Daten genannt

Die Unterstützung des synchronen Verkehrs bietet den Stationen eine garantierte Übertragungskapazität in quasi konstanten Zeitabständen. Dadurch ist es im FDDI auch möglich, andere Informationsarten, wie z.B. bewegte Bilder oder sogar - im eingeschränkten Maße - Sprache zu übertragen. Wird der synchrone Verkehr unterstützt, müssen synchrone Rahmen von einer Station in quasi konstanten Zeitabschnitten gesendet werden. Um dies zu garantieren, muss die Übertragungskapazität des Ringes für diesen Verkehr fest reserviert werden. Der verbleibende Rest der Übertragungskapazität kann erst nach dem Token-Verfahren für den asynchronen Verkehr ausgenutzt werden.

Beim asynchronen Verkehr werden zwei weitere Dienste (Services) unterschieden:

Nonrestricted (Priority) Service	Der Nonrestricted Service, auch Priority Service genannt, ist für alle FDDI-Stationen zugänglich. Jede Station hat acht Parameter, (THT-Pr(k), k=1...8), in denen die maximale Zeit für den Umlauf eines Token steht, in der es einem Frame mit der Priorität (k) erlaubt wird übertragen zu werden.
Restricted Token Service	Der Restricted Token Service ist nur für zwei Stationen zugänglich. Sie ist z.B. geeignet für die Abwicklung eines schnellen Filetransfers.

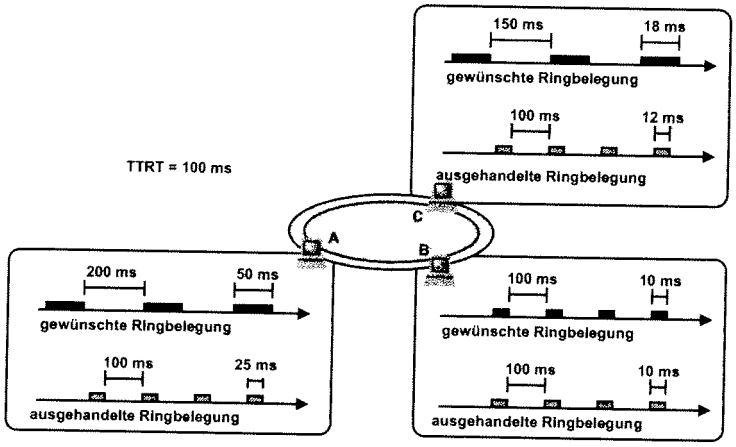


Bild: FDDI Claim-Prozess

Der synchrone Verkehr auf dem FDDI-Ring wird mit Hilfe des Claim-Prozesses unterstützt. Das Zugriffsverfahren bei diesem Verkehr wird auch als Timed-Token-Protocol bezeichnet.

Um den synchronen Verkehr zu realisieren, müssen zwei Parameter zwischen den am synchronen Verkehr beteiligten Stationen ausgehandelt werden, d.h.:

- In welchen Zeitabständen werden die synchronen Rahmen gesendet?
- Wie groß dürfen die zu sendenden synchronen Rahmen sein?

Der Zeitabstand zwischen den Zeitpunkten, zu denen die synchronen Rahmen gesendet werden dürfen, stellt der Parameter TTRT dar. Dessen Wert wird zwischen den am synchronen Verkehr beteiligten Stationen mit Hilfe des Claim-Prozesses in seiner sogenannten Bidding-Phase ausgehandelt. Der Claim-Prozess wird im Bild veranschaulicht. Hier sind drei Stationen am synchronen Verkehr beteiligt. Sie wollen ihre Daten in bestimmten Zeitintervallen senden. Das Zeitintervall einer Station wird im FDDI-Standard durch die Variable T-Bid repräsentiert.
Folgende Sendewünsche existieren:

- Station A: alle 200 ms - Daten über 50 ms,
- Station B: alle 150 ms - Daten über 18 ms,
- Station C: alle 100 ms - Daten über 10 ms,

Nach dem Claim-Prozess wird eine Kompromisslösung gefunden, nach der alle Stationen das Senderecht alle 100 ms erhalten. Der Wert 100 ms ist der kleinste Wert von allen gewünschten Zeitabständen. Dies bedeutet, dass die Stationen, die ihre Daten in größeren Zeitabständen senden wollten, ihre Daten häufiger (alle 100 ms) und in kleineren Portionen senden müssen. Auf diese Art und Weise ist es möglich, dass alle Stationen, die ihre Rahmen synchron (d.h. in konstanten Zeitintervallen) senden wollen, das Token in konstanten Zeitabständen erhalten. Sie müssen ihr Datenvolumen dementsprechend auf die einzelnen Rahmen aufteilen.
Jede Station sendet einen Claim-Rahmen aus, in dessen Datenfeld die von dieser Station gewünschte Token-Umlaufzeit TTRT (Target Token Rotation Time) eingetragen ist, d.h. das gewünschte Zeitintervall bis zur Wiederkehr der Sendeberechtigung. Die Periode, wie lange eine Station ihre Synchrondaten senden kann, wird als Synchronous Allocation (SA) bezeichnet. Bei der Zuweisung von SAs muss die folgende Bedingung erfüllt werden:

$$\sum_i SA_i + D_{max} + F_{max} + T \leq TTRT$$

wobei

SA_i:	Synchronous Allocation für die Station i,
D_{max}:	Signalumlaufzeit im Ring mit maximaler Länge,
F_{max}:	Übertragungszeit des längsten Rahmens (ca. 4500 Bytes),
T:	Token-Übertragungszeit.

Jede Station die einen Claim-Rahmen empfängt, vergleicht die TTRT-Angabe mit der selbst angeforderten TTRT. Bei diesem Vergleich werden zwei Fälle unterschieden:

- Empfangene TTRT < eigene angeforderte TTRT ▸ eigene TTRT durch die empfangene TTRT ersetzen.
- Empfangene TTRT > eigene angeforderte TTRT ▸ empfangene TTRT durch die eigene TTRT ersetzen.

In beiden Fällen wird anschließend das Claim-Frame an die nachfolgende Station weitergeleitet.

Bei der Beendigung des Claim-Prozesses befindet sich nur noch ein Claim-Frame mit der kürzesten TTRT auf dem Ring. Jede Station im Ring kann nun davon ausgehen, dass in diesem Frame der ausgehandelte TTRT-Wert steht, mit dem alle Stationen einverstanden sind. Dieser TTRT-Wert wird als Ringparameter TTRT in jeder Station gespeichert und als niedrigster Wert der Token-Umlaufzeit in den Token Rotation Timer (TRT) jeder FDDI-Station kopiert.

Der Parameter TTRT ist also die vergangene Zeit, in der eine Umkreisung des Token erfolgt sein soll. Bei dem Umlauf können zwei Fälle auftreten:

- Das Senderecht am synchronen Verkehr wird von einigen Stationen nicht wahrgenommen.

- Das Senderecht am synchronen Verkehr wird von allen Stationen wahrgenommen.

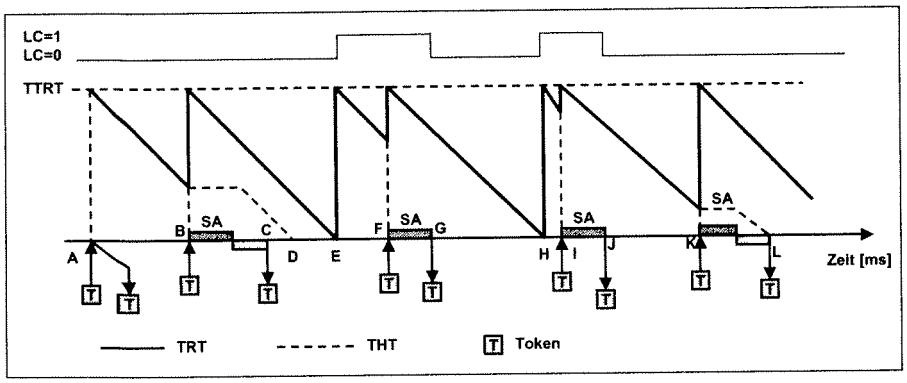
Wenn das Senderecht von einigen Stationen nicht wahrgenommen wird, dann kehrt das Token zu einer Station zurück, bevor der Wert in TTRT erreicht ist.
Wenn alle Stationen ihr Senderecht am synchronen Verkehr wahrnehmen, kann das Token erst nach dem Ankauf von T-Opr zu einer Station zurückkehren. Man kann beweisen, dass die Rückkehr des Token innerhalb der Zeitperiode 2*T-Opr garantiert wird.

Ablauf des Zugriffsverfahrens
Für die Realisierung des Zugriffsverfahren für den synchronen und asynchronen Frame-Verkehr sind folgende Parameter in jeder FDDI-Station vorhanden:

- TRT (Token Rotation Time): Token-Rotationszeit
- THT (Token Holding Time): Token-Haltezeit
- LC (Late Counter): Token-Verspätungsanzeige

Mit dem **TRT-Parameter** misst jede Station für sich die aktuelle Token-Rotationszeit. Das ist die Zeit zwischen dem Absenden und dem Wiederkehren des Token. Diese Zeit ändert sich bei jedem Tokenumlauf und ist davon abhängig, wieviele Stationen das Senderecht wahrgenommen haben. Der minimale TRT-Wert ergibt sich, falls keine Station beim Tokenumlauf das Senderecht wahrgenommen hat. In diesem Fall ist die Zeit TRT die Signalumlaufzeit auf dem Ring. Diese Zeit ist für jede FDDI-Konfiguration in der Näherung konstant und wird als Ringlatenz RL (Ring Latency) bezeichnet. Die Ringlatenz hängt von der Ringlänge und der Anzahl von aktiven Stationen ab und beeinflusst die FDDI-Performance.

- Der **Parameter THT** gibt an, wie lange das Token für das Senden von Asynchron-Daten gehalten werden darf. Die THT-Zeit wird definiert als THT = TTRT – TRT.
- Der **TTRT-Wert (Target Token Rotation Time)** wird nach der Claim-Prozedur ermittelt. Die TTRT-Zeit ist als Tokenrotations-Sollzeit zu interpretieren.
- Der **Parameter LC** dient als eine Markierung für den Zustand, ob das Token später als erwartet angekommen ist, d.h. ob das Token nach dem Ablauf der TTRT-Zeit angekommen ist. Kommt das Token nach der TTRT-Zeit an, wird LC = 1 gesetzt, d.h. das Token ist verspätet (late). Wiederholt sich die Situation, wird LC = 2 gesetzt und der Claim-Prozess gestartet, um die Ursache für die Verspätung festzustellen.



SA : synchronous Allocation
LC : Late Counter
Bild: Zugriff für asynchrone Daten (SA: Synchronous Allocation, LC: Late Counter)

Die Aktionen zu den markierten Zeitpunkten sind:

- **Zeitpunkt A.** Nach der Token-Ankunft wurde der Parameter TRT mit seinem Anfangswert TTRT initialisiert (TRT:= TTRT). Es liegt kein Sendewunsch vor; das Token wird unmittelbar an die Nachbarstation weitergegeben. Der Parameter TRT als Timer wird zurückgezählt.
- **Zeitpunkt B.** Nach der Token-Ankunft wurde modifiziert: THT := TRT und TRT := TTRT. Das Senderecht der Station wird in Anspruch genommen. Zunächst sendet sie ihre Synchrondaten innerhalb der ihr zugewiesenen Zeit SA (Synchronous Allocation). Während dieser Zeit wird der THT nicht zurückgezählt. Nach der Zeit SA steht der Station noch die Zeit THT für das Senden von Asynchron-Daten zur Verfügung. Die Asynchron-Daten wurden abgeschickt und das Token wird weitergegeben. Zu diesem Zeitpunkt wurde die zur Verfügung stehende THT-Zeit für den asynchronen Frame-Verkehr nicht voll ausgenutzt. Die THT-Zeit geht zu dem Zeitpunkt D zu Ende.
- **Zeitpunkt E.** Die Token-Rotation-Sollzeit. TTRT ist abgelaufen und das Token ist während dieser Periode nicht eingetroffen. Es ist verspätet, so dass dieser Zustand mit der Variable LC=1 markiert wird.

- **Zeitpunkt F.** Nach der Token-Ankunft wurde modifiziert: THT:= TRT und TRT := TTRT. Das Senderecht der Station wird in Anspruch genommen. Sie sendet ihre Synchron-Daten innerhalb der ihr zugewiesenen Zeit SA. Nach der Übertragung von Synchron-Daten wurde die Variable LC in den Zustand Null gesetzt.
- **Zeitpunkt K.** Hier wird die THT-Zeit voll für die Übertragung von Asynchron-Daten ausgenutzt.

Es ist ersichtlich, dass die Synchron-Daten höhere Priorität besitzen. Liegen sie zum Senden vor, so werden sie immer nach der Token-Ankunft gesendet. Die Asynchron-Daten können nur dann anschließend gesendet werden, wenn das Token nicht verspätet angekommen ist, d.h. wenn beim Eintreffen des Token LC = 0 war.

Zusammenstellung von einigen MAC-Formaten in LANs

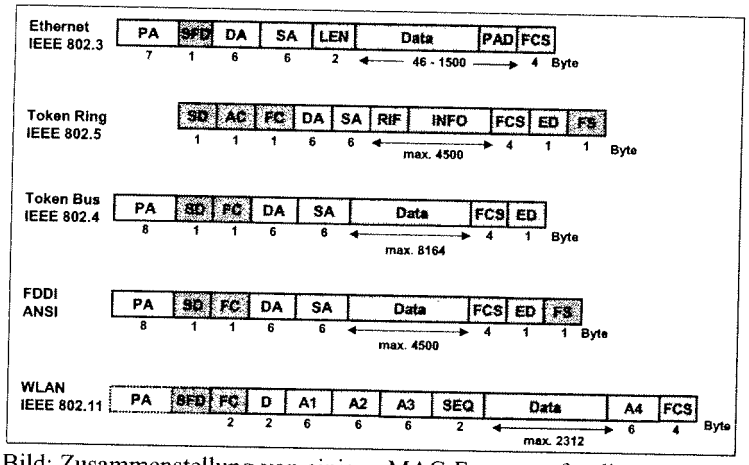


Bild: Zusammenstellung von einigen MAC-Formaten für diverse LANs

Reservierungs-, Scheduling- und Creditverfahren

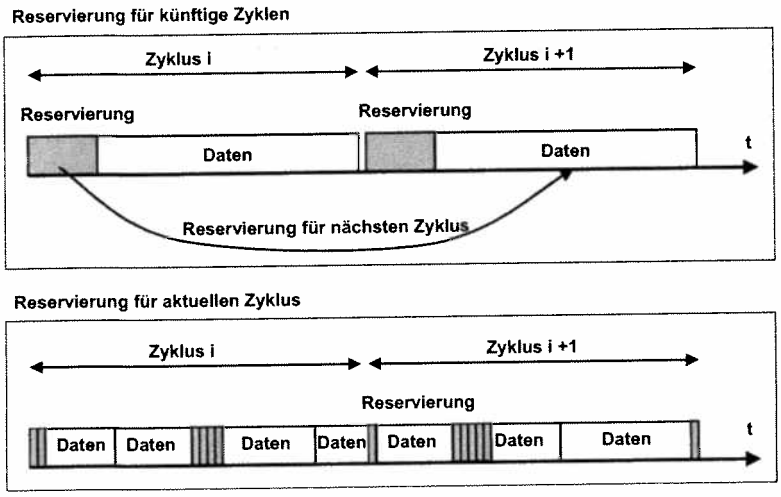


Bild: Reservierungsverfahren

Reservierungs-, Scheduling- und Creditverfahren haben gemein, dass sie jeder Station pro Protokollzyklus eine gewisse Sendekapazität garantieren. Bei Reservierungsverfahren zerfällt ein Zyklus in eine Reservierungsphase, nach deren Abschluss jede aktive Station die ihr zugewiesene Übertragungskapazität kennt, und die sich anschließende Sendephase. Dagegen sind die Zuteilungs- und Sendephase bei den Schedulingverfahren zeitlich verschachtelt, und die Kapazitätszuteilung erfolgt parallel zum Sendevorgang auf der Basis der aktuell beantragten und der bisher genutzten Sendekapazität.
Bei den Reservierungs- und Schedulingverfahren wird sendebereiten Stationen auf Antrag eine feste Kapazität zugewiesen. Beide Verfahren unterscheiden sich in der zeitlichen Folge der Zuteilungs- und Sendephasen.

Quotenbasierte Protokolle (Creditverfahren)
Bei den Creditverfahren stellt der Credit eine obere Schranke für die nutzbare Kapazität pro Zyklus dar. Dieser wird entweder global, wenn alle sendebereiten Stationen ihren Credit verbraucht haben, oder lokal durch ein ständig zirkulierendes Kontrollsignal erneuert. Der Medienzugriff auf einem getakteten Lokalen Netz wird von einigen Protokollen nach der Analyse des Verkehrsflusses des letzten Protokollzyklus durch die Reservierung von Übertragungskapazitäten für benachteiligte Stationen bzw. durch die kurzzeitige Blockierung dominanter Stationen geregelt. Alternativ gibt es weitere Verfahren, die für eine Medienzugriffskontrolle in lokalen hochbitratigen Netzen zur Regelung der asynchronen Datenübertragung zur Standardisierung vorgeschlagen worden sind. Zusätzlich wird ein weiteres Zugriffsprotokoll erwähnt, das ein gleichmäßiges Sendeverhalten der Stationen bewirken soll. Die Algorithmen unterscheiden sich im wesentlichen in ihren Mechanismen zur Festsetzung der Quoten und der Erkennung eines neuen Protokollzyklus.

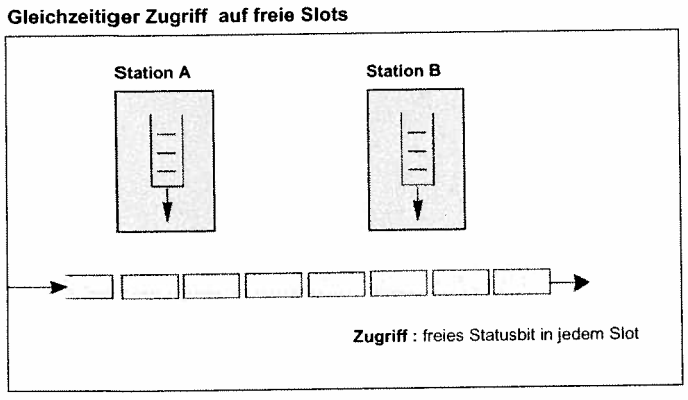


Bild: Zugriff bei getaktetem Ring

In einem **getakteten Ring** kreisen Slots fester Länge auf dem Medium. Jeder Slot führt Kontrolldaten mit sich, aus denen u.a. seine Ziel- und Absenderadresse, sein Typ und sein Zustand (frei / belegt) ersichtlich sind. Eine sendebereite Station erhält die Zugriffsberechtigung, wenn sie einen freien Slot empfängt und das MAC-Protokoll dessen Belegung gestattet.

In Abhängigkeit davon, wie viele Slots jede Station gleichzeitig nutzen darf und ob der Sender oder der Empfänger einen Slot nach erfolgreicher Übertragung wieder freigibt, entsteht eine Vielzahl von Protokollvarianten.

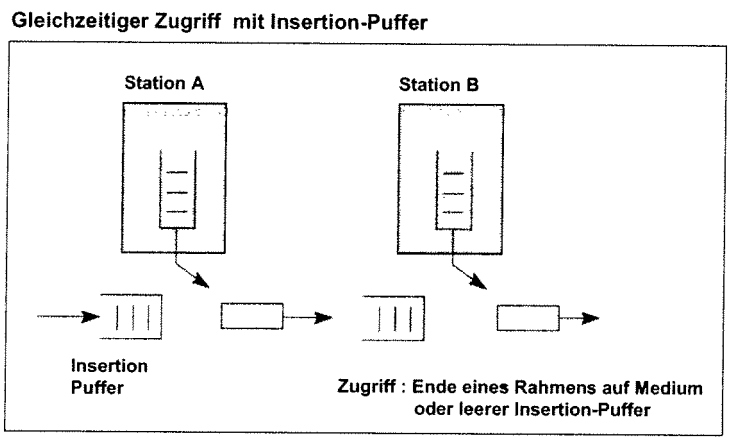


Bild: Zugriff mit Insertion Buffer

Wie beim getakteten Ring kann beim **Buffer Insertion-Ring** eine sendebereite Station das als frei erkannte Medium direkt nutzen. Dabei ist die Übertragungskapazität nicht notwendigerweise in feste Slots aufgeteilt. Pakete von variabler Länge, die nur durch ein protokollspezifisches Maximum begrenzt sind, können gesendet werden. Während des Sendevorganges werden ankommende Daten von ringaufwärts gelegenen Stationen in einem in Datenpfad installierten Schieberegister (Insertion Buffer) zwischengepuffert und erst am Ende des Sendevorganges weitergeleitet. Startet eine Station ihre Übertragung immer erst dann, wenn ihr Insertion Buffer genug Pufferkapazität zur Aufnahme eines Pakets maximaler Länge hat, können auf dem Ring keine Daten verloren gehen.

Je nach Einsatzumgebung und unterliegender Topologie zeigen die aufgeführten Zugriffsmechanismen unterschiedliche Leistungsmerkmale. Um entscheiden zu können, welche Modifikationen und Kombinationen ihren Einsatz auch in lokalen hochbitratigen Netzen ermöglichen, muss erst nach den Anforderungen an solche Systeme gefragt werden.

Getakteter Ring (Slotted Ring) mit dem ATMR-Zugriffsmechanismus

Die Medienzugriffskontrolle nach dem Prinzip des ATM-Rings basiert auf einem verteilt arbeitenden Quoten- oder Creditverfahren und einem Reset-Mechanismus. Das Quotenverfahren übernimmt die Kontrolle des quotierten Zugriffs der einzelnen Stationen. Jede Station darf pro Zyklus maximal die durch die Quote vorgegebene Kapazität des Mediums belegen. Läuft ihre Quote aus, so wird eine Station inaktiv. Der letzte noch aktive Stationen initiiert nach Ablauf ihrer eigenen Quote einen Reset, mit dem die anderen Stationen aktiviert und deren Quoten erneuert werden (Reset-Mechanismus). Der Zeitraum zwischen zwei aufeinanderfolgenden Resets wird als Reset-Periode bezeichnet. Die Dauer dieser Periode ist abhängig sowohl von der Größe der Quote für jede Station als auch von der aktuellen Lastverteilung auf dem Ring. Die Zugriffkontrolle läuft auf beiden Ringen unabhängig ab.

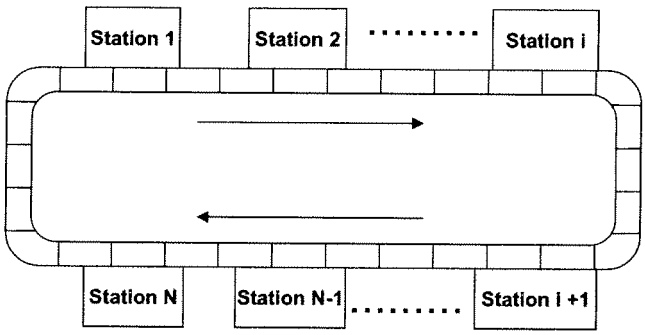


Bild: Getakteter Ring mit Zugriffsmechanismus

Getakteter Ring mit Zugriffsmechanismus

- Zeitschlitzstruktur auf dem Ring,
- Asynchrone Zuordnung der Zeitschlitze nach einem fairen Zugriffsmechanismus (ATMR-Mechanismus)

Der Reset-Mechanismus

Das Ende des aktuellen Protokollzyklus kann mit einem verteilten Kontrollmechanismus wie folgt erkannt werden. Jede noch aktive Station schreibt seine Adresse als sogenannte busy-Adresse in jeden passierenden Zeitschlitz. Inaktive Stationen lassen die Zeitschlitze dagegen unverändert. Empfängt eine Station einen Zeitschlitz mit der eigenen busy-Adresse, erkennt er, dass alle anderen Stationen zu dem Zeitpunkt, zu dem der Zeitschlitz sie passiert hat, inaktiv waren. Diese Station sendet dann, sobald er selbst inaktiv wird, eine Reset-Meldung aus und geht in den sogenannten Hunting-Zustand über. Auch an Stationen, die zwischenzeitlich durch die Ankunft neuer sendebereiter Daten wieder aktiv geworden sind, wird mit der Ankunft der Reset-Meldung die Quote neu initialisiert, womit diese Stationen einen gewissen Kapazitätsverlust hinnehmen müssen. Andererseits kann es wegen der nicht vernachlässigbaren Ringlatenz auch vorkommen, dass mehrere Stationen nahezu gleichzeitig das Ende des Protokollzyklus erkennen und ein Reset-Meldung generieren. Dieser Konflikt wird dadurch gelöst, dass eine Station im Hunting-Zustand ein bei ihr ankommende Reset-Meldung, unabhängig davon, ob es das von ihr gesendet ist, vom Ring entfernt und den Hunting-Zustand wieder verlässt.

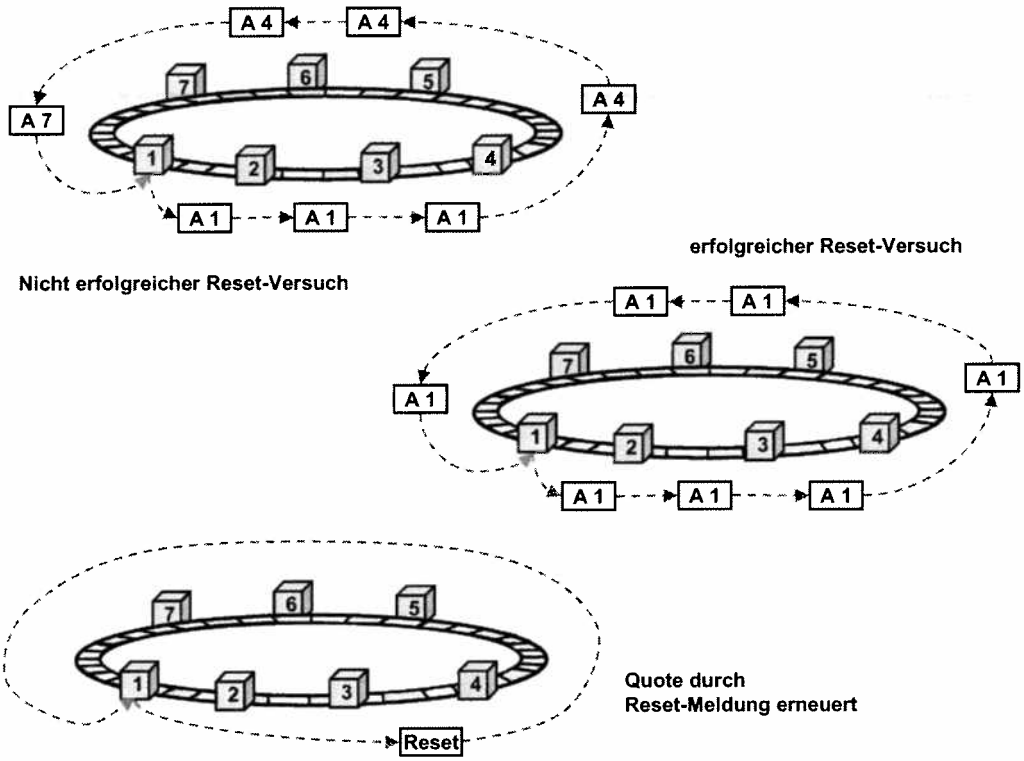


Bild: Reset Mechanismus

ISDN : Integrated Services Digital Network

Das heutige ISDN (Integrated Services Digital Network) ist aus Anwendersicht ein Schmalband-ISDN (S-ISDN) zur Integration verschiedener Kommunikationsdienste in einem einzigen Netz. Während in der Vergangenheit für die unterschiedlichen Dienste wie Datenübertragung, Telefonie usw. in der Regel getrennte Kommunikationsnetze erforderlich waren, unterstützt bereits das Schmalband-ISDN alle Kommunikationsarten. Nachdem sich das Schmalband-ISDN in vielen Länder schon flächendeckend etabliert hat, ist nun auch das Breitband-ISDN (B-ISDN), d.h. ATM (Asynchronous Transfer Mode, Asynchroner Transfer Modus) als ein universelles, alle Dienste integrierendes Breitband-Netz eingeführt worden. Das B-ISDN löst die bestehende Telekommunikations- und Datenverarbeitungs-Infrastruktur in naher Zukunft nicht ab, sondern sie eine sinnvolle Ergänzung. Heute wird unter der Bezeichnung NGN (Next Generation Network) auch das Internet bzw. die IP-Netze zur Integration von Diensten (Services) umgestaltet.

ISDN-Basisanschluss

Der Basisanschluss stellt zwei Nutzkanäle mit je 64 kbit/s in beide Richtungen zur Verfügung. Für eine Telefonverbindung an einem ISDN-Basisanschluss ist pro Übertragungsrichtung ein B-Kanal notwendig, da aber an einem Basisanschluss in jeder Übertragungsrichtung zwei B-Kanäle bereitgestellt werden, können je Basisanschluss zwei gleichzeitige und unabhängige Kommunikationen unterhalten werden.

Der Teilnehmeranschluss ist meist als Bus ausgeführt, an dem mehrere Einrichtungen angeschaltet werden können. Der Anschluss erfolgt über die international genormte S_0-Schnittstelle. Die Nutzkanäle sind nicht bestimmten Endeinrichtungen oder Diensten zugeordnet, sondern werden erst nach Bedarf einer bestimmten Endeinrichtung zugeteilt. Die Signalisierungsinformationen werden in einem getrennten 16 bit/s-Kanal, dem D-Kanal, übertragen. Der Zugriff auf den D-Kanal erfolgt von allen Endeinrichtungen aus in Konkurrenz zueinander, gleichzeitige Übertragungs-Anforderungen werden nacheinander behandelt.

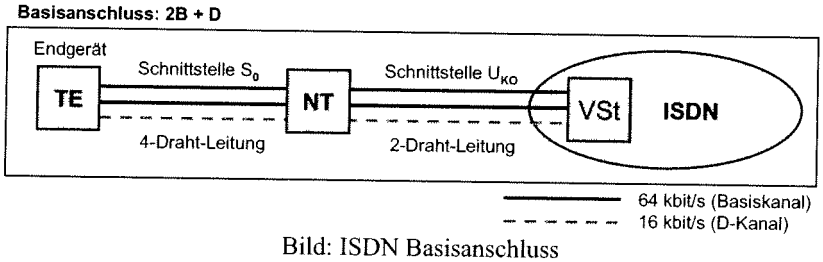


Bild: ISDN Basisanschluss

Basisanschluss
(Basic Access)
2 x B + D = 2 x 64 kbit/s + 16 kbit/s
= 144 kbit/s (mit Overhead: 192 kbit/s)

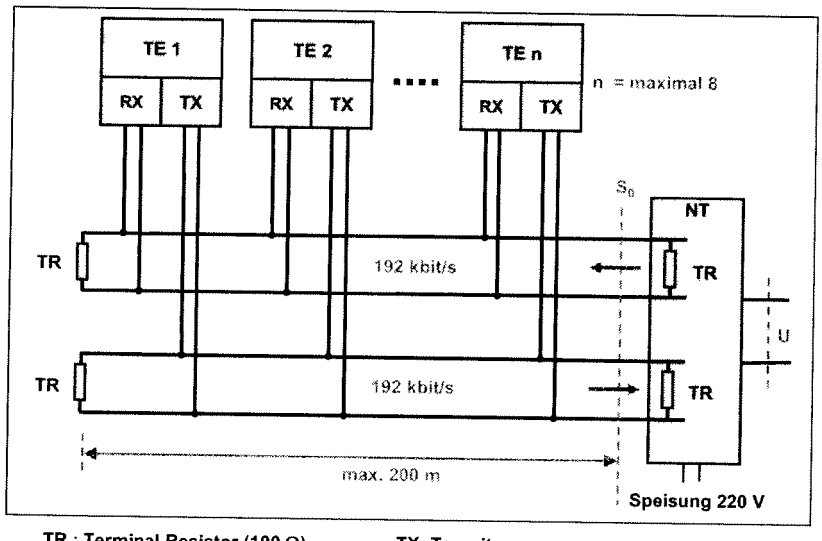


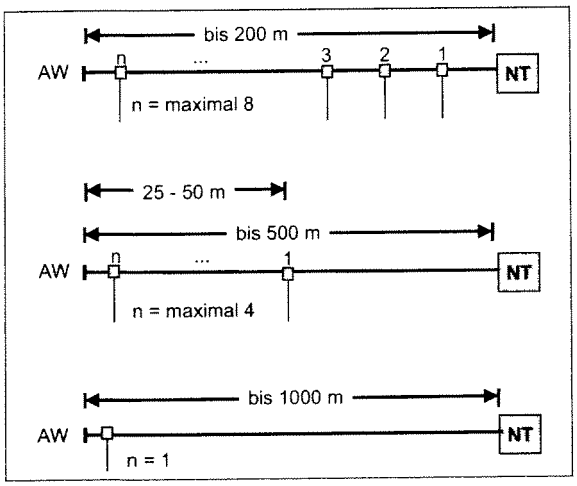
Bild: ISDN Basisanschluss: S_0-Bus-Konfiguration

S_0-Bus und der Zugriffsmechanismus

Die S_0-Schnittstelle befindet sich im Bereich der Installation beim Teilnehmer zwischen NT (Network Termination) und TE (Terminal Equipment).

Die S_0-Schnittstelle ist eine 4-drähtige Schnittstelle, die sowohl als Bus, mit maximal 8 angeschlossenen TE, als auch als Punkt-zu-Punkt-Verbindung eingesetzt werden kann.
Das Vierdraht-Verfahren ermöglicht die Verwendung eines einfachen Übertragungsverfahrens.

Die S_0-Schnittstelle ist ein Bus, an dem maximal 8 Endgeräte angeschlossen werden können. Der Anschluss der Endgeräte erfolgt über kurze (< 10 m) Verbindungskabel. Die Benutzung des für alle Endgeräte gemeinsamen D-Kanals steuert ein standardisierter Buszugriffsmechanismus: CSMA/CA Verfahren (Carrier Sense Multiple Access with Collision Avoidance)



AW: Abschluss-Widerstand

Bild: Basisanschluss-Konfigurationen

Bei längeren S_0-Buskonfiguration können weniger Endgeräte angeschlossen werden.

Der Rahmenaufbau an der S_0-Schnittstelle besteht aus 48 Bits alle 250 µs. Die Lage des Rahmens wird durch die F-Bits gekennzeichnet. Das Rahmenkennungswort ist durch eine Codeverletzung des AMI-Codes mit zwei aufeinanderfolgenden Pulsen gleicher Polarität dargestellt. Die Hilfsbits F_A und N dienen der sicheren Synchronisation auch bei einer Adernvertauschung durch eine zweite Coderegelverletzung mit maximalem Abstand zum Rahmenkennungswort.

Zur Sicherung der Gleichstromfreiheit je Rahmen ist ein Ausgleichsbit L vorhanden, das die Anzahl der Pulse je Rahmen auf eine gerade Zahl ergänzt. Je einem B-Kanalwort von 8 Bit ist ein D Kanalbit zugeordnet.

Um ein Endgerät die rechtzeitige Prüfung zu ermöglichen, ob der Empfänger des NT das gesendete D-Bit empfangen hat und kein weiteres Gerät im D-Kanal gleichzeitig sendet, wird jedes empfangene D-Bit vom NT sofort im E-Kanal zu den Endgeräten als Echo-Signal zurückgeschickt. Damit wird sichergestellt, dass nur ein Endgerät eine D-Kanalmeldung absetzt. Bei Kollisionen muss das Endgerät, das die Kollision feststellt, seine Aktivitäten beenden.

Nutzbitrate:	144 kbit/s (64 + 64 + 16 kbit/s)
Schrittgeschwindigkeit:	192 kbit/s (48 kbit/s Overhead)
Rahmenlänge:	48 Bit in 250 msec
Rahmenfrequenz:	4 KHz (2 x 125 µs)
Schnittstellencode:	AMI
Rahmenkennung:	2 Bit mit Codeverletzung
Rahmenaufbau:	48 ternäre Schritte B- und D-Daten unverwürfelt
Sendeamplitude:	U_{S0}=750 mV
Pegelzuordnung:	log. "0": Pegel (750 mV) log. "1": Pegel (0 V)
Leitungsabschluss:	100Ω ± 5%
Dämpfung auf der Schnittstelle:	≤ 6 dB bei 96 KHz
max. Umlaufverzögerung:	2,7 µs (Bus)
Reichweite:	150 m (Bus) 1500 m (Punkt-zu-Punkt)
Fernspeisung von NT:	40 V+5% /-15%
Fernspeiseleistung:	Normalbetrieb: ≤ 4 W
Notbetrieb:	≤ 410 mW

Bild: Eigenschaften der S_0-Schnittstelle

Die Übertragung von Signalen erfolgt durch die Zuordnung: eine binäre "0" wird durch abwechselndes Potential +0,75 V bzw. -0,75 V codiert, eine binäre "1" erhält keinen Pegel, also 0 V.

Die elektrischen Eigenschaften des Schnittstellensenders sind so ausgelegt, dass ein gesendeter Pegel gegenüber keinem Pegel dominiert.

Ein Ende darf erst dann im D-Kanal senden, wenn es zuvor eine seiner Priorität sprechenden Anzahl von binären "1"-Schritten (kein Pegel) im Zugriffszähler festgestellt hat. Es muss aber seine Sendung sofort, d.h. vor dem Senden des nächsten D-Bits abbrechen, sobald es im D-Echokanal (E-Bit) ein anderes als das von ihm gesendeten Bit festgestellt hat.

Rahmenaufbau an der S_0-Schnittstelle

Rahmen enthält 48 Bit:	16 Bit	B1-Kanal
	16 Bit	B2-Kanal
	4 Bit	D-Kanal
	12 Bit	Synchronisation
12 Bits Synchronisation	2 Bit	Rahmenbits F, F_A - F_A: zusätzliches Rahmenbit (binär 0)
	4 Bit	D-Echokanal E in der Richtung vom NT zum TE
	1 Bit	Aktivierungsbit A
	1 Bit	Multi-Rahmenkennungsbit M
	1 Bit	Ausgleichsbit L
	1 Bit	N-Bit (binär 1)
	1 Bit	Füllbit S (binär 0)

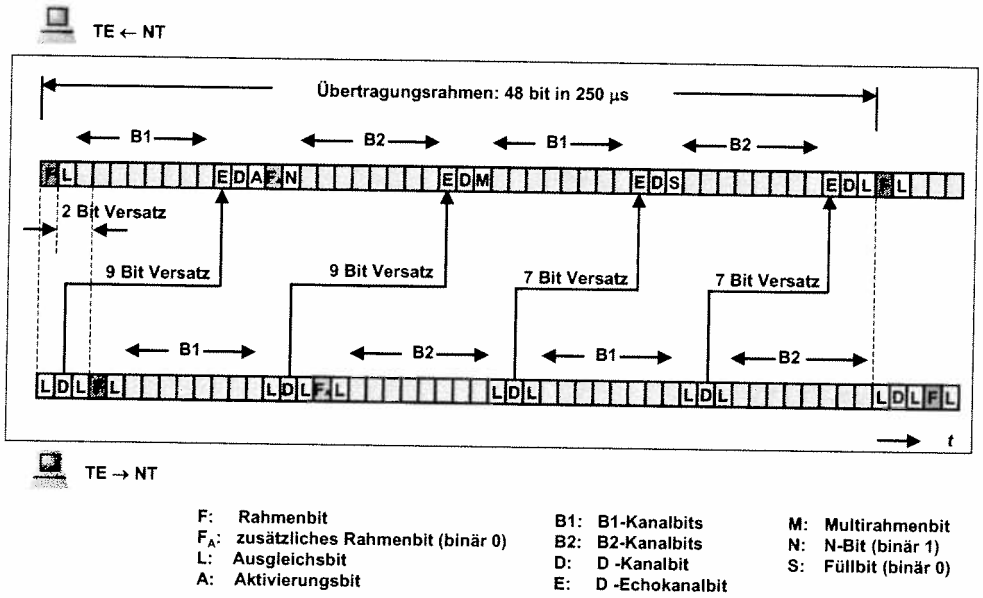


Bild: Rahmenstruktur der S_0-Schnittstelle

Der S_0-Bus sendet im Ruhezustand eine Folge von binären l-Schritten. Eine Information auf dem S_0-Bus unterscheidet sich vom Ruhezustand dadurch, dass auch binäre "0"-Schritte auftreten. Im D-Kanalprotokoll wird sichergestellt, dass nicht mehr als sechs aufeinanderfolgende 1-Schritte auftreten, bevor wieder mindestens ein 0-Schritt folgt. Damit ein Ruhezustand vom Informationszustand unterschieden werden kann, muss eine Folge von mindestens sieben binären l-Schritt erkannt werden.

Entsprechend wird die Priorität eines Endgerätes als eine Folge von mehr als sechs binären 1-Schritten gekennzeichnet, die ein Endgerät erkennen muss, bevor es auf den D-Kanal zugreifen darf. Ein Telefongerät z.B. die Priorität mit acht binären 1-Schritten, ein Datenendgerät von zehn binären 1-Schritten. Das Endgerät mit der geringeren Anzahl der detektierenden binären 1-Schritten hat eine höhere Priorität als ein Endgerät, welches mehr Schritte erkennen muss.

Würde ein Telefongerät mit einem Datenendgerät gleichzeitig um den z.B. freien D-Kanal konkurrieren, dann würde das Telefongerät bereits nach acht 1-Schritten einen Rahmen senden dürfen, während das Datenendgerät noch den Ruhezustand des D-Kanals prüft. Mit dem Senden eines Rahmens durch das Telefongerät, wird zunächst entsprechend dem D-Kanalprotokoll ein Flag mit dem Bitmuster 01111110 ausgesendet. Dadurch wird beim Datenendgerät als neuntes Bit statt der erwarteten "1" die "0" aus dem Flag des Telefongerätes im E-Kanal erscheinend worauf das Datenendgerät seine Aktivitäten einstellt.

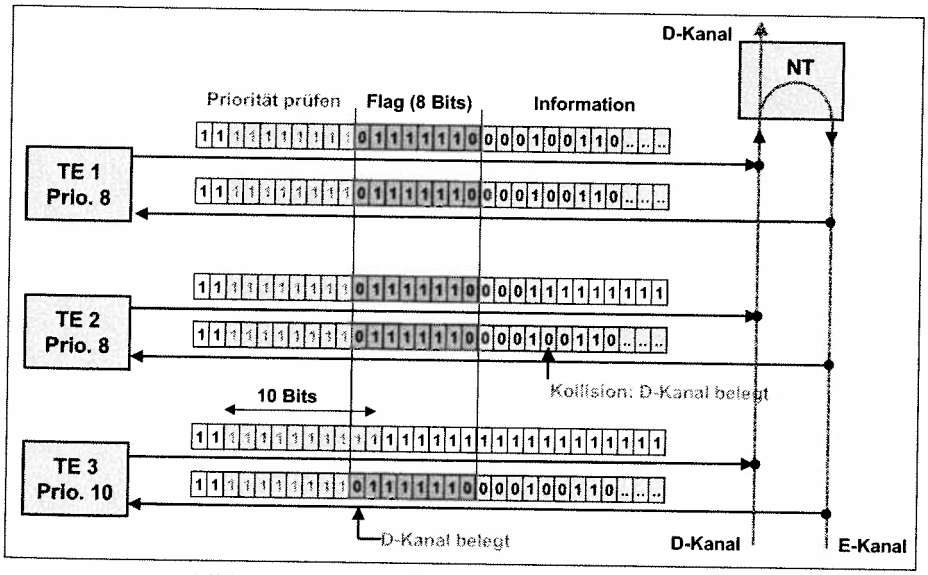


Bild: ISDN: D-Kanal Zugriffsprotokoll (CSMA/CA)

Drei Endgeräte TE 1, TE 2 und TE 3 greifen zeitlich synchron auf den freien D-Kanal zu, um eine Information auszusenden.

Die Endgeräte TE 1 und TE 2 haben die Priorität 8, das Endgerät TE 3 besitzt die Prioritat 10.

Für TE 1 und TE 2 gibt es zunächst keine Unterschiede. Beide Geräte erkennen entsprechend ihrer Priorität für eine Folge von acht binären 1-Schritten den Ruhezustand und dürfen damit auf den D-Kanal zugreifen und werden zunächst ein Flag aussenden. Das Endgerät TE 3 muss entsprechend seiner Priorität zehn binäre 1-Schritte erkennen; dies kann es nicht, da auf dem E-Kanal mit dem neunten Bit die binäre "0" des Flags von den Endgeräten TE 1 bzw. TE 2 erscheint. Das TE 3 erkennt, dass der D-Kanal belegt ist und bricht den Zugriff auf den D-Kanal ab.

Die beiden Endgeräte TE1 und TE 2 arbeiten synchron weiter, bis ein Bit in der auszusendenden Information differiert. Das TE 1 sendet als viertes Informationsbit eine binäre "0" während das TE 2 eine binäre "1" aussendet.

Der binäre 0-Schritt setzt sich gegenüber dem binären 1-Schritt auf dem Bus durch. Das Endgerät TE 2 erkennt eine Kollision und muss seinen Sender ausschalten, während da Endgerät TE 1 weitersenden darf.

Zwei Endgeräte können solange gleichzeitig am D-Kanal senden, wie sie dieselbe Bitfolge ausgeben. Sendet ein Gerät eine binäre "1" und das anders eine binäre "0", dann stellt das Endgerät, das die binäre "1" gesendet hat, im E-Kanal eine binäre "0" fest und muss seinen Sendebetrieb stoppen.

Ein Endgerät das seine Information erfolgreich im D-Kanal aussenden konnte, wird seine Priorität erniedrigen, um anderen Endgeräten am Bus eine höhere Zugriffswahrscheinlichkeit im Gleichzeitigkeitsfall einzuräumen. Greift es beim nächsten Zugriff auf den Bus mit der niedrigeren Priorität erfolgreich zu, kann es seine Priorität wieder erhöhen.

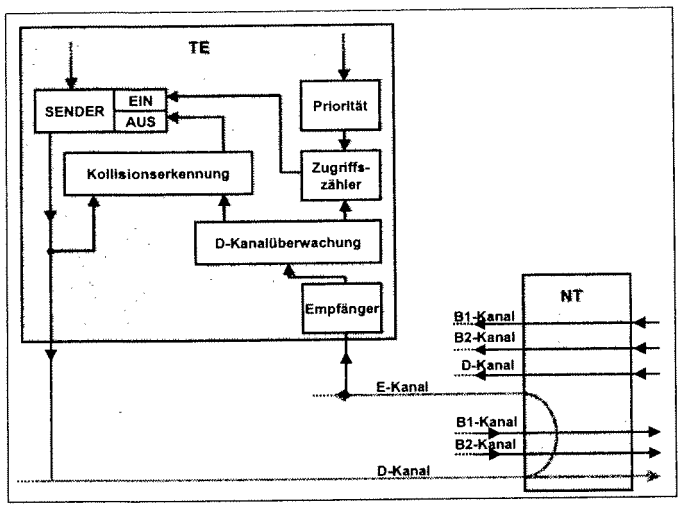


Bild: Buszugriffssteuerung am Basisanschluss

2.2b OSI-Referenzmodell: Schicht 2 – HDLC, LLC, D-Kanal, D_m-Kanal

Dez. 2003

Inhalt:
- Aufgaben und Funktionen
- HDLC (LAPB)

Varianten:
LLC (LANs), D-Kanal (ISDN), D_m-Kanal (GSM), LAPF (Frame Relay), LAPM (Modems)

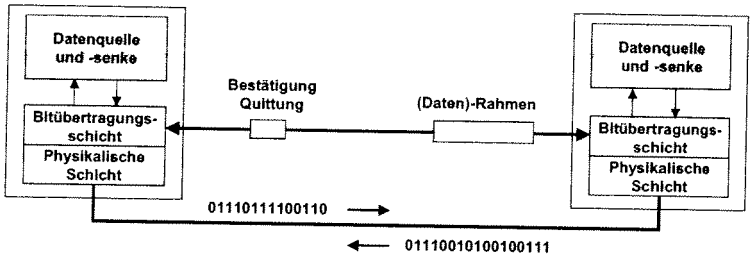


Bild: High-Level Data Link Control

Die Standards dieser Schicht leisten entweder eine zeichenorientierte oder eine bitorientierte Übertragung. Das heute zentrale Protokoll ist **HDLC** (High Level Data Link Control). Dies ist ein sehr flexibles, bitorientiertes Protokoll, das auf bestimmte Anwendungsfälle hin spezialisiert werden kann und mehrere Protokollvarianten hervorgebracht hat:

- **LAPB** (Link Access Procedure for Balanced Mode) wird im Paketvermittlungsnetz X.25 eingesetzt.
- **LAPF** (Link Access Procedure for Frame Relay) wird im Paketvermittlungsnetz FR eingesetzt.
- **LLC** (Logical Link Control) wird in lokalen Netzen verwendet.
- **LAPD** (Link Access Procedure for D-Channels) wird im D-Kanal (Signalisierung) von ISDN genutzt.
- **LAPD$_m$** (Link Access Procedure for D-Channels, Modified) wird im D_m-Kanal (Signalisierung) von GSM genutzt.
- **LAPM** (Link Access Procedure for Modems) wird bei Modemverbindungen eingesetzt.

Unterscheidung
Leitstation, Folgestation, Hybridstation

Zwei verschiedene Konfigurationen des Übertragungsabschnittes
- Unsymmetrisch
- Symmetrisch

Drei Modi für Datenübertragung
- Aufforderungsbetrieb (Normal Response Mode, NRM)
- Spontanbetrieb (Asynchronous Response Mode, ARM)
- Gleichberechtigter Spontanbetrieb (Asynchronous Balanced Mode, ABM)

Bild: HDLC – High-Level Data Link Control

Die Schicht 2 realisiert eine fehlerfreie Punkt-zu-Punkt-Übertragung ganzer Rahmen zwischen benachbarten Stationen. Dabei können entweder zwei Stationen **direkt** miteinander oder mehrere Stationen über ein **Bussystem** verbunden sein. Das Bussystem wirkt als **Broadcastnetz,** d. h. jede Station kann das Signal jeder anderen Station direkt, ohne das Durchlaufen von zwischengeschalteten Systemen empfangen.

Unterschieden wird nach:
- Stationstyp,
- Verbindungskonfiguration,
- Datenübertragungsbetriebsart.

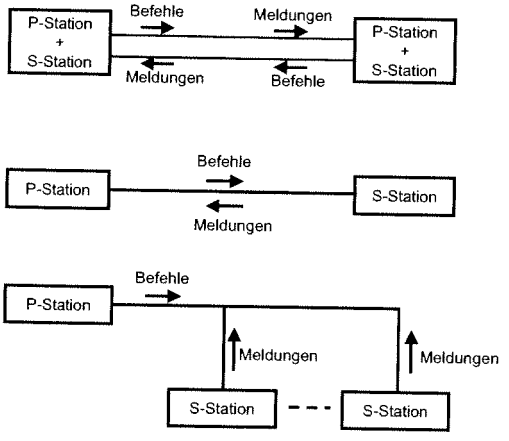


Bild: HDLC Stationsklassen

Drei Stationstypen: Station mit Leitkontrolle, Station mit Folgekontrolle und Hybridstation.

Zwei Verbindungskonfigurationen:
- Die einseitig kontrollierte Verbindung (unbalanced configuration) wird im Punkt-zu-Punkt- und Mehrpunkt-Betrieb eingesetzt. Eine Station besitzt die Leitkontrolle. Die andere Station oder im Mehrpunktbetrieb die anderen Stationen verfügen über eine Folgekontrolle. Betriebsweisen: Halbduplex oder Vollduplex.
- Die beidseitig kombinierte Verbindung (balanced configuration) wird nur im Punkt-zu-Punkt-Betrieb als Hybridstation verwendet (Halbduplex- oder Vollduplex-Betrieb).

Drei Datenübertragungsbetriebsarten:
- Der Normal Response Mode (NRM) ist ein Anrufmodus, bei dem einseitig kontrollierte Kanäle verwendet werden. Die Folgestation kann nur nach Aufforderung durch die Leitstation Daten senden. Beispiel: Datenstationen an Rechner.
- Der Asynchronous Response Mode (ARM) ist ein Spontanmodus, bei dem die Folgekontrolle ohne Aufforderung durch die Leitkontrolle aktiv werden kann und Datenübertragungen ausführen darf.

- Der Asynchronous Balanced Mode (ABM) wird nur in Punkt-zu-Punkt-Verbindungen zwischen zwei Hybridstationen eingesetzt, welche beide die Verbindung überwachen und voll gleichberechtigt aktiv werden können.

HDLC-Stationstypen

Abhängig von der Kontrollverantwortlichkeit der Datenstation werden drei Typen von HDLC-Stationen definiert:

Primäre Station (Primary Station)	P-Station	Sie hat die volle Verantwortung für die Kontrolle und Überwachung der Datenverbindung. Sie ist zuständig für die Initialisierung, Beendigung der Datenverbindung, sowie für das Aufheben von möglichen Fehlersituationen.
Sekundäre Station (Secondary Station)	S-Station	Sie wird von einer P-Station kontrolliert. Beim Auftreten von Fehlern teilt sie dies der P-Station mit und überlässt es der P-Station, die Situation zu klären.
Kombinierte Station (Combined Station)	C-Station	Eine C-Station tritt nur in Kombination mit einer anderen C-Station auf. Beide Stationen kontrollieren die Datenverbindung gleichberechtigt, d.h. jede C-Station kann die Datenverbindung initialisieren, beendigen und Fehlersituationen klären. Eine C-Station beinhaltet gewissermaßen gleichzeitig die Kontrollfunktionen einer P- und einer S-Station.

Leitkontrolle
(in Leitstation)
gibt Befehle an die Folgekontrolle

Folgekontrolle
sendet Meldungen an die Leitkontrolle

Befehle und Meldungen werden im HDLC-Rahmen übertragen

HDLC-Betriebsarten

Unter Berücksichtigung dieser 3 Stationstypen von werden folgende Klassen von HDLC-Prozeduren definiert:

Balanced: Datenverbindungen nach dieser Klasse sind zwischen zwei C-Stationen aufgebaut.

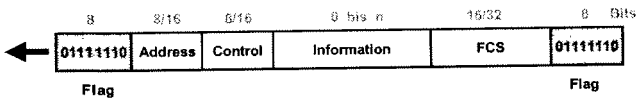
Unbalanced: Datenverbindungen existieren zwischen einer P-Station und einer oder mehreren S-Stationen.

Bild: HDLC-Kontrolle

Synchrones, bitorientiertes Protokoll

- Punkt-Punkt-Verbindungen
- eingesetzt bei X.25; Frame Relay
- abgewandelt in lokalen Netzen (LLC), ISDN (LAPD), Mobilfunk (LAPDm)

Grundlegendes Rahmenformat



Transparenz durch Bitstopfen (Bit Stuffing)

Prüfsumme

- Cyclic Redundancy Check
- $G(x) = x^{16} + x^{12} + x^5 + 1$

Bild: High-Level Data Link Control

HDLC-Rahmenstruktur

Die HDLC-Prozeduren sind bitorientiert, d.h. die Informationsdaten können beliebig codiert sein (im Gegensatz zu zeichenorientierten Prozeduren, bei denen die Informationsdaten nach einem bestimmten Zeichenalphabet codiert sein müssen).

Die Grundstruktur der zu übertragenden Daten besteht in einem Block, der Rahmen (frame) genannt wird. Jeder Rahmen hat das gleiche Erscheinungsbild, unabhängig davon, ob allgemeine Daten, Quittierungen oder Anweisungen in ihm enthalten sind. Mehrere Rahmen können inhaltlich zusammengehören, sie bilden eine Rahmenfolge, die durch eine Nummerierung im Rahmen vom Empfänger überwachbar ist.

HDLC-Rahmenstruktur

Blockbegrenzung (Flag)	Jeder HDLC-Rahmen ist begrenzt durch Flags mit Bitmuster "01111110". Ein einzelnes Flag kann gleichzeitig als Ende-Flag eines Rahmens und als Anfangsflag des nächsten dienen. **Eine Folge von Flags kennzeichnet den Ruhezustand der Übertragungsstrecke.** Treten sieben oder mehr Einsen auf, wird die Datenübertragung abgebrochen. Diese Situation wird als Abort Anweisung genutzt.
	Damit innerhalb des Rahmens jede Bitkombination möglich ist **(Codetransparenz)**, werden vom Sender binäre Nullen immer dann eingefügt, wenn 5 aufeinanderfolgende Einsen im Rahmen enthalten sind (zero Insertion). Auf der Empfangsseite wird dann jede Null entfernt, welche unmittelbar nach 5 aufeinanderfolgenden Einsen folgt (zero deletion). Damit wird vermieden, dass zwischen zwei Flags ebenfalls sechs Einsen hintereinander auftreten, die irrtümlich als Flag interpretiert würden. Dieses Verfahren wird Bitstopfen genannt.
Adress- oder A-Feld (Address-Field)	Das Adressfeld wird nicht nur zur Unterscheidung zwischen verschiedenen Stationen benutzt, es dient auch der Unterscheidung zwischen Befehlen (commands) und Meldungen (responses). Ein HDLC-Rahmen ist ein Befehl, wenn er die Adresse der empfangenden Station beinhaltet. Er ist eine Meldung, wenn er die Adresse der sendenden Station beinhaltet. Eine Adresse, die nur aus

	Einsen besteht, ist eine Rundschreibadresse für alle Stationen (Broadcast). Es besteht die Möglichkeit, das A-Feld byteweise zu erweitern.
Kontroll- oder C-Feld (Control-Field)	Mit Hilfe dieses Feldes lassen sich drei Arten von HDLC-Rahmen unterscheiden: • Informations- oder I-Rahmen (**Information Frame**), • Nummerierte Kontrollrahmen oder S-Rahmen (**Supervisory Frame**), • Nicht nummerierte Kontrollrahmen oder U-Rahmen (**Unnumbered Frame**)
	Das C-Feld beinhaltet Kontrollinformationen für die Überwachung und Kontrolle der Datenverbindung. Das C-Feld kann byteweise erweitert werden.
Informations- oder I-Feld (Information-Field)	Das I-Feld ist nur bei I-Rahmen und bei bestimmten U-Rahmen vorhanden. S-Rahmen beinhalten kein I-Feld.
	Das I-Feld darf beliebig lang sein. Eine Begrenzung dieses Feldes auf eine maximale Länge ist nicht von HDLC vorgeschrieben; sie kann, falls erforderlich, von den Anwendern selbst festgelegt werden.
Blockprüfungs- oder FCS-Feld (Frame Checking Sequence)	Das FCS-Feld beinhaltet 16 Kontrollbits, die eine Erkennung von Rahmen, die durch Übertragungsfehler gestört sind, ermöglichen. Die HDLC-Prozeduren arbeiten nach der ARQ-Methode, d.h. die Fehlerkorrektur erfolgt durch Wiederholung.

Das Adress- (Address) und Kontrollfeld (Control) bezeichnet man als Header Field des Rahmens.

Das Adress- und Kontrollfeld besteht im Basisrahmen jeweils aus einer 8 Bit Information. Bei Bedarf kann jedes Feld um 8 Bit, also ein Byte, erweitert werden. Im erweiterten Adressformat ist die Adresslänge ein Mehrfaches von 7 Bit. Die Bitposition 1 im jeweiligen Adressfeld kennzeichnet die Erweiterung; der Bitwert 0 bedeutet, dass ein weiteres Adressfeld folgt, der Bitwert 1 bedeutet, dass es sich um das letzte Adressfeld handelt. Die Adresse dient zur Adressierung der Empfängerstation bei Befehlen (commands) und zur Adressierung des Senders bei Meldungen (responses).
Eine Station, die als Leitkontrolle arbeitet, sendet nur Befehle, eine Folgekontrolle nur Meldungen und lediglich eine Hybridstation darf Befehle und Meldungen senden. Das Kontrollfeld bezeichnet das Rahmenformat und es enthält die Folgenummern.

Es werden Rahmen unterschieden, ob sie nummeriert oder unnummeriert übertragen werden. Nummerierte Rahmen sind Information, oder Supervisory-Rahmen, Rahmen die der Nachrichtenübertragung und der Befehlsübermittlung dienen.

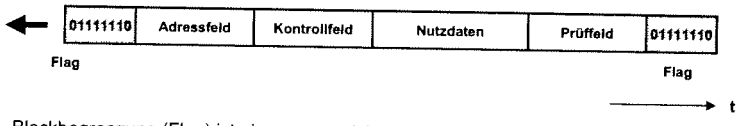
Fluss- und Fehlerkontrolle: Fenster-Verfahren mit ARQ-Mechanismus

Basisformat:	3 Bits	Folgenummernkontrolle mit Wertevorrat von 0 bis 7 (modulo 8)
Erweitertes Format:	7 Bits	Wertevorrat von 0 – 127 (modulo 128)

Das Informationsfeld (Information) ist für nummerierte Rahmen (information frames) vorbehalten. Die Feldlänge ist im HDLC-Standard nicht begrenzt. Die jeweiligen Applikationen definieren Obergrenzen der Informationsfeldlänge; oft muß die Länge ein Vielfaches von 8 Bit, einem Byte, sein.

Das Feld für die Blockprüfung FCS (Frame Checking Sequence) besteht aus 16 Bit. Das CRC-Codewort wird aus dem Inhalt des Adress-, Kontroll- und Informationsfeldes berechnet. optional kann das FCS-Feld auch mit einem 32 Bit langen Codewort ausgestattet sein.

Generatorpolynom CRC-16 (ITU): $x^{16} + x^{12} + x^5 + 1$.



Blockbegrenzung (Flag) ist eine ausgezeichnete Bitfolge (01111110)

Problem: Zufälliges Auftreten von 01111110 im Datenübertragungs-Block

Lösung: Bit Stuffing

- Sender fügt zwischen den Flags nach 5 aufeinanderfolgenden Zeichen „1" ein Zeichen „0" ein.
- Empfänger entfernt zwischen den Flags nach 5 aufeinanderfolgenden Zeichen „1" das darauffolgende Zeichen „0".

Bild: Codetransparenz – Bit Stuffing

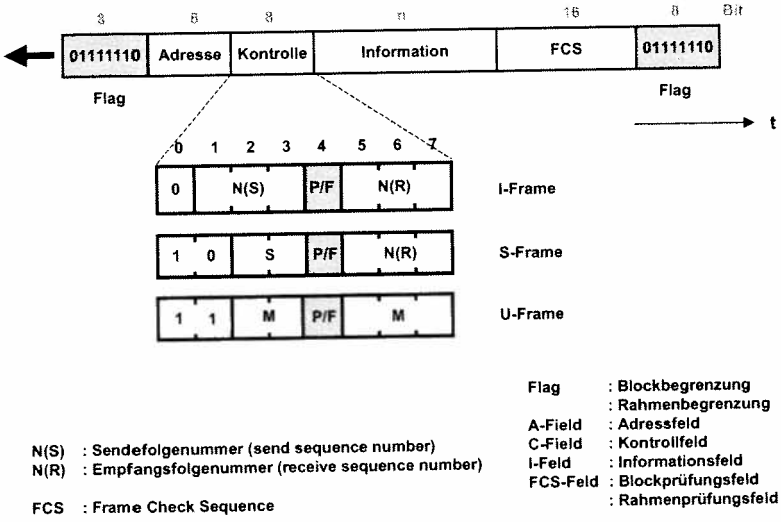


Bild: High-Level Data Link Control

HDLC-Rahmenarten

Bei den HDLC-Prozeduren sind drei Arten von Rahmen definiert: I-, S- und U-Rahmen.

Das 5. Bit des C-Feldes ist das Aufruf/Ende-Bit oder P/F-Bit (Polling/Final-Bit, Bit 4). Wenn dieses Bit gleich "1" ist, dann handelt es sich bei einem Befehl um ein Aufruf-Bit (P-Bit) und bei einer Meldung um ein Ende-Bit (F-Bit). Wenn dieses Bit gleich "0" ist, dann hat es keine besondere Bedeutung. Die Funktion dieses P/F-Bits hängt von der benutzten HDLC-Betriebsart ab.

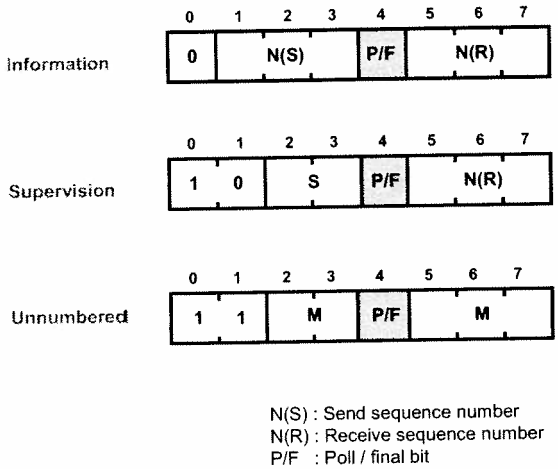


Bild: Kontrollfeld

Kontrollfeld

In dem Kontrollfeld eines S- und I-Rahmen werden zwei Formen von Kontrollanweisungen unterschieden: Befehle (commands) und Antwortmeldungen (responses). Rahmen, die von einer Leitkontrolle gesendet werden, enthalten commands; eine Folgestation sendet responses. Eine Hybridstation darf commands und responses senden.

Ein Information-Rahmen (I-Rahmen) enthält an der Bitposition 1 eine 0 im Kontrollfeld. Die Inhalte der Sendefolge-Nummer N(S) und der Empfangsfolge-Nummer N(R) geben die Nummer des nächsten zu sendenden Rahmen und die Nummer des nächsten zu empfangenden Rahmen an.

Ein Supervisory-Rahmen (S-Rahmen) enthält einen Befehl und eine Empfangsfolge-Nummer N(R) für Quittierungen und Wiederholungsaufforderungen. Kennung: 10 am Anfang des Feldes.

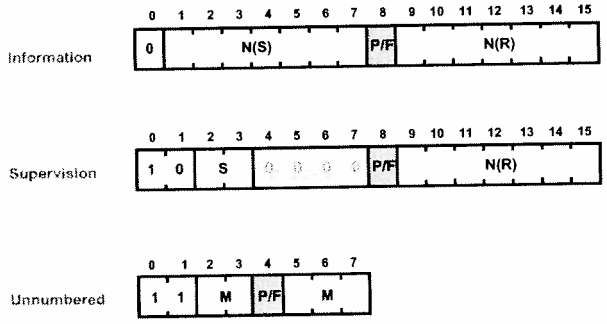


Bild: Erweitertes Kontrollfeld

Für höhere Bitraten oder größere Steckendistanzen (z.B. Satellit) wird ein größerer Nummernbereich benötigt. Dies ist deshalb erforderlich, weil in diesen beiden Fällen viele unquittierten Rahmen ausständig sein können. Anstatt modulo 8 mit 3 Bit, wird so modulo 128 ermöglicht.

Das P/F-Bit bedeutet in NRM und ARM:

P	Poll-Bit	Sendeaufforderung an eine Folgekontrolle
F	Final-Bit	Quittierung des Poll-Bits

Im ABM-Betrieb sind die beteiligten Stationen gleichberechtigt, so dass keine Sendeaufforderungen ergeben. Jede Anfrage mit einem Poll-Bit muss mit einem Final-Bit beantwortet werden.

Informations- oder I-Rahmen (Information Frame)

Der I-Rahmen ist der einzige HDLC-Rahmen mit Nutzinformation in dem Informationsfeld.

Mit der Sendefolgenummer N(S) (Send sequence number) werden die I-Rahmen zyklisch von 0 bis 7 durchnummeriert (Modulo 8). Bei einer Erweiterung des C-Feldes um weitere 8 Bits kann der Modulo-Wert auf 128 erhöht werden, was eine Durchnummerierung der I-Rahmen von 0 bis 127 ermöglicht.

Für die Durchnummerierung der I-Rahmen besitzt die sendende Station eine Kontrollvariable, die Sendefolgevariable V(S) (Send state variable) genannt wird. Diese Variable V(S) ist bei Initialisierung der Verbindung gleich 0 gesetzt. Bevor ein I-Rahmen gesendet wird, wird der Wert von V(S) in das N(S)-Feld eingeschrieben und anschließend wird V(S) um 1 erhöht (Rechnung nach Modulo 8 bzw. 128). Somit wird automatisch gewährleistet, dass der nachfolgende I-Rahmen eine um 1 höhere N(S)-Nummer aufweist.

Die Empfangsfolgenummer N(R) (Receive sequence number) dient als Quittung von I-Rahmen, welche in der betrachteten sendenden Station empfangen wurden. Für diesen Zweck besitzt die empfangende Station eine Empfangsfolgevariable V(R) (Receive state variable), die bei der Initialisierung der Verbindung gleich 0 gesetzt wird. Empfangene Rahmen, welche aufgrund der Prüfung des FCS-Feldes als gestört erkannt sind, werden verworfen. I-Rahmen, die keinen FCS-Fehler aufweisen, werden von der empfangenden Station bearbeitet. Ihre N(S)-Nummer wird zunächst mit dem Wert der Variablen V(R) verglichen. Bei Übereinstimmung wird der empfangene I-Rahmen angenommen und die Variable V(R) um 1 erhöht. Bei Nichtübereinstimmung zwischen N(S)-Nummer und V(R)-Wert liegt ein Fehler in der Reihenfolge der I-Rahmen (Sequenzfehler) vor.

Beim Senden eines I- oder S-Rahmens wird der Inhalt der Empfangsfolgevariable V(R) in das N(R)-Feld des zu sendenden Rahmens eingeschrieben. Wenn eine Station eine N(R)-Nummer gleich m sendet, teilt sie der Gegenstation dadurch mit, dass sie alle I-Rahmen mit den N(S)-Nummern kleiner als oder gleich (m-1) korrekt empfangen hat. Die Gegenstation kann dann mit Hilfe der empfangenen N(R)-Nummer die Kopien der gespeicherten I-Rahmen bis zur N(S)=(m-1) einschließlich löschen.

Um eine eindeutige Zuordnung zwischen empfangener N(R)-Nummer und gesendeter N(S)-Nummer zu gewährleisten, darf eine sendende Station bei Modulo 8 maximal 7 (bzw. bei Modulo 128 maximal 127) unquittierte I-Rahmen haben. Beim Erreichen dieses maximalen Wertes darf sie solange keinen weiteren I-Rahmen senden, bis eine Quittung empfangen wird, welche entweder korrekt empfangene I-Rahmen bestätigt und somit das Senden von neuen I-Rahmen wieder ermöglicht oder eine Wiederholung von I-Rahmen auslöst.

Diese Begrenzung durch den Modulo-Wert hat einen besonderen Einfluss auf die Leistungsfähigkeit von HDLC-kontrollierten Datenverbindungen. Insbesondere bei Übertragungsstrecken mit großer Signallaufzeit wie Satellitenstrecken.

Kontrollrahmen:

RR	00	Receive-Ready	Der RR-Rahmen wird benutzt um zu zeigen, dass weitere Informationsrahmen empfangen werden können, und um korrekt empfangene I-Rahmen zu bestätigen. Dieser Fall tritt dann ein, wenn die empfangende Station momentan keinen I-Rahmen absenden kann, dem diese Quittung mitgegeben werden könnte.
RNR	10	Receive-Not-Ready	Der RNR-Rahmen wird benutzt, um zu melden, dass keine weitere I-Rahmen empfangen werden können. Dieser Zustand der Nicht-Empfangsbereitschaft kann z. B. auftreten, wenn eine Station keinen freien Speicherplatz mehr für I-Rahmen hat.
REJ	01	Reject	Der REJ-Rahmen wird benutzt, um die Wiederholung von I-Rahmen anzufordern. Wenn eine Station einen REJ-Rahmen empfangen hat, wiederholt sie alle unquittierte I-Rahmen; anzufangen ist mit dem I-Rahmen, dessen N(S)-Nummer gleich der im REJ-Rahmen angegebenen N(R)-Nummer ist.
SREJ	11	Selective-Reject	Der SREJ-Rahmen wird benutzt, um die Wiederholung eines einzelnen I-Rahmens anzufordern. Die N(S)-Nummer des zu wiederholenden I-Rahmens ist durch die N(R)-Nummer des empfangenen SREJ-Rahmens angegeben. Diejenige Station, die einen SREJ-Rahmen empfangen hat, wiederholt nur den gewünschten I-Rahmen und nicht alle unquittierten wie im Fall von REJ-Rahmen. Wegen des höheren Aufwandes bei ihrer Implementierung, findet diese selektive Wiederholungsmethode bis jetzt kaum Anwendung. Es wird deshalb im Rahmen dieser Arbeit auf die Benutzung des SREJ-Rahmens verzichtet

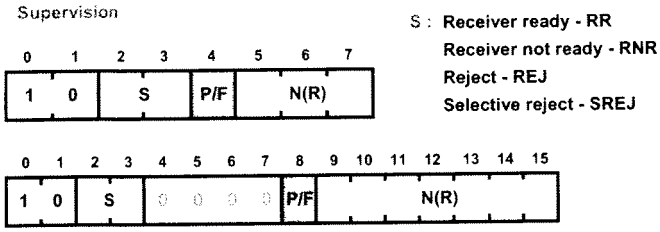


Bild: Supervisory HDLC Frames

Nummerierte Kontrollrahmen, S-Rahmen (Supervisory Frame)
S-Rahmen beinhalten kein Informationsfeld. Das N(R)-Feld hat hier die gleiche Funktion wie jenes in I-Rahmen.

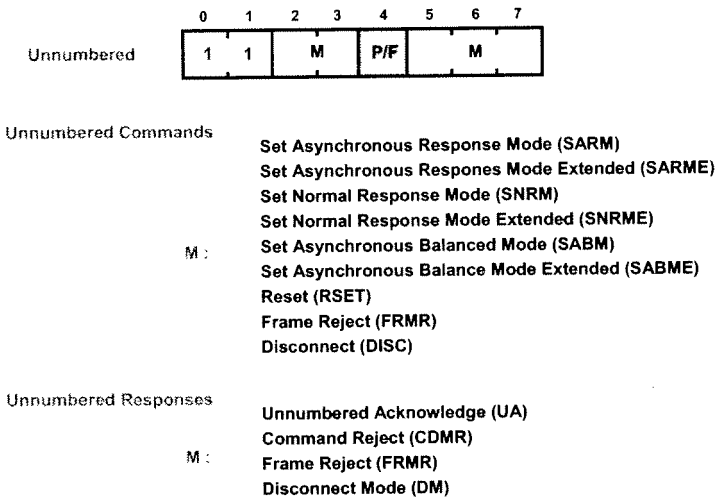
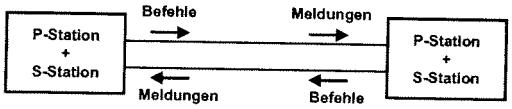


Bild: Unnumbered HDLC Frames

Nicht-nummerierte Kontrollrahmen oder U-Rahmen (Unnumbered Frame)
U-Rahmen beinhalten weder Sendefolgenummern N(S) noch Empfangsfolgenummern N(R), hiervon rührt auch ihr Name als "nicht nummerierter Kontrollrahmen". Sie erlauben Kontrollfunktionen wie Initialisierung, Beendigung der Datenverbindung und Rücksetzen der Variablen V(S) bzw. V(R) im Falle des Auseinanderlaufens dieser Variablen durchzuführen.

SNRM	Set Normal Response Mode	Mit SNRN wird die empfangende Station zu einer Folgekontrolle. Alle Zähler werden auf Null gesetzt und die Betriebsart NRM gestartet. Die Station bleibt in diesem Zustand, bis ein DISC oder SIM eintrifft.
SARM	Set Asynchronous Response Mode	Wahl der Betriebsart ARM. Die den Befehl SARM empfangende Station wird Folgekontrolle. Die Station bleibt in diesem Zustand, bis ein DISC eintrifft. Alle Zähler werden auf Null gesetzt
SABM	Set Asynchronous Balanced Mode	Wahl der Betriebsart ABM. Sende- und Empfangsstation bleibt in diesem Zustand, bis ein DISC eintrifft. Alle Zähler werden auf Null gesetzt.
SNRME	SNRM Extended	Wie SNRM mit erweitertem Kontrollfeld
SARME	SARM Extended	Wie SARM mit erweitertem Kontrollfeld
SABME	SABM Extended	Wie SABM mit erweitertem Kontrollfeld.
DISC	Disconnect	Der Befehl hebt den aktuellen Betriebszustand auf. Die Station geht in den Wartezustand.
DM	Disconnected Mode	Wartezustand mit logischer Verbindungstrennung nach SABM
FRMR	Frame Reject	Sendet der Gegenstation das Kontrollfeld eines ungültigen Rahmens zurück und bezeichnet den Fehler: Kontrollfeld ungültig, ungültige bzw. nicht bekannte Information im Kontrollfeld, Länge eines Informationsfelds zu groß, unzulässiger N(R) Wert.
UA	Unnumbered Acknowledgment	Bestätigung eines U-Rahmens
UI	Unnumbered Information	Austausch von Informationen zwischen den Stationen
RSET	Reset	N(S) und N(R) werden zurückgesetzt
SIM	Set Initialization Mode	Mit SIM werden in der Folgekontrolle systemspezifische Vorgänge eingeleitet und alle Zähler auf Null gesetzt.
RIM	Request Initialization Mode	Anforderung einer Initialisierung durch SIM.
RD	Request Disconnect	Mit RD fordert eine Folgestation ein DISC an
UP	Unnumbered Poll	Aufforderung zu einer Abfrage
XID	Exchange Identification	Austausch von Systemparameter und Statusinformationen
TEST	Test	Mit diesem Befehl wird ein Informationsfeld versendet und vom Empfänger zu Testzwecken zurückgereicht (nur für ABM)



HDLC-Prozedurklassen II

Symmetrische Konfiguration (Balanced)

- totale Symmetrie zwischen den Stationen (kombinierte Stationen)
- nur Punkt-zu-Punkt-Verbindungen
- nur asynchroner Modus

Bild: Symmetrische HDLC Prozeduren

Die Balanced Klasse von HDLC-Prozeduren

Die Balanced Klasse von HDLC-Prozeduren ist nur für Punkt-Punkt-Verbindungen geeignet. Die zwei kombinierten Stationen (oder C-Stationen) an beiden Enden der Verbindung können sowohl Befehle als auch Meldungen senden bzw. empfangen.

Weil beide Stationen bei der Kontrolle der Datenverbindung gleichberechtigt sind, d.h. jede die Verbindung initialisieren, rücksetzen oder beenden, und ferner zu jedem Zeitpunkt Rahmen senden kann, spricht man hier von dem asynchronous balanced mode of operation oder abgekürzt ABM-Betrieb

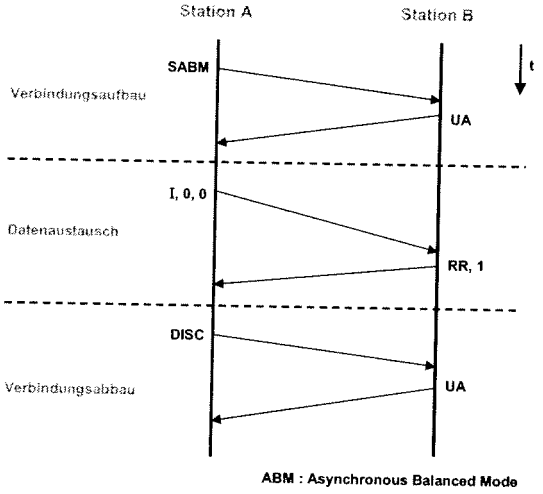


Bild: Datenaustausch in der Betriebsart ABM

Bevor ein Datenaustausch auf Schicht 2 stattfinden kann, muss eine logische Verbindung aufgebaut werden.

Im Beispiel wird mit SABM (Set ABM) eine symmetrische Verbindung aufgebaut. Der Verbindungsaufbau wird abgeschlossen mit dem Response UA (Unnumbered Acknowledgement).

Danach erfolgt der Datenaustausch. Hier Informationsrahmen I(0,0) mit Sende- und Empfangsnummer beide auf Null. Quittiert wird mit Receive Ready RR(1) als Angabe, dass der Empfänger im nächsten Informationsrahmen N(S)=1 erwartet.

Die Verbindung wird abgebaut mit dem Befehl DISC und die Quittung UA vom Empfänger.

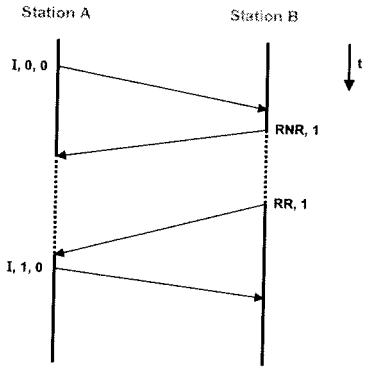


Bild a: Datenaustausch und Flusskontrolle

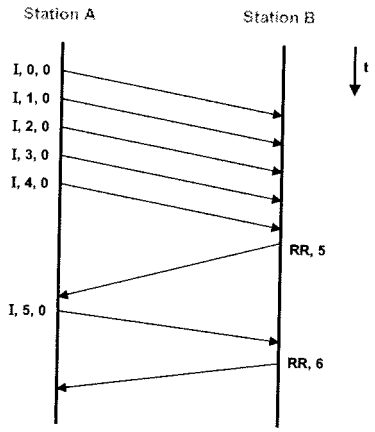


Bild b: Datenaustausch mit Vielfach-Quittierung

Im Bild a:
Wird der Informationsrahmen I(0,0) mit RNR(1), Receive Not Ready, von Station B quittiert und damit wird der Sendstrom gleichzeitig angehalten, bis Station A beim Empfang von RR(1) erneut senden darf. Gesendet wird jetzt Informationsrahmen I(1,0).

Im Bild b:
Werden eine Reihe von Informationsrahmen I(0,0) bis I(4,0) geschickt, die vom Empfangsstation B mit RR(5) gemeinsam quittiert wird. RR(5) bedeutet, dass Station B einen Informationsrahmen mit N(S)=5 erwartet.

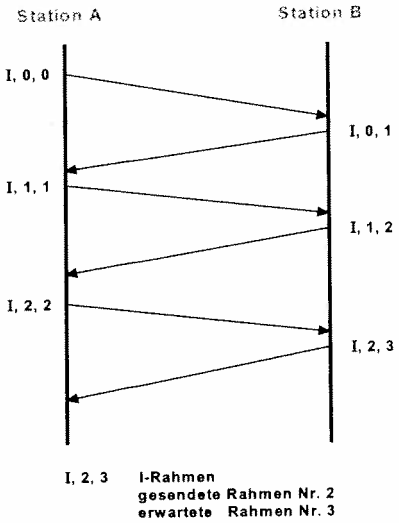


Bild a: Datenaustausch mit Fenster W=1

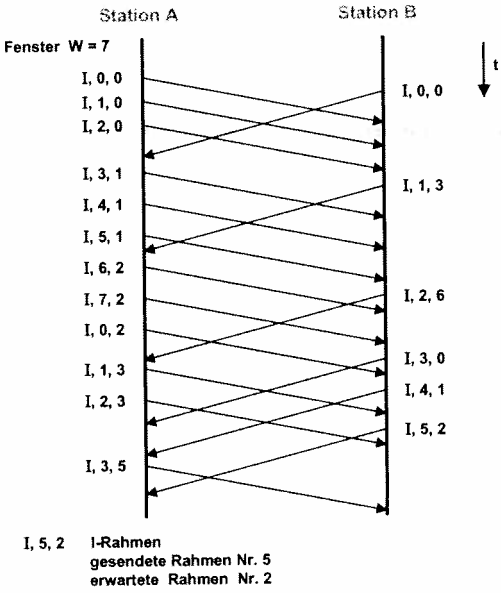


Bild b: Datenaustausch mit Fenster W=7

Im Bild a
werden Informationsrahmen gleichzeitig in beiden Richtungen ausgetauscht. Dadurch können sie direkt zur Quittierung herangezogen werden. Zum Beispiel I(0,0) von Station A wird mit I(0,1) von Station B quittiert. Darauf sendet Station A den Informationsrahmen I(1,1) mit N(S)=1 und N(R)=1, d.h. Station A erwartet I(1,x) von Station B.

Im Bild b
in diesem Szenario ist nun das Fenster W=7 anstatt W=1 und somit muss nicht jeder Informationsrahmen quittiert werden, bevor weiter gesendet werden darf.

Automatische Fehlerkorrektur
Informationsrahmen, die sich aufgrund der Prüfung des FCS-Feldes als gestört erweisen (FCS-Fehler), werden einfach von der empfangenden Station verworfen. Wie diese I-Rahmen danach von der sendenden Station wiederholt werden können, wird im folgenden beschrieben.

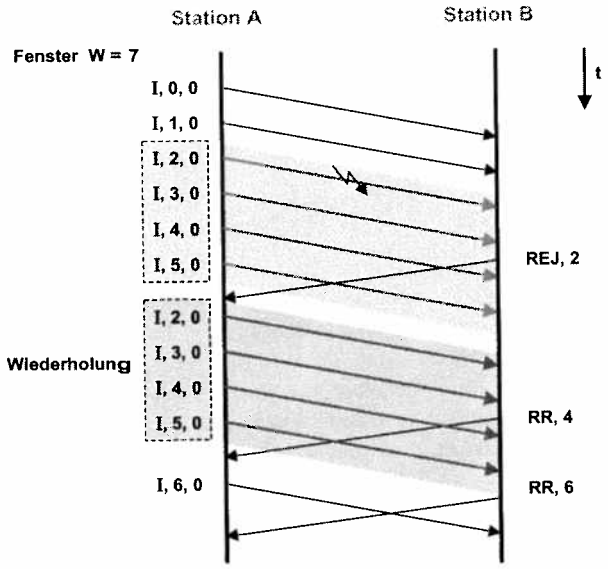


Bild: Datenaustausch mit Fehlerkorrektur: REJ

Wiederholung durch REJ-Rahmen
Sobald eine Station einen Fehler in der Reihenfolge der I-Rahmen entdeckt hat (Sequence-Fehler), kann sie einen REJ-Rahmen senden. Die N(R)-Nummer des REJ-Rahmens ist dabei gleich dem Wert der Empfangsfolgevariablen V(R). Ein Sequence-Fehler tritt dann auf, wenn ein I-Rahmen empfangen wird, der sich zwar durch die FCS-Prüfung als fehlerfrei erweist, dessen Sendefolgenummer N(S) aber nicht mit dem Wert der Variablen V(R) übereinstimmt.

Beim Empfang des REJ-Rahmens wiederholt dann die Gegenstation alle unquittierten I-Rahmen, angefangen mit dem I-Rahmen, dessen N(S)-Nummer gleich der im REJ-Rahmen angegebenen N(R)-Nummer ist. Danach wird eine mögliche Wiederholung wegen des Empfangs eines Rahmens mit gesetztem P/F-Bit unterdrückt, um eine nochmalige Übertragung derselben I-Rahmen zu vermeiden (doppelte Wiederholung). Bis zum korrekten Empfang des gewünschten I-Rahmens darf kein weiterer REJ-Rahmen gesendet werden.

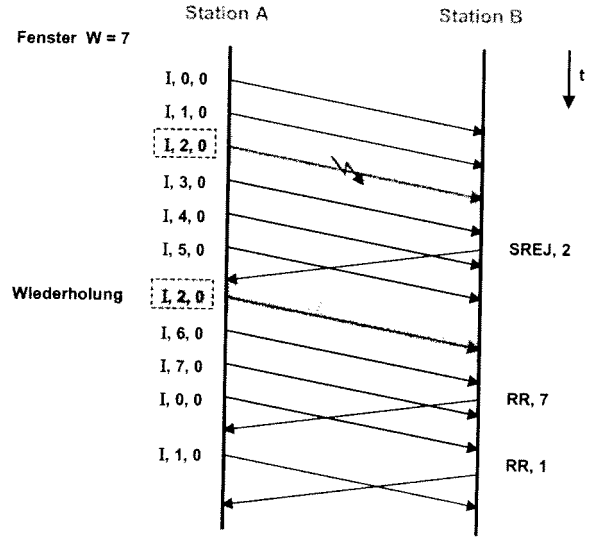


Bild : Datenaustausch mit Fehlerkorrektur: SREJ

Einzelne Rahmen werden mit Selective Reject (SREJ) nochmals angefordert.

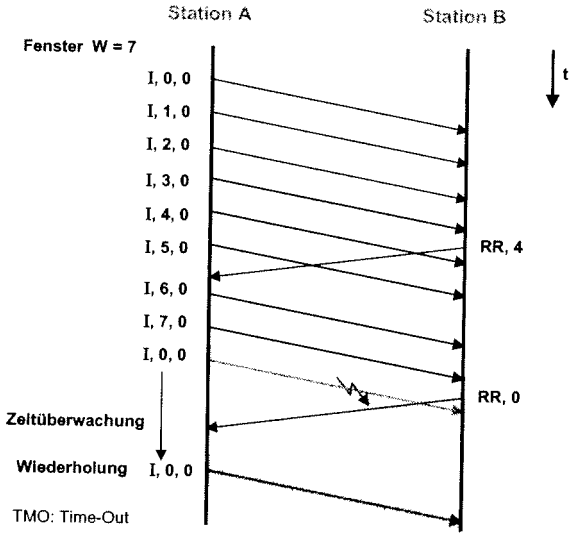


Bild : Datenaustausch mit Fehlerkorrektur: Time-Out

Wiederholung durch Zeitüberwachung

Der letzte einer Serie von I-Rahmen kann nicht mit Hilfe von REJ-Rahmen wiederholt werden, weil nach diesem I-Rahmen kein weiterer folgt und deshalb kein Sequenzfehler auftreten kann. Auch ein durch einen REJ-Rahmen wiederholter I-Rahmen kann im Falle von nochmaliger Störung nicht mehr mit Hilfe eines REJ-Rahmens wiederholt werden. Zur Sicherung gegen solche Fälle wird eine Zeitüberwachung bei der sendenden Station herangezogen.

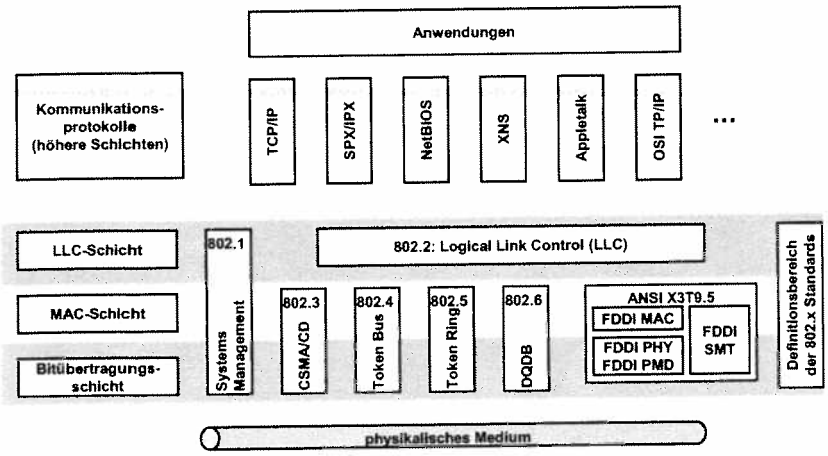
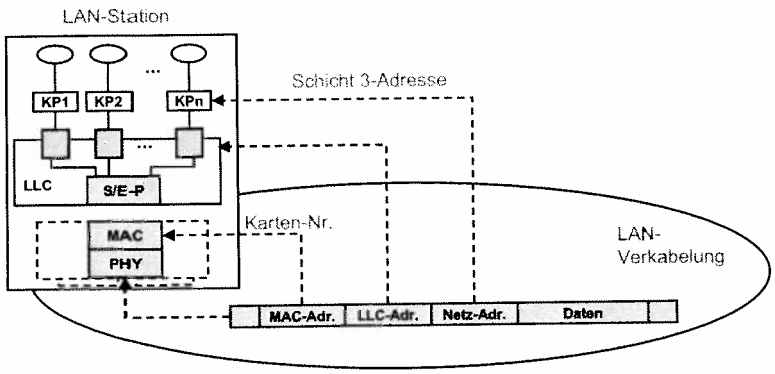


Bild: LAN Protokollstruktur

LANs nach den IEEE-Standards basieren auf ein logisches LAN-Modell. Mit Hilfe dieses Modells wird auf eine besondere Rolle der LLC-Schicht in LANs hingewiesen. Diese Schicht stellt eine Sicherungsschicht im LAN dar und realisiert die Unabhängigkeit der Kommunikationsprotokolle vom LAN-Typ. Diese Schicht kann auch als ein Multiplexer von Kommunikationsprotokollen interpretiert werden. Dabei wird versucht, deutlich zu zeigen, dass die Unterschiede zwischen einzelnen LAN-Typen vor allem in der LAN-Verkabelung, im Zugriffsverfahren und der Bitübertragung liegen, d.h. in der Art und Weise, wie die Daten im LAN-Medium transportiert werden.



KP: Kommunikationsprotokoll

Bild: LAN-Adressierung

Zur Adressierung der Instanzen ist eine Adresse für jede Schicht notwendig:

- IEEE MAC-Adresse (48 Bit)
- LLC- Adresse
- Netzadresse

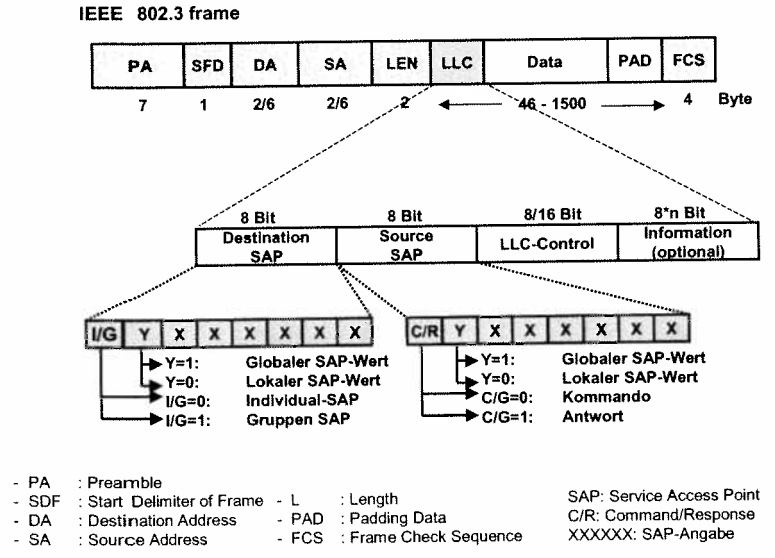


Bild: LLC-Frame: Adressierungsfelder

Der Datenaustausch innerhalb der LLC-Schicht zwischen SAPs, die sich in unterschiedlichen Stationen befinden, wird mit Hilfe von festgelegten LLC-Frames realisiert.

Sie werden auch als Protokolldateneinheiten, LPDUs (PDU: Protocol Data Unit) der LLC-Schicht bezeichnet.

Die LLC-Schicht realisiert ein LAN-Sicherungsprotokoll.

Das LAN-Sicherungsprotokoll nach IEEE 802.2 muss - im Vergleich zum HDLC - zusätzlich folgende Funktionen unterstützen:

- Punkt-zu-Mehrpunkt-Verbindungen (für Multicast und Broadcast),
- verbindungslose und verbindungsorientierte Dienste,
- Multiplex-Funktion.

Die Multiplex-Funktion bedeutet, dass mehrere virtuelle Verbindungen Quell-SAP / Ziel-SAP über ein Paar globaler Sende/Empfangs-Puffer realisiert werden müssen.

Ein LLC-Frame kann variabel lang sein und besteht aus der Quell- und Ziel-SAP-Adresse, einem Kontrollfeld (Control) und einem Informationsfeld (Info). Der Ziel-SAP kann sowohl eine Individual- als auch eine Gruppenadresse sein, um sowohl Punkt-zu-Punkt- als auch Punkt-zu-Mehrpunkt-Verbindungen realisieren zu können. Der Quell-SAP stellt immer eine Individualadresse dar. Für die Angabe, ob es sich um eine Gruppen- oder eine Individual-Adresse handelt, dient das Bit I/G (ähnlich wie bei der MAC-Adresse). Die SAP-Werte werden den einzelnen Kommunikationsprotokollen eindeutig zugeordnet. Diese Zuordnung kann global, d.h. weltweit eindeutig sein, oder sie wird vom Benutzer lokal vorgenommen.

Mit dem Bit Y wird markiert, ob es sich um einen globalen oder einen lokalen SAP-Wert handelt. Dieses Bit entspricht dem G/L-Bit in der MAC-Adresse.

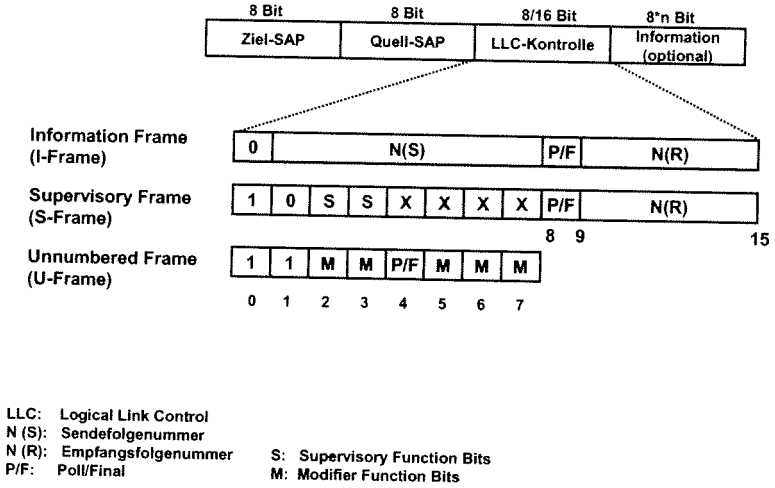


Bild: LLC-Frame: Kontrollfeld

Das Kontrollfeld und der Ablauf des Protokolls ist wie bei HDLC.

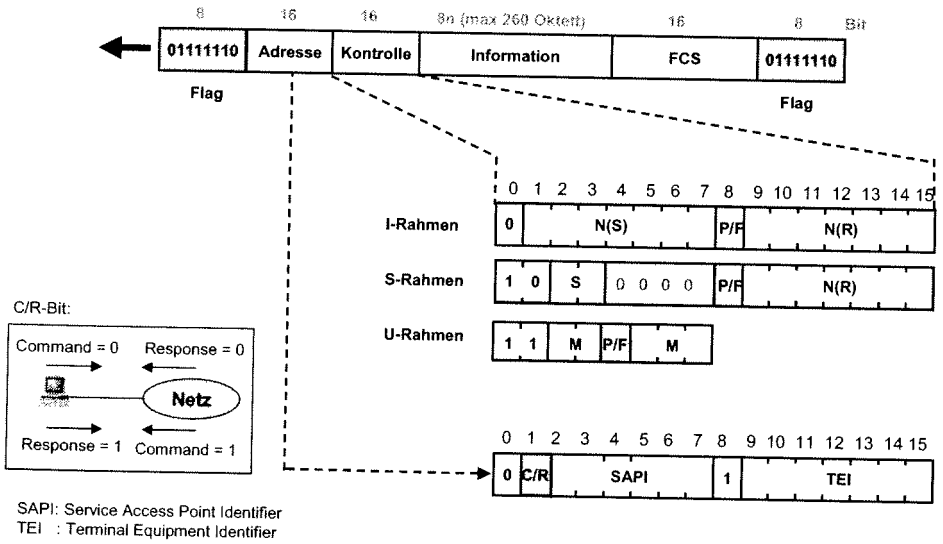


Bild: ISDN D-Kanal: LAPD-Rahmen

Format und Ablauf des D-Kanal Protokolls ist die gleiche wie bei HDLC.

Bei der Adressierung benötigt man neben dem Service Access Point Identifier noch eine Hardware Adresse TEI (Terminal Equipment Identifier), um das richtige ISDN-Gerät aufwählen zu können.
Eine ISDN-Basisanschluss kann bis zu 8 Geräte haben.

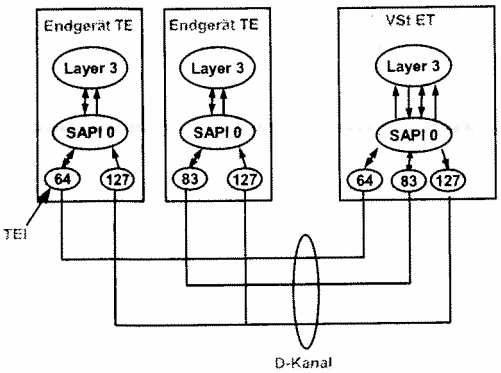


Bild: Adressierung von ISDN-Basisanschlüssen

Das Bild illustriert den Gebrauch von TEI und SAPI.
TEI = 127 ist eine Gruppe-Adresse und ist für die Signalisierung vorgesehen.

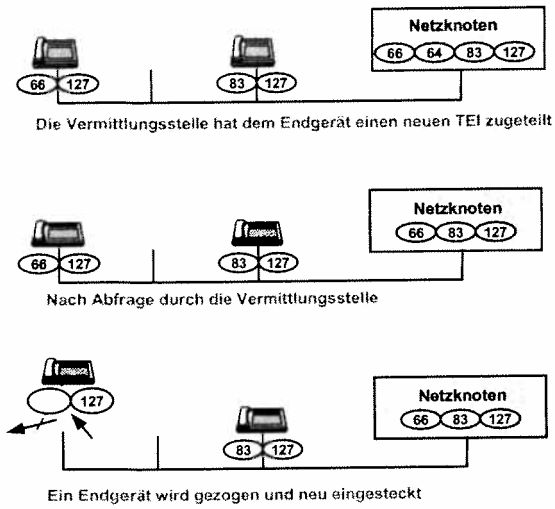


Bild: Vergabe von Endgeräte-Identitäten (TEI)

Ein TEI wird in der Vermittlungsstelle verwaltet. Auf Anfrage wird einen Wert zugeteilt. Da die Vermittlungsstelle nur periodisch aktualisiert, können nicht mehr gültige TEIs existieren

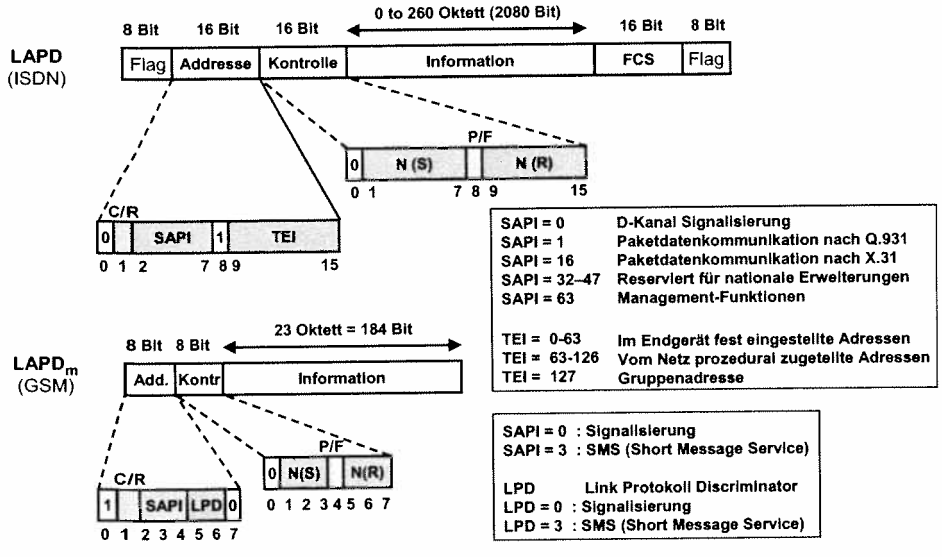


Bild: LAPD und $LAPD_m$ Rahmenstruktur

Beim D_m-Kanal für GSM sind folgende Punkte anders als beim D-Kanal:

- Es wird kein Flag benötigt, weil die Funkschnittstelle Übertragungsbursts konstanter Länge verwendet.
- Adress- und Kontrolfeld sind 8 Bit, anstatt bei ISDN 16 Bit
- Informationsfeld ist maximal 21 Byte lang, anstatt bei ISDN 260 Byte.
- Keine Geräte-Adresse TEI ist notwendig.

Im Bild sind die Wertebereiche und spezielle Zuordnung vom SAPI und TEI zur Information angegeben.

2.2c OSI-Referenzmodell: Schicht 2c - Vernetzung

Version Dez. 2003

- Aufgaben und Funktionen von Vernetzung und Netzkopplungen auf Schicht 2
- Brücken (Bridges), Lokale Brücke, Abgesetzte Brücke
- Transparentes Bridging, Spanning Tree Protocol (Ethernet LANs)
- Source Routing Bridging (Token Ring LANs)
- Virtuelle LANs (Virtual LANs, VLAN)

Netzkopplungen

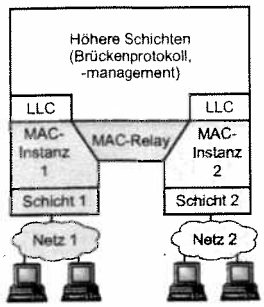
Aus geographischen, historischen, wirtschaftlichen, politischen und organisatorischen Gründen wird die Vernetzung aus Teilnetzen gleicher oder verschiedener Technologien gebildet. Bei Teilnetzen der gleichen Technologie sind mehrheitlich Zuständigkeits- und Sicherheitsfaktoren maßgebend. Sind technologisch ungleiche Netze zu koppeln, so sind zu der physikalischen Anpassung zusätzlich Protokoll- und Datenformat-Umformungen notwendig.

Bridge-Technologien

Viele Unternehmen haben mehrere LANs und möchten diese verbinden. LANs können mit Geräten namens Bridges (Brücken) verbunden werden, die auf der Sicherungsschicht arbeiten. Das bedeutet, dass Bridges den Header auf der Vermittlungsschicht nicht prüfen und Pakete alllerart Protokolle gleichermaßen gut kopieren können.

Es werden sechs Gründe aufgeführt, warum in einem einzelnen Unternehmen mehrere LANs vorhanden sein können.

- Erstens haben viele Universitäts- und Firmenabteilungen ihr eigenes LAN, um damit ihre Personalcomputer, Workstations und Minicomputer zu verbinden. Da sich die Ziele der einzelnen Abteilungen unterscheiden, werden auch verschiedene LANs eingerichtet, ohne die Entscheidung anderer Abteilungen zu berücksichtigen. Früher oder später müssen sie zusammenarbeiten, also wird eine Brücke benötigt. In diesem Beispiel entstanden die verschiedenen LANs aufgrund der Autonomie ihrer Besitzer.
- Zweitens könnte das Unternehmen auf verschiedene geographisch weit voneinander entfernte Gebäude ausgeteilt sein. Hier ist es günstiger, in jedem Gebäude ein LAN einzurichten und diese dann mit Bridges zu versehen, als ein riesiges Koaxialkabel durch das ganze Gebiet zu verlegen.
- Drittens könnte es nötig sein, ein logisches Einzel-LAN in mehrere LANs aufzuteilen, um die Belastung zu verteilen. An vielen Universitäten stehen z.B. für Studenten und Lehrende Tausende von Workstations zur Verfügung. Die Dateien befinden sich normalerweise auf Datei-Servern und werden von den Benutzern an einer Workstation bei Bedarf heruntergeladen. Bei Systemen diesen Umfangs können nicht alle Workstations an ein einzelnes LAN angeschlossen werden. Die insgesamt benötigte Bandbreite wäre zu hoch. Statt dessen werden mehrere LANs über Bridges verbunden. Jedes LAN enthält einen Workstation Cluster mit einem eigenen Datei-Server, so dass der Großteil des Verkehrs auf ein einzelnes LAN beschränkt ist und das Backbone nicht belastet.
- Viertens könnte ein einzelnes LAN zwar die anfallende Arbeit bewältigen, aber die physische Entfernung zwischen den am weitesten voneinander entfernten Maschinen ist zu groß (z.B. mehr als die von 802.3 unterstützten 2,5 km). Auch wenn die Kabelverlegung einfach ist, wird das Netz wegen der extremen Umlaufzeit nicht den Anforderungen gerecht. Die einzige Lösung ist die Unterteilung des LANs und die Installation von Bridges zwischen den einzelnen Segmenten. Das bedeutet, dass die physische Ausdehnung eines Netzes mit Bridges erweitert werden kann.
- Fünftens ist die Zuverlässigkeit zu betrachten. Bei einem einzelnen LAN kann ein defekter Knoten, der andauernd Unsinn sendet, das ganze LAN beeinträchtigen. Bridges können an kritischen Stellen wie Notausgängen eingebaut werden, um den teuflischen Knoten davon abzuhalten, das ganze System lahmzulegen. Im Gegensatz zu einem Repeater, der nur kopiert, was er sieht, kann eine Bridge so programmiert werden, dass nicht alles weitergegeben wird.
- Sechstens können Bridges zur Sicherheit eines Unternehmens beitragen. Die meisten LAN-Schnittstellen haben einen Gemischtmodus: Dem Computer werden alle Pakete übergeben, nicht nur die an ihn adressierten. Werden an verschiedenen Stellen Bridges eingesetzt und empfindliche Daten einfach nicht weitergeleitet, können Teile des Neues so isoliert werden, dass keine Daten mehr entweichen können.



- **Transparente Bridge**
  - Lernen der Lokation von Endsystemen
  - Filtern bzw. Weiterleiten von Dateneinheiten
  - Erkennen von Schleifen in der Netztopologie
- **Source-Routing-Bridges**

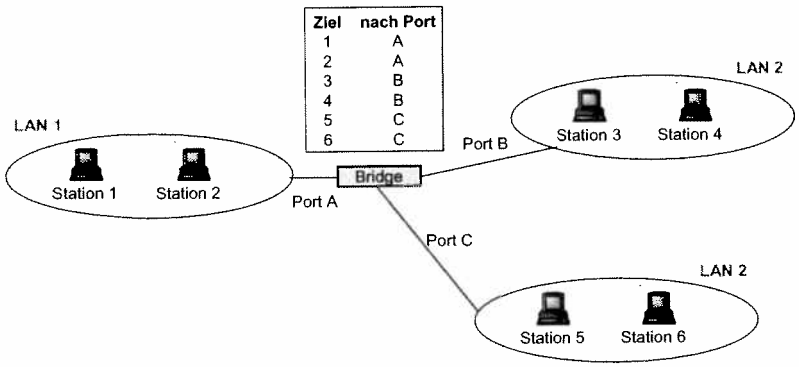
Es gibt verschiedene Arten von Bridges.

Betrachtet werden:
- Transparent Bridge,
- Source-Routing Bridge,
- Remote Bridge.

Bild: LAN-Kopplung mit Bridges

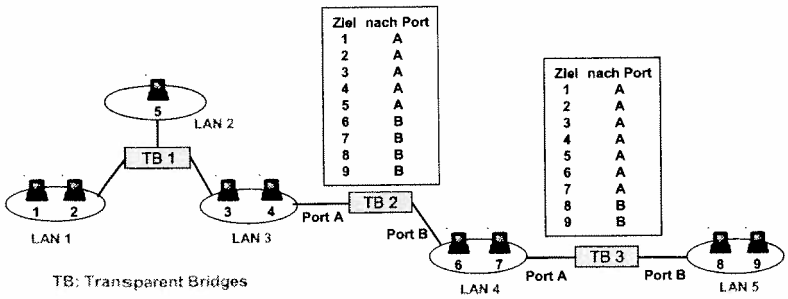
Transparente Bridges

Die erste 802-Bridge ist die transparente Bridge oder Spanning-Tree-Bridge. Das ausschlaggebende Anliegen derjenigen, die diese Auslegung unterstützten, war die völlige Transparenz Aus ihrer Sicht muss es bei einer Anlage mit mehreren LANs möglich sein, eine von IEEE genormte Bridge zu kaufen, sie anzuschließen, und dann soll das Netz sofort laufen. Es sollte nicht nötig sein, die Hardware zu ändern, die Software zu ändern, die Adressierung zu ändern oder die Routing-Tabellen oder Parameter zu laden - nichts dergleichen. Nur die Kabel einstecken und fertig. Die bereits bestehenden LANs sollten nicht in Mitleidenschaft gezogen werden.



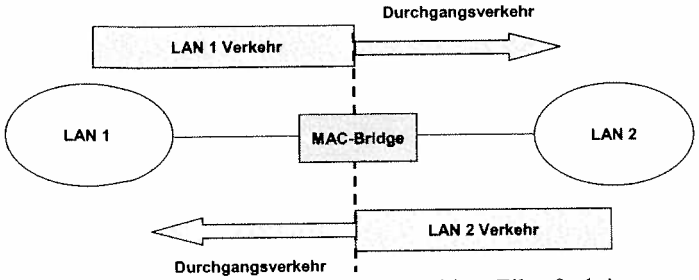
Eine transparente Bridge arbeitet im Gemischtmodus und akzeptiert jeden Rahmen von allen angeschlossenen LANs. Als Beispiel betrachte man ein Bridge mit drei LANs. Durch eine Weiterleitungstabelle können ankommende Rahmen über den richtigen Port an jede Station weitergeleitet werden.

Bild: Transparent Bridges: Weiterleitungstabelle



Bei mehreren Bridges erhalten die Tabellen die Informationen, in welchen LAN-Teilen sich die Stationen befinden.

Bild: Transparent Bridges: Weiterleitungstabelle



Kommt ein Rahmen an, muss sich die Bridge entscheiden, ob er verworfen oder weitergegeben wird, und im letzteren Fall, auf welches LAN er auszugeben ist. Diese Entscheidung wird durch das Nachschlagen der Zieladresse in einer großen Hash-Tabelle innerhalb der Bridge gefällt. Die Tabelle kann jeden möglichen Empfänger und den dazugehörigen Port (das dazugehörige LAN) ausgeben. Ein MAC-Bridge ist somit auch ein Filter.

Bild: Hauptaufgabe einer MAC-Bridge: Filterfunktion

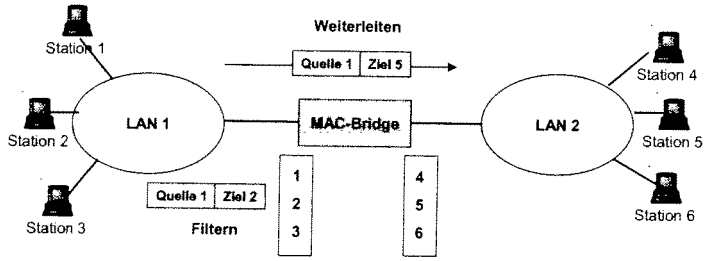
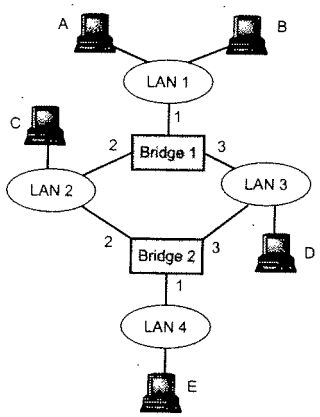


Bild: MAC-Bridge: MAC-Adressen als Filter

Bei der erstmaligen Installation der Bridges sind die Hash-Tabellen leer. Keine der Bridges weiß, wo welches Ziel liegt, so dass der Flooding-Algorithmus angewandt wird. Jeder eintreffende Rahmen für ein unbekanntes Ziel wird auf jedes angeschlossene LAN ausgegeben, außer auf das, von dem er angekommen ist. Mit der Zeit lernt die Bridge, wo die verschiedenen Ziele liegen. Irgend wann sind ihr alle Ziele bekannt und alle Rahmen werden an das jeweils richtige LAN abgegeben, Damit ist auch keine weitere Flooding-Anwendung mehr nötig.

Die Topologie kann sich ändern, wenn Maschinen und Bridges ein- und ausgeschaltet oder verlegt werden. Für die dynamische Topologie wird die Ankunftszeit des Rahmens in den Hash-Tabelleneintrag mit aufgenommen. Jedesmal, wenn ein bereits eingetragener Rahmen ankommt, wird die Zeit des Eintrags aktualisiert. Damit stellt die Zeitangabe im Eintrag den letzten Zeitpunkt dar, an dem ein Rahmen von dieser Maschine gesehen wurde.

In periodischen Abständen überprüft nun ein Prozess die Hash-Tabelle der Bridge und löscht alle Einträge, die älter als ein paar Minuten sind. Wird ein Computer von seinem LAN getrennt, an eine andere Stelle im Gebäude verlegt und dort wieder angeschaltet, ist er innerhalb weniger Minuten wieder lauffähig, ohne dass manuelle Eingaben erforderlich sind. Dieser Algorithmus bedeutet auch, dass der Verkehr zu einer mehrere Minuten lang untätigen Maschine geflutet werden muss, bis sie selbst wieder einen Rahmen versendet.



- Bridge 1 empfängt Rahmen von A an C
- Bridge 1 lernt, dass A über LAN-Port 1 erreichbar ist
- Kennt Bridge 1 Station C, so leitet sie den Rahmen über LAN-Port 2 weiter
- Fluten bei unbekannter Zieladresse
- Spanning Tree
- Filterdatenbasis:
  - Zieladresse
  - Ausgangsport
  - Zeitgeber
- Filtern: Rahmen mit lokalen Adressen werden nicht über Bridge weitergeleitet (z. B. Daten von A an B)

Bild: Transparentes Bridging

Die Routing-Prozedur für einen eingehenden Rahmen hängt vom Quell- und vom Ziel-LAN wie folgt ab:

- Sind Ziel- und Quell-LAN identisch, wird der Rahmen verworfen
- Sind Ziel- und Quell-LAN verschieden, wird der Rahmen weitergegeben
- Ist das Ziel-LAN unbekannt, wird die Flooding-Technik angewandt

Immer wenn ein Rahmen ankommt, muss dieser Algorithmus angewandt werden. Es gibt spezielle VLSI-Chips, die die Tabelleneinträge alle paar Mikrosekunden überprüfen und auf den neuesten Stand bringen.

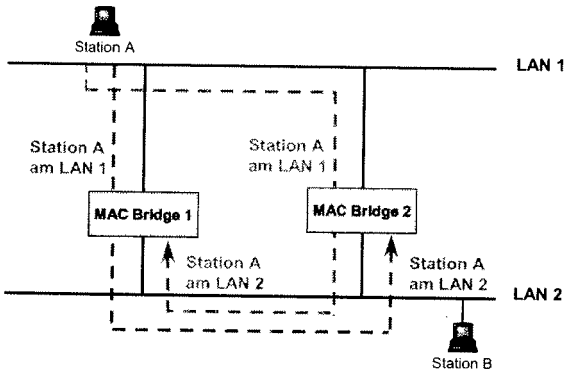


Bild: Transparent Bridges: Schleifenbildung

Um die Zuverlässigkeit noch weiter zu erhöhen, werden bei manchen Anlagen zwei oder mehr Bridges parallel zwischen zwei LANs benutzt. Aber auch diese Anordnung verursacht zusätzliche Probleme, weil in der Topologie Schleifen erzeugt werden.

Ein einfaches Beispiel dieser Problematik kann bei der Behandlung eines Rahmens F von Station A mit unbekanntem Ziel beobachtet werden. Jede Bridge folgt den normalen Regeln für unbekannte Ziele und flutet. In diesem Beispiel bedeutet das lediglich, Rahmen F nach LAN 2 zu kopieren. Kurz danach erkennen Bridges 1 und 2 einen Rahmen mit unbekanntem Ziel und kopieren ihn auf LAN 1. Dieser Kreislauf setzt sich unendlich fort.

Die Lösung für dieses Problem sicht die Kommunikation der Bridges untereinander und die Überlagerung der aktuellen Topologie mit einem überspannenden Baum (Spanning-Tree) vor, der jedes LAN erreicht. Um eine fiktive schleifanlose Topologie aufzubauen, werden einige potentielle Verbindungen zwischen den LANs ignoriert. Im Beipiel 1 gibt es fünf über fünf Bridges zusammengeschlossene LANs. Diese Konfiguration kann in einem Graphen dargestellt werden, in dem die LANs als Knoten erscheinen. Je zwei durch eine Bridge verbundene LANs werden durch eine Kante verbunden. Der Graph kann auf

Grund von wenigen Regeln auf einen überspannenden Baum reduziert werden. Bei diesem überspannenden Baum gibt es genau einen Pfad von jedem LAN zu jedem anderen. Haben die Bridges einmal Übereinkunft über den überspannenden Baum getroffen, erfolgen alle Übertragungen zwischen den LANs über den überspannenden Baum. Da von jeder Quelle zu jedem Ziel ein eindeutiger Pfad führt, sind Schleifen unmöglich.

Um einen überspannenden Baum aufzubauen, sendet jede Bridge alle paar Sekunden ihre Kennung (d.h. eine vom Hersteller installierte und garantiert eindeutige Seriennummer) und eine Liste aller anderen ihr bekannten Bridges zwischen den LANs. Die Bridge mit der niedrigsten Seriennummer bildet die Wurzel. Dann wird ein Baum mit kürzeltmöglichen Pfaden von der Wurzel zu jeder Bridge aufgebaut und das LAN zusammengestellt. Dieser Baum ist der sogenannte Spanning-Tree. Fällt eine Bridge oder ein LAN aus, wird ein neuer Baum berechnet.

Aus diesem Algorithmus entsteht ein einheitlicher Weg von jedem LAN zur Wurzel und damit zu jedem anderen LAN. Obwohl der Baum alle LANs umfasst, müssen nicht unbedingt alle Bridges im Baum enthalten sein (um Schleifen zu vermeiden). Sogar nach der Erstellung des überspannenden Baums läuft der Algorithmus weiter, um Änderungen in der Topologie automatisch zu erfassen und die Konfiguration (den Baum) entsprechend anzupassen.

Bridges können auch zur Verbindung von weit entfernten LANs benutzt werden. In diesem Modell besteht jede Anlage aus einer Reihe von LANs und Brücken, von denen eine mit einem WAN verbunden ist. Rahmen für entfernte LANs werden über das WAN weitergereicht. Hier kann der grundlegende Algorithmus des Spanning-Tree angewandt werden, aber vorzugsweise mit gewissen Optimierungen bzw. der Minimierung des WAN-Verkehrsvolumens

Spanning Tree-Algorithmus

Der Spanning Tree-Algorithmus (ST-Algorithmus) wurde im Standard IEEE 802.1d festgelegt. Damit der ST-Algorithmus funktioniert, muss sichergestellt sein, dass die Bridges (heute auch Switches) bestimmte Informationen über die Topologie der LAN-Vernetzung bekommen können. Dazu wird ein Protokoll benutzt, um bestimmte Angaben zwischen den Bridges austauschen zu können. Für den Transport dieser Angaben dient ein Paket, das standardmäßig Konfigurations-BPDU (Configuration Bridge Protocol Data Unit) genannt und auch als Hallo-Paket bezeichnet wird. Die Bridges verschicken die Konfigurations-PDU, um sich gegenseitig kennenzulernen und die Angaben zu übermitteln, die notwendig sind, um aus einer beliebigen primären Vernetzungs-Topologie eine sekundäre Baum-Topologie zu erreichen. Diese Baum-Topologie garantiert die gleichen Kommunikationsbeziehungen und vermeidet die Zirkulation von MAC-Frames (Schleifenbildung). Um diese Baum-Topologie zu verwirklichen, werden nach dem ST-Algorithmus einige Bridges als redundant erklärt und vom restlichen System logisch abgetrennt.

Für den Einsatz des ST-Algorithmus müssen bestimmte Festlegungen getroffen werden, dazu gehören u. a.:

- Jede Bridge hat eine eindeutige Kennung (Bridge-ID), die voreingestellt wird und mit Hilfe des Bridge-Managements verändert werden kann. Sie ist 6 Bytes lang.
- Jeder Bridge-Port muss eindeutig gekennzeichnet werden (Port-ID).
- Jedem Bridge-Port müssen die entsprechenden Portkosten (Port Cost) zugewiesen werden. Diese Kosten werden zugewiesen, um die sekundäre Baum-Topologie zu beeinflussen. Die Kosten eines Ports zu einem LAN können z.B. umgekehrt proportional zur Bitrate im LAN oder direkt proportional zur LAN-Auslastung sein. Die Kosten eines Ports zu einem WAN können die Übertragungskosten widerspiegeln.
- Wenn zwei LANs über mehrere Bridges parallel verbunden sind, muss die Wichtigkeit von einzelnen Bridges durch die Bridge-Prioritäten (Bridge Priority) definiert werden.

Wichtige Begriffe und Parameter beim ST-Algorithmus sind:

- **Root-Bridge (Wurzel-Bridge):** Die Bridge, die die Wurzel der Baumtopologie darstellt. Als Root-Bridge dient die Bridge mit der niedrigsten Kennung (Bridge-ID).
- **Root-Port:** Der Root-Port einer Bridge ist der, über den die niedrigsten Übertragungskosten zur Root-Bridge entstehen.
- **Root-Path (Root-Pfad):** Die Route zwischen einem Root-Port und der Root-Bridge, auf der die niedrigsten Übertragungskosten entstehen.
- **Root Path Cost (RPC):** Root-Pfadkosten: Mit jedem Root-Port sind die Kosten RPC verbunden. Sie stellen die Summe von Kosten aller Root-Ports auf dem Root-Pfad dar.

Struktur der Konfigurations-BPDU.

- **Protocol-ID (Protokollkennung):** Beinhaltet einen konstanten Wert von 0.
- **Protocol Version-ID (Protokollversion-Kennung):** Beinhaltet einen konstanten Wert von 0.
- **BPD U Type:** Beinhaltet einen konstanten Wert von 0.
- **Flags TC und TCA:** TCA (Topology Change Acknowledge): Ist das höchstwertige Bit TCA gesetzt, dann muss eine Topologieänderungsinformation nicht bestätigt werden.
- **Root-ID:** Besteht aus einer zwei Byte langen Priorität und der Kennung der Root-Bridge (6 Byte).
- **Root Path Cost:** Hier werden die Root-Pfadkosten, d.h. die Kosten der billigsten Route zur Root-Bridge, angegeben.

- **Bridge-ID:** Die Kennung der Bridge, die diese BPDU gesendet hat. Hier steht die 2 Byte große Bridge-Priorität und die 6 Byte große Bridge-ID.
- **Port-ID:** Der Port, über den die BPDU gesendet wurde. Beinhaltet 1 Byte Port-Priorität und 1 Byte für die Port-ID.
- **Message Age (Alter der Nachricht):** Die geschätzte Zeit in Einheiten von 1/256 s ab dem Absenden der BPDU durch die Root-Bridge.
- **Max Age (Maximales Alter):** Die Zeit in Einheiten von 1/256 s, nach der die Nachricht gelöscht werden soll.
- **Hello Time:** Die Zeitperiode in Einheiten von 1/256 s zwischen dem Absenden von zwei Konfigurations-BPDUs durch die Root-Bridge.
- **Forward Delay:** jeder Bridge-Port kann sich nur in festgelegten Zuständen befinden. Einer dieser Zustände ist Blocking, in dem der Port blockiert wird. Im Zustand Blocking kann keine Übertragung über den Port stattfinden. Ein anderer Zustand ist Forwarding, in dem die Übermittlung von MAC-Frames über den Port stattfinden kann. Der Wert Fortvard Delay gibt den Zeitraum in Einheiten von 1/256 s an, für den die Bridges in jedem der Zwischenzustände verbleiben sollen, bevor sie einen Port vom Zustand Blocking in den Zustand Forwarding versetzen.

Der ST-Algorithmus erfolgt in fünf Schritten:

Schritt 1: Auswahl der Root-Bridge
Um eine Baum-Topologie zu erzeugen, muss die Root-Bridge ausgewählt werden. Als Root-Bridge dient die Bridge mit der niedrigsten ID. Um die Root-Bridge festzustellen, sendet jede Bridge ein Konfigurations-BPDU als Broadcast-Nachricht über alle ihre Ports und gibt als Root-ID ihre eigene ID an. Empfängt eine andere Bridge diese Konfigurations-BPDU, dann vergleicht sie ihre eigene ID mit der Root-ID. Ist die Root-ID niedriger als die ID der betreffenden Bridge, sendet sie diese BPDU als Broadcast-Nachricht weiter. Ist die Root-ID größer als die ID der betreffenden Bridge, trägt sie die eigene ID als Root-ID ein und sendet diese BPDU weiter. Nach einer gewissen Zeit setzt sich die Bridge mit der niedrigsten ID als Root-Bridge durch.

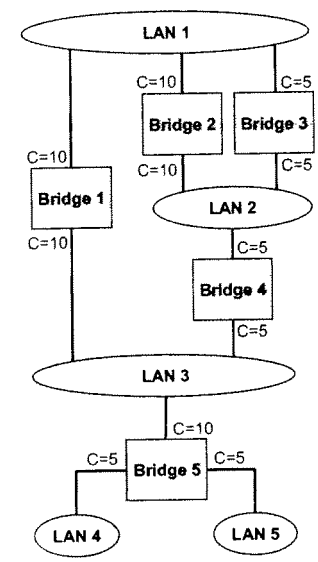
Schritt 2: Bestimming der Root-Bridge-Kosten
Wie bereits erwähnt wurde, stellt die RPC die Summe von Root-Portkosten auf dem Pfad zur Root-Bridge dar. In der Praxis werden als Portkosten oft 1 angenommen, so dass der RPC-Wert die Anzahl von Bridges auf dem Weg zur Root-Bridge angibt.

Schritt 3: Bestimming der Root-Ports
Jede Bridge (ausgenommen die Root-Bridge) bestimmt ihren Root-Port: jede Bridge entscheidet, welcher von ihren Ports als Root-Port dienen soll. Es wird der Port ausgewählt, über den die Route-Kosten (RPC) die kleinsten sind. Gibt es mehrere Wege über verschiedene Ports und sind die RPCs gleich, dann wird der Port mit der höchsten Priorität als Root-Port verwendet. Werden keine Prioritäten gesetzt, wird der Port mit der niedrigsten ID als Root-Port ausgewählt.

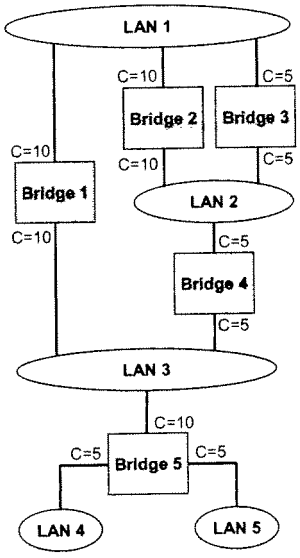
Schritt 4: Bestimming der Designated Ports für jedes LAN und WAN
Für jedes LAN wird ausgewählt, über welche Bridge der Außen-Datenverkehr abgewickelt wird: Wird ein LAN an mehrere Bridges angeschlossen, so dass über jede davon der Außenverkehr abgewickelt werden kann, dann führt in diesem Fall über jede Bridge mindestens ein Weg zur Root-Bridge. Um eine Baum-Topologie zu erzeugen, darf der Außen-Datenverkehr nur über eine Bridge stattfinden. Eine Bridge für jedes LAN mit den geringsten Übertragungskosten RPC zur Root-Bridge gewinnt den Wettbewerb und wird für den Außen-Datenverkehr ausgewählt (Designated Bridge). Gibt es mehrere Bridges mit dem gleichen RPC-Wert, gewinnt die Bridge mit der niedrigsten ID. Den Port in der Designated-Bridge, über den den Außen-Datenverkehr abgewikkelt wird, bezeichnet man als Designated-Port. Pro LAN kann nur ein Designated-Port vorhanden sein. Alle Ports der Root-Bridge sind grundsätzlich designated.

Schritt 5: Entfernung von allen Bridges ohne Designated Port
Die Bridges, die nicht ausgewählt wurden, sperren ihre Ports (Zustand Blocking), hören aber weiterhin mit, um im Fall eines Bridge-Ausfalls zum Einsatz zu kommen.

Entdeckung eines Ausfalls und erneute Aktivierung des ST-Algorithmus
Wenn eine aktive Bridge (Root, Designated) oder irgendein aktiver Bridge-Port (Designated-Port) ausfällt, so wird dies mit Hilfe des Timers (Message Age) in irgendeiner Bridge entdeckt. Ist Message-Age größer als Max-Age, kann dies bedeuten, dass eine aktive Komponente (ganze Bridge oder nur ein aktiver Port) ausgefallen ist. Diejenige Bridge, die das bemerkt hat, verschickt eine Nachricht, die Topologie-Änderungsanzeige BPDU (topology change notification BPDU). Daraufhin wird der ST-Algorithmus erneut aktiviert.



Routing over Bridges (Spanning Tree)



1) Determine the Root Bridge

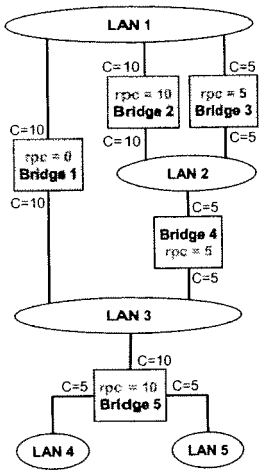
Ausgangspunkt:

1) Bridges haben eine eindeutige Identifikationsnummer.
2) Jeder Port eines Bridges wird einen Kostenfaktor zugewiesen

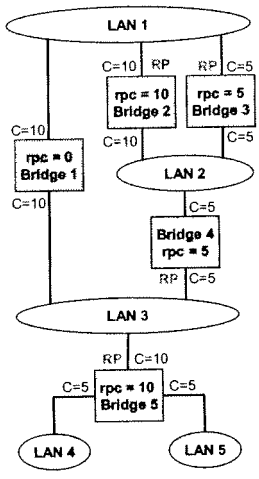
Spanning Tree Algorithmus:

1. Wahl des Root-Bridge als Bridge mit der niedigsten Identifikationsnummer.
2. Berechnung der niedrigsten Wurzelpfadkosten für jeden Bridge.
3. Bestimmung des Root-Bridge Ports für jeden Bridge. Dies ist der Port mit der niedrigsten Wurzelpfadkosten
4. Bestimmung des Designated Ports für jedes LAN. Dies ist der Port eines Bridges, der ein LAN mit den geringsten Kosten mit dem Root-Bridge verbindet.
5. Entfernung von allen Bridges ohne Designated Port

Bild: Beispiel 1: Spanning Tree Algorithmus (1)



2) Bestimme RPC für jede Bridge

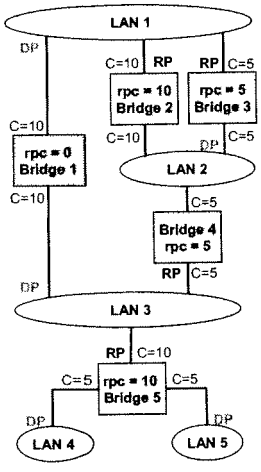


3) Bestimme Route Bridge Port für alle Bridges

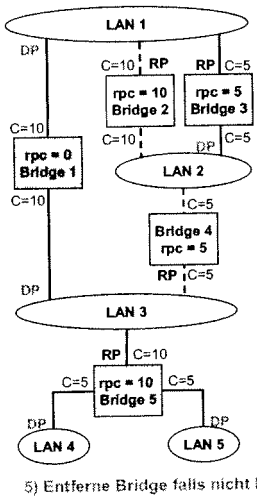
Bridge 1 ist Root Bridge

C Cost
DP Designated Port
RP Root Port
RPC Root Path Cost

Bild: Beispiel 1:
Spanning Tree Algorithmus (2)



4) Bestimme Designated Port für alle LANs



5) Entferne Bridge falls nicht DP

Bridge 1 ist Root Bridge

C Cost
DP Designated Port
RP Root Port
RPC Root Path Cost

Bild: Beispiel 1:
Spanning Tree Algorithmus (3)

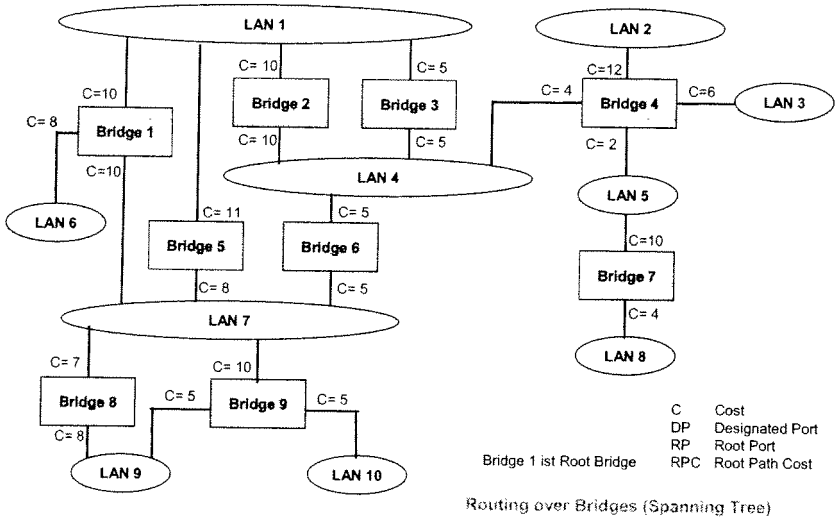


Bild: Beispiel 2:
Spanning Tree Algorithmus (1)

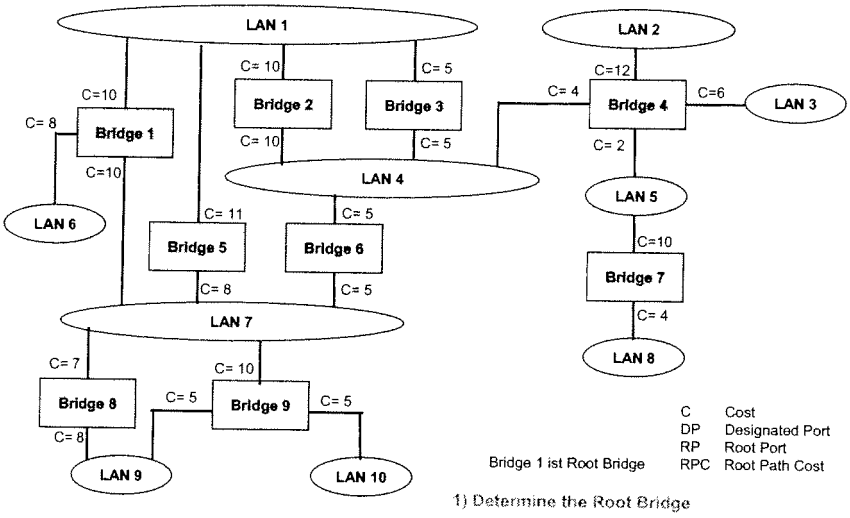


Bild: Beispiel 2:
Spanning Tree Algorithmus (2)

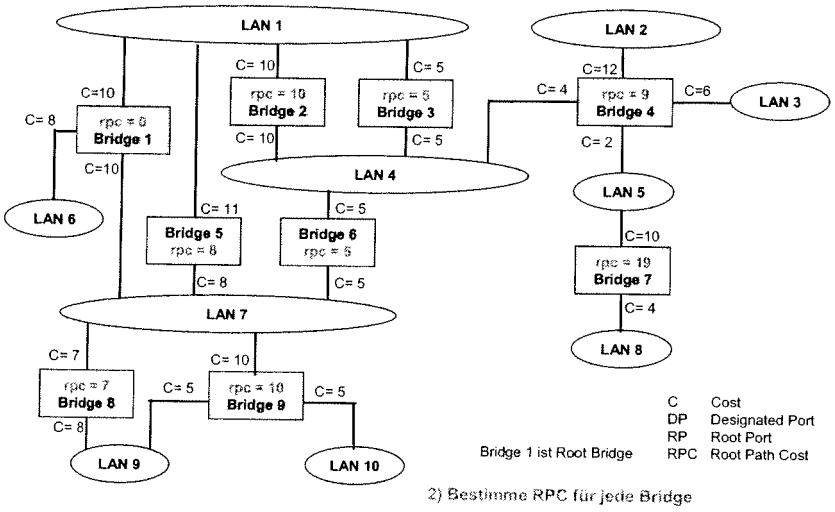


Bild: Beispiel 2:
Spanning Tree Algorithmus (3)

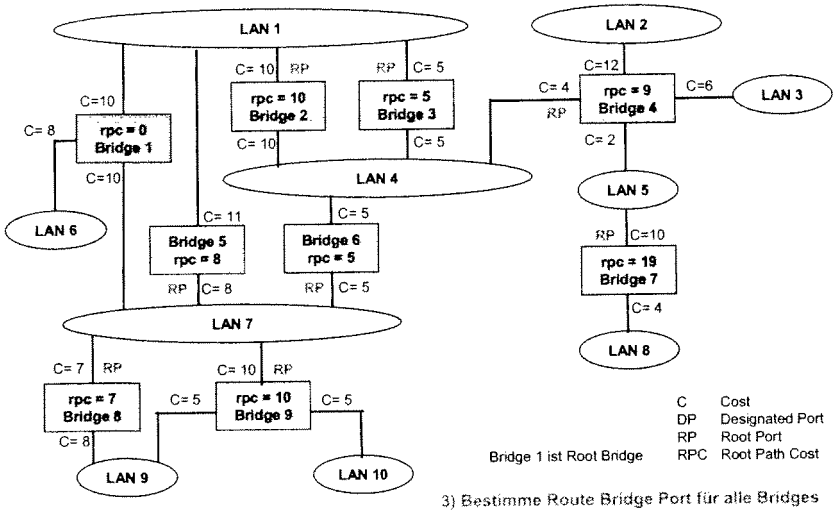


Bild: Beispiel 2:
Spanning Tree Algorithmus (4)

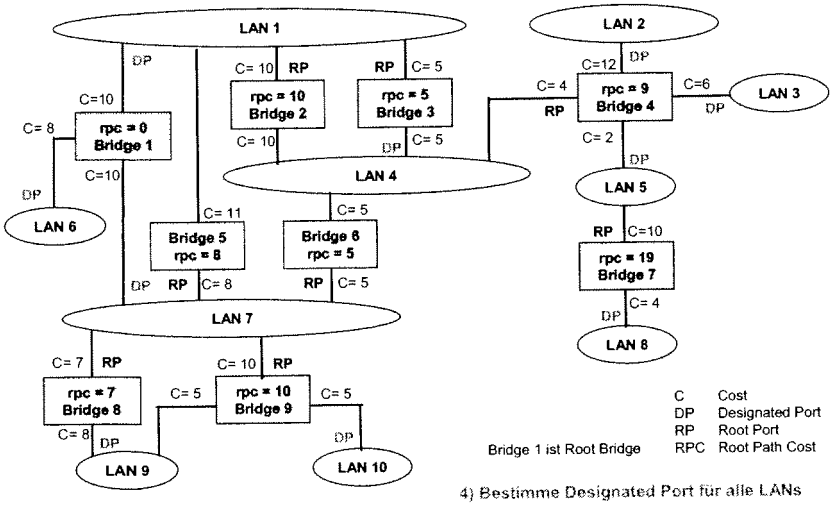


Bild: Beispiel 2:
Spanning Tree Algorithmus (5)

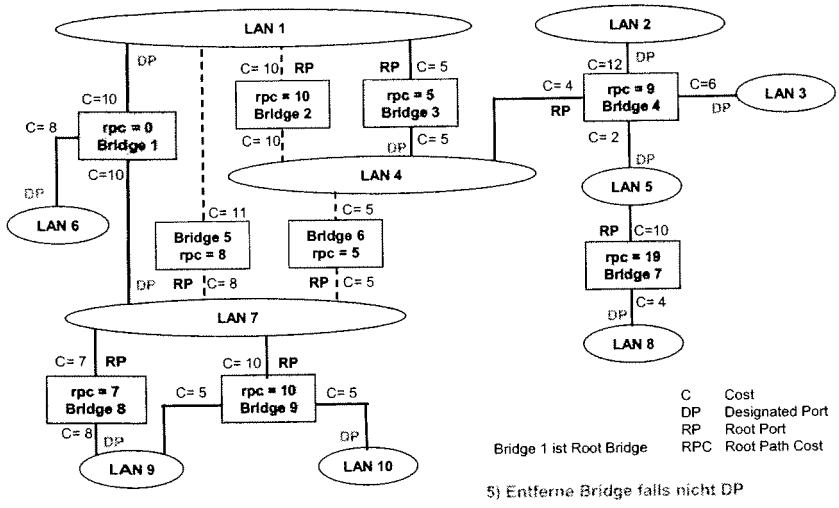


Bild: Beispiel 2:
Spanning Tree Algorithmus (6)

- Einkapselung von MAC-Dateneinheiten (keine Umsetzung)
- Remote-Bridges treten paarweise auf
- Nur zur Kommunikation zwischen LAN 1 und LAN 2
- Transparente Verbindung
- Keine Kommunikation von LANs 1 oder 2 mit dem WAN
- Virtuelle Anschlüsse

Bild: Remote Bridges

Remote-Bridges

Bridges werden vorwiegend zum Verbinden von zwei oder mehr entfernten LANs benutzt, z. B. in einem Unternehmen mit Niederlassungen und/oder Fertigungsstätten mit je einem eigenen LAN an verschiedenen Orten. Im Idealfall werden alle LANs miteinander verbunden, um so einen globalen Netzverbund zu realisieren

Dieses Ziel kann erreicht werden, indem man in jedem LAN eine Bridge installiert und die Bridges paarweise über Punkt-zu-Punkt-Leitungen (z.B. Standleitungen des Telefonnetzes) miteinander verbindet. Für die Punkt-zu-Punkt-Leitungen sind verschiedene Protokolle möglich, z. B. ein Standardprotokoll der Sicherungsschicht und das Einfügen kompletter MAC-Rahmen in das Nutzdatenfeld. Diese Strategie Funktioniert am besten, wenn alle LANs identisch sind und die einzige Aufgabe nur darin besteht, Rahmen zum richtigen LAN zu befördern. Eine andere Alternative wäre das Entfernen des MAC-Headers und -Teilers in der Quell-Bridge, wobei man dann den Rest in das Nutzdatenfeld des Punkt-zu-Punkt-Protokolls einfügt. An der Ziel-Bridge kann dann ein neuer MAC-Header und MAC-Trailer erzeugt werden. Dieser Ansatz hat aber den Nachteil, dass die beim Zielhost ankommende Prüfsumme nicht die ist, die vom Quellhost berechnet wurde. Aus diesem Grund werden eventuell im Bridge-Speicher vorhandene fehlerhafte Bits nicht aufgedeckt.

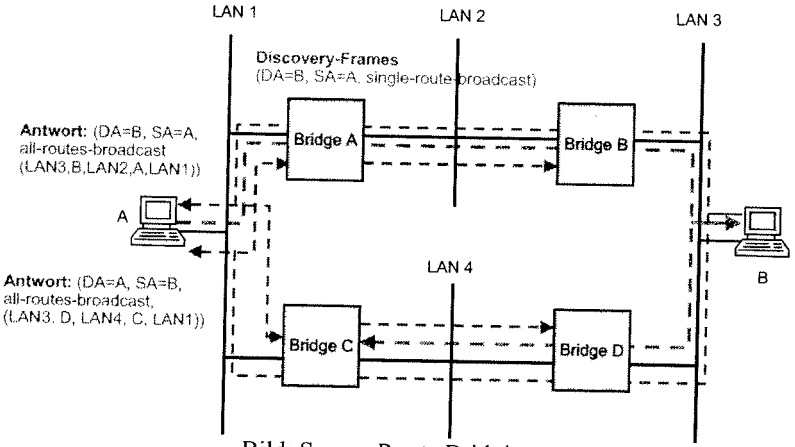


Bild: Source Route Bridging

Source-Routing-Bridges

Transparente Bridges haben den Vorteil der einfachen Installation. Man steckt sie einfach ein. Andererseits nutzen sie die Bandbreite nicht optimal, weil sie nur einen Teil der Topologie (den überspannenden Baum) berücksichtigen. Im wesentlichen basiert Source-Routing auf der Annahme, dass der Sender eines Rahmens weiß, ob sich das Ziel in seinem eigenen LAN befindet. Sendet er einen Rahmen an ein anderes LAN, setzt die Quellmaschine das High-Order-Bit der Quelladresse auf 1. Danach setzt sie in den Rahmen-Header den genauen Pfad, den der Rahmen folgen muss.

Dieser Pfad wird wie folgt ausgebaut: Jedes LAN hat eine eindeutige, aus 12 Bit bestehende Nummer. Jede Bridge hat eine 4 Bit große Nummer, durch die sie innerhalb ihres LANs eindeutig identifiziert wird. Zwei Bridges, die weit auseinander liegen, können also beide z.B. die Nummer 3 haben, während Bridges im gleichen LAN eindeutig nummeriert werden müssen. Eine Route ist eine Folge von Bridge, LAN und Bridge-Port-Nummern.

Eine Source-Routing-Bridge ist nur an den Rahmen interessiert, bei denen das High-Order-Bit des Ziels auf 1 steht. Erkennt sie einen solchen Rahmen, tastet sie die Route ab und sucht die Nummer des LANs, in dem der Rahmen angekommen ist. Folgt der LAN-Nummer ihre eigene Nummer, gibt die Bridge den Rahmen an das LAN weiter, dessen Nummer nach ihrer Nummer folgt. Folgt der LAN-Nummer die Nummer einer anderen Bridge, leitet sie den Rahmen nicht weiter.

Dieser Algorithmus eignet sich für drei mögliche Implementierungen:

- **Software:** Die Bridge läuft im Gemischtmodus und kopiert alle Rahmen in ihrem Speicher, um zu sehen, ob das werthöchste Zielbit auf 1 gesetzt wurde. Trifft das zu, wird der Rahmen weiter bearbeitet, andernfalls nicht.
- **Hybrid:** Die LAN-Schnittstelle der Bridge untersucht das Zielbit und übergibt der Bridge ausschließlich Rahmen mit gesetztem Bit. Diese Schnittstelle kann leicht in die Hardware integriert werden. Sie reduziert die Zahl der von der Bridge zu prüfenden Rahmen.
- **Hardware:** Die LAN-Schnittstelle untersucht nicht nur das werthöchste Zielbit, sondern sieht auch noch in der Route nach, ob ihre Bridge an der Weitergabe beteiligt ist. Nur Rahmen, die übertragen werden müssen, kommen bei der Bridge an. Diese Implementierung stellt den höchsten Hardware-Aufwand, verringert aber die Anzahl der Durchgänge zwischen CPU und Bridge, da alle irrelevanten Rahmen ausgesondert werden.

Diese drei Implementierungen unterscheiden sich in Preis und Leistung. Bei der ersten entstehen keine zusätzlichen Hardwarekosten für die Schnittstelle, aber es wird eine sehr schnelle CPU für die Bearbeitung aller Rahmen benötigt. Bei der letzten ist ein spezieller VLSI-Chip erforderlich, aber man verlagert so einen Großteil der Rechenarbeit von der Bridge auf den Chip, so dass entweder eine langsamere CPU benutzt werden oder die Bridge mehr LANs bedienen kann.

Beim Source-Routing wird vorausgesetzt, dass jede Maschine des Netzverbunds die Route zu jeder anderen Maschine genau kennt. Wie diese Routen ermittelt werden, ist ein wichtiger Teil des Source-Routing-Algorithmus. Dem Grundkonzept zufolge gibt die Quelle einen Broadcast-Rahmen aus, um herauszufinden, wo sich das Ziel befindet, falls es nicht bekannt ist. Dieser Suchrahmen (Discovery Frame) wird von jeder Bridge gesendet. Er erreicht damit jedes LAN im Netzverbund. Kommt die Antwort zurück, fügen die Bridges ihre Kennung ein, so dass der Sender den zurückgelegten Weg sehen und endgültig die beste Route ermitteln kann.

Hat ein Host einmal einen Weg zu einem bestimmten Ziel gefunden, wird dieser in einem Cache-Speicher abgelegt, so dass der Suchprozess beim nächsten Mal nicht erneut durchgeführt werden muss. Bei dieser Methode entsteht zwar nicht die oben beschriebene Rahmenexplosion, sie belastet aber die Hosts mit zusätzlichem Verwaltungsaufwand. Außerdem ist der Algorithmus insgesamt nicht transparent, was ja ursprünglich eines der Hauptziele war.

Der wichtigste Unterschied zwischen den zwei Bridge-Typen ist die Unterscheidung zwischen verbindungsloser und verbindungsorientierter Netztechnik. Die transparente Bridge hat kein Konzept einer virtuellen Verbindung und leitet jeden Rahmen unabhängig von allen übrigen weiter. Demgegenüber ermittelt die Source-Routing-Bridge anhand von Suchrahmen eine geeignete Route und benutzt künftig immer diese Route.

Die transparente Bridge ist für die Hosts völlig unsichtbar und uneingeschränkt mit allen vorhandenen 802-Produkten kompatibel. Die Source-Routing-Bridge ist weder transparent noch kompatibel. Um Source-Routing anwenden zu können, müssen die Hosts das Bridge-Schema kennen und aktiv teilnehmen. Die Aufteilung eines vorhandenen Netzes in zwei LANs, die durch eine Source-Routing-Bridge verbunden werden, setzt Änderungen der Host-Software voraus.

Transparente Bridges erfordern kein Netzmanagement. Die Bridges konfigurierten sich selbst automatisch auf die gegebene Topologie. Bei Source-Routing-Bridges muss der Netzmanager die LAN- und Bridge-Nummern manuell konfigurieren. Fehler wie doppelte LAN- oder BridgeNummern lassen sich nur sehr schwer abgrenzen, weil sie verursachen können, dass einige Rahmen in Schleifen kreisen. Zwei vormals getrennte Netze können beim Einsatz von transparenten Bridges beispielsweise direkt miteinander verbunden werden, während beim Source-Routing eventuell viele LAN-Nummern manuell geändert werden müssen.

Einer der wenigen Vorteile der Source-Routing-Bridge ist der, dass sie theoretisch optimales Routing bietet, während die transparente Bridge auf den Spanning-Tree begrenzt ist. Source-Routing eignet sich auch gut, wenn parallele Bridges eingesetzt werden, um die Belastung auf die LANs aufzuteilen. Die Lokalisierung von Zielen wird bei transparenten Bridges durch das Backward-Learning und bei Source-Routing-Bridges durch Suchrahmen vorgenommen. Backward-Learning hat den Nachteil, dass die Bridge warten muss, bis ein Rahmen von einer bestimmten Station eingeht, um ihre Position zu erfassen. Der Nachteil von Suchrahmen besteht darin, dass sie sich in einem umfangreichen Netzverbund exponentiell vermehren.

Die Handhabung von Störungen unterscheidet sich bei den beiden Verfahren beträchtlich. Transparente Bridges erkennen Störungen auf anderen Bridges und LANs sowie Änderungen der Topologie schnell und automatisch, da sie laufend die Steuerrahmen der verschiedenen Komponenten prüfen. Hosts bekommen diese Änderungen überhaupt nicht mit.

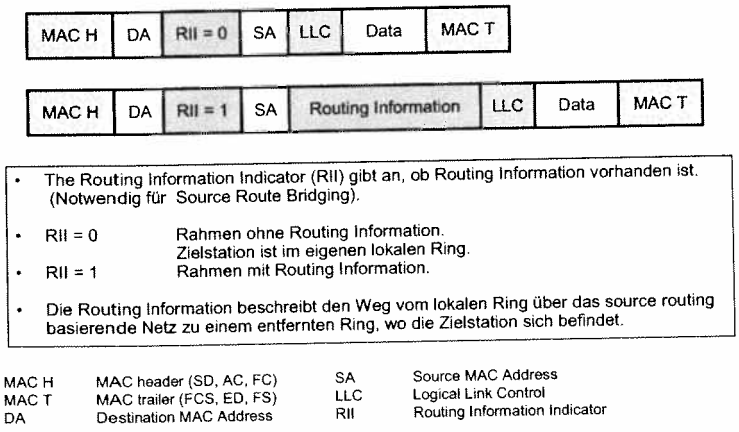


Bild: IEEE 802.5 Rahmenformat mit RII

Beim Source-Routing ist die Situation ganz anders. Wenn eine Bridge versagt, nehmen die Stationen, deren Route über sie führt, anfänglich nur wahr, dass ihre Rahmen nicht mehr bestätigt werden. Sie warten das Timeout ab und versuchen es immer wieder. Endlich folgern sie, dass etwas nicht in Ordnung ist. Sie wissen aber immer noch nicht, ob das Problem mit dem Ziel selbst oder mit dem gewählten Weg zusammenhängt. Nur durch die Versendung eines weiteren Suchrahmens erfahren sie, ob das Ziel ansprechbar ist. Wenn unglücklicherweise eine Haupt-Bridge ausfällt, müssen viele Hosts den Ablauf der Timer abwarten und neue Suchrahmen aussenden, bevor das Problem gelöst ist, auch wenn ein alternativer Weg verfügbar ist. Diese höhere Fehleranfälligkeit ist eine der größten Schwächen aller verbindungsorientierten Systeme.

Was die Komplexität und die Kosten anbelangt, bestehen viele Kontroversen. Hat die Source-Routing-Bridge einen VLSI-Chip, der nur die weiterzugebenden Rahmen einliest, hat sie einen etwas niedrigeren Rahmenverarbeitungsaufwand zu bewältigen und bietet im Verhältnis zu den getätigten Hardwareinvestitionen eine bessere Leistung. Ohne diesen Chip schneidet sie schlechter ab, weil dann der Verarbeitungsaufwand pro Rahmen (Ermitteln der Route im Rahmen-Header) wesentlich höher ist.

Source-Routing erhöht auch die Komplexität der Hosts. Sie müssen Routen speichern, Suchrahmen senden und Routeninformationen in jeden Rahmen kopieren. Alle diese Dinge erfordern mehr Speicher und CPU-Leistung. Da eine Installation in der Regel viel mehr Hosts als Bridges umfasst, erscheint es vorteilhafter, die nötige Komplexität und Mehrkosten in wenigen Bridges als in vielen Hosts zu realisieren.

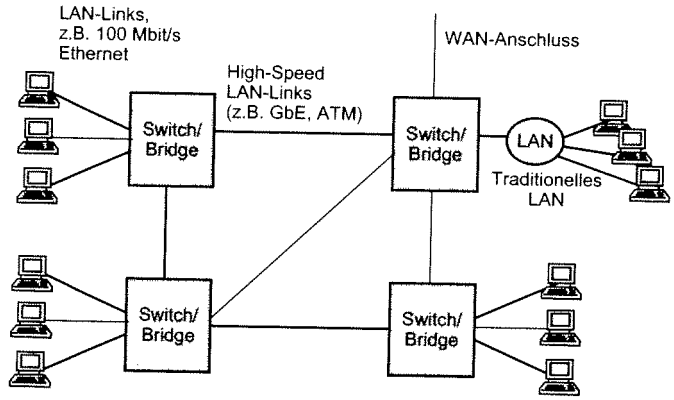


Bild: LAN Switching

Heutige LANs verwenden mehrheitlich Switches an denen die Rechnerstationen direkt oder über Ethernet Kollisionsdomainen angeschlossen sind. Die Switches sind oft über Gigabit-Ethernet (GbE) Links miteinander verbunden.

Ein Layer-2 Switch ist als eine transparente Brücke zu betrachten. Somit muss auch in Switched Ethernet-LANs ein Spanning Tree aufgebaut werden.

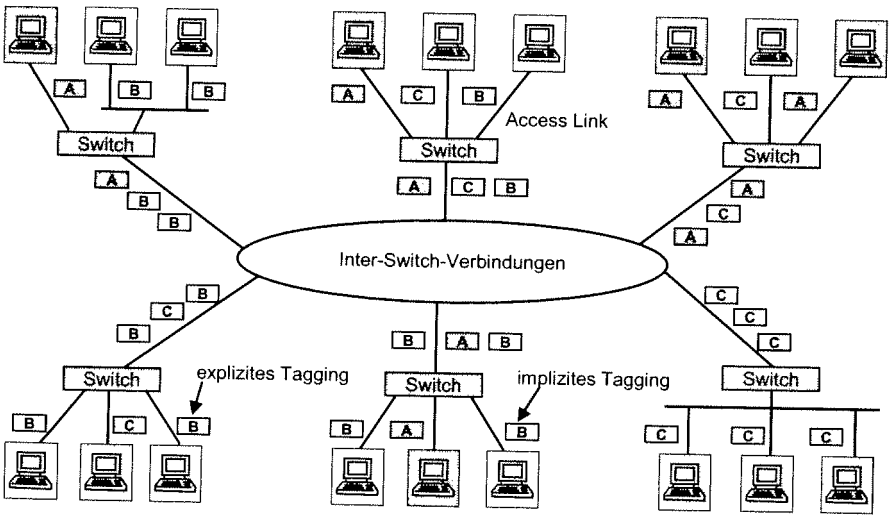


Bild: Virtuelle LANs mit IEEE 802.1Q Tagging

Durch einen sogenannten IEEE 802.1Q Tag können Virtuelle LANs (VLANs) aufgebaut werden. Es gibt verschiedenen Gruppen von Stationen, die zu einem VLAN gehören. Ihre Rahmen werden nur an Stationen innerhalb einer Gruppe weitergeleitet.

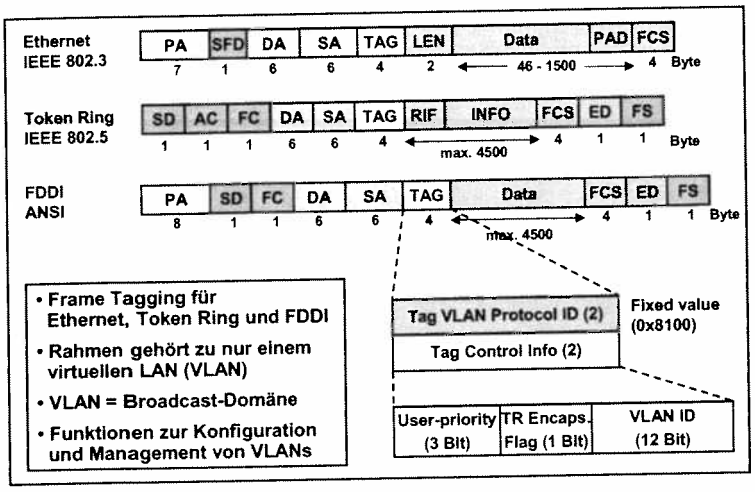


Bild: IEEE 802.1Q: Virtueller LAN

Virtual LANs (IEEE 802. 1Q)

Die traditionellen LANs (Ethernet, Token Ring, FDDI) haben alle einen gemeinsamen Nachteil: Es handelt sich um Shared-Media-Technologien. Das heißt, der Anwender muss sich seine Bandbreite mit allen anderen Teilnehmern teilen. Dadurch entstand die Idee, durch geeignete technische Maßnahmen in den Verteilerräumen nicht nur die Bandbreite eines technischen LAN-Segments zu erhöhen, sondern die von einer konventionellen Technologie angebotene Bandbreite einer einzelnen Station dauerhaft und exklusiv zur Verfügung zu stellen (IEEE 802.1p). So wäre man nicht gezwungen, die strukturierte Verkabelung, die Adapterkarten in der Workstation oder die Software zu ändern. Durch die Einführung der Switching-Technologie baute man zwar flachere Netzstrukturen auf, musste aber mit den Schwierigkeiten von Broadcast-Stürmen und fehlender Sicherheit leben. Virtuelle LANs (VLANs) nach IEEE 802.1Q sollen dieses Problem in den Griff bekommen.

Dedicated-Ethernet ist beispielsweise eine solche Switching-Technologie, die nur eine Änderung in den Verteilerräumen notwendig werden lässt. Stationen werden durch einen Dedicated-Ethernet-Switch-Port mit dem Netz verbunden und nicht über einen Repeater Port. Mehrere Dedicated-Ethernet-Switches können dann wiederum durch ein High-Speed-Backbone miteinander verknüpft werden. Dabei bekommt jede angeschlossene Station 10 Mbit/s für eine Netzverbindung (Mikrosegmentierung). Im Extremfall der Mikrosegmentierung, d.h., eine Endstation pro Switch-Port, liegt dabei der Backbone des Netzes im Switch selber.

Technisch gesehen lässt sich diese Technik mit einem Bridge-Port vergleichen: Pakete werden durch ihre Zieladresse an den passenden Empfängerport geschickt. Dadurch sind Kollisionen zwischen den Arbeitsstationen und dem Switch ausgeschlossen. Wie bei einer Bridge wechseln dabei Lern- und Arbeitsphasen. In der Lernphase nimmt der Switch neue Zieladressen in die Adressliste auf und verdrängt bei einer vollen Liste die Adressen, die länger nicht mehr benutzt wurden. Der Speicherplatz für die Adressen ist bei Dedicated Ethernet deutlich reduziert worden, wodurch der benötigte Platz für die Zwischenspeicherung der Pakete sinkt und die Rechenleistung bei der Datensuche ebenfalls verringert wird. Weitere Optimierungen entstehen durch das Weglassen klassischer Bridge-Funktionen wie den Methoden zur Schleifenerkennung oder Paketfilterung, die hier nicht benötigt werden. Um die Kosten bzw. den nötigen Platz auf dem Chip weiter zu reduzieren, implementierte man eine neue Methode zur Weiterleitung von Paketen, die als Cut-Through-Switching bezeichnet wird. Das Verfahren erlaubt die Weiterleitung eines Pakets bereits nach Auswertung der Zieladresse. Das heißt, die Datenpakete werden nur bis zur Layer-2-Zieladresse (MAC-Adresse) überprüft und danach weiter transportiert. Somit wird nicht mehr das vollständige Datenpaket zwischengespeichert und auf Fehler untersucht (Store-and-Forward-Technik). Die Latenzzeit des Systems ist sehr kurz und unabhängig von der Paketlänge immer gleich. Dadurch ist dieses Verfahren wesentlich schneller als konventionelle Architekturen, was durch die besser werdende Qualität der Übertragungsstrecken ermöglicht wird. Dies ist ein genereller Trend, auch bei Protokollen der höheren Schichten.

Eine weitere Möglichkeit, Switching in ein klassisches Ethernet einzuführen, ist die Segmentierung. Bisherige Arbeitsgruppen bestehen noch aus 10-Mbit/s-Strängen, die mit Repeatern unterteilt bzw. verlängert sind. Dadurch müssen sich Arbeitsstationen und Server diese 10 Mbit/s teilen. Durch einen Switch lässt sich der Ethernet-Strang segmentieren, indem alle Repeater an den Switch angeschlossen werden. Jedes Segment verfügt anschließend über eine eigene Bandbreite von 10 Mbit/s, die sich jetzt nur noch die Arbeitsstationen in den jeweiligen Segmenten teilen müssen. Die Server bekommen ein einzelnes Segment, um die dedizierte Bandbreite von 10 Mbit/s (Ethernet) oder 100 Mbit/s (Fast-Ethernet) zur Verfügung stellen zu können. Dies kann bis zur Mikrosegmentierung (ein Switch stellt einer Arbeitsstation exklusiv die 10 Mbit/s Gesamtbandbreite zur Verfügung) vorgenommen werden.

Switches werden demnach hauptsächlich zur Segmentierung eingesetzt, um die Datenlast in das Backbone zu verlagern. Bei einer Endstation pro Port (Mikrosegmentierung) kann sogar der Backbone des Netzes im Switch selbst vorhanden sein, wodurch man sehr hohe Datenraten (1 Gbit/s) erzielen kann. Wie alle Verfahren der Schicht 2 ist aber auch das LAN-Switching nicht in der Lage Broadcast-Grenzen aufzubauen. Das heißt, es handelt sich bei geswitchten Netzen um ein logisches Netz, welches nur eine einzelne Broadcast-Domäne besitzt. Broadcast-Meldungen können sich demnach im gesamten Netz ausbreiten und belasten das Netz unnötig. Zusätzlich ist es nicht möglich, Sicherheits- und Schutzzonen aufzubauen, da Switches der Schicht 2 Netze nur aufgrund der Adresseninformationen der Hardware-Adresse (MAC-Address) trennen. Dies macht die Einführung von VLANs notwendig.

Das Konzept eines VLANs soll erreichen, dass physikalisch getrennt sitzende Anwender in frei definierbaren logischen Gruppen zusammengefasst werden können. Dadurch entfällt der Verwaltungsaufwand bei Umzügen von Mitarbeitern innerhalb des Unternehmens bzw. es können unterschiedliche Arbeitsgruppen quer durch die Unternehmenshierarchie gebildet werden. Eine freie Zuordnung aller Netzressourcen zu den entsprechenden Subnetzen ist damit verbunden. Alle Teilnehmer in einem Subnetz können ohne Einschränkung miteinander kommunizieren. Broadcasts werden somit nur innerhalb der Subnetze weitergeleitet. Für eine Kommunikation von Teilnehmern unterschiedlicher Netze ist der Einsatz einer höheren Vermittlung, z.B. eines Routers notwendig. VLANs ermöglichen somit eine höhere Flexibilität und eine flachere Netzstruktur. Voraussetzung für VLANs ist eine strukturierte Verkabelung, der Einsatz von Switching-Komponenten und Netzmanagement aller Netzkomponenten.

Probleme können allerdings auftreten, wenn nicht ausschließlich Switching-Techniken verwendet werden. Dadurch müssen Konversionen anderer Netztypen wie Token Ring, FDDI oder Ethernet durchgeführt werden. Diese Pakete müssen nicht nur ganz zwischengepuffert, sondern auch bestimmte Felder neu berechnet und ersetzt werden. Mit steigendem Anteil derartiger Pakete sowie durch unterschiedliche Datenrate der Switches (Uplinks und Downlinks), wird der Vorteil des Cut-Through-Switching aufgehoben. D.h., es findet wieder ein Store-and-Forward statt, Cut-Through wird nur im Switch selbst vorgenommen. Weiterhin besitzen viele PCs keine Adapterkarten, die die volle Datenrate unterstützen. Insbesondere bei Arbeitsplatzrechnern auf der Client-Seite ist dies der Fall. Selbst bei einer guten Adapterkarte können die Netzprotokolle den effektiven Durchsatz stark beeinträchtigen. Neben den einfachen Treibern sind es vor allem das Protokoll TCP/IP, das zwar sehr weit verbreitet sind, aber doch erhebliche Rechenzeit beanspruchen. Eine weitere Frage ist die einer geeigneten Backbone-Technologie für den Aufbau großer Dedicated Ethernets, da die Switches unter sich und mit den Servern eine Verbindungstechnologie benötigen, die deutlich schneller als 10 Mbit/s ist. Hier würden sich Fast-/Gigabit-Ethernet-Konzepte anbieten, um die gewonnenen Vorteile nicht wieder zu verlieren.

Ein weiteres Problem bei geswitchten Netzen ist, dass es sich um ein einzelnes logisches Netz handelt. Das gesamte Netz bleibt eine einzelne Broadcast-Domäne, wodurch sich Broadcast-Meldungen über das gesamte Netz ausbreiten. Wenn mehr als 200 Clients sich in einer Broadcast-Domäne befinden, hat das ernsthafte Performance-Engpässe zur Folge. Ein Lösungsansatz ist die Bildung virtueller LANs (VLAN), die eine logische Zuordnung ermöglichen und dementsprechend auch Broadcast-Meldungen ablehnen können. Dementsprechend bieten VLANs zwei herausragende Eigenschaften:

- Begrenzung von Broadcast-Stürmen, die das gesamte Netz erheblich belasten können.
- Sicherheitsvorkehrungen durch Filterung bzw. Gruppenbildung.

Ein Layer-2-Switch kann VLANs auf Basis von Switch-Ports bilden. Eine Methode zur Definition eines virtuellen Netzes ist die Zuordnung von Ports. Alle Stationen, die an einem bestimmten Port eines Switching-Systems liegen, werden als Teil des virtuellen Netzes aufgefasst, und eine Menge von Switch-Ports im physikalischen Gesamtnetz bilden das gesamte virtuelle Netz. Dies kann durch MAC-Adressen oder nach den SAP-Informationen der Teilschicht Logical Link Control (LLC) vorgenommen werden. Die Switching-Systeme besitzen einen Lern-Algorithmus, der dem in traditionellen Brücken ähnlich ist. Dies bedeutet, dass eine Station den Ort einfach wechseln kann und dennoch Mitglied des virtuellen Netzes bleibt, ohne dass eine Rekonfiguration in der Endstation erforderlich wäre. So können unabhängig von der Platzierung eines Switches Arbeitsgruppen geschaffen werden. Weiterhin bietet die Orientierung an den Data-Link-Adressen den Vorteil der Protokolltransparenz: Im Gegensatz zu Router-basierten Techniken können auch innerhalb einer Arbeitsgruppe unterschiedliche Protokolle der Schichten 3 bis 7 benutzt werden. Durch diese Konstruktion verbleibt der Verkehr innerhalb einer logischen Workgroup bzw. innerhalb eines virtuellen Netzes. Broadcasts auf einem virtuellen Netz werden nicht auf andere virtuelle Netze weitergeleitet. Einen Schritt weiter geht der Ansatz eines Layer-3-Switches. Dieser baut das gesamte VLAN auf der Grundlage von einem oder mehreren Protokollen auf. Das heißt, VLANs können auf der Schicht 3 mit dem IP Protokoll realisiert werden.

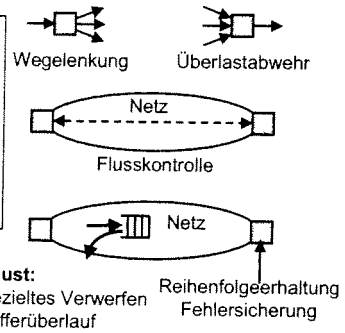
Diese Möglichkeit besitzt die folgenden Vorteile:

- IP-Strukturen werden anhand von Konzepten in ein Unternehmen eingeführt. Die Planung eines VLANs würde solche Konzepte erweitern, wodurch der Planungsaufwand gering gehalten wird.
- Bei häufig anstehenden Umzügen braucht keine IP-Konfiguration auf den Clients, Routern und IP-Switches vorgenommen werden.
- Unterschiedliche Standorte eines Unternehmens können mit einem VLAN-Konzept erreicht werden.

2.3 OSI-Referenzmodell: Schicht 3 - Vermittlung

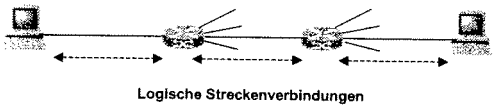
Version Dez. 2003

Inhalt

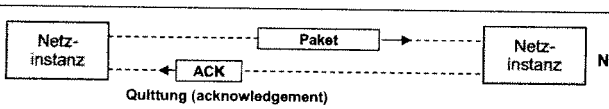


Die Vermittlungsschicht (Netzschicht) ist dafür verantwortlich, Pakete von einem Endsystem über das Netz zu einem Ziel-Endsystem zu leiten.

Hauptthemen sind: Wegelenkung, Überlastabwehr, Flusskontrolle der einzelnen Paketflüsse sowie Reihenfolgeeinhaltung und Fehlersicherung bei Verlust von Paketen im Fall von gezieltem Verwerfen oder bei Pufferüberlauf in den Zwischenknoten.



Ziel:
Vermittlung (routing) von Paketen durch das Netz



Aufgaben:

1) Auf- und Abbau der Schicht-3 Verbindung
2) Übertragung von Schicht-3 Datenblöcken
3) Wegelenkung (routing)
4) Reihenfolgeerhaltung
5) Flusskontrolle, Überlastabwehr
6) Fehlersicherung

Bild: Schicht 3 - Vermittlungsschicht

Schicht 3: Vermittlungsschicht (N: Network)
Durch Wegelenkung (Leitungsvermittlung) bzw. Routing (Paketvermittlung) verknüpft die Vermittlungsschicht gesicherte logische Punkt-zu-Punkt Verbindungen zu Endsystemverbindungen (von Endsystem zu Endsystem). Die Endsysteme werden dadurch direkt oder abschnittsweise über Transitsystemen miteinander verbunden. Zu den Aufgaben der Vermittlungsschicht gehören auch die Abwicklung der Paketflüsse durch Flusskontrolle sowie Überlastabwehr in Falle von Stausituationen. Eine Fehlersicherung kann fehlende Pakete (beispielsweise durch einen Pufferüberlauf) oder eine Verletzung der Paketreihefolge auffangen. Zu dieser Schicht gehört ebenfalls die Signalisierung sowie Nummerierung und Adressierung.

1) **Verbindungsauf- und abbau**

2) **Betreiben von Netzverbindungen**
Multiplexen von Netzverbindungen (*Multiplexing*)
Blocking und Segmentieren
- für bessere Auslastung der Netzverbindung

3) **Wegwahl** (*Routing*)

4) **Reihenfolgeerhaltung** (Sequencing)

5) **Flusskontrolle** (Flow Control)
Überlastabwehr (Congesttion Contol)

6) **Fehlererkennung** (Error Detection)
Fehlerbehebung (Error Recovery)

Bild: Funktionen der Netzschicht

1) **Netzadressierung**
Einrichtung von Verbindungsendpunkt-Identifikatoren
Einrichtung und Sicherstellung der Dienstgüte-Parameter
Verbindungsabbau (Connection Release)

2) **Betrieb von Netzverbindungen**
Übertragung von Netz-Dienstdateneinheiten
Beschleunigte Übertragung (Expedited Data, optional)
Unbedingter Verbindungsabbruch (Reset, optional)

3) **Wegelenkung**

4) **Reihenfolgeerhaltung** (Sequencing)

5) **Flusskontrolle** (Flow Control)
Überlastabwehr (Congesttion Contol)

6) **Benachrichtigung über Fehler** (Error Notification)

Bild: Dienste der Netzschicht

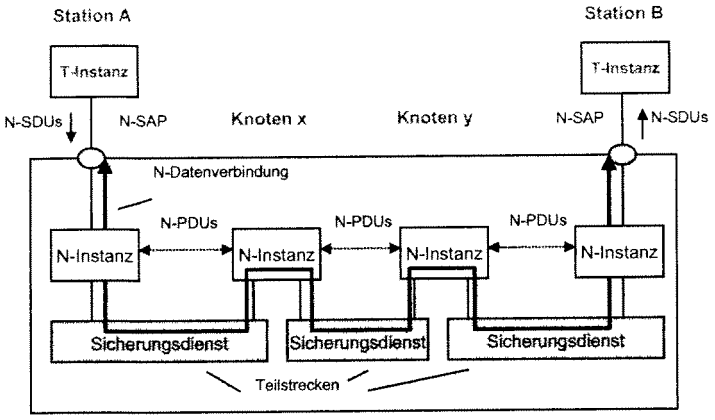


Bild: Ende-zu-Ende Vermittlungsdienst

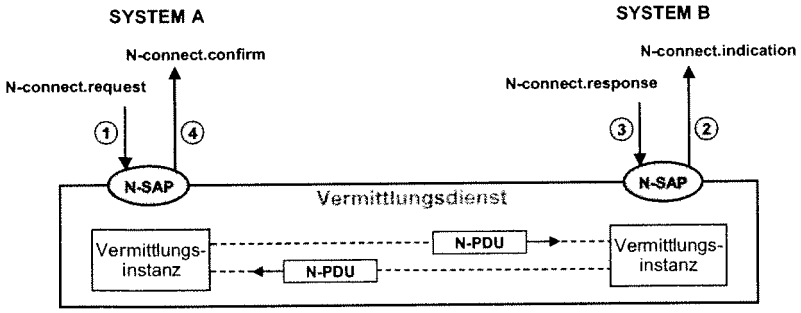


Bild: Vermittlungsdienst : Primitive

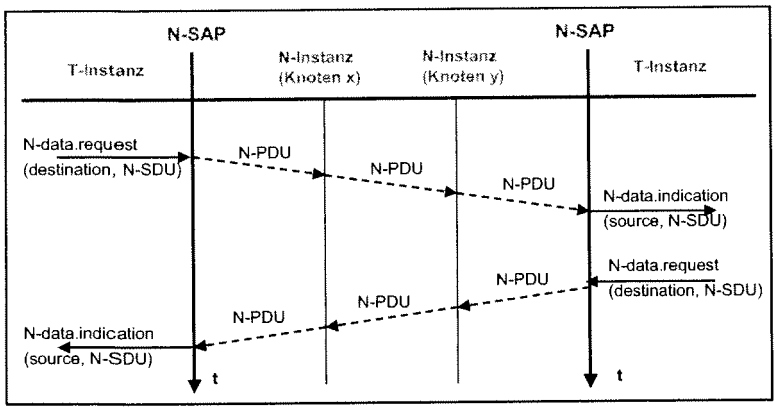


Bild: Ende-zu-Ende Vermittlung von Dateneinheiten

Dienst	req.	ind.	resp.	conf.	Parameter
Aufbau/Abbau:					
N-connect	x	x	x	x	Adressen der Verbindung vorrangiger Datentransfer, Bestätigungen, QoS, Information N-SDU
N-disconnect	x	x			Antwort. Adresse (bei Rückweisung), Grund
Transferphase:					
N-data	x	x			Information N-SDU
N-data_acknowledge	x	x			
N-expedited_data	x	x			Information N-SDU
N-reset	x	x	x	x	Adressen der Verbindung

QoS = Quality of Service (Dienstgüteparameter)

Bild: Verbindungsorientierte Vermittlungsdienste

Aufgaben der Vermittlungsschicht

Die Vermittlungsschicht ist für die folgenden Aufgaben zuständig:

- **Netzverbindungen über Teilnetze hinweg:** Eine Netzverbindung kann über eine Anzahl von Teilnetzen führen, deren Dienstgüte erhebliche Unterschiede aufweisen können. In solchen Fällen gibt es zwei Möglichkeiten:
  - Die Teilnetze werden direkt miteinander verbunden. Dann ist die Dienstgüte des Gesamtnetzes vergleichbar mit der schlechtesten Dienstgüte der Teilnetze.
  - Das schlechteste Teilnetz wird durch zusätzliche Funktionen mit einer höheren Dienstgüte ausgestattet, die sich im Gesamtnetz bemerkbar macht.
- **Routing:** dient der Ermittlung geeigneter Kommunikationspfade zwischen Quellen- und Zielsystem. Ein Pfad kann zahlreiche Zwischensysteme enthalten.
- **Überlastabwehr:** Dieser Mechanismus tritt in Aktion bei Überlast in einzelnen Netzknoten, Teilnetzen oder im gesamten Netz.
- **Flusskontrolle:** Hier handelt es sich um die Kontrolle von einzelnen Datenflüssen. Diese Flüsse können sich auf Teilstrecken oder auf Ende-zu-Ende Strecken beziehen.
- **Erhaltung der Paketreihenfolge:** Die Vermittlungsschicht kann möglicherweise die reihenfolgerichtige Zustellung der Pakete gewährleisten. Falls nicht, muss sich die darüber liegende Transportschicht darum kümmern.
- **Fehlererkennung:** Fehler sollen soweit möglich erkannt werden. Dazu werden auch Dienste der Sicherungsschicht genutzt.
- **Fehlerbehebung:** Fehler sollen in sinnvollem Umfang behoben werden. Im einfachsten Fall können fehlerbehaftete Pakete verworfen werden; falls die Vermittlungsschicht verbindungsorientiert arbeitet, können Übermittlungswiederholungen bei der Fehlerbehebung helfen.
- **Vereinbarung und Sicherstellung einer bestimmten Dienstgüte:** Eine zu Beginn der Netzverbindung ausgehandelte Dienstgüte soll für die Verbindungsdauer garantiert sein. Hier kommen unter andere die folgenden Parameter in Betracht:
  - **Durchsatz:** Die Anzahl der pro Zeiteinheit korrekt übertragenen Nutzdaten.
  - **Verzögerung:** Sie wird bestimmt durch die Laufzeit auf den Übertragungsstrecken und die Warte- und Bearbeitungszeiten in den Routern. Dabei sind zwei Komponenten wichtig: die Ende-zu-Ende Verzögerung und die Verzögerungsschwankung.
  - **Restfehlerrate:** Verhältnis der nicht berichtigten fehlerhaften, verlorenen oder duplizierten Pakete zur Paketgesamtzahl.
  - **Verfügbarkeit des Netzes:** Sie wird hauptsächlich durch Verfügbarkeit der Zwischenknoten und der Teilstrecken bestimmt.
  - **Zuverlässigkeit:** Wahrscheinlichkeit, dass Pakete fehlerfrei beim richtigen Empfänger ankommen.
  - **Überlastabwehr:** Die dem Anwender zugesagte Dienstgüte soll durch lokale Überlastung von Netzknoten und Teilstrecken nicht verschlechtert werden.

- Durchsatz **(Throughput)**
  pro Zeiteinheit korrekt weitergeleitete Daten

- Übermittlungsverzögerung **(Transit Delay, End-to-End Delay)**
  zusammengesetzt aus Laufzeit eines Paketes und Summe der Verarbeitungszeiten in beteiligten Knoten

- Verzögerungsschwankung **(Delay Jitter)**

- Restfehlerrate **(Residual Error Rate)**
  Verhältnis von nicht entdeckten fehlerhaften, dupliziert oder verlorengegangenen Paketen zu Anzahl der insgesamt weitergegebenen Pakete

- Verfügbarkeit des Dienstes **(Service Availability)**
  z.B. von Verfügbarkeit der Netzknoten beeinflusst

- Zuverlässigkeit **(Reliability)**
  beeinflusst durch etwaige Ausfälle von Übertragungskanälen

Bild: Netzschicht: Dienstgüte-Parameter

Leitungs- und Paketvermittlung

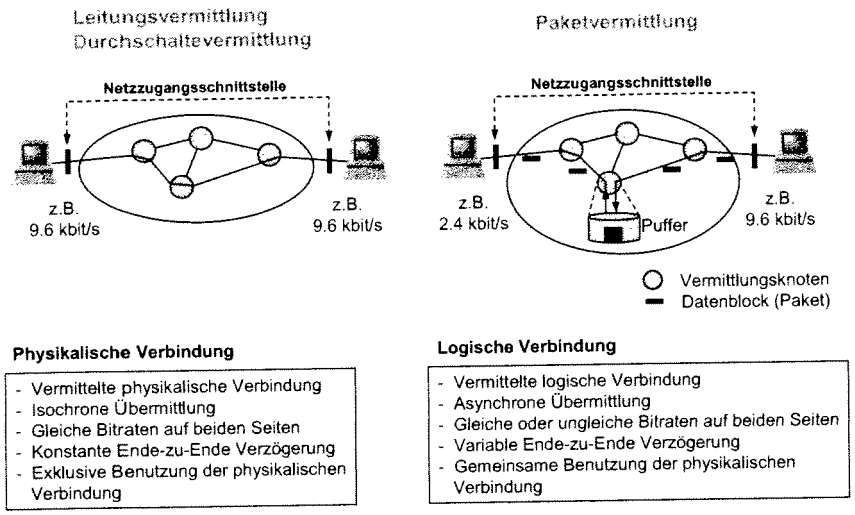


Bild: Vermittlungsprinzipien

Leitungsvermittlung: Es handelt sich hier nur um Wegelenkung (Routen) beim Aufbau einer physikalischen Ende-zu-Ende Verbindung. **Wichtige Beispiele**: Telefonverbindung, Bypass-Verbindung mit SDH oder WDM.

Paketvermittlung: Alle Funktionen sind vorhanden. Zwei Aufgabenbereiche sind zu betrachten:

1) Aufbau von Ende-zu-Ende Pfaden oder Einzelverbindungen zwischen Quelle und Ziel (nur Wegelenkung).
2) Übermittlung von Paketen innerhalb dieser von Ende-zu-Ende Pfade oder Einzelverbindungen, wobei alle Funktionen vorhanden sein können, inklusive die Wegelenkungsfunktion selbst.

Die **Leitungsvermittlung** (circuit switching) ist im Telefonnetz nach wie vor von großer Bedeutung. In der Regel wird eine Wahlverbindung (switched circuit) zu Beginn einer Kommunikationsbeziehung aufgebaut und nach deren Ende wieder abgebaut. Eine Standleitung (Mietleitung, leased line) oder allgemeiner eine Standverbindung ist eine zwischen zwei Teilnehmern fest geschaltete Verbindung.

Synchrone Multiplexverfahren werden eingesetzt, um auf einem breitbandigen, physikalischen Kanal gleichzeitig viele Verbindungen bereitzustellen. Hierfür werden, je nach physikalischem Kanal, die Multiplexverfahren TDM, FDM, WDM und CDM eingesetzt. Dabei erhöht CDM die erforderliche Bandbreite, sodass dies Verfahren nur bei Funk und Glasfasersystemen sinnvoll ist, und nur für Zugangssysteme eingesetzt wird. Es handelt sich deshalb um CDMA. **Beispiele:** UMTS, Satellitenfunk und passive optische Glasfaser Anschlussnetze (PON, Passive Optical Network).

Durch den Verbindungsaufbau entsteht eine Wartezeit bis zum Beginn der Kommunikation. Dafür steht jederzeit eine garantierte Bandbreite zur Verfügung und die Verzögerung auf dem Übertragungsweg ist konstant und minimal. Die Verbindungskosten sind proportional zur Verbindungsdauer, auch wenn darin Pausen enthalten sind.

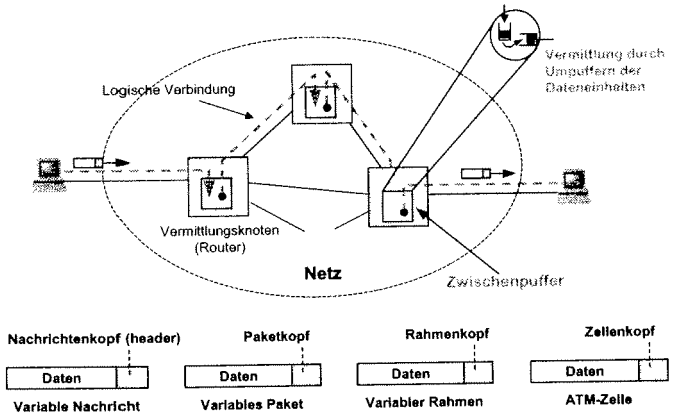


Bild: Sendungs-, Paket-, Rahmen- und Zellenvermittlung

Die **Paketvermittlung** (packet switching) bildet die Basis der eigentlichen Rechnernetze. Bei der verbindungslosen Paketübertragung werden Datagramme (datagram) einzeln und unabhängig voneinander übertragen. Die verbindungsorientierte Paketübertragung nutzt virtuelle Verbindungen (Kanäle), die - ähnlich wie bei der Leitungsvermittlung - auf- und abgebaut werden. Die zu übertragenden Ursprungsdaten werden in der Regel in viele Pakete zerteilt, die sequenziell übertragen werden. Der Fall der Nachrichtenvermittlung (message switching) ist hingegen dadurch gekennzeichnet, dass eine vollständige Nachricht des Benutzers auf einmal übertragen wird.

Das Source Routing (Token Ring) kann als Sonderfall der Paketvermittlung betrachtet werden. Alle Formen der Paketvermittlung benötigen Zwischenpuffer, die Pakete so lange zwischenpuffern bis sie weitergeleitet werden können. Deshalb wird auch der Begriff Store-and-Forward für die Paketvermittlung verwendet.

Bei der Paketvermittlung (packet switching) werden Nutzdaten in Pakete (packet) aufgeteilt, die zusammen mit anderen Paketen im asynchronen Zeitmultiplex über Teilstrecken übertragen werden. Teilstrecken sind über Router mit weiteren Teilstrecken verbunden, wodurch eine teilweise vermaschte Topologie entsteht. Die verschiedenen Varianten der Paketvermittlung bieten den Vorteil, dass die verfügbare Übertragungskapazität den Teilnehmern entsprechend ihrem Bedarf dynamisch zugeordnet werden kann. Die Kosten sind von der Zahl (und Länge) der übertragenen Pakete abhängig, entspre-

chen also der tatsächlichen Nutzung des Netzes. Als Nachteil ergibt sich bezogen auf eine einzelne Kommunikationsbeziehung eine nicht garantierte Bandbreite sowie eine relativ große und variable Verzögerung.

Bei der Paketvermittlung werden die Zwischensysteme im Netz als Router bezeichnet. Der grundlegende Ablauf in einem Router besteht aus dem Zwischenpuffer ankommender Pakete (store), der Ermittlung des nächsten Zwischensystems auf dem Weg zum Ziel (Routing-Entscheidung, routing decision) und der Weitergabe (forwarding) über eine Warteschlange an der richtigen Ausgabeschnittstelle. Die Routing-Entscheidung wird anhand der Zieladresse - die sich im Header eines Pakets befindet - und der Routing-Tabelle getroffen. Der Begriff Routing bezieht sich auf die Erstellung der Routing-Tabellen.

In Abhängigkeit von Übertragungsfehlern, überlasteten oder zeitweise ausgefallenen Teilstrecken und Routern können bei der Paketvermittlung diverse Fehler entstehen: (Für die Beseitigung dieser Fehler ist meistens die Transportschicht zuständig)

- Pakete können verloren gehen.
- Die Pakete einer Kommunikationsbeziehung können in falscher Reihenfolge beim Empfänger ankommen.
- Ein Paket kann mehrfach (als Duplikat) beim Empfänger ankommen.

Verbindungsorientierte Paket- und Zellenvermittlung
Die verbindungslose Paketvermittlung wird durch das Prinzip Store-and-Forward und Auswertung der Gesamtadresse relativ langsam. Die Pakete werden vollständig gepuffert, Adressen ausgewertet und Prüfsummen überprüft bzw. neu berechnet. Zur Erhöhung der effektiven Übertragungsgeschwindigkeit wurden Konzepte wie Fast Packet Switching bzw. Fast Packet Relaying entwickelt. Die Grundidee dabei ist es, Pakete so schnell als möglich weiterzugeben. Das geht nur bei einfachen Paketstrukturen, bzw. wenn nur wenige Inhalte des Headers ausgewertet werden müssen. Hierzu ist der Aufbau einer virtuellen oder logischen Ende-zu-EndeVerbindungspfad notwendig, sodass das Routen aufgrund von einem kurzen Pfadkennung im Paketheader und den initialisierten Routingtabellen in den Zwischenknoten erfolgen kann (X.25, FR, ATM, MPLS). Zusätzlich wird angestrebt, das Routen möglichst vollständig in Hardware zu realisieren (ATM).

Die Unterscheidung zwischen verbindungsloser und verbindungsorientierter Kommunikation ist deshalb auf der Vermittlungsschicht von besonderer Bedeutung.

- **Ein verbindungsloser Netzdienst (CLNS: Connectionless Network Service)** überträgt jedes einzelne Paket (auch als Datagramm bezeichnet) unabhängig von vorangehenden oder folgenden Paketen. Dabei wird die Übertragung nicht garantiert, dieses Verhalten wird als Best-Effort bezeichnet. Für jedes Paket wird in jedem Zwischenknoten eine Routing-Entscheidung getroffen. Deshalb muss jedes Paket die Zieladresse enthalten. Als Konsequenz dieses Verfahrens können die einzelnen Pakete unterschiedliche Wege nehmen. Je nach Verzögerung (Lauf- und Wartezeiten) kann die Reihenfolge des Eintreffens beim Empfänger verschieden sein von der Reihenfolge beim Absenden. Zudem können Datagramme verloren gehen oder Duplikate dem Empfänger zugestellt werden. Da die Datagramme einer Kommunikationsbeziehung unabhängig voneinander übertragen werden, ist eine Flusskontrolle nicht möglich. Ebenso kann dem Dienstnutzer keine Zusicherung bezüglich der erbrachten Dienstgüte gegeben werden. **Beispiel:** IP-Netze.

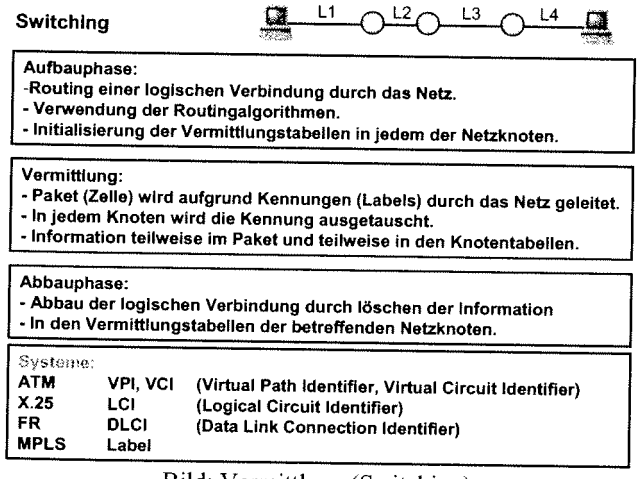


Bild: Vermittlung (Switching)

- **Ein verbindungsorientierter Netzdienst (CONS: Connection-Oriented Network Service)** baut zuerst eine virtuelle oder logische Verbindung durch das Netz auf. Dazu wird ein Datagramm verwendet, das in den durchlaufenen Knoten die aufzubauende Verbindung bekannt gibt und dafür eine Verbindungsidentifikation (Kennung, Label) erhält. Wenn die Verbindung aufgebaut ist, nehmen alle folgenden Pakete denselben Weg. Somit genügt es, den Paketen die Verbindungsidentifikation mitzugeben. Adressen sind dann nicht mehr erforderlich. Es ist sichergestellt, dass die Pakete in der richtigen Reihenfolge beim Empfänger ankommen. Flusskontrolle, Dienstgüteaushandlung und Abrechnung und Tariffierung sind durchführbar. **Beispiele:** X.25, FR, ATM, MPLS.

Vergleich der Vermittlungstechniken
Eine direkte Verbindung (bei der Leitungsvermittlung) benötigt keine Zwischenpufferung im Netz. Bei Store-and-Forward wurde bei der Nachrichtenvermittlung (Message Switching) zunächst eine Zwischenpufferung auf Massenpuffer realisiert. Heutige Paketvermittlungstechniken verwenden Zwischenpufferung auf der Basis von schnellen Halbleiterpuffern. Ein weiteres Unterscheidungsmerkmal ist die Existenz (bei der Leitungsvermittlung ist das Konzept einer PDU nicht notwendig) bzw. Länge der verwendeten PDUs (Protocol Data Unit).

Vergleich der Vermittlungstechniken

Vermittlungstechnik	Verzögerung	Art der Zwischenpufferung	PDU (Protokolldateneinheit)
Leitungsvermittlung	minimal	direkte Verbindung	transparenter Kanal
Nachrichtenvermittlung	hoch	Store-and-Forward	variable Länge (komplette Nachricht)
Paketvermittlung	mittel	Store-and-Forward	variable Länge
Frame Relay Vermittlung (Schicht 2)	klein	Store-and-Forward	variable Länge
Zellvermittlung	sehr klein	Store-and-Forward	feste kleine Länge

Routing

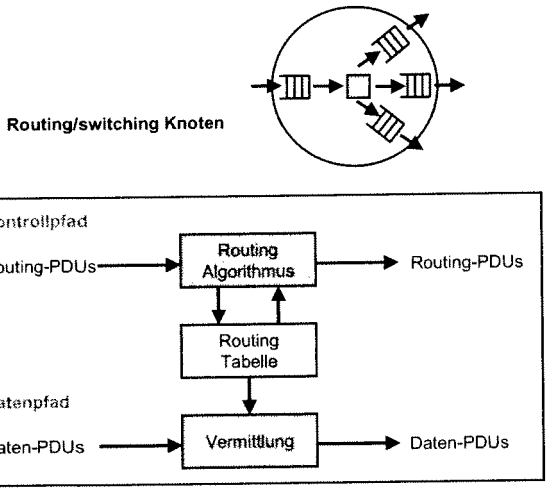


Bild: Kontroll- und Datenpfad

Das **Routing** (Verkehrslenkung Leitweglenkung, Wegewahl,) ermittelt Wege (Pfade, Routes) von einem Quellen- zu einem Zielsystem. Zwischen Quellen- und Zielsystem liegen (in der Regel mehrere) **Router** (Vermittlungsrechner). Die Router ermitteln einen Weg (Route) auf Basis der Adresse des Zielsystems oder der Adresse eines Subnetzes, in dem sich das gesuchte Zielsystem befindet.

Weitere Begriffe: Die Bezeichnung Gateway wird im Zusammenhang mit dem Internet manchmal für Router verwendet. Ein Router wird auch als Switch bezeichnet, wenn er tabellen-orientiert Zellen (ATM) oder Pakete (MPLS) vermittelt. Brücken oder Ethernet-Switches (übertragen Datenrahmen zwischen Teilnetzen, allerdings auf Basis der Hardwareadresse, nicht der Netzadresse. Es wird zunehmend von Layer-x-Switches gesprochen. Sie vermitteln Rahmen (Schicht 2) oder Paketen (Schicht 3) mittels Hardware, statt durch Software, wobei für Layer 4-7 Switches zusätzlich noch Informationen der betreffenden PDU-Headers ausgewertet werden.

Grundidee des Routing
Die Grundidee des Routing in Paketnetzen geht davon aus, dass in jedem Zwischensystem (Router) eine Routing-Tabelle vorhanden ist. Der Router extrahiert die in einem ankommenden Paket enthaltene Zieladresse und sieht in seiner Routing-Tabelle nach, an welches nächste Zwischensystem das Paket weiterzugeben ist. Falls der Zielknoten direkt mit dem Ziel verbunden ist, ist kein Zwischensystem, sondern das Ziel selbst in der Routing-Tabelle eingetragen.

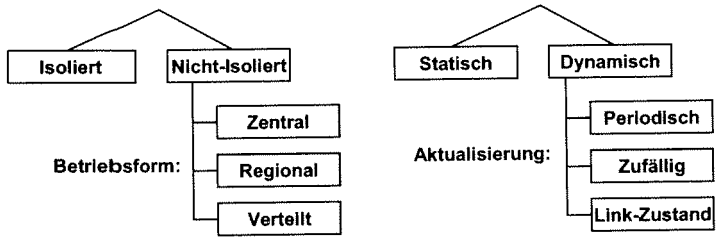


Bild: Einteilung von Routingmechanismen

Ein einfaches Routingkriterium wählt offensichtlich kürzeste Wege, auf denen die kleinste Anzahl von Zwischensystemen zu durchlaufen ist. In der Praxis werden jedoch auch andere Kriterien (sog. Metriken) zur Wegewahl verwendet.

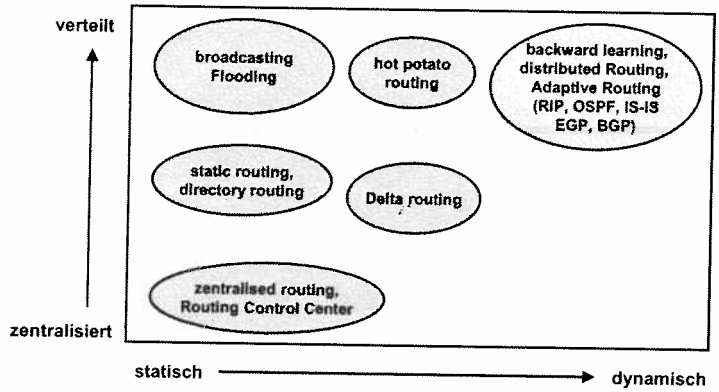


Bild: Routingmechanismen

Beim Aufbau von Datenverbindungen über vermaschte Netze besteht die Aufgabe, den Verkehr auf möglichst kurzem Wege und kurzer Zeit zu führen. Die Verkehrslenkung (Routing) umfasst die Auswahl der Wegeabschnitte beim Aufbau von Datenverbindungen. Netzstruktur und Verkehrslenkung haben einen wesentlichen Einfluss auf die kostenoptimale Verkehrsführung unter Einhaltung einer garantierten Verkehrsgüte (Grade-of-Service). Zur Erreichung dieses Ziels werden zunehmend komplexere Verkehrslenkungsverfahren eingesetzt:

a) Feste Verkehrslenkung,
b) Alternative Verkehrslenkung,
c) Adaptive Verkehrslenkung.

Es wird zwischen Routing-Verfahren, Routing-Strategien und Routing-Algorithmen unterschieden.

- **Routing-Verfahren** geben eine summarische, wenig detaillierte Beschreibung, wie das Routing durchgeführt wird und welche Teile das Verfahren umfasst.
- **Routing-Strategien** beschreiben etwas genauer, wie geeignete Wege unter Beachtung festgelegter Kriterien ermittelt werden.
- **Routing-Algorithmen** beschreiben exakt und vollständig, wie eine Routing-Strategie als Algorithmus formuliert wird, der direkt (eins-zu-eins) in ein Programm für einen Router umgesetzt werden kann.

Es ist sinnvoll, den Vorgang der Wegewahl (route discovery) und den der **Weitergabe von Paketen** (forwarding) strikt auseinander zu halten.

- Das Forwarding besteht darin, eine Routing-Tabelle auf ein bestimmtes Paket anzuwenden.
- Die Routing-Tabelle muss natürlich zuerst aufgestellt werden. Dieser Vorgang heißt Routing. Routing-Tabellen können manuell erstellt werden. Aus verschiedenen Gründen ist jedoch eine Erstellung mit Hilfe von Routing-Protokollen vorzuziehen.

Weiter ist das Routing in Abhängigkeit der jeweils betrachteten Kommunikationsbeziehung unterschiedlich durchzuführen:

- Die meisten Routing-Verfahren sind für die 1: 1 -Kommunikation **(Unicast)** ausgelegt.
- Routing-Verfahren für **Multicast** (1:n, wobei n für eine Teilmenge aller möglichen Empfänger steht, auch als Gruppenkommunikation bezeichnet) werden zukünftig wichtiger (Video-Konferenz, Video-Server).
- **Broadcast** ist ein Sonderfall des Multicast, bei dem alle Teilnehmer eines Netzes bzw. eines Subnetzes als Empfänger angesprochen sind. In Diffusionsnetzen ist ein Broadcast inhärent realisiert, indem jeder Knoten sowieso alle Pakete empfängt. In Non Broadcast Multiple Access Netzen mit verbindungsorientierter Kommunikation über Punkt-zu-Punkt-Verbindungen, z. B. ATM, Frame Relay und X.25) ist dies nicht der Fall, Broadcasts müssen deshalb durch mehrfache Routing-Vorgänge nachgebildet werden.

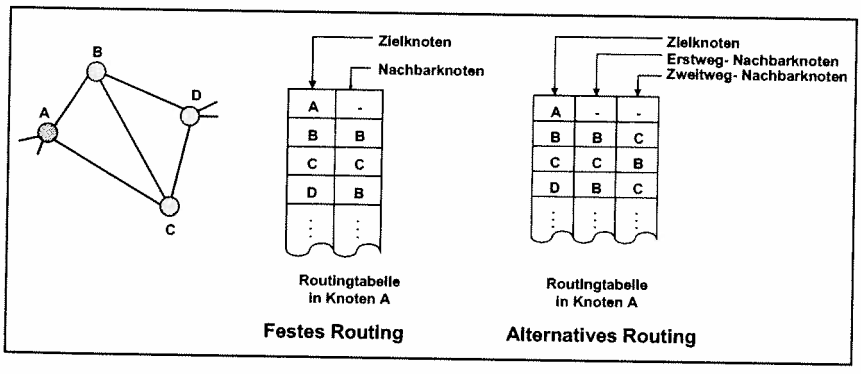


Bild: Festes und alternatives Routing

Bei **fester Verkehrslenkung** erfolgt die Auswahl der Wegeabschnitte zwischen Ursprung und Ziel nach Kriterien der kürzesten Entfernung unabhängig vom Belegungszustand des Netzes.

Bei **alternativer Verkehrslenkung** wird der aktuelle Belegungszustand in den einzelnen Netzknoten berücksichtigt. Die Auswahl eines von mehreren Wegeabschnitten erfolgt durch Absuchen in einer fest vorgegebenen Reihenfolge.

Bei adaptiver Verkehrslenkung erfolgt die Auswahl der Wegeabschnitte nach netzweiten Bewertungskriterien aufgrund des momentanen Belegungszustandes des gesamten Netzes.

Beispiele für Pfadverkehrslenkung:
Telefon-Fernnetz, pfadorientierte Paketvermittlungsnetze, SDH-Übertragungsverbindungen, Wellenlängenverbidungen

Feste Verkehrslenkung
Verkehrslenkungstabelle enthält Strukturinformationen nach Kriterien wie die kürzeste Entfernung

- Anwendung bei Durchschalte- oder Paketvermittlung möglich
- Änderung nur bei Netzstrukturänderungen (selten) oder durch Netzführung für bestimmte Zeitdauer zur Erreichung eines bestimmten Ziels wie
  - Ausgleich tageszeitlicher Unterschiede
  - Umgehung einer ausgefallenen Trasse

Alternative Verkehrslenkung
Überlauf von Erstweg auf Zweitweg bei vollbelegtem Erstweg

- Mehrfachüberlauf möglich
- Staffelung nach Kriterien der kürzesten Entfernung
- Begrenzung der Anzahl von Alternativen sinnvoll
- Anwendungen bei Durchschalte- und Paketvermittlung möglich

Verkehrslenkung	Merkmal	Bewertungskriterien	
		CS (Circuit-Switching)	PS/MS (Packet/Message Switching)
fest	ein Weg	--	--
alternativ	Erstweg + Folgeweg(e) je Knoten	Belegungszustand abgehender Leitungsbündel	Warteschlangenlänge abgehender Kanäle
adaptiv	mehrere Wege	von Ursprung bis Ziel durchgehend belegbarer Pfad im Rahmen zugelassener Wegabschnitte	Erwartungswert der Ursprungs-Ziel-Durchlaufzeit (Anzahl Wegabschnitte, Warteschlangenlängen)

a) Zentralisierte, adaptive Verkehrslenkung
Einführung eines Netzkontrollzentrums

- Periodische Registrierung das Belegungszustandes jedes Knotens
- Berechnung des jeweils optimalen Start-Ziel-Weges für jedes Ursprung-Ziel Paar
- Periodisches Laden der neuen Verkehrslenkungstabellen für nächsten Zeitabschnitt

Nachteil:

- Sicherheit gegen Ausfall
- Verwaltungsaufwand (Netz-Overhead)
- Alterung der Aktualität

b) Verteilte, adaptive Verkehrslenkung
Austausch von Belegungszustands-Informationen mit Nachbarknoten (periodisch oder Verbindungs-individuell)

Realisierung bei CS:

- Einführung zentraler Zeichenkanäle getrennt vom Nutzwegenetz
- Signalisierung über spezielles Signalisiernetz vom Ursprung bis zum Ziel
- Wegeauswahl nach Prinzip des kürzesten Weges mit gewissen Alternativen
- Durchschaltung nur im Falle eines durchgehend freien Pfades

Nachteil:

- Zeitaufwand
- Erfordert schnelles Signalisiernetz

Realisierung bei PS:

- Periodischer Austausch von expliziten Verkehrslenkungstabellen mit allen Nachbarknoten
- Neuberechnung des neuen, günstigsten Nachbarknotens für jedes Ziel sowie der verbesserten Durchlaufszeitschätzung aus den empfangenen Informationen der Nachbarknoten und der erwarteten Verzögerung zu den Nachbarknoten
- Sukzessive Ausbreitung der aktualisierten Informationen über das Netz

Nachteil:

- Aktualität erfordert häufigen Austausch (Overhead)
- Robust gegen Einzelstörungen

c) Hierarchische und nichthierarchische Verkehrslenkung

- Hierarchische Verkehrslenkung liegt vor, wenn sich die Verkehrslenkung in der Staffelung der ausgesuchten Verbindungswege an der Netzhierarchie orientiert. Dies erfolgt im allgemeinen durch alternative Verkehrslenkung.
- Nichthierarchische Verkehrslenkung liegt vor, wenn mehrere Alternativen unabhängig von der Netzhierarchie zur Auswahl stehen und wenn der Verbindungsversuch alle Alternativen ausschöpft. Hierzu ist ein schnelles Signalisiernetz erforderlich, um diese Möglichkeiten voll ausschöpfen zu können.

Routing-Verfahren
Routing-Verfahren beschreiben, wie Routing-Tabellen erstellt werden.

Es gibt verschiedene Verfahrenstypen:

- **Statische Verfahren** basieren auf Routing-Tabelle, die einmal erstellt und dann nicht mehr verändert. Die Routing-Tabelle wird aufgrund festgelegter **Routing-Metriken** ermittelt. Statische Routing-Verfahren können jedoch nicht auf Veränderungen im Netz reagieren, so dass ihr Nutzen begrenzt ist.
- **Adaptive (dynamische) Routing-Verfahren** können sich der aktuellen Situation im Netz anpassen, indem die Routing-Tabellen regelmäßig oder bei Bedarf angepasst werden. Basis für die Anpassung sind ebenfalls Routing-Metriken.
- **Isolierte Routing-Verfahren** wählen den Ansatz, dass jeder Knoten nur die ihm verfügbare, lokale Information für seine Routing-Entscheidungen verwendet.
- **Zentrale Routing-Verfahren** übertragen die Ermittlung der Routing-Tabellen einer zentralen Stelle, die aufgrund ihrer umfassenden Information über den Zustand des Netzes qualitativ hochwertige Routing-Entscheidungen treffen kann. Die Reaktionsgeschwindigkeit auf Veränderungen im Netz kann jedoch gering sein. Ein zentral gesteuertes Routing erfordert eine ausfallsichere Plattform, um den Ausfall der gesamten Routing-Funktion zu verhindern. Außerdem kann es einen Engpass bilden, der die gesamte Übertragungsleistung des Netzes ungünstig beeinflusst.
- **Verteilte Routing-Verfahren** sind dadurch gekennzeichnet, dass jeder Router seine Routing-Entscheidungen selbstständig auf Basis der ihm zur Verfügung stehenden Information ermittelt. Die Nachteile des zentralen Routing werden dabei vermieden. In der Praxis werden hauptsachlich verteilte, adaptive Routing-Verfahren eingesetzt. Die wichtigsten Verfahren verwenden Distanz-Vektor-Algorithmen und Link-State-Algorithmen.

Die genannten Routing-Verfahren bzw. Elemente daraus lassen sich in vielfältiger Weise kombinieren.

Routing-Verfahren Fluten
Fluten (flooding) ist ein isoliertes, nicht adaptives verfahren. Isoliert bedeutet, dass jeder Knoten nur die ihm verfügbare lokale Information verwendet. Diese kann die Länge einer Warteschlange vor einer abgehenden Leitung oder den Zustand eines Nachbarn beinhalten. Das Verfahren gibt jedes erhaltene Paket an alle Nachbarknoten weiter, mit Ausnahme des Knotens, von dem das Paket erhalten wurde. Dadurch entstehen viele Duplikate im Netz. Falls deren Lebensdauer nicht begrenzt wird, wird das Netz in kürzester Zeit hoffnungslos überlastet sein. Jedes Duplikat kann einen Zeitstempel erhalten, der es ermöglicht, das Paket nach Ablauf einer bestimmten Zeitspanne zu vernichten. Wenn einem Paket ein Zählwert (hop count) mitgegeben wird, der nach Durchlaufen eines jeden Zwischenknotens um Eins dekrementiert wird, kann das Paket beim Erreichen des Zählwertes null vernichtet werden. Das Fluten ist ein einfaches Verfahren, das zu einer hohen Netzlast führt. Es ist sehr robust und funktioniert auch dann, wenn viele Knoten ausfallen. Der kürzeste Weg wird immer gefunden, wenn auch später eintreffende Duplikate erkannt und verworfen werden müssen.

Routing-Verfahren Hot Potato
Ein Knoten, der ein Paket zur Weitergabe erhält, betrachtet dieses als "heiße Kartoffel", die er schnellstmöglich wieder loswerden möchte. Dazu kann das Paket auf die abgehende Leitung mit der kürzesten Warteschlange gelegt werden. Die Folge ist, dass Pakete erhebliche Umwege nehmen können, da nicht sichergestellt ist, dass die gewählte Leitung einen günstigen Weg in Richtung auf das Ziel ergibt. Das Hot-Potato-Verfahren ist empfindlich gegen Überlast, denn es werden immer noch Pakete angenommen, wenn der Weg zum Ziel bereits verstopft ist.

Praxisrelante Routing-Algorithmen

Die beiden Verfahren Distanz-Vektor-Routing und Link-State-Routing sind in der Praxis sehr wichtig.

- Beim Distanz-Vektor-Verfahren wird ein kürzester Weg gewählt, der die kleinstmögliche Anzahl von Zwischensystemen (hops) enthält.
- Beim Link-State-Verfahren ist jeder Teilstrecke (link) ein Gewicht nach einer festgelegten Metrik (z. B. Kosten, Distanz, Bandbreite, Auslastung) zugeordnet. Ein kürzester Weg ist dadurch gekennzeichnet, dass die Summe der Gewichte minimal ist.

Distanz-Vektor-Algorithmus
Der Distanz-Vektor-Algorithmus (auch als **Bellman-Ford-Algorithmus** bekannt) wird für die verteilte Berechnung von Routing-Tabellen verwendet. Dabei berechnet zunächst jeder Knoten für sich eine Routing-Tabelle. Die Einträge sind Tupel, die - wie der Name des Verfahrens andeuten soll - je eine Adresse (Vektor) und die zugehörige Distanz enthalten. Die Tupel werden den benachbarten Knoten mitgeteilt und zur Aktualisierung (update) deren Routing-Tabellen genutzt. Nach einiger Zeit (Konvergenzdauer) besitzen alle Knoten optimale Routing-Tabellen. Das Distanz-Vektor-Verfahren wird periodisch im Abstand weniger Sekunden durchgeführt. Damit kann der Ausfall einzelner Knoten oder Kanten (Übertragungsstrecken) berücksichtigt werden. Ein Knoten, der keine periodische Routing-Information liefert, gilt als ausgefallen. Die umgebenden Knoten ändern daraufhin ihre Routing-Tabellen so, dass der ausgefallene Knoten umgangen wird, soweit bestehende Pfade dies zulassen.

Beim Bellman-Ford-Algorithmus ist jede Kante des Graphen mit einem Gewicht belegt, die Distanz zum Ziel ist als Summe der Gewichte auf dem Weg zum Ziel definiert. Die Routing-Tabelle enthält für jeden Eintrag ein Feld, das die Distanz zum Zielknoten (auf einem Pfad entsprechend dem angegebenen Next Hop) enthält. Jeder Knoten sendet die ihm bekannten Wertepaare (Ziel, Distanz) an seine Nachbarn. Wenn ein Knoten eine Nachricht von seinem Nachbarn erhält, prüft er alle Einträge und ändert seine Routing-Tabelle, falls der Nachbar einen kürzeren Pfad zu einem Ziel kennt.

Ein Vorteil des Distanz-Vektor-Algorithmus ist seine Einfachheit. Der größte Nachteil liegt in der langen Konvergenzdauer. Dies führt dazu, dass bei raschen Änderungen der Topologie Inkonsistenzen in den Routing-Tabellen entstehen, die zu großen Verzögerungen und zu Paketverlusten führen können.

Link-State-Routing, Dijkstra-Algorithmus
Das Link-State-Routing (auch Link-Status-Routing) wird auch als **SPF-Routing** (Shortest Path First) bezeichnet, obwohl andere Routing-Verfahren ebenfalls kürzeste Pfade ermitteln. Das Verfahren beinhaltet - wie das Distanz-Vektor-Verfahren - eine verteilte Berechnung des Routing. Die zwischen den Knoten ausgetauschten Nachrichten beinhalten den Status einer Verbindung zwischen zwei Knoten, der durch ein Gewicht in einer bestimmten Metrik ausgedrückt wird. Diese Nachrichten werden per Broadcast an alle Knoten gesendet. Damit besitzt jeder Knoten die globale und vollständige Zustandsinformation über das Netz. Jeder Knoten kann nun für sich einen Graphen für das Netz erstellen. Anschließend berechnet jeder Knoten seine Routing-Tabelle mit Hilfe des Dijkstra-Algorithmus. Das Routing kann also - wie beim Distanz-Vektor-Verfahren - an den aktuellen Zustand des Netzes adaptiert werden. Die Adaption findet schneller statt, da alle Knoten gleichzeitig über Statusänderungen informiert werden.

Die Grundidee des Link-State-Routing geht davon aus, dass zunächst die Topologie des Netzes ermittelt wird. Dazu sind die folgenden Schritte notwendig:
- Jeder Router kümmert sich selbst darum, seine Nachbarn und ihre Namen kennen zu lernen.
- Jeder Router bildet ein LSP (Link State Packet) mit den Namen seiner Nachbarn und den Gewichten der zugehörigen Links.
- Die LSP werden an alle Router verschickt, jeder Router puffert die zuletzt erhaltenen LSP aller anderen Router.
- Damit kennt jeder Router die vollständige Topologie des Netzes. Dies ermöglicht den einzelnen Routern die Berechnung von Pfaden zu jedem Ziel.

Der **Dijkstra-Algorithmus** wird nun zur Berechnung der kürzesten Wege ausgeführt. Der Algorithmus geht von einem bestimmten Knoten, dem Quellenknoten, aus und berechnet eine Routing-Tabelle für diesen Knoten. In der Routing-Tabelle sind für alle möglichen Zielknoten die nächsten Knoten, die in Richtung auf den Zielknoten zu durchlaufen sind, und die Distanz D von jedem Knoten zum Quellenknoten enthalten. Für jeden Knoten im Netz ist eine Routing-Tabelle zu ermitteln.
Für den Dijkstra-Algorithmus sind nebst der Beschreibung des Graphen einige Datenstrukturen erforderlich. Die Knoten werden von 1 bis n nummeriert, damit kann die Knotennummer als Index zum Datenzugriff verwendet werden. D ist ein Vektor, dessen i-te Komponente den aktuellen Wert der kürzesten Distanz vom Quellenknoten zum Knoten i enthält. Die i-te Komponente des Vektors R puffert den nächsten Knoten (next hop), der auf dem Weg zum Knoten i zu durchlaufen ist. Die Menge S der noch zu untersuchenden Knoten kann als doppelt verkettete Liste von Knotennummern gepuffert werden.

Der Dijkstra-Algorithmus lässt verschiedene Metriken zu. Im einfachsten Fall ist die Distanz gleich der Anzahl der durchlaufenen Zwischensysteme. Dazu werden alle Gewichte auf den Wert 1 gesetzt. In WANs kann die Bandbreite eines Link als Gewicht sinnvoll sein. Gewichte können auch die Ansicht des Netzadministrators (administrative policy) zu bevorzugten Pfaden widerspiegeln.

Pfad-Vektor-Algorithmus
Das Pfad-Vektor-Verfahren ist dem Distanz-Vektor-Verfahren ähnlich. Statt der Distanz zum Ziel wird jedoch ein Pfad zum Ziel angegeben. Dieser enthält eine Sequenz der zu durchlaufenden Routing-Bereiche (sogenannte Autonomous Systems, (AS). Das Verfahren BGP (Border Gateway Protocol) ist ein Pfad-Vektor-Protokoll, das im Internet verwendet wird. Es verwendet keine Metriken. Durch die vordefinierten Pfade wird ein Policy-based routing realisiert, das es dem Netzbetreiber erlaubt, bestimmte Pfade auszuschließen oder uninteressant zu machen.

Überlastsabwehr (Staukontrolle, Congestion Control)

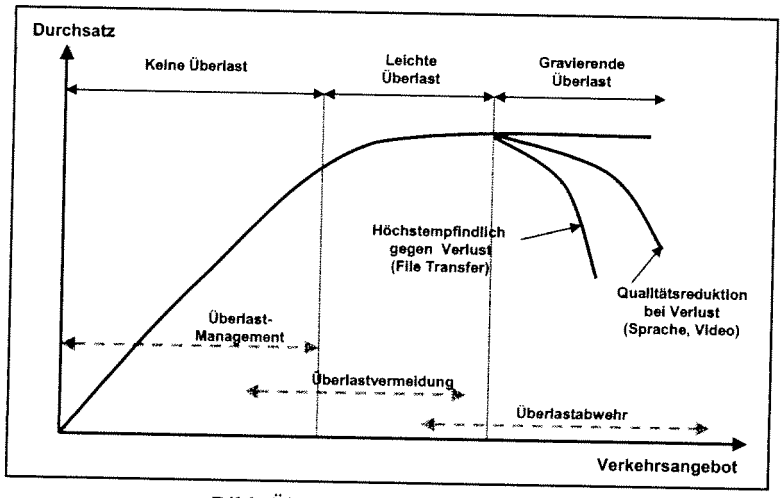


Bild: Überlastabwehr: Durchsatz

Ein Netz kann mit seinen Betriebsmitteln (Teilstrecken, Router) eine bestimmte Last (load, Vermittlungsanforderungen) aufnehmen. Wenn diese Last an die Grenzen der Netz- und Knotenkapazitäten stößt, entsteht eine Überlast, auf die das Netz in geeigneter Weise reagieren muss.

In einem **Leitungsvermittlungsnetz** wird das Eintreten von Netzüberlast verhindert. Falls die gewünschte physikalische Verbindung (Telefon- oder Bypass-Verbindung mit SDH oder WDM) mangels freier Teilstrecken nicht geschaltet werden kann, wird der Verbindungswunsch abgelehnt. Bei vielen erfolglosen Verbindungswünschen werden die beteiligten Vermittlungssysteme aber trotzdem eine hohe Belastung oder Überlast ausgesetzt.

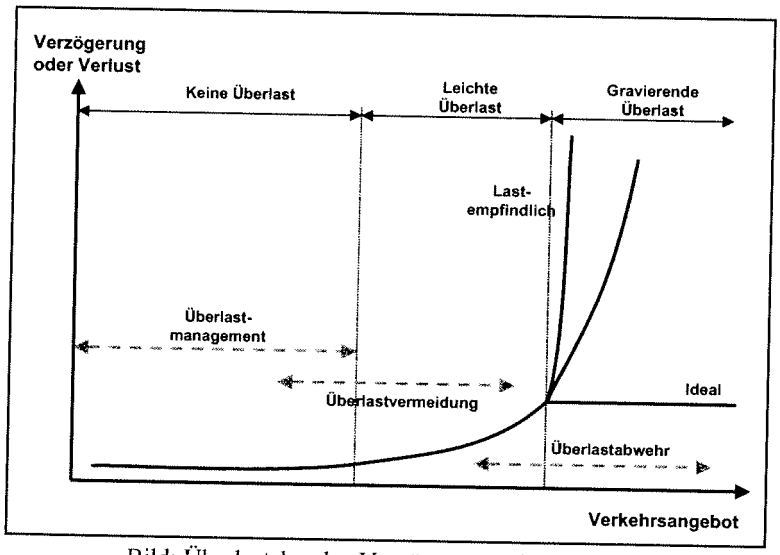


Bild: Überlastabwehr: Verzögerung oder Verlust

Bei **Paketvermittlungsnetzen** unterscheidet man wieder zwischen dem Aufbau der virtuellen Pfade oder Verbindungen und der Vermittlung von Paketen. Im ersten Fall verhindert eine Verbindungszugangskontrolle (CAC, Connection Access Control) das Entstehen von Netzüberlastsituationen.

Bei der Paketvermittlung selbst entstehen Überlastsituationen, wenn temporär zu viele Pakete gleichzeitig übertragen werden müssen. Dadurch können Teilstrecken und Router überlastet werden. Dies führt zu verzögerten Vermittlungen und Paketverlusten, die mit zunehmender Last stark zunehmen.

Falls keine geeigneten Maßnahmen ergriffen werden, kann eine Überlast zum Kollaps führen. Die Aufgabe der Überlaststeuerung besteht also darin, bei jeder Teilstrecke und jedem Knoten die Last auf einen bestimmten Wert zu begrenzen.

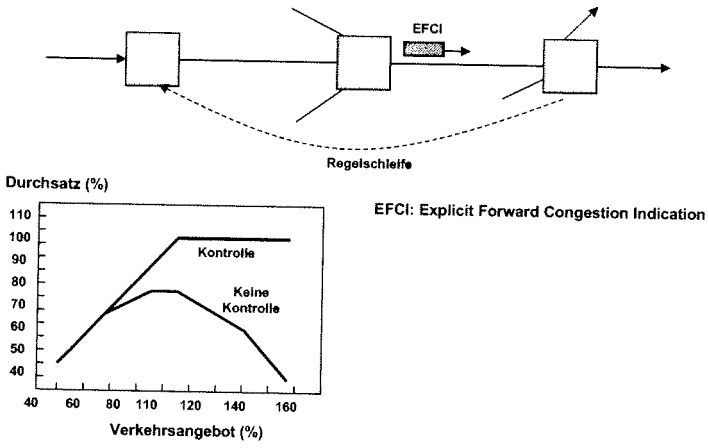


Bild: Überlastabwehr durch Erkennung, Meldung an Zielknoten und Rückmeldung an Quellknoten zur Drosselung des Paketflusses.

Die Durchsatz- bzw. Verzögerungskurven, die sowohl für überlastete Netzteile als auch für überlastete Netzknoten gelten, können in folgende Bereiche eingeteilt werden:

Region 1: Linearer Anstieg bei steigendem Angebot.

Region 2: Beginn der Sättigung. Die Übertragungsleitungen arbeiten immer öfters mit voller Kapazität.

Region 3: Überlast. Die Puffer in den Netzknoten füllen sich und bei Überlauf müssen Pakete verworfen werden. Durch Vermittlungsverzögerungen und die Paketverluste gibt es immer mehr Paketwiederholungen, die dazu führen, dass das Netz immer stärker belastet wird, aber der eigentliche Nutzdurchsatz abnimmt.

Überlastproblematik in Paketvermittlungsnetzen

Das Verkehrsgeschehen in Paketvermittlungsnetzen, und somit auch die Überlastproblematik, wird bestimmt durch die Wechselwirkung zwischen den Verkehrschwankungen und der Betriebsmittelvergabe. Das Problem der Überlast und die Abwehrmaßnahmen umfassen deshalb:

- Charakterisierung des angebotenen Verkehrs,
- Aspekte zur verkehrsgerechten Realisierung von Paketvermittlungsnetzen,
- Ursachen und Indikatoren für Überlastsituationen,
- Klassifizierung und Beschreibung von Überlastabwehrstrategien.

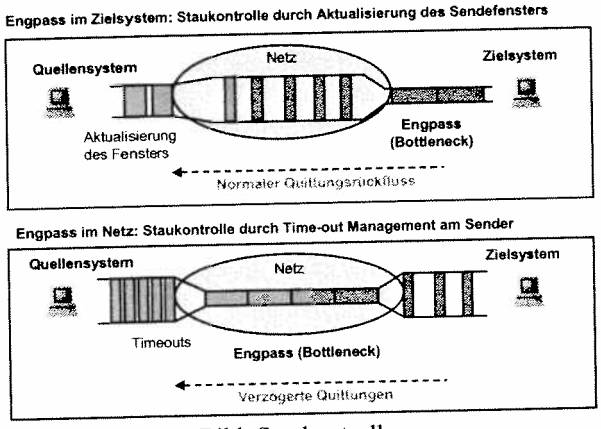


Bild: Staukontrolle

Darüber hinaus unterscheidet man zwischen den Anforderungen für den Verbindungsaufbau und dem Datenaustausch selbst. Abgesehen von sporadischen Häufungen spielt der Verkehrsanteil der Verbindungsaufbau-Pakete eine untergeordnete Rolle. Das gesamte Verkehrsangebot ist jedoch abhängig von der Anzahl der gleichzeitig bestehenden virtuellen Verbindungen und dem stochastischen Ablaufgeschehen innerhalb dieser Verbindungen.

Charakterisierung des angebotenen Verkehrs

Die Verkehrscharakteristiken in Paketvermittlungsnetzen sind durch folgende zwei grundsätzlichen Betriebsarten bestimmt:

a) Dialogbetrieb mit den Merkmalen:

- niedriges Datenvolumen,
- vorwiegend kurze Pakete,
- kurze Übertragungsdauer und lange Pausen,
- kurze Quittierungszeiten erforderlich,
- lokaler Hauptverkehr tagsüber.

b) Stapelbetrieb mit den Merkmalen:

- hohes Datenvolumen,
- vorwiegend Pakete mit maximaler Länge,
- lange Übertragungsdauer und kurze Pausen,
- längere Quittierungszeiten zugelassen,
- lokaler Hauptverkehr häufig erst abends und nachts.

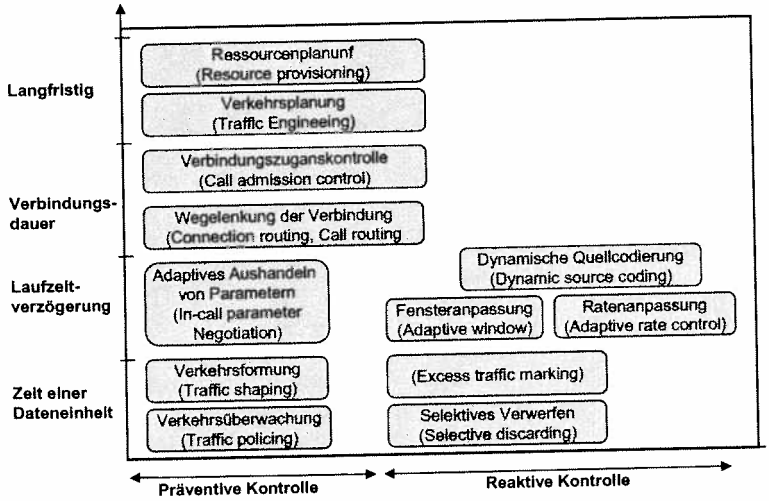


Bild: Mechanismen zur Verkehrskontrolle

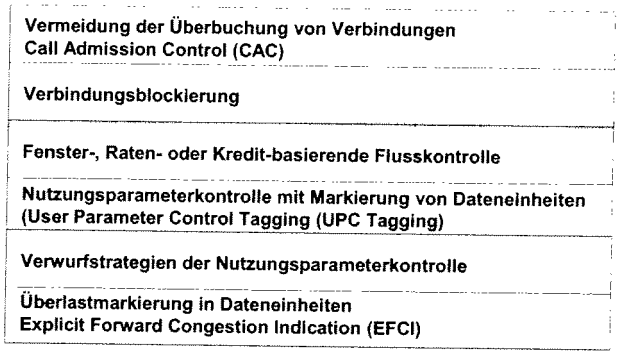


Bild: Überlastvermeidung

Verfahren zur Überlastabwehr
Grundsätzlich kommen folgende Verfahren in diversen Kombination zum Tragen:

- **Überdimensionierung des Netzes** (overprovisioning): Das Netz wird so großzügig ausgelegt, dass keine Überlast auftreten kann. Dieser Ansatz ist aus wirtschaftlichen Gründen kaum praktikabel.
- **Regulierung von neuen Kommunikationsverbindungen (CAC, Call Admission Control):** analog zum Telefonnetz werden neue Kommunikationsbeziehungen nur zugelassen, wenn genügend freie Kapazitäten im Netz vorhanden sind.
- **Überwachung des Zugangsverkehrs (Policing):** Überprüfung von Netzzugangsströmen gemäß Verkehrskontrakt und Markieren oder Verwerfen von Dateneinheiten am Netzrand.
- **Verkehrsformung (Traffic Shaping):** Glättung von Datenspitzen.
- **Drosselung von Quellen:** Die Quellen können vom Netz aufgefordert werden, vorübergehend weniger Verkehr in das Netz einzuspeisen. Dies können die Quellen auch von sich aus tun, wenn sie eine zu hohe Netzbelastung feststellen. Verfahren dieser Art werden beispielsweise in TCP genutzt.
- **Selektives Verwerfen:** Verwerfen von markierten aber auch von nicht-markierten Dateneinheiten gemäß einer Verwerfungsstrategie im Netz selbst.

Überlastproblematik in Paketvermittlungsnetzen
Das Verkehrsgeschehen in Paketvermittlungsnetzen, und somit auch die Überlastproblematik, wird bestimmt durch die Wechselwirkung zwischen dem stochastischen Verkehr und der Betriebsmittelvergabe. Das Problem der Überlast und die Abwehrmaßnahmen umfassen deshalb:

- Charakterisierung des angebotenen Verkehrs,
- Aspekte zur verkehrsgerechten Realisierung von Paketvermittlungsnetzen,
- Ursachen und Indikatoren für Überlastsituationen,
- Klassifizierung und Beschreibung von Überlastabwehrstrategien.

Darüber hinaus unterscheidet man zwischen den Anforderungen für den Verbindungsaufbau und dem Datenaustausch selbst. Abgesehen von sporadischen Häufungen spielt der Verkehrsanteil der Verbindungsaufbau-Pakete eine untergeordnete Rolle. Das gesamte Verkehrsangebot ist jedoch abhängig von der Anzahl der gleichzeitig bestehenden virtuellen Verbindungen und dem stochastischen Ablaufgeschehen innerhalb dieser Verbindungen.

Aspekte zur verkehrsgerechten Realisierung von Paketvermittlungsnetzen
Die Realisierung von Paketvermittlungsnetzen beruht auf dem Zusammenspiel von Hardware- und Softwaretechnologie, Übertragungs- und Vermittlungstechnik, Wirtschaftlichkeit und verkehrstheoretischen Gesichtspunkten. Dabei ist die Verwirklichung der einzelnen Verkehrskriterien bedingt durch die Kapazität der Übertragungsstrecken, die Rechnerleistung sowie die Pufferkapazität der Netzknoten und die Regeln, nach denen diese Betriebsmittel den Paketen zugewiesen werden (z.B. Pufferzuteilung, Verkehrslenkung, Datenflusskontrolle und Überlastabwehrstrategie).

Entwurf, Dimensionierung und Betrieb von Paketvermittlungsnetzen werden somit von den folgenden, teilweise widersprüchlichen Zielsetzungen entscheidend beeinflusst:

- niedrige Quittierungszeiten für Dialogverkehr und Realzeitanwendungen,
- hoher Durchsatz für Stapelverkehr,
- faire Zuteilung der Betriebsmittel an die einzelnen Anwenderprozesse,
- optimale Auslastung der Betriebsmittel,
- hohe Netzverfügbarkeit,
- allgemeine Zugänglichkeit des Netzes,
- hohe Zuverlässigkeit der Paketübermittlung,
- Wirtschaftlichkeit.

- Die **Quittierungszeit**, definiert als die Zeitdauer zwischen dem Absenden eines Paketes und der Bestätigung über den korrekten Empfang am Zielort, ist für den Dialog- und Realzeitbetrieb dann optimal ausgelegt, wenn sie mit einer gewissen Wahrscheinlichkeit eine Zeitobergrenze nicht überschreitet (z.B. 95 % weniger als 0.5 Sekunden). Kurze Quittierungszeiten bedingen im wesentlichen eine geringe Anzahl von Übertragungsabschnitten und möglichst kurze Warteschlangenlängen in den einzelnen Netzknoten. Auch eine bevorzugte Abfertigung kann die Wartezeiten für dringende Pakete in den Netzknoten verringern.
- Der **Durchsatz**, definiert als die mittlere Anzahl von Paketen pro Sekunde, steht dagegen bei Stapelbetrieb im Vordergrund. Für einen hohen Durchsatz soll die Datenflusskontrolle zwischen Ursprung und Ziel den Datenaustausch möglichst wenig bremsen. Dies verlangt ein großes Fenster. Somit können große Warteschlangen entstehen und die Quittierungszeiten sind entsprechend länger.
- Eine **faire Zuteilung der Betriebsmittel** erfordert Regeln, um zu verhindern, dass Anwenderprozesse aufgrund einer günstigen geographischen Position oder infolge eines hohen Datenvolumens in der Lage sind, einen übermäßigen Betriebsmittelanteil zu belegen.
- Eine **optimale Auslastung der Betriebsmittel** steht in engem Zusammenhang mit den drei vorangehenden Kriterien; eine entsprechende Optimierung ist abhängig von der Gewichtung dieser Zielsetzungen.
- Eine **hohe Netzverfügbarkeit** erfordert eine Redundanz vieler Hardwarekomponenten in den Netzknoten und die Möglichkeit, bei Bedarf auf andere Übertragungsstrecken auszuweichen.
- Eine **allgemeine Zugänglichkeit** bedingt eine Vielzahl von Zusatzeinrichtungen, die es erlauben, zeichenorientierte Datenendgeräte am Paketvermittlungsnetz anzuschließen oder einen Zugang über andere Nachrichtennetze zu ermöglichen.
- Eine **hohe Zuverlässigkeit** der Paketvermittlung fordert neben der Fehlersicherung auf den einzelnen Übertragungsstrecken das Aufbewahren von Paketkopien bis zur Bestätigung des korrekten Empfangs und die Paketwiederholung beim Ausbleiben einer Quittung. Die Fehlersicherung auf den verschiedenen Protokollebenen verlängert jedoch auch die Quittierungszeit, und vorzeitige Paketwiederholungen wirken durchsatzmindernd.
- **Wirtschaftlichkeit** verhindert schließlich eine Überdimensionierung der Betriebsmittel. Dabei gilt: je wirtschaftlicher das Netz ausgelegt ist, desto weniger Spielraum verbleibt für die Bewältigung eines erhöhten Verkehrsangebots.

Überlastsituationen
In Analogie zu dem Straßenverkehr ist das Entstehen von Überlastsituationen in Paketvermittlungsnetzen von komplexer Natur. Solche Situationen sind typisch für die dynamische Wechselwirkung zwischen stochastischem Verkehrsangebot und einem verteilten System mit einer beschränkten Zahl von Betriebsmitteln.

Kennzeichnend für ein überlastetes Netz oder Netzteil ist eine Abnahme des Durchsatzes und eine Verlängerung der Quittierungszeiten. Solange das Verkehrsangebot unterhalb der Verkehrskapazität des betrachteten Netzteiles bleibt, steigt der Durchsatz mitwachsendem Verkehrsangebot an: zuerst linear und anschließend etwas geringer. Wird jedoch in einem Netz ohne Überlastabwehrstrategie die Verkehrskapazität überschritten, so nimmt der Blindlastanteil durch Paketwiederholungen und gegenseitige Verkehrsbehinderung sehr stark zu, so dass der Durchsatz entsprechend geringer wird. Im Extremfall kann eine Verklemmungssituation auftreten.

Dieses ungünstige Verhalten kann mit Hilfe von verschiedenen Abwehrmaßnahmen verhindert werden.
Verschiedene Ursachen können eine Überlast auslösen:
- Unangemessene System- und Netzplanung können Systemengpässe verursachen, die sich oft auch auf andere Teile des Netzes auswirken. Zu diesen systeminternen Ursachen gehören ungenügende Puffer-, Verarbeitungs- und Übertragungskapazitäten, ungünstige Ablaufsteuerung in den Netzknoten, Vermittlungsprotokolle.
- Der Ausfall von Übertragungsabschnitten, Verarbeitungs- oder Puffereinheiten bedeutet eine Kapazitätsminderung und je nach Rekonfigurationsverhalten eines Systems kann dies eine Überlastsituation auslösen.
- Eine große Anzahl von gleichzeitig bestehenden virtuellen Verbindungen, die alle für sich eine Datenflusskontrolle besitzen, können wegen ihrer stoßartigen Betriebsweise temporär ein Gesamtverkehrsangebot erzeugen, das ein Vielfaches der Nennkapazität der Netzkomponenten beträgt. Es entstehen also ausgeprägte Lastspitzen.
- Eine temporäre Blockierung am Empfangsort verursacht einen Rückstau von Paketen im Netz, der eine Überlastsituation verursachen kann.
- Ein langandauernder hoher Datenverkehr kann ebenfalls eine Überlastsituation entstehen lassen.
- Eine Häufung von Anforderungen für den Aufbau von virtuellen Verbindungen kann morgens auftreten, wenn Banken, Geschäfte und Reisebüros Verbindungen mit ihren Kommunikationspartnern initiieren. Ein derart hoher Verbindungsaufbauaufwand kann die betroffenen Rechner in den Netzknoten stark überlasten.

Als Reaktion auf diese Primärursachen können einige Nebenwirkungen entstehen, die die Überlastsituation noch verschärfen:
- Paketwiederholungen verursachen eine zusätzliche Netzbelastung, die im Normalfall zu vernachlässigen ist. Werden jedoch Paketwiederholungen als Reaktion auf eine Überlastsituation im Netz ausgelöst, so kann diese Blindlast ein beträchtliches Ausmaß annehmen und das Netz derart überlasten, dass der Paketverkehr total zusammenbricht.

- Überlastete Verkehrsströme beanspruchen infolge blockierter Pakete einen hohen Pufferbedarf. Durch diesen Pufferengpass werden auch alle anderen Verkehrsströme behindert und dies kann leicht dazu führen, dass die Übertragungskapazität nicht voll ausgenutzt werden kann.
- Insbesondere in Überlastsituationen können als Folge von gegenseitigem Warten auf das Freiwerden von Betriebsmitteln Verklemmungssituationen (Deadlocks) entstehen.

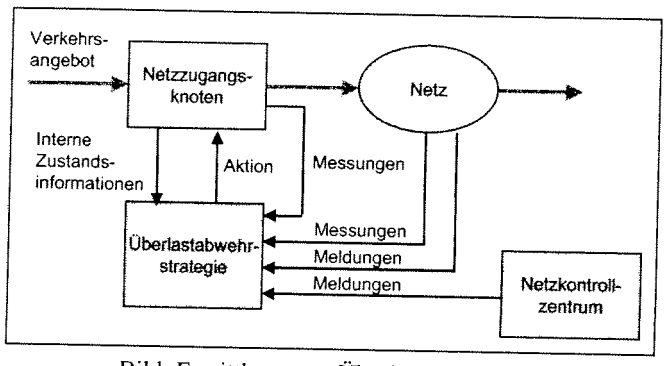


Bild: Ermittlung von Überlastindikatoren

Überlastindikatoren
Zur möglichst frühzeitigen Erkennung von Überlastsituationen benötigt ein Netzknoten Indikatoren.

Diese Überlastindikatoren werden ermittelt aus:
- Messungen im Netz und im Netzknoten selbst,
- internen Zustandsinformationen,
- Meldungen von anderen Netzknoten und vom Netzkontrollzentrum.

Die Durchführung einer Messung (Zeiten oder Zählvorgänge) erfordert ein entsprechendes Messintervall, so dass die Messwerte einen Zustand in der unmittelbaren Vergangenheit darstellen. Die Präzision, mit der das zukünftige Netz- oder Systemverhalten vorausgesagt werden kann, hängt vom Schätzungsverfahren, von der Häufigkeit und der Genauigkeit der Messungen sowie von der Länge des Messintervalls ab.

Zu dieser Kategorie von Überlastindikatoren gehören:
- Auslastung der Übertragungsstrecken, aus der die gesamte Verkehrslast (Pakete, Wiederholungen und Verwaltungsarbeit des Übertragungsprotokolls) auf den einzelnen abgehenden Übertragungsstrecken ermittelt werden kann.
- Anzahl der Paketwiederholungen (Vermittlungsebene) als Indikator für möglicherweise überlastete Zielrichtungen.
- Quittierungsverzögerung als Maß für die Quittierungszeiten der verschiedenen Zielrichtungen.

Bei internen Zustandsinformationen handelt es sich um einen gegenwärtigen Zustand, aus dem direkt auf eine bevorstehende Überlastsituation rückgeschlossen werden kann.

Dies geschieht durch die Überwachung von:
- Warteschlangenlängen, aus denen einerseits die zukünftige Netzlast in die verschiedenen Zielrichtungen ermittelt werden kann und andererseits als Maß für einen Rückstau dienen.
- Pufferbelastung (Pakete und Kopien) zur Anzeige von drohenden Engpässen.
- Anzahl der gesetzten Time-Outs (Vermittlungsebene), aus der sich die im Netzknoten noch zu quittierende Netzlast je Richtung ermitteln lässt.

Durch Meldungen von benachbarten Netzknoten oder von den Zielknoten wird jeder Netzknoten über deren Belastungssituation in Kenntnis gesetzt. Diese Meldungen erfolgen entweder in regelmäßigen Abständen oder aufgrund einer wesentlichen Belastungsänderung. Darüber hinaus erhält jeder Netzknoten Meldungen vom Netzkontrollzentrum.

Klassifizierung und Beschreibung von Überlastabwehrstrategien
Zur Verhinderung von Überlastsituationen, die insbesondere in Paketvermittlungsnetzen völlig unerwartet entstehen können, werden neben Methoden für die Erkennung von Überlast diverse Abwehrstrategien benötigt.

Dabei sind bei der Entwicklung und Implementierung von Überlastabwehrstrategien folgende Ziele zu verfolgen:
- Die Wirkungsgeschwindigkeit soll dem geographischen Wirkungsbereich (lokal oder global) angepasst sein.
- Anstatt einer abrupten soll eine gleichmäßige Wirkung erzielt werden.
- Der Verwaltungsaufwand soll niedrig und unabhängig von der Netzbelastung sein.
- Die Maßnahmen sollen selektiv sein, so dass sie sich lediglich auf bestimmte Verkehrsströme auswirken.
- Die Maßnahmen sollen jedoch auch fair sein, so dass keine Verkehrsströme übermäßig benachteiligt werden.

Hierarchische Gliederung
Eine effiziente Überlastabwehr in Paketvermittlungsnetzen erfordert eine Hierarchie von genau aufeinander abgestimmten Abwehrmaßnahmen.
- Auf der Vermittlungsebene existieren drei Bereiche, und zwar der Netzzugang, der Bereich zwischen Ursprungs- und Zielknoten und der Bereich zwischen benachbarten Netzknoten.

- Auf der Transportebene befindet sich die Datenflusskontrolle zwischen den Anwenderprozessen, die für diesen individuellen Verkehrsfluss Überlastabwehrfunktionen zu erfüllen hat.
- Auf der hierarchisch höchsten Ebene ist das Netzkontrollzentrum zu finden.

Wirkungsbereich und Wirkungsgeschwindigkeit
In engem Zusammenhang mit der hierarchischen Implementierung stehen auch der geographische Wirkungsbereich und die Wirkungsgeschwindigkeit der Überlastabwehrstrategien.

In bezug auf den geographischen Wirkungsbereich kann unterschieden werden zwischen:
- **lokalen Überlastabwehrstrategien:** Netzzugang, Netzknoten selbst. Sie basieren auf Informationen, die im Netzknoten selbst aufgrund seines internen Zustandes, aufgrund von Messungen oder Meldungen vorhanden sind. Die lokale Überlastabwehrstrategie soll dem Entstehen von lokalen Überlastsituationen oder Verkehrsbehinderungen zuvorkommen.
- **globalen Überlastabwehrstrategien:** gesamtes Netz, Netzbereich, benachbarte Netzknoten, Beziehungen zwischen Netzendknoten, Beziehungen zwischen Anwenderprozessen, Regelung der Netzzugänge. Sie beruhen auf einer statisch oder dynamisch festgelegten Begrenzung der Anzahl von Paketen und sie sollen vermeiden, dass diese Zahl überschritten wird. Die zur Überlastabwehrmaßnahme notwendigen Informationen stehen i.a. nicht sofort zur Verfügung, sondern müssen durch Meldungen von entfernten Netzknoten bereitgestellt werden.

Da einerseits eine globale Überlastabwehrstrategie die Bildung von lokalen Überlastsituationen in ihrem Wirkungsbereich nicht verhindern kann und andererseits eine lokale Überlastabwehrstrategie nur eine suboptimale Auslastung der einzelnen Betriebsmittel bewirken kann, ist für einen optimalen Netzbetrieb ihre Kombination unentbehrlich.

Hinsichtlich der Wirkungsgeschwindigkeit gilt allgemein, dass je höher die hierarchische Implementierungsstufe ist, und damit je größer der geographische Wirkungsbereich, desto langsamer kann und darf die Überlastabwehrstrategie wirken.

Damit gilt für die Rangordnung in abnehmender Wirkungsgeschwindigkeit: Netzknoten selbst - Umgebung der Netzknoten - Netzbereich bzw. Beziehung zwischen Netzendknoten oder Anwenderprozessen - gesamtes Netz. Der Charakter der Überlastabwehr ändert sich somit vom hochdynamischen zum quasi-statischen.

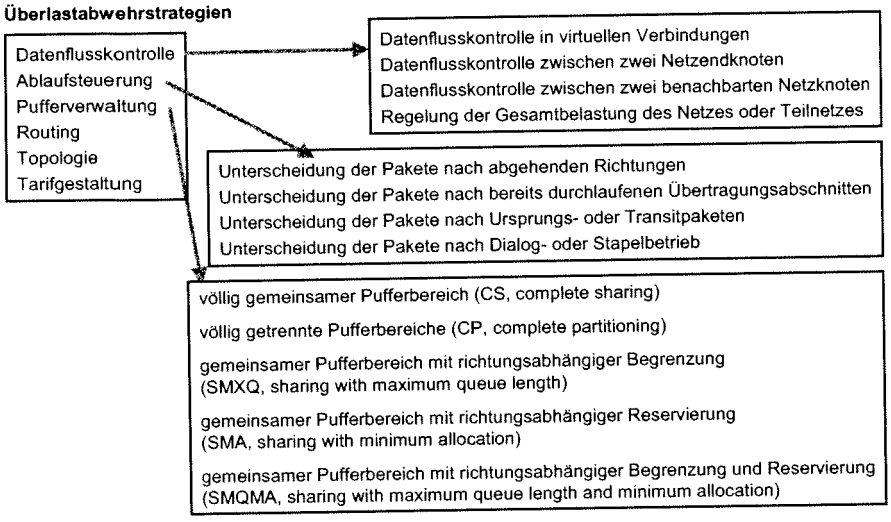


Bild: Überlastabwehrmechanismen

Art der Realisierung
Bei einer Klassifizierung der Überlastabwehrstrategien nach der Art ihrer Realisierung können die folgenden Möglichkeiten identifiziert werden:

- Datenflusskontrolle,
- Ablaufsteuerung,
- Pufferverwaltung,
- Verkehrslenkung,
- Topologie,
- Tarifgestaltung.

Über die Zeitspanne zwischen dem Moment der Überlasterkennung und dem Beginn der Abwehrmaßnahmen können folgende Aussagen gemacht werden:

- Für Überlastabwehrstrategien, die den Netzknoten selbst betreffen, kann die entsprechende Abwehrmaßnahme sofort getroffen werden, da die Erkennung und die Ausführung direkt im Netzknoten stattfindet. Es handelt sich hierbei um die Umorganisation der Paketpufferung, Änderung in der Abfertigungsreihenfolge oder um eine Umstellung auf eine andere Paketannahmestrategie.
- Überlastabwehrstrategien, die den Netzzugang regeln, wirken ebenfalls-verzögerungsfrei, sofern die Überlasterkennung im Netzendknoten selbst stattfindet. Werden die Abwehrmaßnahmen von einem anderen Netzknoten eingeleitet, z.B. mit Drosselungspaketen, so muss eine entsprechende Verzögerungszeit für das Eintreffen dieser Pakete berücksichtigt werden.
- Bei Überlastabwehrstrategien, die sich über das Paketvermittlungsnetz hinweg oder einen Teil des Netzes erstrecken, muss eine stochastische Wirkungsverzögerung einbezogen werden.

Dies ist auch dann notwendig, wenn diese Netzsteuerungspakete mit Priorität vermittelt werden. Die Größe der Verzögerung hängt im wesentlichen von der geographischen Distanz ab.

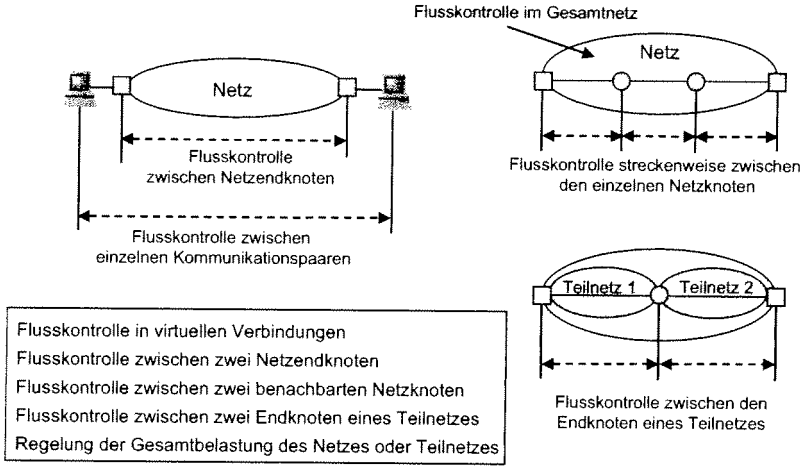


Bild: Datenflusskontrolle

Datenflusskontrolle

Eine zweite wichtige Gruppe von Überlastabwehrstrategien beruht auf einer Datenflusskontrolle. Sie gehören somit zu den globalen Überlastabwehrstrategien. Mechanismen dieser Art verwenden entweder die Begrenzung der Paketzahl im betreffenden Netzteil (Fenstermechanismus, Transportberechtigung (Permit) oder den Austausch von Meldungen (Start/Stop, Drosselung, Betriebsmittelreservierung). Je nach Umfang des gesteuerten oder geregelten Bereiches bzw. Art der Methode kann eine weitere Unterteilung vorgenommen werden.

Aufgabestellung

Wie viele Dateneinheiten dürfen vom Sender hintereinander gesendet werden, ohne dass der Puffer beim Empfänger überläuft (d.h.Paketverluste entstehen)?

Anforderungen

- Einfachheit
- Möglichst geringe Nutzung von Netzressourcen
- Stabilität

Varianten

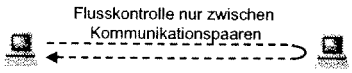
Closed Loop
- Rückkopplung, um zu verhindern, dass Empfänger überschwemmt wird.
- Quelle adaptiert ihren Datenstrom entsprechend.

Open Loop
- Beschreibung des Verkehrs mit anschließender Ressourcenreservierung und Überwachung des eingehenden Verkehrs.

Bild: Flusskontrolle

1. Generation: Berücksichtigung der Leistungsfähigkeit des Kommunikationspartners

- On-Off
- Stop-and-Wait
- Statisches Fenster



2. Generation: Zusätzliche Berücksichtigung der Leistungsfähigkeit des Netzes

-Messungen
- Kontrollvarianten
- Kontrollpunkt
- Explizit vs. Implizit
- Ende-zu-Ende vs. Hop-by-hop
- Dynamisches Fenster vs. dynamische Rate

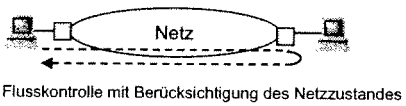


Bild: Flusskontrolle (Closed Loop)

Fensterbasierende Flusskontrolle:

Begrenzung der Anzahl von der Quelle ausgesendeten Dateneinheiten durch eine veränderliche Fenstergröße, die durch Senden von Daten und Rückmeldungen geändert wird.

Ratenbasierende Flusskontrolle :

Anpassung der Quellenübertragungsrate unter Verwendung eines Feedbackalgorithmus.

Kreditbasierende Flusskontrolle :

Zuteilung einer Gutschrift für die Anzahl der zu sendenden Dateneinheiten. Ist das Guthaben aufgebraucht, muss die Quelle auf eine neuerliche Zuteilung von Krediten gewarteten.

Bild: Methoden der Flusskontrolle

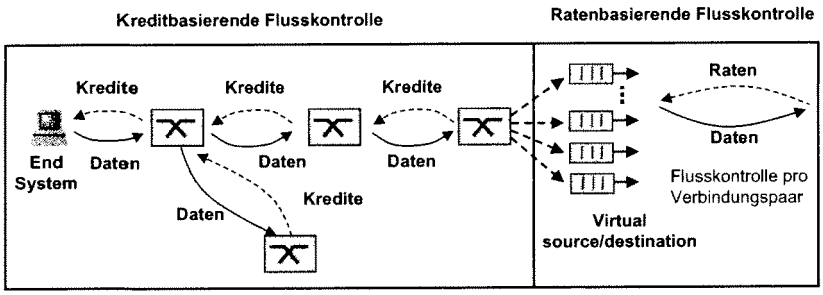
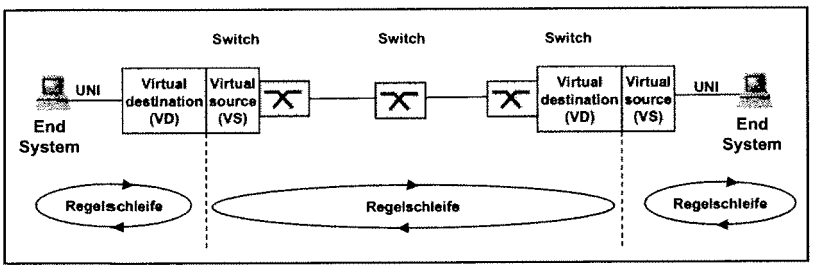


Bild: Mischformen: Kredit- und Ratenkontrolle



UNI: User Network Interface

Bild: Mehrere Regelschleifen

a) Datenflusskontrolle in virtuellen Verbindungen

Bezieht sich die Datenflusskontrolle auf eine einzige Verbindung (Transportebene), so vermag sie zwar die virtuelle Verbindung gegen eine exzessive Belastung zu schützen, kann aber wegen der vielen gleichzeitigen virtuellen Verbindungen das Paketvermittlungsnetz nicht vor Überlastsituationen bewahren. Dennoch übernimmt die individuelle Datenflusskontrolle eine wichtige Aufgabe, denn wenn bei mehreren virtuellen Verbindungen die Paketrate des Sendeprozesses größer ist als die des Empfangsprozesses, so ist das Paketvermittlungsnetz durch Rückstau schnell überlastet. Die Datenflusskontrolle begrenzt die Paketzahl pro virtuelle Verbindung, und ein momentan überlasteter Empfangsprozess kann mit einer entsprechenden Meldung seinen Datenfluss vorübergehend stoppen. Darüber hinaus haben Quittierungsverzögerungen als Folge einer Netzüberlastung eine bremsende Wirkung auf den Datenfluss in den betreffenden virtuellen Verbindungen. Auf diese Weise kann auch die individuelle Datenflusskontrolle dazu beitragen, dass die Überlastsituation sich nicht weiter zuspitzt. Andererseits können längere Quittierungsverzögerungen aber auch eine zusätzliche Netzbelastung durch Paketwiederholungen verursachen. Wenn jedoch der sendeseitige Netzendknoten über Informationen bezüglich Netzverzögerungen verfügt, können die individuellen Zeitüberwachungen auf der Transportebene des Anwenderprozesses durch entsprechende Meldungen adaptiv eingestellt werden.

b) Datenflusskontrolle zwischen zwei Netzendknoten

In diesem Falle wird der Gesamtfluss zwischen zwei Netzendknoten gesteuert. Dabei ist es unwesentlich, ob die einzelnen Pakete bereits zu einer individuellen Datenflusskontrolle gehören oder nicht. Die Betrachtungen gelten somit auch für den Datagrammbetrieb. Das Hauptziel besteht darin, Eintritts- und Austrittsrate für diesen Verkehrsstrom aufeinander abzustimmen. Bei einer Verstopfung der Verkehrsabgänge im entfernten Netzendknoten soll der Paketfluss im Ursprungsknoten gestoppt werden.

c) Datenflusskontrolle zwischen zwei benachbarten Netzknoten
Auch zwischen benachbarten Netzknoten ist eine Datenflusskontrolle erforderlich. Sie hat die Aufgabe, Überlastsituationen in einem Netzknoten durch Beschränkung der Menge der eintreffenden Pakete aus einem benachbarten Knoten Grenzen zu setzen. Je mehr Nachbarknoten existieren, um so schwieriger kann aber auf diese Weise eine Knotenüberlastung verhindert werden.

d) Regelung der Gesamtbelastung des Netzes
Diese als isarithmetrische Datenflusskontrolle bezeichnete Methode (denn sie hält die Anzahl von Paketen im Netz konstant), verwendet eine feste Anzahl von Transportberechtigungen (Permits), die durch die Paketübermittlung im Netz zirkulieren. Ein Paket kann nur dann befördert werden, wenn der Netzknoten über ein Permit verfügt. Das Paket führt dieses Permit bis zum Zielknoten mit, wo es nach Abgabe dem Zielknoten zur Verfügung steht. Wegen Problemen wie die Häufung von Pemits, geringer Durchsatz bei Stapelbetrieb, Möglichkeit zur lokalen Überlastung und Garantie, dass keine Permits verloren gehen sollen, hat diese Methode im wesentlichen nur noch eine historische Bedeutung.

Choke-Pakete
Es handelt sich um ein Prinzip, das sowohl für virtuelle Verbindungen als auch Datengramme angewandt werden kann. Jeder Router im Teilnetz überwacht die Auslastung seiner Ausgangsleitungen und andere Ressourcen. Er kann z.B. jede Leitung mit einer echten Variablen u mit einem Wert zwischen 0,0 und 1,0 in Verbindung setzen, was die jeweils letzte Auslastung der betreffenden Leitung repräsentiert. Um eine gute Schätzung von u sicherzustellen, kann periodisch ein Muster der momentanen Leitungsauslastung (entweder 0 oder 1) genommen und u entsprechend der folgenden Formel aktualisiert werden: $u_{neu} = a\, u_{alt} + (1- a)\, f$, wobei die Konstante a bestimmt, wie schnell der Router die letzte Historie vergisst.

Bewegt sich u über diesen Schwellenwert hinaus, tritt die Ausgangsleitung in einen Warnzustand ein. Jedes neu ankommende Paket wird geprüft, um festzustellen, ob seine Ausgangsleitung diejenige ist, die sich im Warnzustand befindet. Ist das der Fall, sendet der Router ein Choke-Paket an den Quellendsystem zurück (die Adresse wird im Paket vorgefunden). Das Originalpaket wird gekennzeichnet (ein Header-Bit wird gesetzt), so dass keine weiteren Choke-Pakete auf dem Pfad erzeugt werden. Bei Empfang des Choke-Pakets durch das Quellendsystem muss dieser den an das offene Ziel gesendeten Verkehr um x Prozent reduzieren. Da wahrscheinlich andere Pakete zum gleichen Ziel auf dem Weg sind und ihrerseits Choke-Pakete erzeugen, sollte das Datenendsystem die Choke-Pakete, die sich auf dieses Ziel beziehen, über ein bestimmtes Intervall ignorieren. Kommt eines an, ist die Leitung selbstverständlich immer noch überlastet, so dass das Datenendsystem den Fluss noch weiter reduziert und die Choke-Pakete wieder ignoriert. Kommen während der abgetasteten Periode keine weiteren Choke-Pakete an, kann das Datenendsystem den Fluss wieder erhöhen. Die diesem Protokoll eigene Bestätigung trägt zur Vermeidung von Überlastungen bei, kann aber keinen Datenfluss drosseln. Von diesem Algorithmus für Überlastungsüberwachung wurden mehrere Varianten vorgeschlagen. Eine davon sieht vor, dass die Router mehrere Schwellenwerte führen. Je nachdem, welcher Schwellenwert überschritten wurde, kann das Choke-Paket eine milde Warnung, eine scharfe Warnung oder ein Ultimatum enthalten. Bei einer anderen Variante wird anstelle der Leitungsauslastung die Warteschlangenlänge oder die Pufferauslastung als Auslösesignal herangezogen. Die gleiche exponentielle Gewichtung kann wie bei u auch auf diese Parameter angewandt werden.

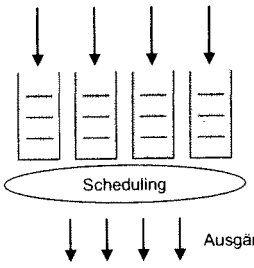
Hop-by-Hop Choke-Pakete
Bei hohen Geschwindigkeiten und großen Entfernungen ist das Versenden eines Choke-Pakets zu den Quellsystemen nicht geeignet, weil die Reaktion zu langsam ist. Bei einem alternativen Ansatz wird das Choke-Paket auf jeder durchlaufenen Teilstrecke wirksam.

Load-Shedding
Kann eine Überlastung durch keine der genannten Methoden eingedämmt werden, können Router mit schwerem Geschütz auffahren: dem Load-Shedding. Das ist eine witzige Art, Router anzuweisen, dass sie Pakete, die sie nicht bewältigen können, wegwerfen sollen. Der Begriff stammt aus der Welt der Stromerzeugung, wo er die absichtliche Abschaltung bestimmter Bereiche bezeichnet, um das gesamte Stromnetz vor dem Zusammenbruch zu bewahren, wenn der Stromverbrauch das Angebot um ein Vielfaches übersteigt.

Jitter-Kontrolle
Das Jitter (Verzögerungsschwankungen) kann in Grenzen gehalten werden, indem man die erwartete Übertragungszeit für jede Teilstrecke entlang des Pfads berechnet. Kommt ein Paket bei einem Router an, prüft der Router, um wie weit das Paket gegenüber dem Plan verfrüht oder verspätet ist. Diese Information wird im Paket gepuffert und bei jeder Teilstrecke aktualisiert. Ist das Paket dem Plan voraus, wird es entsprechend lang zurückgehalten. Hinkt es hinter dem Plan her, versucht der Router, es schneller weiterzugeben. Der Algorithmus zur Ermittlung, welche Pakete um eine Ausgangsleitung konkurrieren, kann immer das Paket wählen, das am weitesten hinter dem Plan zurückliegt. Auf diese Weise werden vorauseilende Pakete verlangsamt und nachhinkende Pakete vorgezogen. In beiden Fällen wird das Jitter reduziert.

Überlastungsüberwachung für Multicasting

Alle bisher behandelten Algorithmen zur Überlastungsüberwachung betreffen Nachrichten von einer Quelle an ein Ziel. In diesem Abschnitt wird eine Möglichkeit beschrieben, Multicast-Flüsse von mehreren Quellen an mehrere Ziele zu handhaben. Wir stellen uns als Beispiel mehrere Fernsehsender in geschlossenem Kreislauf vor, die Audio- und Videoströme an eine Gruppe von Empfängern übertragen, die alle eine oder mehrere Sender gleichzeitig einschalten und nach eigenem Ermessen zwischen den Sendern umschalten können. Ein möglicher Anwendungsbereich nach diesem Beispiel sind Videokonferenzen, bei denen jeder Teilnehmer nach Wunsch den momentanen Sprecher beobachten kann. In vielen Multicast-Anwendungen können Gruppen ihre Mitgliedschaft dynamisch ändern. So kann man in eine Videokonferenz eintreten und nach einer Weile wieder abschalten oder auf eine andere Verbindung umschalte. Unter diesen Bedingungen funktioniert der Ansatz, die Sender im voraus Bandbreite reservieren zu lassen, nicht gut, weil jeder Sender alle Ein- und Austritte der Gruppenmitglieder laufend mitverfolgen und den Spanning-Tree bei jeder Änderung neu erzeugen müsste. Bei einem System zur Übertragung von Kabelfernsehsendungen mit Millionen von Teilnehmern ist das ganz und gar undenkbar.



Unterscheidung der Pakete nach abgehenden Richtungen
Unterscheidung der Pakete nach bereits durchlaufenen Übertragungsabschnitten
Unterscheidung der Pakete nach Ursprungs- oder Transitpaketen
Unterscheidung der Pakete nach Dialog- oder Stapelbetrieb

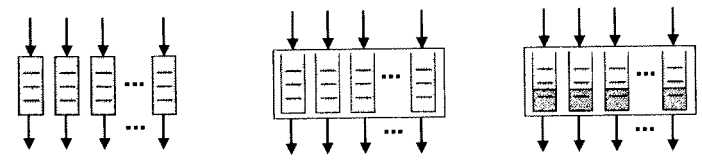
Bild: Ablaufsteuerung (Scheduling)

Ablaufsteuerung

Mit Hilfe der Ablaufsteuerung in den Netzknoten kann die Vermittlungsreihenfolge von Paketen, die zu verschiedenen Verkehrsströmen gehören, abgeändert werden. Dies ist der Fall bei Benutzerprioritäten (Dialog- oder Stapelbetrieb) und bei dynamischen Prioritäten (z.B. zuerst die Pakete, die am Ziel angekommen sind, dann die abgehenden Pakete und danach erst die neuen Pakete). Darüber hinaus können Pakete einzelner Verkehrsströme je nach Stau in den Ausgangswarteschlangen benachbarter Netzknoten zurückgestellt werden, so dass die Übertragungskapazität von Verkehrsströmen ohne nachfolgenden Stau genutzt werden kann. Eine derartige Betriebsweise setzt aber einen entsprechenden Meldungsaustausch zwischen den Netzknoten voraus.

Weighted Fair Queueing

Die Verwendung von Choke-Paketen birgt ein Problem, nämlich, dass die Maßnahme von den Quellendsystemen auf freiwilliger Basis ergriffen wird. Nehmen wir an, dass ein Router andauernd Pakete von vier Quellen bekommt und an alle vier ein Choke-Paket sendet. Eins davon reduziert sein Volumen ordnungsgemäß zurück, während die anderen drei einfach weitermachen. Das Ergebnis ist, dass das drosselnde System einen noch kleineren Anteil an der Bandbreite erhält. Um dieses Problem zu vermeiden und die Einhaltung dieser Regel attraktiver zu gestalten, hat Nagle (1987) den Algorithmus namens Fair Queueing vorgeschlagen. Im wesentlichen sieht dieser Algorithmus vor, dass Router für jede Ausgangsleitung mehrere Warteschlangen haben, d.h. je eine für jede Quelle. Ist eine Leitung frei, tastet der Router die Warteschlangen im Rundumverfahren ab und nimmt das erste Paket der nächsten Warteschlange heraus. Auf diese Weise erhält das Datenendsystem Gelegenheit, eines von n Paketen zu senden, wenn n Endsysteme um eine bestimmte Ausgangsleitung konkurrieren. Durch Versenden mehrerer Pakete wird dieser Bruchteil nicht verbessert. Bei diesem Algorithmus ist problematisch, dass er allen Endsystemen die gleiche Priorität gibt. In vielen Situationen ist es wünschenswert, den Datei- und anderen Servern mehr Bandbreite zu geben als Clients. Sie sollten deshalb zwei oder mehr Byte pro Zeittakt mehr erhalten. Dieser geänderte Algorithmus heißt Weighted Fair Queueing.



völlig getrennte Pufferbereiche (CP, complete partitioning)
völlig gemeinsamer Pufferbereich (CS, complete sharing)
gemeinsamer Pufferbereich mit richtungsabhängiger Begrenzung (SMXQ, sharing with maximum queue length)
gemeinsamer Pufferbereich mit richtungsabhängiger Reservierung (SMA, sharing with minimum allocation)
gemeinsamer Pufferbereich mit richtungsabhängiger Begrenzung und Reservierung (SMQMA, sharing with maximum queue length and minimum allocation)

Bild: Pufferverwaltung

Pufferverwaltung

Eine umfangreiche Gruppe von Überlastabwehrstrategien wird mit Hilfe der Pufferverwaltung realisiert. Im wesentlichen geht es hier um Regeln zur gezielten Abweisung von Paketen. Das Ziel ist die Gesamtoptimierung der Netzbetriebsmittel unter beliebigen Lastsituationen. Da es sich hierbei um lokale Überlastabwehrstrategien handelt, kann dieses Ziel nur zum Teil erreicht werden. Bei völliger Pufferreservierung findet nie ein Pufferüberlauf statt. Die Puffer sind dann aber äußerst gering ausgenutzt. Werden hingegen die Pufferplätze völlig nach dem momentanen Bedarf vergeben, so müssen Pakete bei einem vollen Puffer willkürlich abgewiesen werden, so dass durch Paketwiederholungen eine erhebliche Blindlast entstehen kann. Überlastabwehrstrategien verwenden deshalb eine Pufferreservierung, die zwischen diesen

beiden Extremfällen liegt. Ihre Realisierungsform hängt von den Kri- terien zur Unterscheidung der Pakete ab.

Vier Kriteriengruppen hierzu sind:

a) Unterscheidung der Pakete nach abgehenden Richtungen
Maßgebend hierfür ist die Pufferorganisation für die einzelnen abgehenden Richtungen, die in folgende Software-Organisationsformen unterteilt werden können:

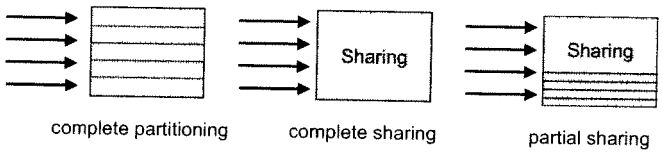
- völlig gemeinsamer Pufferbereich (CS, complete sharing),
- völlig getrennte Pufferbereiche (CP, complete partitioning),
- gemeinsamer Pufferbereich mit richtungsabhängiger Begrenzung (SMXQ, sharing with maximum queue length),
- gemeinsamer Pufferbereich mit richtungsabhängiger Reservierung (SMA, sharing with minimum allocation),
- gemeinsamer Pufferbereich mit richtungsabhängiger Begrenzung sowie Reservierung (SMQMA, sharing with maximum queue length and minimum allocation).

Bei einem völlig gemeinsamen Puffer für sämtliche Richtungen (CS) ist der Puffer vorwiegend mit Paketen eines dominierenden Verkehrsstromes belegt. Pakete, die für eine Richtung bestimmt sind und einen kleineren Verkehr darstellen, müssen deshalb öfters wegen eines verstopften gemeinsamen Puffers abgewiesen werden, obwohl der betreffende Übertragungskanal größtenteils frei ist. Andererseits ist bei völlig getrennten Pufferbereichen (CP) die Pufferausnutzung gering.
Diese beiden Organisationsformen sind deshalb nicht sehr geeignet. Durch eine richtungsabhängige Begrenzung der maximalen Pufferplatzbelegung (SMXQ) kann vermieden werden, dass Verkehrsströme den Gesamtpuffer verstopfen können.

b) Unterscheidung der Pakete nach bereits durchlaufenen Übertragungsabschnitten
Ein wichtiges Ziel einer Überlastabwehrstrategie besteht darin, die Entstehung von Blindlast durch Paketwiederholungen zu verhindern. Deshalb soll die Wahrscheinlichkeit für die Abweisung von Paketen mit zunehmendem Fortschreiten durch das Netz abnehmen. Dazu wird jedes Paket durch eine sogenannte Pufferklasse gekennzeichnet. Beim Betreten des Paketvermittlungsnetzes erhält es die Klasse 0 und nach jedem Übertragungsabschnitt wird die Klasse um eins erhöht. Mit jeder Erhöhung der Pufferklasse nimmt auch die Grenze für die maximale Pufferbelegung zu, so dass mit dieser Maßnahme der erzielte Effekt erreicht wird. Darüber hinaus wird auf diese Weise ein verklemmungsfreier Betrieb garantiert.

c) Unterscheidung der Pakete nach Ursprungs- oder Transitpaketen
Eine wirksame Methode, die das Entstehen einer Blindlast verhindern kann, ist die Abweisung von Paketen direkt am Netzzugang. Als Entscheidungskriterium für das Akzeptieren oder Abweisen von Paketen aus dem Anschlussnetz verwendet man:

- Anzahl der Ursprungspakete im Netzknoten,
- Gesamtanzahl der Pakete im Netzknoten.



complete partitioning (vollständige Unterteilung der Bandbreite)

complete sharing (vollständige gemeinsame Nutzung der Bandbreite)
keine Unterteilung nach Klassen

partial sharing (teilweise gemeinsame Nutzung der Bandbreite)
Reservierung von Teilbereichen für einzelne Klassen
sonst gemeinsame Nutzung

Bild: Verwaltung der Übertragungskapazität
(Bandwidth management)

d) Unterscheidung der Pakete nach Dialog- oder Stapelbetrieb
In Paketvermittlungsnetzen mit einer anwendungsorientierten Prioritätseinteilung kann das Abweisen von Paketen, die sich bereits im Netz befinden, vorwiegend vermieden werden, wenn eine Möglichkeit zur Auslagerung gegeben ist. Die kurzzeitige Auslagerung bezieht sich auf Stapelpakete, denn für sie kann eine größere Durchlaufzeit in Kauf genommen werden. Auf diese Weise wird bei Bedarf für einen kurzen Augenblick Pufferplatz für Pakete mit harten Zeitbedingungen zur Verfügung gestellt. Die Lastspitze kann somit vom Netzknoten selbst aufgefangen werden und wird nicht in unkontrollierter Weise auf Nachbarknoten ausgedehnt.

Überlastungsüberwachung in Teilnetzen mit logischen Verbindungen
Die bisher beschriebenen Methoden zur Überlastungsüberwachung basieren auf der offenen Schleife. Sie versuchen, im voraus Überlastungssituationen zu vermeiden, anstelle der späteren Korrektur.

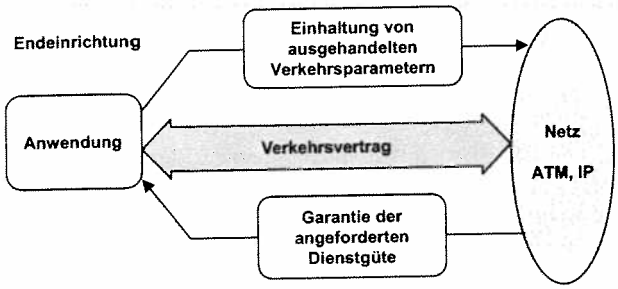


Bild: Verkehrsvertrag

Beim Aufbau einer logischen Verbindung ist die Verhandlung einer Vereinbarung zwischen dem Endgerät und dem Netz oder Teilnetz eine wichtige Strategie Diese Vereinbarung definiert normalerweise das Volumen und die Art des Verkehrs, die geforderte Dienstqualität sowie andere Parameter. Um seine Verpflichtungen aus dieser Vereinbarung zu erfüllen, reserviert das Netz in der Regel Ressourcen auf dem Pfad, wenn die Verbindung aufgebaut wird. Diese Ressourcen können eine Tabelle und Pufferplatz in den Routern sowie Bandbreite auf den Leitungen beinhalten. Auf diese Weise ist eine Überlastung durch Aufbau neuer logischer Verbindungen sehr unwahrscheinlich, weil alle erforderlichen Ressourcen im Rahmen der getroffenen Vereinbarung vorhanden sind.

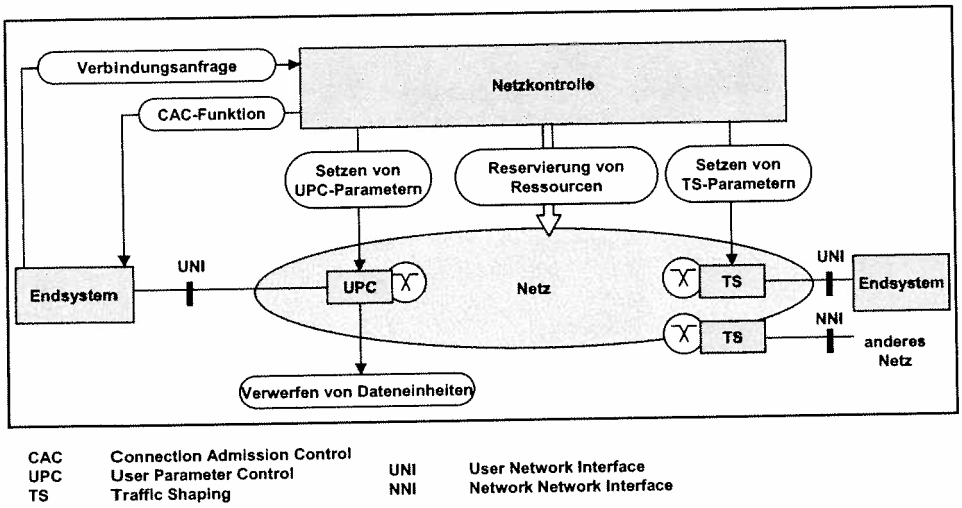


Bild: Aufbau und Überwachung einer logischen Verbindung.

Ein zentraler Mechanismus ist die Regelung der Verbindungsannahme (Admission Control). Das Konzept ist einfach. Wurde eine Überlastung angezeigt, werden keine weiteren logischen Verbindungen mehr aufgebaut, bis das Problem beseitigt wurde. Alle Versuche, auf der Transport-schicht neue Verbindungen aufzubauen, schlagen fehl.

Verkehrslenkung
Die Verkehrslenkung dient dazu, den Paketverkehr möglichst gleichmäßig über das Netz zu verteilen, so dass eine optimale Betriebsmittelausnutzung angestrebt werden kann. Darüber hinaus erhöht sie bei Ausfällen von Übertragungsstrecken oder Netzknoten die Verfügbarkeit des Netzes durch Bereitstellung von Alternativwegen. Im Bezug auf Überlastabwehr ist die Verkehrslenkung als eine wichtige, aber langsam wirkende Maßnahme zu betrachten.

Topologie
Mit der Festlegung der geographischen Struktur des Paketvermittlungsnetzes werden gleichzeitig wesentliche Randbedingungen für die Überlastabwehr bestimmt. Dazu gehören vor allem die Netzvermaschung und die Netzhierarchie. Diese beiden Faktoren sind maßgebend für die Anzahl der direkten Wege, die Anzahl der alternativen Wege, die Anzahl der Übertragungsstrecken zwischen Ursprungs- und Zielknoten sowie die Netzrekonfigurationsmöglichkeiten bei Ausfällen von Betriebsmitteln. Die Netztopologie muss deshalb stets bei der Implementierung von Überlastabwehrmechanismen einbezogen werden.

Tarifgestaltung
Auch die Tarifgestaltung kann als Mittel zum Abbau von Betriebsmittelengpässen herangezogen werden. Falls Engpässe aufgrund von statistischen Auswertungen nach Art, Zeit und Ort festgestellt sind, lässt sich durch eine geeignete Gebührenpolitik eine zeitliche Verteilung des Verkehrsangebotes erreichen. Zum Beispiel durch Verlegung des Stapelbetriebes in die billigeren Nachtstunden.

Traffic-Shaping

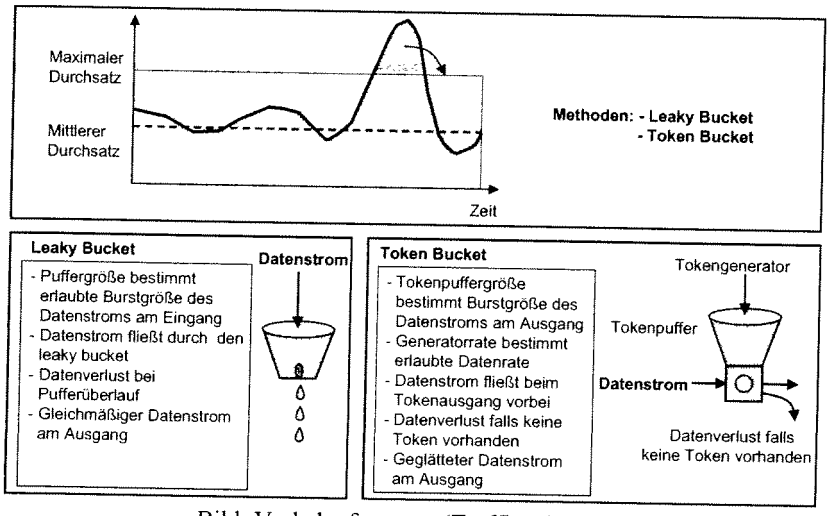


Bild: Verkehrsformung (Traffic-Shaping)

Eine der vorrangigen Ursachen für Überlastungen sind Verkehrsspitzen, d.h. der Datenverkehr fließt nicht die ganze Zeit über im gleichen Volumen. Viele Überlastungen würden nicht auftreten, wenn man Endsystemen so auslegen könnte, dass sie ständig in einer universellen Rate übertragen. Eine andere offene Schleifenmethode zwingt die Stationen, Pakete in einer besser vorhersagbaren Rate zu übertragen. Dieser Ansatz heißt Traffic-Shaping und wird vorwiegend in ATM-Netzen angewandt.

Beim Traffic-Shaping wird die durchschnittliche Rate der Datenübertragung reguliert. Im Gegensatz zu den Schiebefensterprotokollen, die an früherer Stelle beschrieben wurden, wird hier also nicht die Datenmenge, sondern die Übertragungsrate begrenzt. Wird eine virtuelle Verbindung eingerichtet, vereinbaren der Benutzer und das Teilnetz (d.h. der Kunde und der Netzbetreiber) ein bestimmtes Verkehrsmuster für diese Verbindung. Solange der Kunde seinen Teil der Vereinbarung erfüllt und Pakete nur nach Vereinbarung sendet, gewährleistet der Betreiber deren zeitgerechte Zustellung. Auf diese Weise werden im Traffic-Shaping Überlastungen eingedämmt. Solche Vereinbarungen sind bei Dateitransfers weniger wichtig, haben aber eine große Bedeutung für Echtzeitdaten, z.B. Audio- und Videoverbindungen, bei denen Überlastungen nicht vorkommen sollten.

Vor diesem Hintergrund stellt sich natürlich die Frage, wie der Netzbetreiber wissen kann, ob der Kunde die Vereinbarung einhält und was geschehen soll, wenn das nicht der Fall ist. Die Überwachung von Verkehr im Rahmen solcher Vereinbarungen nennt man allgemein Traffic-Policing Traffic-Shaping und -Policing sind bei Teilnetzen mit virtuellen Verbindungen einfacher als bei solchen mit Datengrammen. Allerdings kann auch bei Teilnetzen mit Datengrammen das gleiche Konzept auf Verbindungen der Transportschicht angewandt werden.

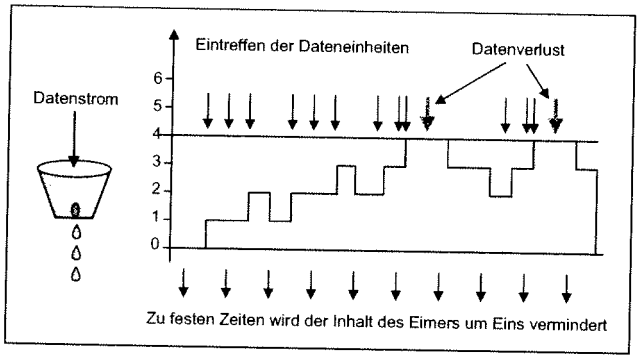
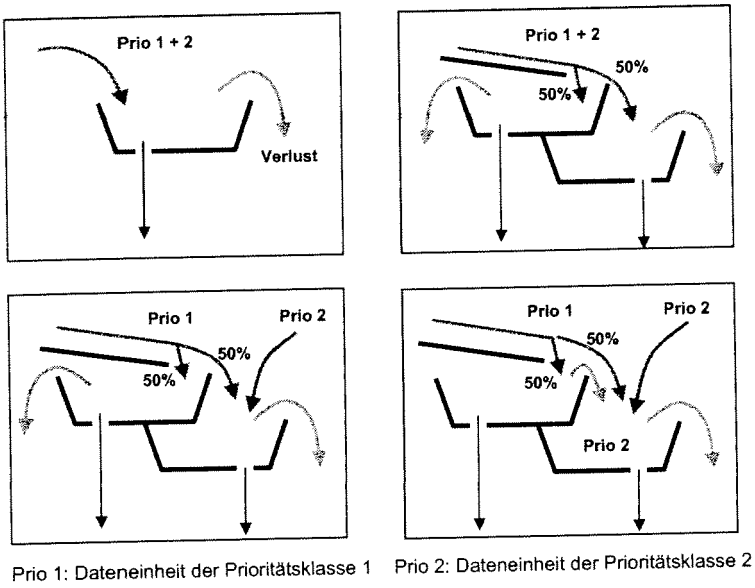


Bild: Leaky Bucket-Verfahren

Der Leaky-Bucket-Algorithmus
Wir stellen uns nun einen Eimer mit einem kleinen Loch im Boden vor. Gleichgültig, in welcher Geschwindigkeit Wasser in den Eimer eingefüllt wird, hat der Ausfluss immer die gleiche Rate, wenn Wasser vorhanden ist, und Null, wenn der Eimer leer ist. Ist der Eimer voll, läuft überschüssiges Wasser über den Eimerrand aus und geht verloren (d.h. es kommt nie am Ausgangsstrom unten im Loch an).

Das gleiche Konzept kann auf Pakete angewandt werden. Vom Konzept her ist jedes Datenendgerät an das Netz über eine Schnittstelle angeschlossen, die einen rinnenden Eimer enthält. Das ist eine endliche interne Warteschlange. Kommt ein Paket in der Warteschlange an, wenn der Eimer voll ist, wird es verworfen. Mit anderen Worten, versucht ein Prozess im Datenendgerät, ein Paket zu senden, während die maximale Anzahl bereits in der Warteschlange steht, wird das Paket verworfen. Diese Vorkehrung kann in die Hardware-Schnittstelle integriert oder vom Betriebssystem des Datenendgeräts simuliert werden. Die Methode heißt Leaky-Bucket-Algorithmus.

Das Datenendgerät kann pro Zeittakt ein Paket in das Netz einspeisen. Das kann, wie gesagt, durch die Schnittstellenkarte oder das Betriebssystem erzwungen werden. Dieser Mechanismus gibt einen ungeraden Paketfluss von den Benutzerprozessen im Endgerät in einen geraden Paketfluss in das Netz aus, so dass Verkehrsspitzen geglättet werden und das Risiko von Überlastungen stark reduziert wird.



Prio 1: Dateneinheit der Prioritätsklasse 1 Prio 2: Dateneinheit der Prioritätsklasse 2

Bild: Kombination von Leaky Buckets

Haben alle Pakete die gleiche Größe (z.B. ATM-Zellen), kann dieser Algorithmus wie eben beschrieben angewandt werden. Bei Paketen mit variabler Größe ist es meist besser, anstelle eines Pakets eine feste Anzahl von Bytes pro Zeittakt zuzulassen. Lautet die Regel beispielsweise 1024 Byte pro Zeittakt, kann ein einzelnes 1024-Byte Paket, zwei 512-Byte Pakete, vier 256-Byte Pakete usw. pro Zeittakt zugelassen werden. Ist die verbleibende Bytezahl zu niedrig, muss das nächste Paket auf den nächsten Zeittakt warten.

Die Implementierung des Leaky-Bucket-Algorithmus in seiner Ursprungsform ist einfach. Der rinnende Eimer stellt eine endliche Warteschlange dar. Kommt ein Paket an, wird es in die Warteschlange gestellt, sofern Platz vorhanden ist. Andernfalls wird es verworfen. Bei jedem Zeittakt wird ein Paket übertragen (es sei denn, die Warteschlange ist leer).

Der Leaky-Bucket-Algorithmus auf der Grundlage von Bytezahlen wird fast auf die gleiche Weise implementiert. Bei jedem Zeittakt wird ein Zähler auf n initialisiert. Umfasst das erste Paket in der Warteschlange weniger Bytes als der momentan im Zähler stehenden Wert, wird es übertragen und der Zähler wird um diese Anzahl von Bytes erhöht. Solange der Zähler noch nicht seinen Schwellenwert erreicht hat, können weitere Pakete übertragen werden. Ist der Restwert im Zähler niedriger als die Länge des nächsten in der Warteschlange anstehenden Pakets, wird die Übertragung bis zum nächsten Zeittakt unterbrochen, dann wird die restliche Bytezahl überschrieben.

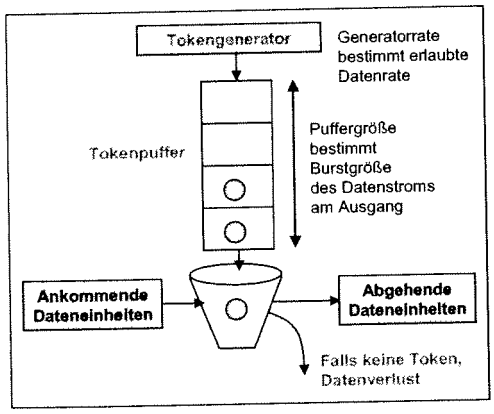


Bild: Token-Bucket mit Markenpool

Token-Bucket-Algorithmus

Der Leaky-Bucket-Algorithmus erzwingt ein straffes Ausgabemuster mit einer Durchschnittsrate, gleichgültig, welche Verkehrsspitzen auftreten. Bei vielen Anwendungen ist es besser, die Beschleunigung von Ausgaben bei bestimmten Verkehrsspitzen zuzulassen. Dafür wird ein flexiblerer Algorithmus benötigt, vorzugsweise einer, der keine Daten verliert. Ein solcher Algorithmus ist der Token-Bucket-Algorithmus. Bei diesem Algorithmus hält der rinnende Eimer Token, die von einer Uhr mit einer Geschwindigkeit von einem Token pro Zeiteinheit erzeugt werden. Der Token-Bucket-Algorithmus bietet eine andere Form der Verkehrsgestaltung als der Leaky- Bucket-Algorithmus. Letzterer lässt nicht zu, dass die Endsysteme träge bleiben, Pakete ansammeln und diese dann mit hohen Verkehrsspitzen alle auf einmal übertragen. Der Token-Bucket Algorithmus lässt dieses Ansammeln zu, aber nur bis zur maximalen Eimergröße von *n*. Dieses Merkmal bedeutet, dass Spitzen von bis zu *n* Paketen gleichzeitig übertragen werden können, so dass auch auf dem Ausgabestrom gewisse Spitzen vorkommen, was aber zu schnelleren Bestätigungen führt.

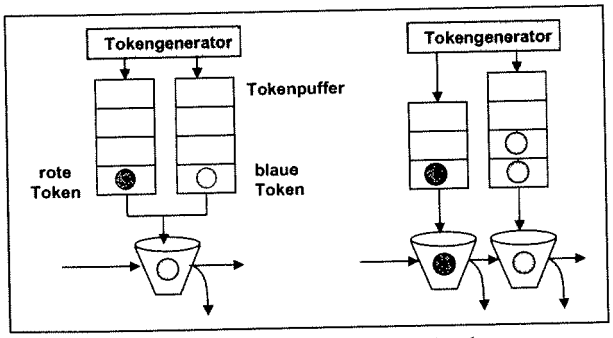


Bild: Kombination von Token-Buckets

Ein weiterer Unterschied zwischen den zwei Algorithmen ist der, dass der Token-Bucket-Algorithmus Token wegwirft, wenn der Eimer voll ist, aber nie Pakete. Demgegenüber werden beim Leaky-Bucket-Algorithmus Pakete weggeworfen, wenn der Eimer voll ist. Auch hier ist eine Variante möglich, bei der jedes Token dazu berechtigt ist, anstelle eines Pakets k Bytes zu übertragen. Ein Paket kann nur übertragen werden, wenn genügend Token verfügbar sind, um die Lange in Bytes abzudecken. Angebrochene Token werden zur späteren Verwendung aufgehoben.

Die Implementierung des Token-Bucket-Algorithmus in seiner Grundform besteht lediglich in einer Variablen für die Zählung der Token. Der Zähler wird einmal pro Zeiteinheit erhöht und nach der Versendung eines Pakets je um eins gesenkt. Fällt der Zähler auf Null, dürfen keine Pakete mehr übertragen werden. Bei der Variante mit Bytezählung wird der Zähler pro Zeiteinheit um k Byte erhöht und um die Länge jedes gegen deren Pakets gesenkt. Der Token-Bucket lässt Verkehrsspitzen zu, aber nur bis zu einer bestimmten Höchstlänge. Beim Token-Bucket-Algorithmus liegt potentiell das Problem vor, dass er wieder große Spitzen zulässt, obwohl das Spitzenintervall durch sorgfältige Auswahl von der Tokenrate und die Tokenpuffergröße reguliert werden kann. Häufig ist es wünschenswert, die Spitzenrate zu reduzieren, aber nicht zurück bis zum niedrigsten Wert des ursprünglichen Leaky-Bucket.

Fluss-Spezifikationen

Die Trafffic-Shaping-Methode ist am wirksamsten, wenn Sender, Empfänger und Teilnetz gemeinsam eine Vereinbarung treffen. Um eine Übereinkunft zu erreichen, muss das Verkehrsmuster ganz genau definiert werden. Eine solche Übereinkunft nennt man Flussspezifikation. Sie besteht aus einer Datenstruktur, die sowohl das Muster des eingespeisten Verkehrs als auch die von den Anwendungen gewünschte Dienstqualität beschreibt. Eine Flussspezifikation kann auf die über eine virtuelle Verbindung gesendeten Pakete oder auf eine Folge von Datengrammen von einer Quelle an ein oder mehrere Ziele zutreffen.

Merkmale der Eingabe

- Gewünschte Dienstqualität
- Sensitivitätsverlust (Byte)
- Intervallverlust
- Spitzenverlust (Pakete)
- Minimal feststellbare Verzögerung
- Maximale Paketgröße (Byte)
- Token-Bucket-Rate (Byte/s)
- Token-Bucket-Größe (Byte)
- Maximale Übertragungsrate (Byte/s)
- Maximale Verzögerungsabweichung
- Qualitätsgarantie

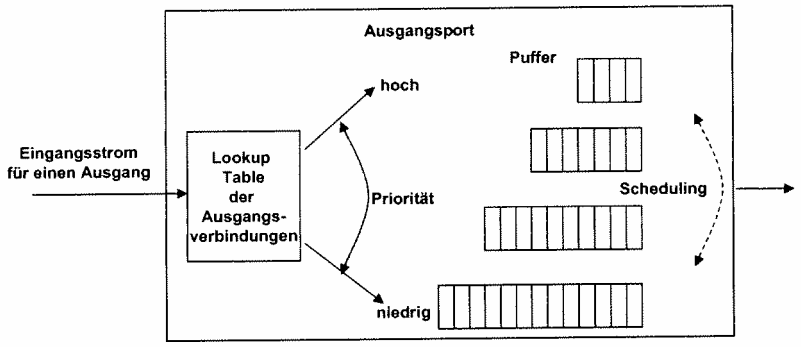


Bild: Warteschlangen mit Prioritäten

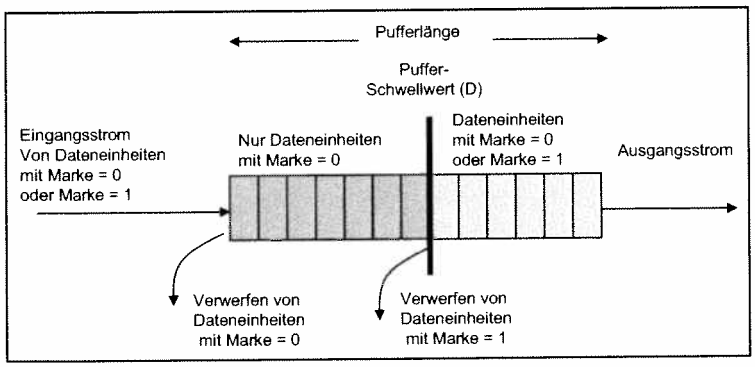


Bild: Selektives Verwerfen von Dateneinheiten

Fehlersicherung

Automatische Fehlerkorrektur-Verfahren
Erkennung und Behandlung von fehlerhaften Paketen stehen in engem Zusammenhang mit der Datenflusskontrolle. Auch hier sind die entsprechenden Aufgaben hierarchisch über die einzelnen Protokollebenen verteilt.

In einem Paketvermittlungsnetz erfordern die folgenden Situationen eine Fehlerbehandlung:
- Bitübertragungsfehler durch Störungen auf der Übertragungsleitung, Hardware-Defekte oder ähnliche Ursachen, fehlende Pakete durch Ausfall eines Netzknotens oder einer Leitung, Softwarefehler oder die bewusste Unterdrückung von Paketen in Überlastsituationen,
- Pakete mit Sequenzfolgefehlern durch Verlust eines Paketes oder bei individueller Übermittlung von Paketen über unterschiedliche Übertragungswege,
- Paketkopien durch Wiederholung eines Paketes bei Verlust oder verzögertem Eintreffen der Quittung (Time-Out).

Abschnittsweise Fehlersicherung
Zur Erkennung und Behebung von Übertragungsfehlern enthält jeder Datenblock einen Fehlersicherungsteil, dessen Kontrollbits sich aus den Informationsbits nach einem bestimmten Schema ableiten lassen. Diese Fehlersicherung findet abschnittsweise statt und wird von der Sicherungsebene (Ebene 2) ausgeführt. Die Fehlererkennung kann entweder eine Paritätsprüfung sein oder wird als zyklische Redundanzprüfung mit Hilfe von Generatorpolynomen durchgeführt.

Beim Empfänger werden die Kontrollbits nach demselben Schema wie beim Sender ermittelt, so dass sich mit einem Vergleich zwischen errechneten und empfangenen Kontrollbits fehlerhafte Blöcke erkennen lassen. Blöcke mit Übertragungsfehlern werden in Paketvermittlungsnetzen durch eine wiederholte Übertragung korrigiert (ARQ-Methode, Automatic Repeat Request). Bei dieser Methode wird beim Sender eine Kopie des übertragenen Blockes gespeichert. Der Empfänger prüft den empfangenen Block auf Fehlerfreiheit. Bei einem positiven Ergebnis nimmt der Empfänger den Block an und es wird eine positive Quittung zurückgesendet, so dass die gespeicherte Kopie gelöscht werden kann. Ein fehlerhafter Block wird vom Empfänger unterdrückt und dessen Wiederholung wird mit einer negativen Quittung veranlasst.

Als Antwort auf eine negative Quittung stehen zwei Wiederholungsmechanismen zur Auswahl:
- Bei **nichtselektiver Wiederholung** werden sowohl der fehlerhafte Block als auch alle nachfolgenden Blöcke wiederholt. Am Empfänger werden alle Blöcke bis zum Eintreffen des angeforderten Blockes unterdrückt. Dadurch wird stets die richtige Reihenfolge der Blöcke beim Empfänger gewährleistet.
- Bei **selektiver Wiederholung** wird nur der fehlerhafte Block wiederholt. In diesem Falle muss der Empfänger selbst die richtige Reihenfolge der empfangenen Blöcke wiederherstellen. Dazu ist neben dem erhöhten Aufwand an Intelligenz auch zusätzlicher Speicheraufwand erforderlich.

Zusätzlich wird der letzte Block in einer Folge von Blöcken zeitüberwacht. Dazu wird eine Zeitbegrenzung bei Beginn der Blockübertragung gesetzt und beim Eintreffen der entsprechenden Quittung zurückgesetzt. Bei Ablauf der Zeitüberwachung (Timeout) wird dieser letzte Block erneut gesendet oder es werden Maßnahmen getroffen, um den Grund für das Ausbleiben der letzten Quittung feststellen zu können. Die Anzahl der Wiederholungen ist begrenzt.

Ende-zu-Ende Fehlersicherung
Währenddem die Bitübertragungsfehler abschnittsweise erkannt und korrigiert werden, ist es die Aufgabe der Ende-zu-Ende Fehlersicherung, fehlende Pakete, doppelte Pakete sowie Sequenzfolgefehler zu erkennen und anschließend zu beheben. In Paketvermittlungsnetzen, in denen die Pakete einer virtuellen Verbindung über verschiedene Wege vermittelt werden dürfen, führt sie darüber hinaus die Paketreihung durch. Die Erkennung am Empfangsort erfolgt mit Hilfe der Sequenzfolgenummer, die am Sendeort durch die Überwachung der Paketquittierungszeit (Time-Out).

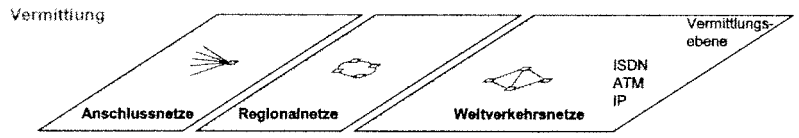
Beim Empfang eines doppelten Paketes wird dieses Paket lediglich unterdrückt, in allen anderen Fällen geschieht die Fehlerbehebung durch Paketwiederholung. Paketwiederholungen werden entweder anlässlich diesbezüglicher Anforderungen (selektiv oder nicht selektiv) oder infolge einer Quittierungszeitüberschreitung vorgenommen. Zu diesem Zweck muss für jedes Paket bis zur Quittierung eine Kopie am Sendeort abgespeichert werden.

2.3 OSI-Referenzmodell: Schicht 3 - Vermittlungssysteme

Version: Dez. 2003

Inhalt

- ISDN (Basis-/Multiplexanschluss, Verbindungsaufbau, Datenkommunikation über B-Kanal/D-Kanal)
- X.25 (Netzstruktur, logische Verbindung)
- ATM (Netzstruktur, logische Verbindung)
- Signalisierung (Analogleitung, D-Kanal, SS7)
- Netzintelligenz



Leitungsvermittlung

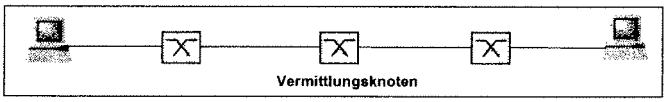
GSM	Global System for Mobile Communication
ISDN	Integrated Services Digital Networks

Paketvermittlung

GPRS	General Packet Radio Service
UMTS	Universal Mobile Telecommunication System
X.25	X.25 Packet Switching
FR	Frame Relay
ATM	Asynchronous Transfer Mode
IP	Internet Protocol

Bild: Netztechnologien: Vermittlung

Leitungsvermittlung (physikalische Verbindung)



- Vermittelte physikalische Verbindung zwischen den Endsystemen
- Isochrone Übermittlung (keine Verzögerungsschwankungen)
- Konstante Ende-zu-Ende Verzögerung
- Keine Daten von anderen Benutzern

Paketvermittlung (logische Verbindung)

- Vermittelte logische Verbindung zwischen den Endsystemen
- Synchrone Übermittlung (Echtzeitanwendung, minimale Verzögerungsschwankungen)
- Asynchrone Übermittlung (Datenanwendung, größere Verzögerungsschwankungen)
- Variable Ende-zu-Ende Verzögerung
- Physikalische Verbindung wird mit anderen Benutzern geteilt

Bild: Physikalische und logische Verbindung

In der Vermittlungstechnik wird zwischen Leitungs- und Paketvermittlung unterschieden. Bei der Leitungsvermittlung (Durchschaltevermittlung) ist eine physikalische Verbindung zwischen den Endsystemen vorhanden. Dies bedeutet, dass alle gesendete Bits nach einer konstanten Verzögerung beim anderen Benutzer ankommen. Die Übermittlung ist deshalb isochron. Man spricht von Übermittlung (Übertragung plus Vermittlung), weil es sich hier um eine Zusammenschaltung von vermittelten Übertragungsabschnitten handelt. Bei Paketvermittlung hat man eine logische Verbindung zwischen beiden Endsystemen. Dies bedeutet an beiden Enden der Verbindung existieren Sofware Module (Instanzen, entities), die eine logische Verknüpfung bezüglich der Adressierung und des momentanen Zustandes des Datenaustausches herstellen.

Viele logische Verbindungen teilen sich die Netzressourcen (physikalische Leitungen sowie Puffer und Rechenleistung in den Netzknoten) und somit kommt es zu Stausituationen, die Verzögerungsschwankungen hervorrufen. Bei Echtzeitverbindungen (Telefonie, Videokonferenz) werden die Ende-zu-Ende Verzögerungsschwankungen durch geeignete Maßnahmen minimalisiert und begrenzt. Dies kann beispielsweise erreicht werden durch Prioritäten, Ressourcenreservierung und einen Puffer zur Ausgleich der Verzögerungsschwankungen im empfangenden Endsystem. Durch trotzdem verbleibende Verzögerungsschwankungen spricht man hier nicht von einer isochronen Übermittlung, sondern von einer synchronen Übermittlung. Die Kommunikation bei allen anderen Anwendungen ist einem wesentlich größeren Verzögerungsschwankungsbereich unterworfen. Die Übermittlung wird als asynchron bezeichnet.

ISDN : Integrated Services Digital Network

ISDN integriert verschiedenartige Dienste wie Sprach-, Daten- und Bildkommunikation in einem Netz. Der Benutzer benötigt dafür nur einen Netzzugang (UNI: User Network Interface). Das heutige ISDN (Integrated Services Digital Network) ist aus Anwendersicht ein Schmalband-ISDN (S-ISDN) zur Integration verschiedener Kommunikationsdienste in einem einzigen Netz. Während in der Vergangenheit für die unterschiedlichen Dienste wie Datenübertragung, Telefonie usw. in der Regel getrennte Kommunikationsnetze erforderlich waren, unterstützt bereits das Schmalband-ISDN alle Kommunikationsarten. Nachdem sich das Schmalband-ISDN in vielen Länder schon flächendeckend etabliert hat, ist nun auch das Breitband-ISDN (B-ISDN), d.h. ATM (Asynchronous Transfer Mode, Asynchroner Transfer Modus) als ein universelles, alle Dienste integrierendes Breitband-Netz eingeführt worden. Das B-ISDN löst die bestehende Telekommunikations- und Datenverarbeitungs-Infrastruktur in naher Zukunft nicht ab, sondern sie eine sinnvolle Ergänzung. Heute wird unter der Bezeichnung NGN (Next Generation Network) auch das Internet bzw. die IP-Netze zur Integration von Services umgestaltet.

Netzaufbau
ISDN kann unterschiedliche Netze als Basis nutzen. Dabei werden Nutzdaten und Signalisierungsdaten getrennt übertragen (Außer-Band-Signalisierung, Out-of-Band Signalling). Nutzdaten können übertragen werden durch:

- leitungsvermittelte Übertragung im B-Kanal,
- paketvermittelte Übertragung im B-Kanal,
- paketvermittelte Übertragung im D-Kanal.

Dem Anwender stellt ISDN B-Kanäle (Bearer Channel) für Nutzdaten und D-Kanäle (Data Channel) für die Signalisierung zur Verfügung. Je nach Anschlusstyp **Basisanschluss** oder **Primär-Anschluss** sind unterschiedliche Datenraten verfügbar.

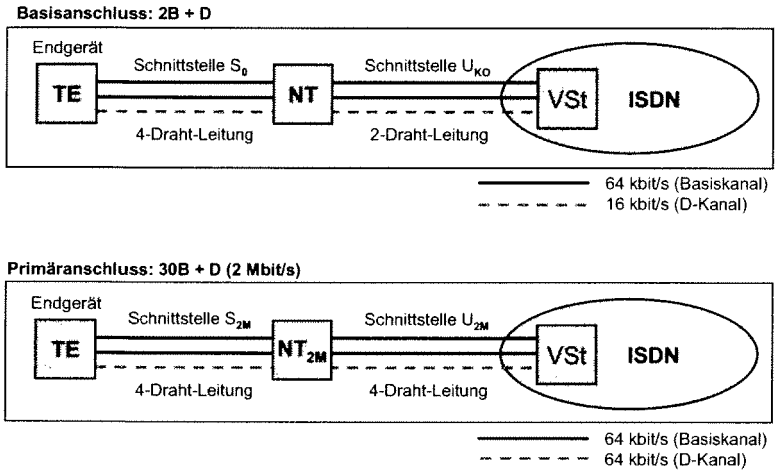
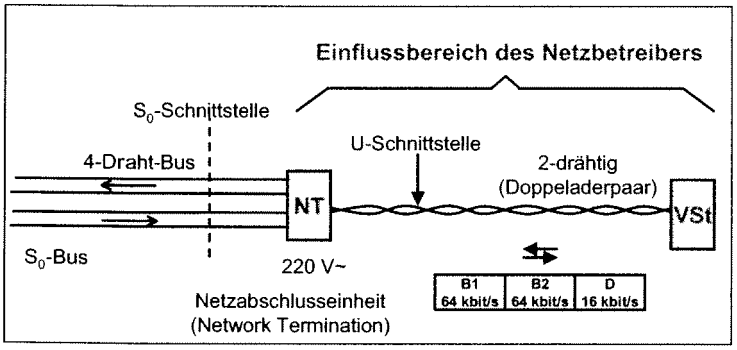


Bild: ISDN Basis- und Primäranschluss

Basisanschluss
(Basic Access)
2 x B + D = 2 x 64 kbit/s + 16 kbit/s
= 144 kbit/s (mit Overhead: 192 kbit/s)

Primärmultiplexanschluss (Primary Rate Access)
30 x B + D = 30 x 64 kbit/s + 64 kbit/s
= 1984 kbit/s (mit Overhead: 2048 kbit/s)

Primärmultiplexanschluss (Primary Rate Access) USA, Japan
23 x B + D = 23 x 64 kbit/s + 64 kbit/s
= 1536 kbit/s (mit Overhead: 1544 kbit/s)



VST: Vermittlungsstelle

Bild: ISDN Basisanschluss

ISDN-Basisanschluss
Der Basisanschluss stellt zwei Nutzkanäle mit je 64 kbit/s in beide Richtungen zur Verfügung. Für eine Verbindung an einem ISDN-Basisanschluss ist je Übertragungsrichtung ein B-Kanal notwendig, da aber an einem Basisanschluss in jeder Übertragungsrichtung zwei B-Kanäle bereitgestellt werden, können je Basisanschluss zwei gleichzeitige und unabhängige Kommunikationen unterhalten werden. Der Teilnehmeranschluss ist meist als Bus ausgeführt, an dem mehrere Einrichtungen angeschaltet werden können.

Der Anschluss erfolgt über die international genormte S_0-Schnittstelle. Die Nutzkanäle sind nicht bestimmten Endeinrichtungen oder Diensten zugeordnet, sondern werden erst nach Bedarf einer bestimmten Endeinrichtung zugeteilt. Die Signalisierungsinformationen werden in einem getrennten 16 bit/s-Kanal, dem D-Kanal, übertragen. Der Zugriff auf den D-Kanal er-

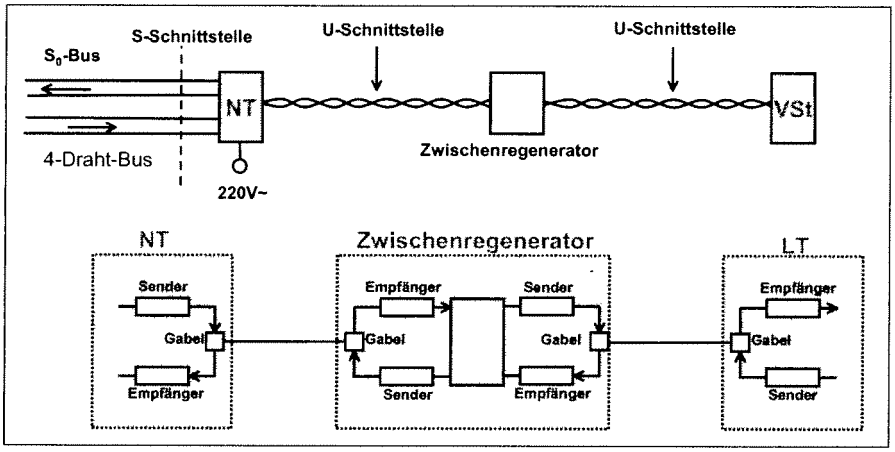
folgt von allen Endeinrichtungen aus in Konkurrenz zueinander, gleichzeitige Übertragungs-Anforderungen werden nacheinander behandelt.

S_0-Bus

Die S_0-Schnittstelle befindet sich im Bereich der Installation beim Teilnehmer zwischen NT (Network Termination) und TE (Terminal Equipment). Die S_0-Schnittstelle ist eine vierdrähtige Schnittstelle, die sowohl als Bus, mit maximal 8 angeschlossenen TE, als auch als Punkt-zu-Punkt-Verbindung eingesetzt werden kann. Das Vierdraht-Verfahren ermöglicht die Verwendung eines einfachen Übertragungsverfahrens.

Primäranschluss und Schnittstelle S_{2M}

Wenn eine Datenverarbeitungsanlage oder ein LAN am ISDN angeschlossen werden soll, ist der ISDN-Basisanschluss mit zwei Kanälen nicht ausreichend, um den Kommunikationsanforderungen nachzukommen. Dasselbe gilt für die Betreiber von Telekommunikationsanlagen, die als private ISDN-Knoten zu sehen sind. Eine große Daten- oder Telekommunikationsanlage kann entweder über mehrere Basisanschlüsse oder über einen ISDN-Primärratenanschluss, Zugang zum ISDN haben. Die teilnehmerseitige Schnittstelle wird dabei als S_{2M}-Schnittstelle bezeichnet. Bei einem Primärratenanschluss gibt es ausschließlich Punkt-zu-Punkt-Verbindungen. Die Schnittstelle besteht aus 30 B-Kanälen mit je 64 kbit/s als Nutzkanälen und einem D-Kanal mit ebenfalls 64 kbit/s als Signalisierungskanal. Die Schnittstelle S_{2M} wird mit PCM-30-basierenden Multiplexsystemen mit einer Bitrate von ca. 2 Mbit/s realisiert.



NT: Network Termination LT: Line Termination VST: Vermittlungsstelle

Bild: ISDN Basisanschluss

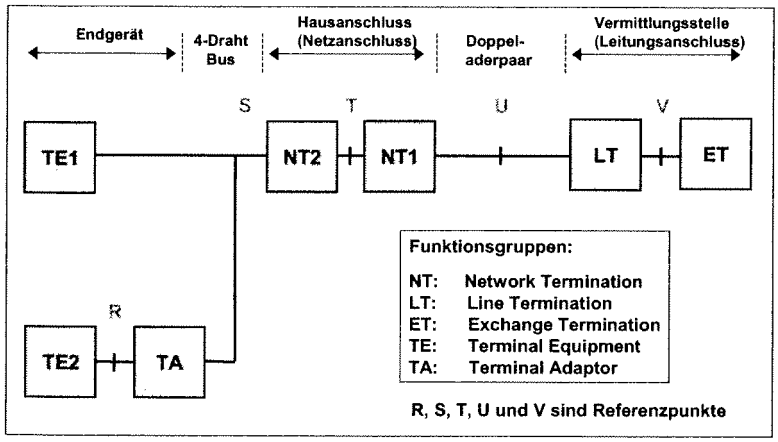
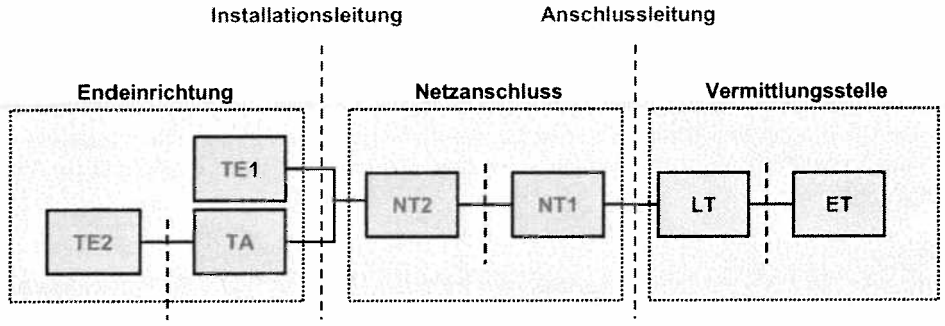


Bild: ISDN Basisanschluss: Referenzkonfiguration

Der ISDN-Anschluss wurde von ITU-T in Funktionsgruppen aufgeteilt, um verschiedene notwendige Funktionen voneinander abzugrenzen.
Die Referenzpunkte werden mit R bis V bezeichnet, sie müssen aber nicht mit den physikalischen Schnittstellen zusammenfallen. Um Referenzpunkte am Basisanschluss zu kennzeichnen, werden sie mit einem Index 0 versehen.



TE Endgerät	TA Endgeräteanpassung	NT2 Netzanschluss 2	NT1 Netzabschluss 1 LT Leitungsabschluss	ET Vermittlungsabschluss
Endgerätefunktion	Schnittstellen-anpassung	B-Kanal-Zuweisung	Leitungs-übertragung	B-Kanal-Zuweisung
Benutzerschnittstelle	Bitratenanpassung	Endgeräte-verwaltung	2/4 Draht.-Wandlung	Funktionsprüfung
Signalisierung	Signalisierung	Signalisierung	Funktionsprüfung	Signalisierung

Bild: ISDN Basisanschluss: Referenzkonfiguration

Funktionseinheiten

ET	Exchange Termination	Ein Vermittlungsknoten (Exchange Termination) bearbeitet alle schnittstellenbezognen Aufgaben der Schichten 1, 2 und 3.
LT	Line Transmission Termination	Der LT ist eine Leitungsübertragungseinrichtung zwischen der Teilnehmeranschlussleitung und dem ET-Übergabeverfahren. Die Funktion besteht damit aus einer Umsetzung der Übertragungsverfahren zwischen einem relativ niedrigratigen Teilnehmeranschluss und einem hochratigen Multiplexanschluss auf der Vermittlungsseite.
TE1	Terminal Equipment 1	Der Endgerätetyp 1 ist ein ISDN-Endgerät, z.B. ISDN-Telefon, ISDN-Multifunktions-Endgerät, ISDN-Faxgerät und ISDN-Interface-karten für PCs.
TE2	Terminal Equipment 2	Der Endgerätetyp 2 ist ein Endgerät, das die ISDN-Interface Empfehlungen nicht erfüllt. Damit sind alle Endgeräte gemeint, die z.B. Schnittstellen nach den V- und X-Empfehlungen besitzen.
TA	Terminal Adapter	Ein Terminal Adapter passt ein TE 2 an die NT 2 Gegebenheiten an. Damit können die analogen oder digitalen nicht-ISDN-Endgeräte auch am ISDN betrieben werden
NT1	Network Termination 1	Der Netzabschluss 1 bedient die Teilnehmeranschlussleitung zum LT und generiert ein leitungsneutrales Übergabeverfahren für den NT 2.
NT2	Network Termination 2	Der Netzabschluss 2 bedient den Endgerätezugang und das leitungsneutrale Übergabeverfahren zum NT 1. Der Endgerätezugang kann ein Einzelterminal oder eine Telefonanlage sein. Typische Vertreter für einen NT 2 sind ein LAN oder eine Telefonanlage.

Aufgaben der Funktionseinheiten

	Schichten	Aufgaben
ET		- Multiplex-, Demultiplexfunktionen - Verbindungsüberwachungsfunktionen - Fehlerüberwachung und Alarmierung - Kontroll- und Testfunktionen - LAP-D Protokolle (Schicht 2) - Signalisierungsfunktionen (Schicht 3)
LT		- Umsetzen der Übertragungsverfahren zwischen Teilnehmer- und Vermittlungsseite - Ableiten und regenerieren von Takten - Fehlerüberwachung und Alarmerzeugung - Fernstromversorgung des Teilnehmerbereichs
NT1	1	- Umsetzen von Übertragungsverfahren - Überwachungsfunktionen der Leitung, - Überwachung/Schalten von Testschleifen - Ableiten und regenerieren von Takten
NT2	1, 2 und 3	- Umsetzen von Übertragungsverfahren - Protokollbearbeitung Schicht 2 und 3 - Vermittlungsfunktionen Schicht 3 - Multiplexfunktionen - Wartungsfunktionen

ISDN-Schichtenmodell

Bei der Betrachtung des ISDN-Schichtenmodells sind Endgerät, Ortvermittlungsstelle und Fernvermittlungsstelle zu unterscheiden.

- Für die Nutzdaten wird auf der Schicht 1 eine transparente logische Verbindung aufgebaut. Die Empfehlungen 1.430 (für S_0-Schnittstelle) und 1.431 (für S_{2M}-Schnittstelle) gelten für B- und D-Kanäle im Endgerät und in der Ortvermittlung.
- Für die Signalisierung existieren für den Netzanschluss drei Schichten. Schicht 2 verwendet LAPD (Link Access Procedure für D Channel, Empfehlungen Q.920 und Q.921). Auf Schicht 3 wird DSS1 (Digital Signalling System No. 1 eingesetzt. DSS 1 wird europaweit genutzt und deshalb kurz als **Euro-ISDN** bezeichnet.

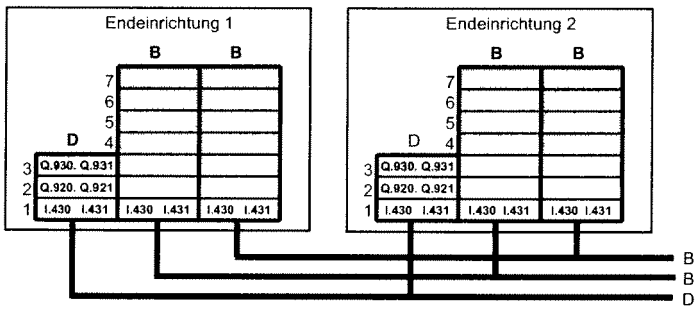
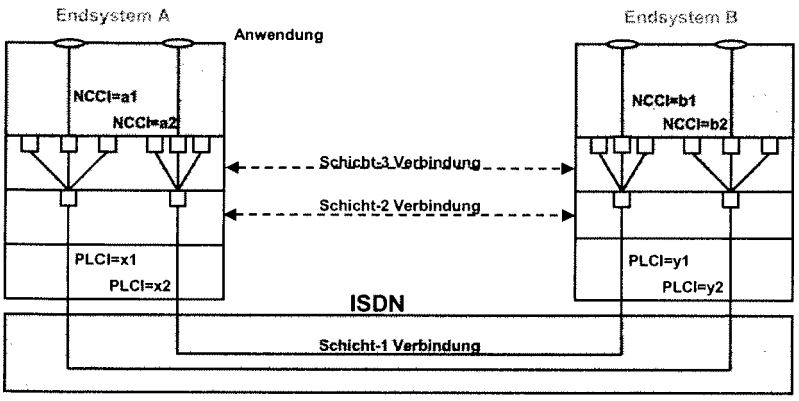


Bild: ISDN Schichtenmodell

Für die Kommunikation zwischen den Schichten werden Dienstelemente (Primitiven) festgelegt. Jeder Schicht ist im Referenzmodell ein Dienst zugeordnet, den diese Schicht für die nächsthöhere Schicht durch die Instanzen erbringt. Eine Instanz ist eine Abstraktion von Prozessen und Software-Programmen. Eine Schicht-3-Instanz ist in der Regel ein Software-Modul, das in einem Prozessor abläuft. Schicht-2-Instanzen werden teils in Hardware, und teils in Software realisiert, Schicht-1-Instanzen werden überwiegend in Hardware realisiert.



NCCI: Network Control Connection Identifier
PLCI: Physical Link Connection Identifier

Bild: ISDN Schichtverbindungen

Schicht-Verbindungen

Eine physikalische B-Kanalverbindung in ISDN ist eine Schicht-1-Verbindung. Mehrere virtuelle Verbindungen können darüber realisiert werden. Eine physikalische B-Kanalverbindung ist eine ungesicherte Bitübertragung, erst durch den Einsatz einer höheren Schicht-2-Verbindung kann die Bitübertragung gesichert werden. Die Qualität der Übertragung wird mittels des D-Kanal-Protokolls der Schicht 2 kontrolliert. Eine virtuelle Schicht-3-Verbindung basiert üblicherweise auf einer Schicht-2-Verbindung. Die Schicht 2 kann in Sonderfällen leer sein (ungesicherte Datenübertragung), dann setzt die Schicht-3-Verbindung direkt auf einer physikalischen Schicht-1-Verbindung auf.

Schicht-3-Verbindungen werden lokal durch den NCCI (Network Control Connection Identifier) identifiziert. Schicht-1-Verbindungen werden lokal mit einem PLCI (Physical Link Connection Identifier) gekennzeichnet. Auf diese Art wird eine physikalische ISDN-Verbindung durch zwei PLCIs eindeutig markiert: der lokale PLCI auf der Seite des Endsystems A und der lokale PLCI auf der Seite des Endsystems B. Eine Schicht-3-Verbindung wird durch zwei NCCIs eindeutig festgelegt.

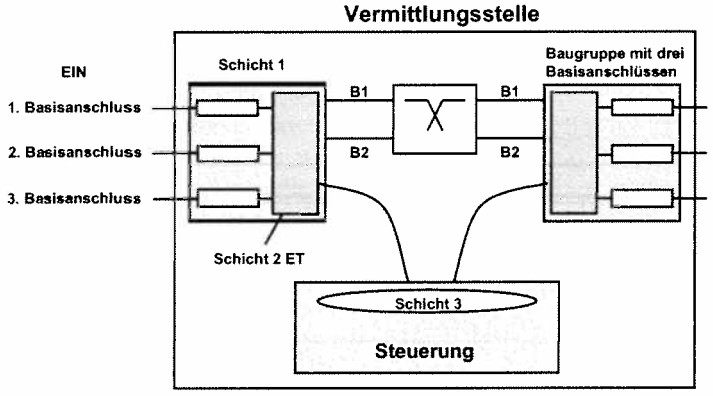


Bild: Implementierung des D-Kanal-Protokolls

Aufgaben der unteren drei Schichten:

Schicht 1: Die Bitübertragungsschicht (physical layer) stellt die synchronisierte Übertragung der binären Signale in den Kanälen zwischen Endeinrichtung und Netz gleichzeitig in beiden Richtungen sicher.

Schicht 2: Die Sicherungsschicht (data link layer) sichert den Nachrichtenaustausch der Schicht 3 zwischen den Endstellen und der Teilnehmervermittlungsstelle, zusätzlich ist hier der Transport von paketvermittelten Daten vorgesehen.

Schicht 3: Die Vermittlungsschicht (network layer) beschreibt die eigentliche Signalisierung zwischen Endeinrichtungen und Teilnehmervermittlungsstelle

Beispiele für die D-Kanal Signalisierung auf Schicht 3:

- SETUP: Teilnehmer hat abgehoben
- INFO: Wahlinformationen
- SETUP: Teilnehmerruf
- DISC: Teilnehmer hat aufgelegt

Vermittlungsarten

Es gibt drei Vermittlungsarten, die entsprechend den Übermittlungsdiensten unterschieden werden:

- leitungsvermittelte Verbindungen (B-Kanal)
- paketvermittelte Verbindungen (B-Kanal)
- paketvermittelte Verbindungen (D-Kanal)

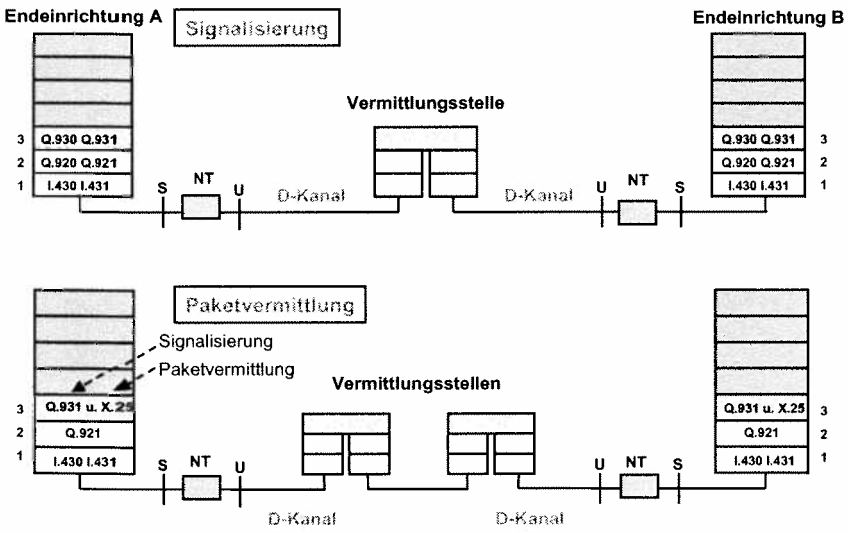


Bild: ISDN Verwendung des D-Kanals

Signalisierung im D-Kanal

Alle Signalisierungsinformationen der Schicht 3 zum Verbindungsaufbau und Verbindungsabbau erfolgt durch das D-Kanal Protokoll.

Paketvermittlung im D-Kanal

Bei dieser Übermittlungsart werden zum Beispiel X.25-Schicht-3 Pakete im D-Kanal transportiert. Die Übermittlung dieser Pakete ist ein Dienst der Schicht 2 des D-Kanals, der zusätzlich zur eigentlichen Aufgabe, der Übermittlung der Signalisierungsinformationen der Schicht 3, erbracht wird.

Leitungsvermittelte Verbindungen

Alle Telefonverbindungen und die gemieteten Datenverbindungen verwenden leitungsvermittelte Verbindungen. Dabei werden die Nutzkanäle transparent Ende-zu-Ende vermittelt. Aufgrund der Signalisierung im D-Kanal werden dazu die Kop-

peleinrichtungen in den Vermittlungsstellen durchgeschaltet. Für den B-Kanal werden vom ISDN nur Schicht-1-Funktionen bereitgestellt, wobei die Nutzinformationsübermittlung und die Signalisierung über unterschiedliche Kanäle erfolgt. Die Schichten 1 und 2 werden für den D-Kanal separat für jeden Leitungsabschnitt durch die Vermittlungsstelle bearbeitet.

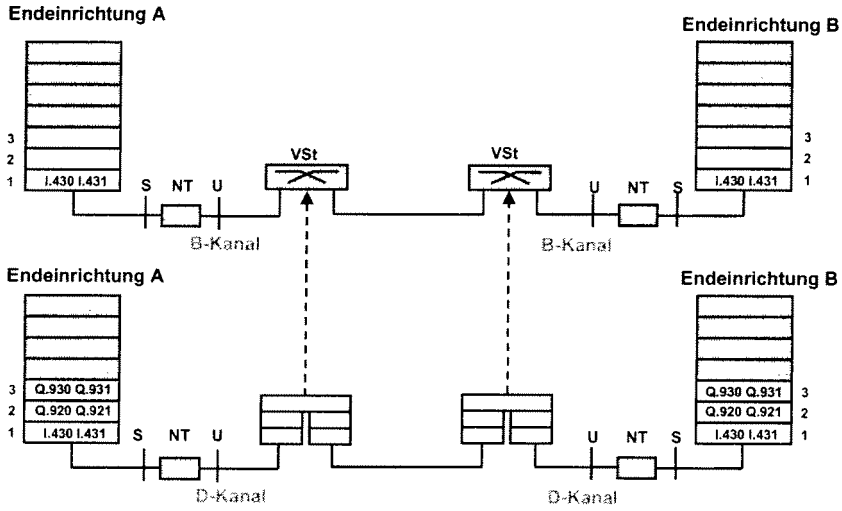


Bild: ISDN Leitungsvermittelte Verbindung

Die Schicht 1 ist für die Bitübertragung zwischen den Endeinrichtungen und der Vermittlungsstelle eines Basisanschlusses zuständig. Die Schicht 2 sichert die Übertragung der Signalisierung für einen Vermittlungsabschnitt zwischen einem Endgerät und der Vermittlungsstelle. Bei den leitungsvermittelten Verbindungen über den B-Kanal erfolgt die Benutzer-Netz-Signalisierung für alle leitungsvermittelten Verbindungen eines Anschlusses über den D-Kanal. Beim D-Kanal interpretiert das Netz die Schichten 1 bis 3, beim B-Kanal nur die Schicht 1.

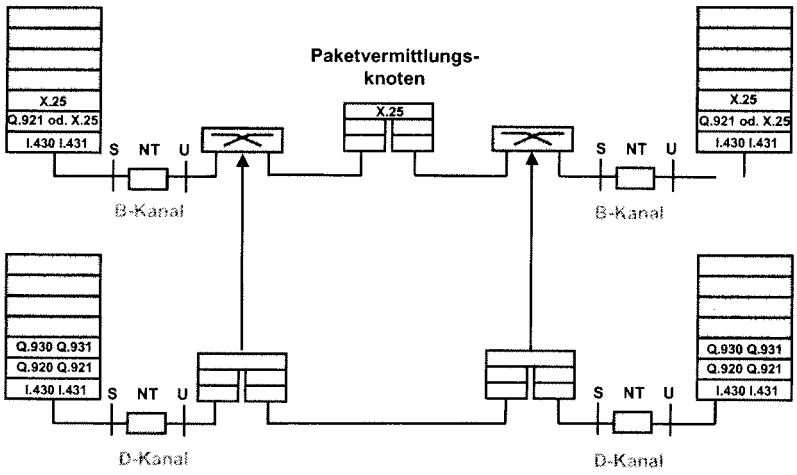


Bild: ISDN im B-Kanal paketvermittelte Verbindung

Paketvermittelte Verbindung im B-Kanal

Wir betrachten den leitungsvermittelte Zugang zu einem Paketvermittlungsnetz. Endgeräte nach X.25, die im Nutzkanal eine Verbindung zu anderen X.25 Endgeräten im ISDN aufbauen möchten, benötigen eine Schicht-3-Instanz, da bei X.25 die Nutzinformationen mit den Signalisierungsinformationen als Pakete zusammenhängen. Die leitungsvermittelten Abschnitte bedienen sich dabei der D-Kanal Signalisierung, während die paketvermittelten Abschnitte die X.25-Signalisierung und Nutzdatenübermittlung im gleichen Kanal verwenden. Die Nutzdaten werden bei dieser Übermittlung durch die X.25-Schicht 2 gesichert übertragen.

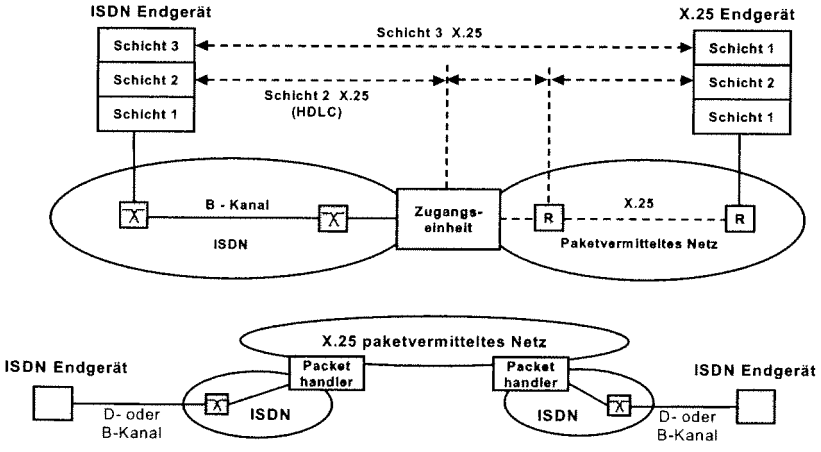
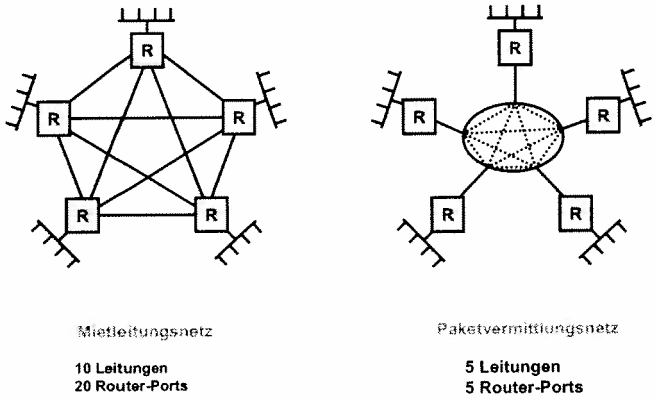


Bild: ISDN Paketvermittlung im B-Kanal

Die Datenkommunikation zwischen einem ISDN- und einem X.25 Endgerät erfolgt über eine Zugangseinheit (Packet Handler) zum X.25 Paketvermittlungsnetz. Der ISDN-Teil ist eine eine Einwahlverbindung, die eine vermittelte physikalische Verbindung für die transparente Übermittlung von Paketen bereitstellt.

Die Datenkommunikation zwischen zwei ISDN-Endgeräten über ein X.25 Paketvermittlungsnetz benötigt zwei Packet Handler. Die Paketvermittlung im ISDN-Abschnitt kann über den B- oder D-Kanal stattfinden.

X.25 Paketvermittlung



Die Bilder zeigen einen Vergleich bezüglich der Anzahl der Leitungen und Ports für ein Mietleitungsnetz und ein Paketvermittlungsnetz.

Bild: Mietleitungen oder Paketvermittlung

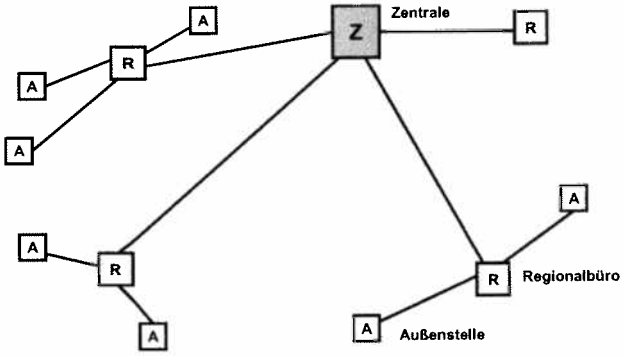


Bild: Firmennetz mit Mietleitungen

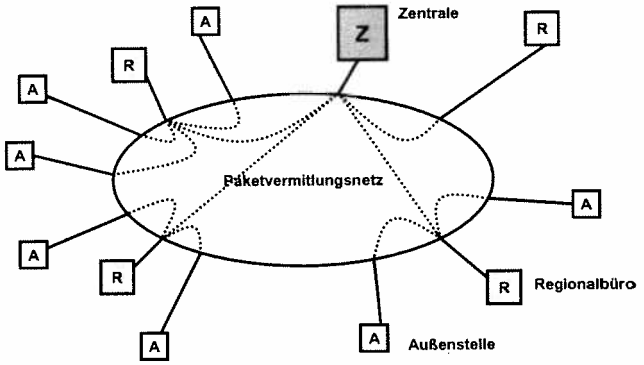


Bild: Firmennetz – Paketvermittlungsnetz

Paketvermittelnde Datennetze (X.25)

Mit X.25 wird kurz ein öffentliches, paketvermittelndes Netz bezeichnet. Es beschreibt die Schnittstelle zwischen einem Endgerät und dem Netz. Datenraten von 300 bit/s bis 64 kbit/s sind standardisiert, und seit 1992 auch bis 2 Mbit/s. Es ist für heutige Vorstellungen ein langsames Netz. X.25 wurde für die Verwendung von schlechten analogen Übertragungsstrecken mit einer hohen Bitfehlerrate ausgelegt. Kassensysteme und Bankautomaten basieren vorwiegend auf X.25. Diese Schnittstelle erlaubt eine flächendeckende Datenkommunikation und ist weltweit verfügbar. In Anbetracht besserer Übertragungsleitungen wird es jedoch zunehmend durch Frame Relay konkurrenziert.

Netzaufbau

Die Endgeräte-Seite werden als DTE (Data Terminal Equipment) bezeichnet. Die Vermittlungsknoten-Seite heißt im ITU-T-Standard DCE (Data Circuit Equipment). Netze unterschiedlicher Netzbetreiber werden über eine X.75-Schnittstelle gekoppelt. Die im Innern eines Netzes verwendeten Schnittstellen können davon verschieden sein. Diese Schnittstelle hat weniger Primitiven, ist sonst wie X.25.

Der X.25-Protokollstapel

X.25-Netze stellen permanente (PVC: Permanent Virtual Circuit) oder vermittelte (SVC: Switched VC) virtuelle Verbindungen mit den Phasen Verbindungsaufbau, Datenübertragung und Verbindungsabbau zur Verfügung.

- Schicht 1 nutzt X.21 und X.21bis.
- Schicht 2 verwendet **LAPB,** das von HDLC abgeleitet ist.
- Schicht 3 führt das X.25 Protokoll aus; es wird auch als PLP (Packet Layer Protocol) bezeichnet.

Die Felder des PLP-Pakets bedeuten:

- **GFI (General Format Identifier):** zur Identifikation des Pakets als Daten- oder Kontrollpaket, zur Flusskontrolle und zur Empfangsbestätigung.
- **LCI (Logical Channel Identifier):** zur Identifikation des logischen Kanals auf der DTE/DCE-Schnittstelle. Die Netzschicht stellt der übergeordneten Transportschicht maximal 4096 logische Kanäle zur Verfügung, die die Mehrfachausnutzung der physikalischen Anschlussleitung erlaubt. Die LCI-Werte haben nur lokale Bedeutung. Jede virtuelle Verbindung besteht aus einer Folge, von Teilstrecken mit jeweils eigenem LCI-Wert. Diese werden vom Netz während des Verbindungsaufbaus für jede Teilstrecke getrennt bestimmt. Das Routing der übertragenen Pakete wird dann auf Basis der LCI-Werte durchgeführt.
- **PTI (Packet Type Identification):** zur Identifikation des Pakettyps. Neben Datenpaketen gibt es 16 verschiedene Typen für Kontrollpakete.
- **Nutzdaten:** enthält die Daten der höheren Protokollschichten. Bei Datenpaketen sind dies Nutzdaten, bei Kontrollpaketen sind es Informationen zur Kontrolle der Verbindung (z. B. X.121-Adressen).

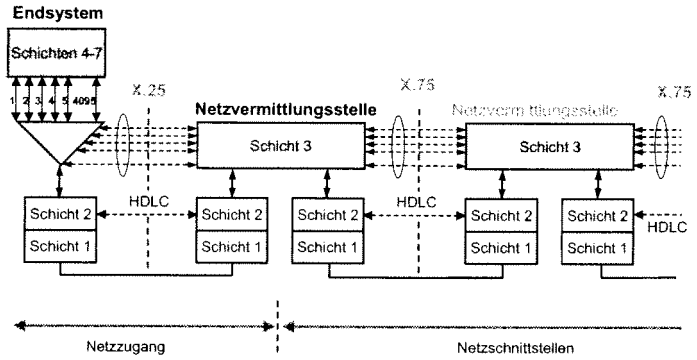


Bild: X.25 und X.75 Schnittstellen

Unter dem Schlagwort X.25 sind die Konzepte für die Datenübermittlung in Form von Paketen und für den Aufbau von Netzen mit der Paketvermittlung zu verstehen.
Hauptsächlich existieren zwei X.25-Varianten:

- X.25 DTE-DCE
- X.25 DTE-DTE

X.25 DTE-DCE regelt den Datenverkehr zwischen einer Datenendeinrichtung DTE (Data Terminal Equipment) und einer DCE (Data Communication Equipment) eines Netzknotens.

Diese Variante von X.25 wird in Paketvermittlungsnetzen eingesetzt, so daß diese Netze im weiteren auch kurz X.25-Netze genannt werden. X.25 DTE-DTE regelt den Datenverkehr zwischen den zwei Datenendeinrichtungen, die entweder direkt über eine feste physikalische Leitung oder über ein Netz mit Leitungsvermittlung (d.h. über eine geschaltete physikalische Leitung) verbunden sind. Diese Variante von X.25 beschreibt die Datenübermittlung in Form von Paketen über eine physikalische Punkt-zu-Punkt-Verbindung, d.h. DTE-DTE-Verbindung. Sie wird für die Übermittlung von paketierten Daten über das ISDN angewandt

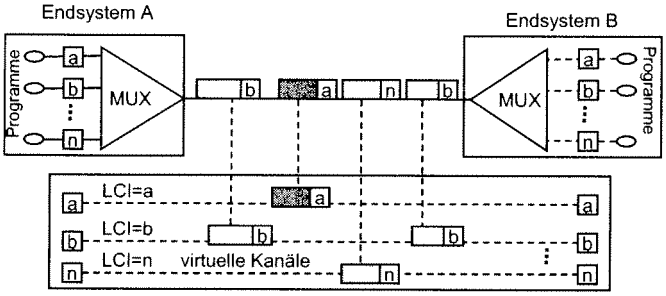


Bild: X.25 logische Verbindungen

Hier wird das Prinzip der parallelen Kommunikation nach X.25 über eine physikalische Leitung illustriert. Wie hier ersichtlich ist, wird eine Verbindung von zwei Multiplexern in den beiden kommunizierenden Rechnern logisch nachgebildet. Zwischen diesen Rechnern wird eine Reihe von Paketen über eine Leitung übertragen. Jedes Paket enthält Angaben hinsichtlich der Ports im Multiplexer. Als ein Port ist hierbei ein Sende-/Empfangs-Puffer im Speicher zu interpretieren.

Derartige Angaben werden als logischer (virtueller) Kanal bezeichnet. Damit lässt sich eine serielle Übertragung einer Reihe von Paketen als eine parallele Übertragung über mehrere logische Kanäle mit den Nummern a, b, ..., n auslegen.
Für die Zuordnung eines Pakets zu einer virtuellen Verbindung erhält jedes Daten-Paket eine logische Kanalnummer LCI (Logical Channel Identifier), die auch als Port-Nummer im Multiplexer bezeichnet werden kann. Die Überwachung des Paketflüsse wird für jeden logischen Kanal separat durchgeführt.

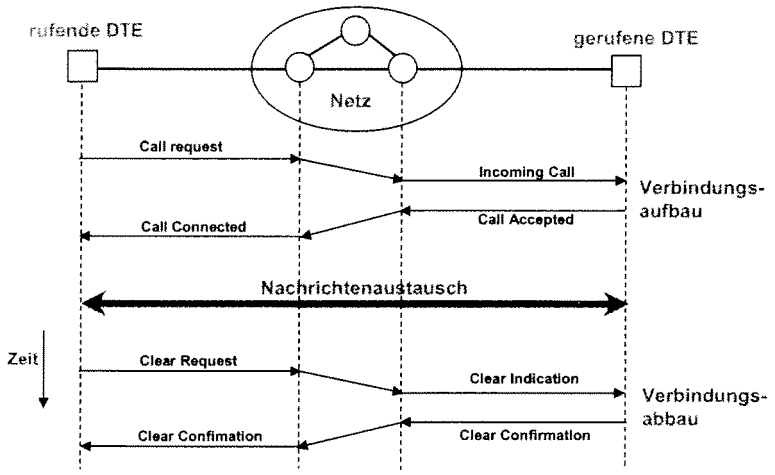


Bild: Verbindungsaufbau bei X.25 Paketvermittlung

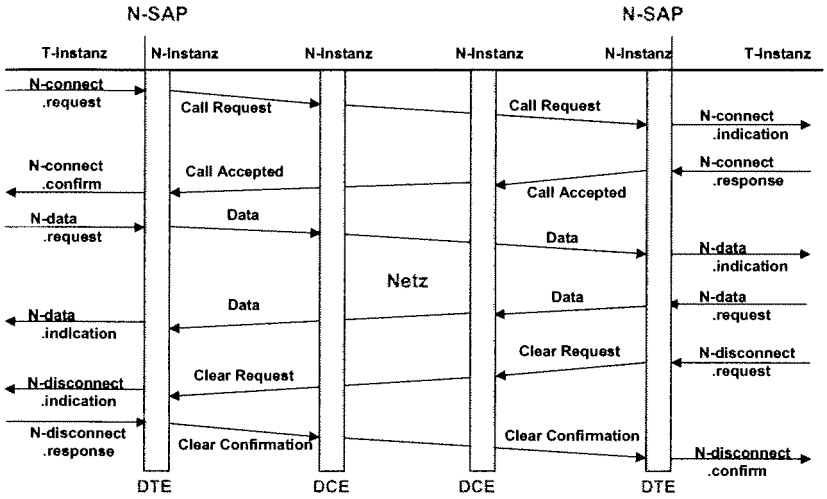
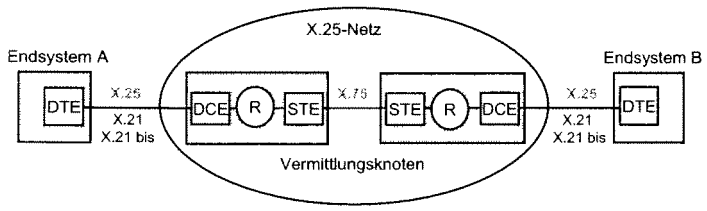


Bild: Paketvermittlung nach X.25



DTE : Data Terminal Equipment
DCE : Data Communication Equipment
STE : Signalling Terminal Exchange
R: Routing

Bild: Schnittstellen X.25 und X.75

X.25 DTE-DCE stellt alle Definitionen für einen Anschluss eines paketfähigen Endsystems an ein X.25-Netz zur Verfügung.

Zwischen den Knoten im X.25-Netz erfolgt die Kontrolle nach dem X.75-Protokoll, das eine Modifikation des X.25-Protokolls ist.

Ein Kommunikationsmodul für den Verbund von X.25-Netzknoten wird als STE (Signalling Terminal Exchange) bezeichnet.

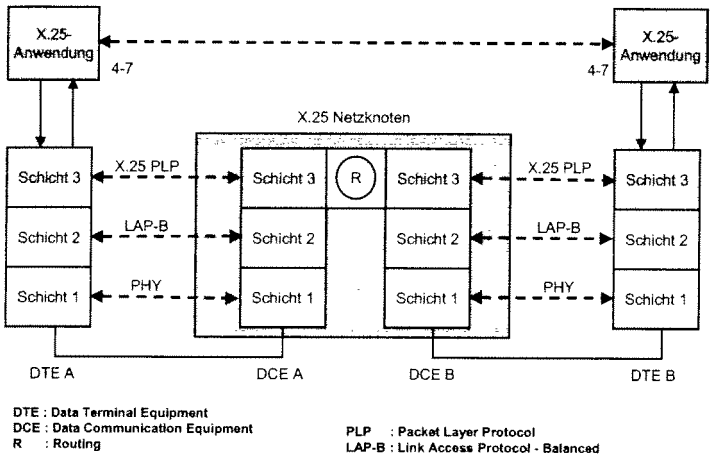


Bild: X.25 Protokoll-Schichten

Die Funktionen der einzelnen Schichten in DTE und DCE sind:

Schicht 1 (Bitübertragungsschicht): beschreibt die physikalische Schnittstelle. Es sind hier folgende Schnittstellen möglich: X.21-, X.21bis- und auch V-Schnittstellen. Welche Schnittstelle in konkretem Fall eingesetzt wird, ist von den Fähigkeiten der TE abhängig.

Schicht 2 (Sicherungsschicht): beschreibt das Kontrollverfahren zur Übertragung von Datenblöcken an der Schnittstelle DTE/DCE. Es wird eine Variante der HDLC-Prozedur (High Level Data Link Control) verwendet, die als LAP-B (Link Access Procedure Balanced) bezeichnet wird.

Schicht 3 (Vermittlungsschicht): legt die Struktur der Kontrollinformation und der Daten innerhalb der Pakete fest. Das Protokoll der Vermittlungsschicht wird als PLP (Packet Layer Protocol) bezeichnet und ist für den Verbindungsauf- und -Abbau, sowie die Übertragung der Datenpakete während einer Verbindung verantwortlich. Hier können gleichzeitig mehrere sogenannte virtuelle Verbindungen über eine physikalische Leitung abgewickelt werden.

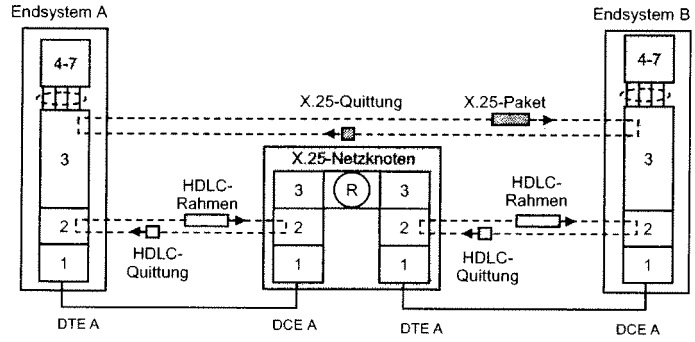


Bild: X.25 Flusskontrolle

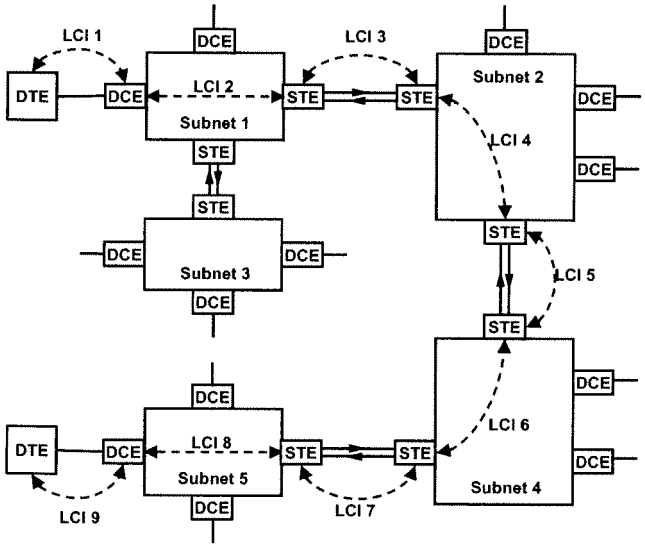


Bild: X.25 Virtuelle Ende-zu-Ende-Verbindung

Virtuelle Ende-zu-Ende Verbindungen

Es können folgende Verbindungen existieren:

- feste (permanente) virtuelle Verbindungen und
- virtuelle Wählverbindungen

Eine virtuelle Wählverbindung existiert nach Bedarf und nur von dem Zeitpunkt einer Verbindungsherstellung bis zu dem Zeitpunkt des Verbindungsabbaus. Für diese Zeit sind die beiden Endstellen virtuell miteinander verbunden. Die Wählverbindung ist durch die drei Phasen Aufbau einer Verbindung, Datentransfer und den Abbau einer Verbindung gekennzeichnet. Eine feste virtuelle Verbindung ist durch eine permanente Zuordnung der logischen Kanäle gekennzeichnet. Es werden keine Auf- und Abbauphasen benötigt. Die feste virtuelle Verbindung ist permanent in der Datentransferphase.

Für die Zuordnung eines Paketes zu einer virtuellen Verbindung erhält jedes Paket im Header eine logische Kanalnummer LCI (Logical Channel Identifier), die sich aus einer Gruppennummer (LGN) und einer Nummer (LCN) innerhalb der Gruppe zusammensetzt. Auf diese Art und Weise ist über eine physikalische Leitung die parallele Kommunikation Programm-zu-Programm möglich. Der logische Kanal ist immer existent. Entweder ist er einer virtuellen Verbindung zugeordnet oder er ist frei. Es können 4096 unabhängige Kanäle an einem Anschluss gebildet werden. Dies resultiert aus der Tatsache, dass 16 Kanalgruppennummern und 256 logische Kanalnummern in jeder Gruppe vergeben werden können. Die Aufgabe einer X.25-Paketvermittlung ist, virtuelle Ende-zu-Ende-Verbindungen durch die Kopplung der logischen Kanäle in Netzknoten zu realisieren. Dazu müssen die Logical Channel Identifier mit Hilfe von Vermittlungstabellen umgesetzt werden, so dass eine korrekte Verknüpfung der logischen Kanäle in Netzknoten erfolgen kann.

Es sind zwei Klassen von X.25-Netzdiensten zu unterscheiden:

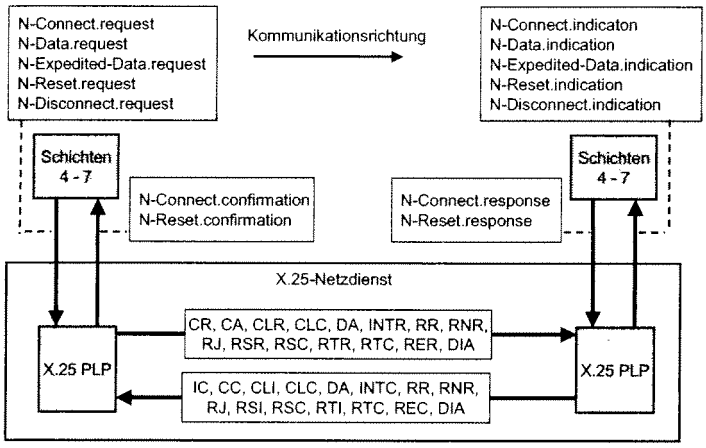
CONS	**Verbindungsorientierter Netzdienst (Connection-Mode Network Service).** Bei diesem Dienst wird eine virtuelle Ende-zu-Ende-X.25-Verbindung (im weiteren kurz X.25-Verbindung genannt) zwischen zwei NSAPs (Network Service Access Point) in den kommunizierenden DTEs aufgebaut. Damit werden zwei NSAPs in den beteiligten DTEs für die Dauer des Datentransfers logisch verbunden. Ein NSAP stellt eine weltweit eindeutige X.25-Netzadresse dar. Innerhalb der Datentransferphase werden die Netzadressen in Datenpaketen nicht übertragen. Die Reihenfolge von empfangenen Datenpaketen am Ziel-DTE stimmt mit der Reihenfolge beim Absenden in der Quell-DTE überein.
CLNS	**Verbindungsloser Netzdienst (Connectionless-Mode Network Service).** Bei diesem Dienst besteht keine X.25-Verbindung zwischen den kommunizierenden DTEs. Bei jedem abgeschickten Datenpaket müssen beide Netzadressen (Quell- und Ziel-Netzadresse) übertragen werden. Die Reihenfolge von empfangenen Datenpaketen am Ziel-DTE kann mit der abgeschickten Reihenfolge in der Quell-DTE nicht übereinstimmen.

In X.25-Netzen wird hauptsächlich der verbindungsorientierte Dienst CONS realisiert. Die verbindungslose Dienst hat keine große Relevanz für die Praxis und wird nicht weiter betrachtet.

Pakettypen

Um den verbindungsorientierten X.25-Netzdienst zur Verfügung zu stellen, verwendet das Protokoll X.25-PLP folgende Gruppen von Protokolldateneinheiten, PDUs (Protocol Data Unit), die üblicherweise als X.25-Pakete bezeichnet werden. Es ist hierbei zu bemerken, daß dasselbe Paket an der Sendeseite (an der Empfangsseite DCE => DTE) unterschiedlich genannt wird.

Pakettyp		**Protokollfunktion**
DTE => DCE	DCE => DTE	
Call Request (CR) Call Accepted (CA)	Incoming Call (IC) Call Confirmation (CC)	Verbindungsaufbau
Clear Request (CLR) Clear Confirmation (CLC)	Clear Indication (CLI) Clear Confirmation (CLC)	Verbindungsabbau
Data (DA) Interrupt Request (INTR)	Data (DA) Interrupt Confirmation (INTC)	Datentransfer
Receiver Ready (RR) Receiver Not Ready (RNR) Reject (RJ) Reset Request (RSR) Reset Confirmation (RSC)	Receiver Ready (RR) Receiver Not Ready (RNR) Reject (RJ) Reset Indication (RSI) Reset Confirmation (RSC)	Flusskontrolle
Restart Request (RTR) Restart Confirmation (RTC)	Restart Indication (RTI) Restart Confirmation (RTC)	Restart
Diagnostic (DIA)	Diagnostic (DIA)	Netzdiagnose
Registration Request (RER)	Registration Confirmation (REC)	Registrierung



Die Zusammenarbeit einer X.25-Anwendung innerhalb der vierten Schicht (Transportschicht) und der dritten Schicht wird mit Hilfe eines Satzes von Primitiven realisiert. Um die X.25-Netzdienste zu erbringen, werden innerhalb der dritten Schicht zwischen den beteiligten Datenendeinrichtungen bestimmte X.25-Pakete ausgetauscht.

Bild: Zusammenarbeit zwischen X.25-Anwendungen und dem X.25-PLP

Die einzelnen Primitiven haben folgende Bedeutung:

N-Connect	wird verwendet, um eine virtuelle X.25-Verbindung aufzubauen
N-Data	dient der Übergabe von normalen (nicht dringlichen) Daten
N-Expedited data	dient der Übergabe von dringlichen Daten
N-Reset	ermöglicht es, eine virtuelle X.25-Verbindung in einen festgelegten Ausgangszustand zu versetzen
N-Disconnect	wird verwendet, um eine bestehende virtuelle Netzverbindung abzubauen

Die ersten drei Bytes aller Pakettypen haben die gleiche Struktur.

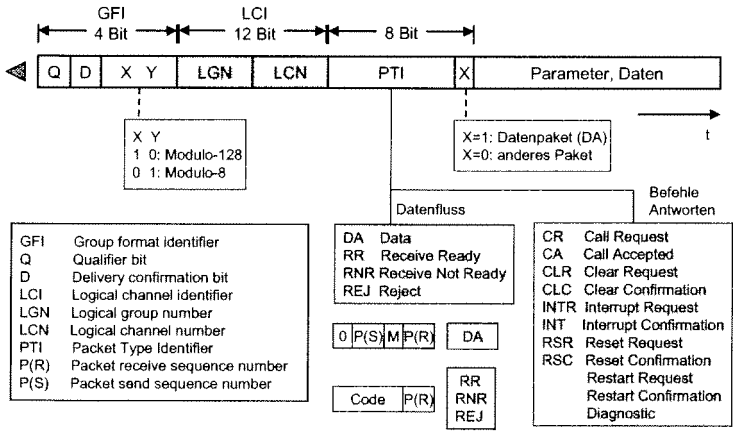


Bild: Allgemeine Struktur der X.25-Pakete

Die ersten drei Bytes der X.25-Pakete

GFI (General Format Identifier)	Die GFI-Angaben legen das Grundformat für den restlichen Paketteil fest. Die einzelnen Bits haben folgende Funktionen:	
	Q/A-Bit (Qualifier-/Address-Extension-Bit)	Das Q-Bit (Qualifier-Bit) wird nur in Datenpaketen verwendet und dient zur Unterscheidung zwischen Nutzerdaten und Steuerdaten im Rahmen der ITU-T-Empfehlung X.29. In anderen Pakettypen hat dieses Bit keine Bedeutung.
		Das A-Bit (Address-Extension-Bit) wird in Paketen für den Verbindungsaufbau und den Verbindungsabbau benutzt. Ist A-Bit = 0, so wird das X.121-Adreßformat verwendet. Ist das A-Bit = 1, so werden andere Adressformate benutzt.

	D-Bit (Delivery-Confirmation-Bit)	Das D-Bit kann in Paketen für den Verbindungsaufbau und in Datenpaketen benutzt werden. In allen anderen Pakettypen ist D-Bit = 0. Die D-Bit-Funktion hängt mit dem M-Bit in Datenpaketen DA zusammen. Ist D-Bit = 1, wird eine Ende-zu-Ende-Quittung des Datenpaketes vor der Partner-Datenendeinrichtung angefordert.
	XY-Bits	Ist XY = 10 (bzw. XY = 01), so werden die Sende- und Empfangsfolgenummern in Daten-, RR-, RNR- und REJ-Paketen nach dem Modulo-128 (bzw. Modulo-8) verwendet Bei der Numerierung nach dem Modulo-128 handelt es sich um das sogenannte erweiterte Paketformat.
LCI (Logical Channel Identifier)	Der LCI setzt sich aus LGN (Logical Group Number) und LCN (Logical Channel Number) zusammen. Mit den 12 Bits des LCI können bis zu 4096 logische Kanäle definiert werden. Mit der LGN können diese logischen Kanäle in 16 Gruppen zu jeweils 256 Kanälen aufgeteilt werden. Mit der LGN wird die Kanal-Gruppe identifiziert. Mit der LCN werden die einzelnen Kanäle innerhalb einer Gruppe markiert.	
PTI (Packet Type Identifier)	Der PTI definiert den jeweiligen Pakettyp. Die Angaben in diesem Feld dienen der Unterscheidung einzelner Pakete.	

Weitere Angaben in X.25-Paketen sind:

Calling/Called address length	Hier wird die Länge der DEE-Adresse angegeben
Called/Calling address	Hier wird die Adresse (nach X.121) der gerufenen/rufenden DTE übertragen. Um die ISO-Netzadressen, d.h. NSAP-Adressen auch zu unterstützen, wird eine Adresserweiterung im Feld Facility (Leistungsmerkmale) benutzt.
Facility length	Hier wird die Länge des Facility-Feldes angegeben
Facility (Leistungsmerkmale)	X.25 erlaubt eine Vielzahl von zusätzlichen Funktionen, die optional sind und als Leistungsmerkmale bezeichnet werden. In diesem Feld können die Leistungsmerkmale vereinbart werden.

Für die Nummerierung und Quittungen werden folgende Nummern verwendet:

P(S)-Sendefolgenummer (Send Sequence Number)	Mit dieser Nummer werden die zu sendenden Datenpakete (DA) fortlaufend an der Sendeseite nummeriert
P(R)-Empfangsfolgenummer (Receive Sequence Number)	Diese Nummer gibt der Empfangsseite an, dass alle Datenpakete mit den Nummern bis zu P(R)-1 einschließlich korrekt im Ziel-Endsystem aufgenommen wurden und dass das nächste Datenpaket mit der Nummer P(R) erwartet wird.

Kommunikation nach X.25-PLP

Im weiteren wollen wir die wichtigsten Abläufe bei der Steuerung der Kommunikation nach dem X.25-PLP in kompakter Form darstellen.

Hierbei sind zwei Möglichkeiten zu unterscheiden, nach denen eine virtuelle X.25-Verbindung für eine X.25-Anwendung zur Verfügung gestellt wird:

- Fall 1: Einbettung des Primitives N-Connect.request in das Datenpaket DA,
- Fall 2: Umsetzung des Primitives N-Connect.request in das Paket CR.

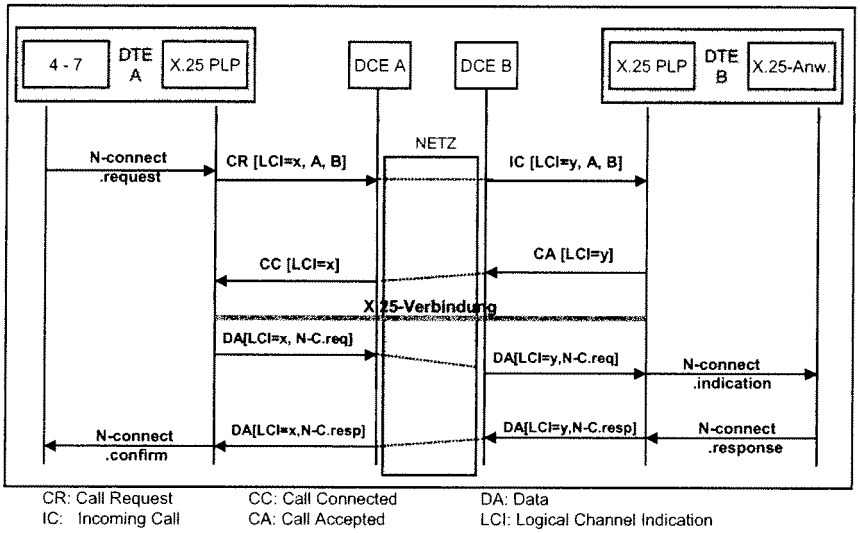


Bild: Aufbau einer virtuellen X.25-Verbindung
mit der Einbettung von N-CONNECT-req (N_C.req) in ein DA-Paket

Zunächst betrachten wir den Fall 1. Mit dem Primitiv N-Connect.request wird von der X.25-Anwendung der Aufbau einer virtuellen Verbindung initiiert. Daraufhin sendet die Quell-DTE das Paket Call Request (CR) an die Ziel-DTE. Das Paket CR enthält u.a. die zugeordnete Nummer des logischen Kanals (LCI = x) und die NSAP-Adressen von Quell- und Ziel-DTEs (d.h. A und B). Das empfangene CR-Paket in der Ziel-DTE hat die Bedeutung eines Verbindungsaufbau-Wunsches und wird als Incoming Call (IC) bezeichnet. Im letzten Netzknoten wird ein logischer Kanal für die gewünschte Verbindung reserviert und seine Nummer LCI = y im IC-Paket an die Ziel-DTE übergeben.

Wird der Wunsch nach einer X.25-Verbindung in der Ziel-DTE akzeptiert, so wird dies mit dem Paket Call Accepted (CA) bestätigt. An dieser Stelle ist zu bemerken, dass im Paket CA, das von der Ziel-DTE ins Netz geschickt wird, keine DTE-Adressangaben außer dem LCI enthalten sind. Dies ist der größte Vorteil der verbindungsorientierten Kommunikation nach X.25, dass die oft langen Adressangaben nur im ersten Paket CR übertragen werden müssen. Das empfangene CA-Paket in der Quell-DTE stellt eine Bestätigung, Call Confirmation (CC), dar und enthält die lokal beim CR zugeordnete LCI = x. Dieses Beispiel soll verdeutlichen, dass die LCIs nur lokale Bedeutung haben. Kommt an die Quell-DTE das Paket CC an, steht eine virtuelle X.25-Verbindung für die X.25-Anwendungen zur Verfügung.

Im nächsten Schritt wird das Primitiv N-Connect.request in ein Datenpaket DA eingebettet und als Nutzdaten an die Ziel-DTE übertragen. Hier wird das N-Connect.request an die X.25-Anwendung als N-Connect.indication übergeben. Akzeptiert die X.25-Anwendung die gewünschte Verbindung, so wird das Primitiv N-Connect.response in einem Paket DA als Nutzdaten an die Quell-DTE übertragen. Hier wird das N-Connect.response aus dem Paket DA herausgenommen und an die X.25-Anwendung als Primitiv N-Connect.confirm übergeben. Damit wird die Verfügbarkeit einer virtuellen X.25-Verbindung und die Bereitschaft der Partner-Anwendung in der Ziel-DTE, Daten zu empfangen, signalisiert.

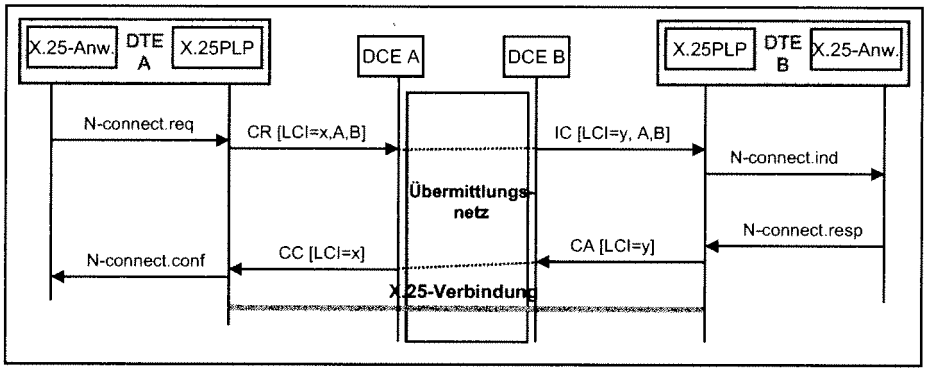


Bild: Aufbau einer virtuellen X.25-Verbindung
mit der Umsetzung von N-CONNECT-req in ein CR-Paket

Im Fall 2 wird der Verlauf beim Verbindungsaufbau beschleunigt, indem das Primitiv N-Connect.request in der Quell-DTE in das Call Request (CR) umgesetzt wird. Das im Zielnetzknoten empfangene Paket CR wird als Incoming Call (IC) an die Ziel-DTE geschickt. Hier wird das Paket IC in das Primitiv N-Connect.indication umgesetzt und an die X.25-Anwendung übergeben. Die Empfangsbereitschaft der X.25-Anwendung in Form von N-Connect.response wird in das Call Accepted (CA) umgesetzt und an die Quell-DTE übertragen. Hier wird der Empfang des Paketes CC der X.25-Anwendung mittels des Primitives N-Connect.confirm mitgeteilt.

Für den Abbau einer virtuellen X.25-Verbindung ist zu bemerken, dass der Abbau der X.25-Anwendung nur angezeigt und nicht bestätigt wird.

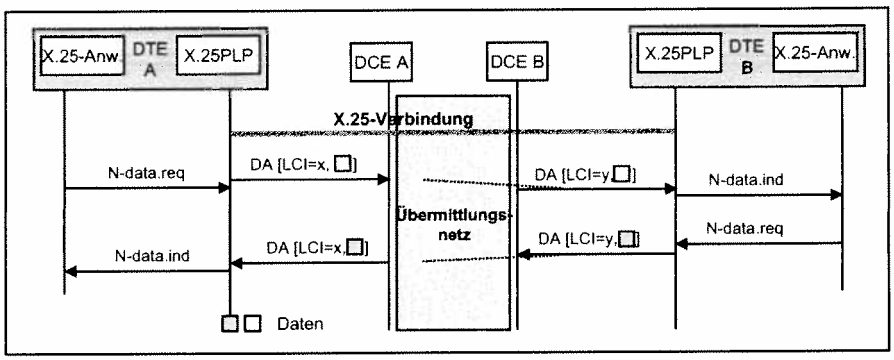


Bild: Abbau einer virtuellen X.25-Verbindung

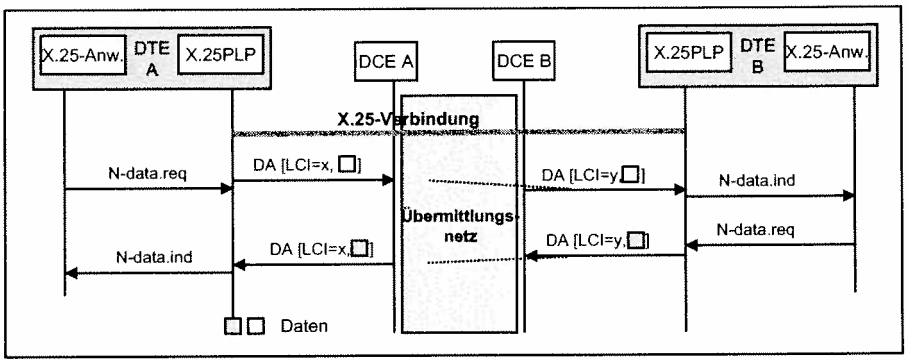


Bild: Datenaustausch zwischen entfernten X.25-Anwendungen

Zur Übergabe von Daten zwischen entfernten X.25-Anwendungen dient das Primitiv N-Data. Wurde eine virtuelle X.25-Verbindung aufgebaut, so besteht die Möglichkeit, die Datenpakete in beide Richtungen über diese Verbindung zu senden.

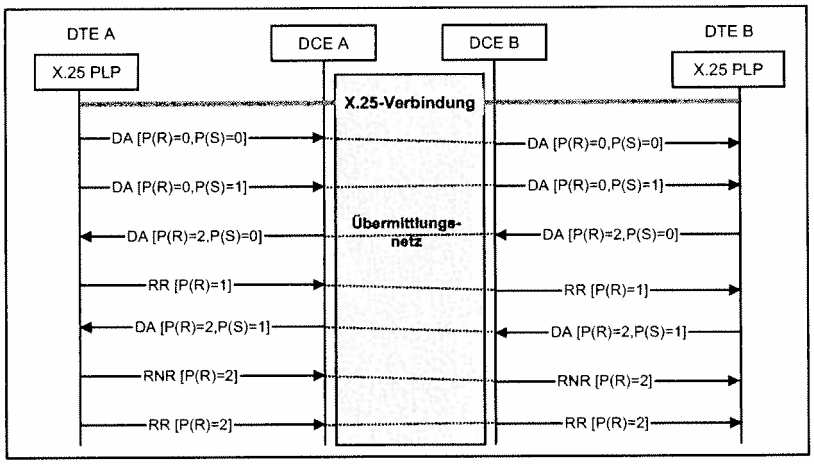


Bild: Datenaustausch nach X.25
P(S): Sendefolgenummer, P(R): Empfangsfolgenummer

Die Nummern P(S) und P(R) sind folgendermaßen zu interpretieren:

- Mit der P(S)-Sendefolgenummer (Send Sequence Number) werden die zu sendenden Datenpakete (DA) fortlaufend an der Sendeseite nummeriert.
- Mit der P(R)-Empfangsfolgenummer (Receive Sequence Number) gibt die Empfangsseite an, dass alle empfangenen Datenpakete mit den P(S)-Nummern bis zu P(R)-1 einschließlich korrekt im Ziel-Endsystem aufgenommen wurden und dass das nächste Datenpaket mit der Nummer P(R) erwartet wird.

Die DTE A sendet die ersten zwei Datenpakete mit den P(S)-Nummern 0 und 1. Daraufhin sendet die DTE B das erste Datenpaket mit P(S) = 0 und teilt der DTE A mit P(R) = 2 mit, dass als nächstes das Datenpaket mit P(S) = 2 erwartet wird. Die DTE A hat vorläufig keine Daten zu senden, Daten können jedoch empfangen werden. Dies wird der DTE B mit RR (Receive Ready) mitgeteilt und gleichzeitig angegeben, dass das nächste Datenpaket von der DTE B mit P(S) = 1 (P(R) = 1) erwartet wird. Nach dem Empfang des nächsten Datenpakets (P(S) = 1) signalisiert die DTE A mit RNR (Receive Not Ready), dass sie vorläufig nicht in der Lage ist, weitere Datenpakete zu empfangen. Mit RNR wird auch angegeben, mit welcher P(S)-Nummer das nächste Datenpaket erwartet wird. Diese Nichtbereitschaft wird zu einem späteren Zeitpunkt mit RR aufgehoben.

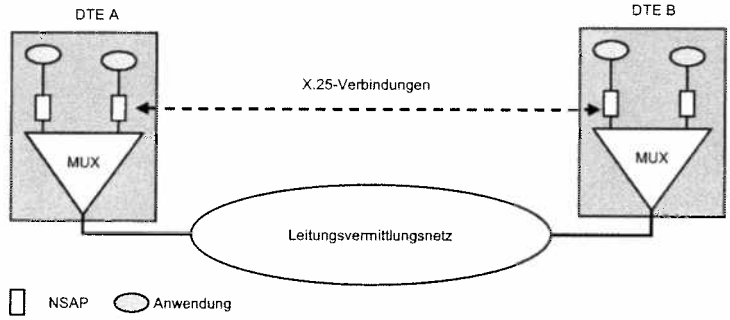


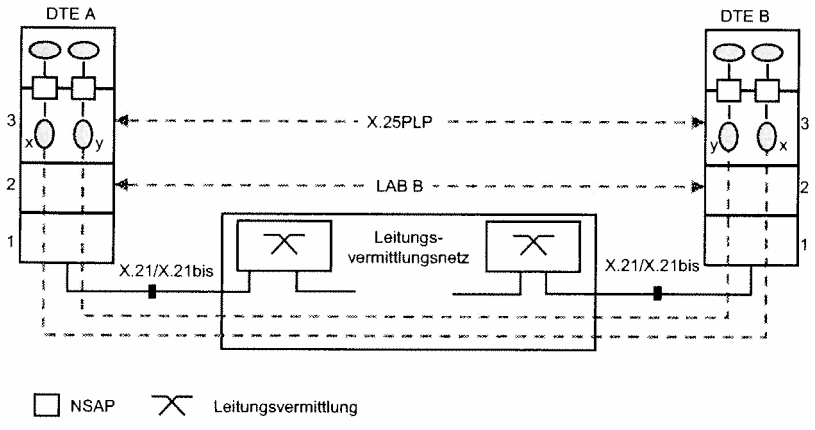
Bild: Bedeutung des Protokolls X.25 DTE-DTE

Protokoll X.25 DTE-DTE

Die Übermittlung von Daten in Form von Paketen zwischen einer Datenendeinrichtung und dem Kommunikationsmodul DCE in einem X.25-Netzknoten erfolgt nach dem Protokoll X.25 DTE-DCE. Das Protokoll X.25 DTE-DTE kann für die Übermittlung von paketierten Daten zwischen zwei kommunizierenden Datenendeinrichtungen eingesetzt werden über:

- ein Leitungsvermittlungsnetz bzw.
- eine physikalische Punkt-zu-Punkt-Verbindung.

Das X.25-Konzept ist als eine Systemlösung für die parallele Kommunikation Programm-zu-Programm zu interpretieren. Logisch gesehen ist das Protokoll X.25 DTE-DTE als eine Kopplung von zwei statistischen Multiplexern zu interpretieren. Die Ports von diesen Multiplexern repräsentieren die Netzadressen NSAP und eine logische Verbindung zwischen zwei Ports stellt eine X.25-Verbindung nach dem Protokoll X.25 DTE-DTE dar.



Das Protokoll X.25 DTE-DTE erlaubt die Realisierung mehrerer logische Kanäle über eine physikalische Leitung. Ein logischer Kanal wird mit einer Nummer LCI (Logical Channel Identifier) gekennzeichnet und stellt eine Kommunikationsbeziehung zwischen zwei Puffern in den kommunizierenden Datenendeinrichtungen dar. Die Hauptfunktion des Protokolls X.25 besteht in der Bereitstellung von X.25-Verbindungen zwischen den kommunizierenden DTEs.

Eine solche Verbindung stellt eine Beziehung zwischen zwei NSAPs in beteiligten DTEs dar. Diese Verbindungen können auf unbegrenzte Zeit (permanente Verbindung) nach Bedarf aufgebaut werden (Wählverbindungen). Die praktische Bedeutung des Protokolls X.25 DTE-DTE über eine physikalische Punkt-zu-Punkt-Verbindung besteht darin, dass über diese Verbindung eine parallele Kommunikation stattfinden kann, so dass diese Verbindung besser ausgelastet wird.

Das Prinzip der Datenkommunikation nach dem Protokoll X.25 DTE-DTE über ein Leitungsvermittlungsnetz veranschaulicht das folgende Bild. Ein Datennetz mit Leitungsvermittlung (z. B. ISDN) hat die Aufgabe, die Bitströme zwischen den Datenendeinrichtungen zu transportieren. In den Netzknoten werden nur die physikalischen Kanäle miteinander verbunden (Leitungsvermittlung). Das Leitungsvermittlungsnetz stellt eine physikalische Ende-zu-Ende-Verbindung dar und erlaubt damit eine transparente Bitübertragung.

Frame Relay (FR)

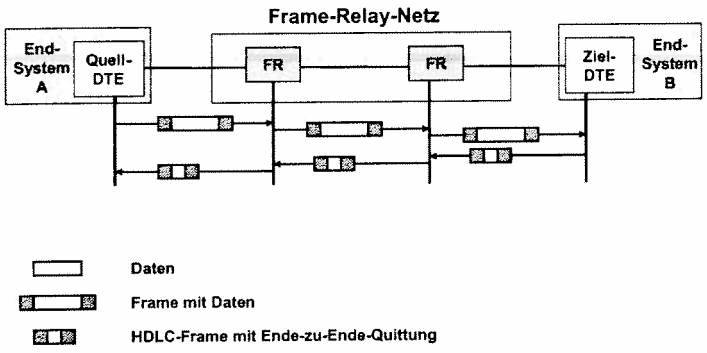


Bild: Paketvermittlung in Frame-Relay-Netzen

Frame Relay ist ein Rahmenvermittlungsverfahren, das in Schicht 2 abläuft. Rahmen werden nur Ende-zu-Ende quittiert. Rahmen, die in Zwischenknoten als fehlerhaft identifiziert werden, werden verworfen.

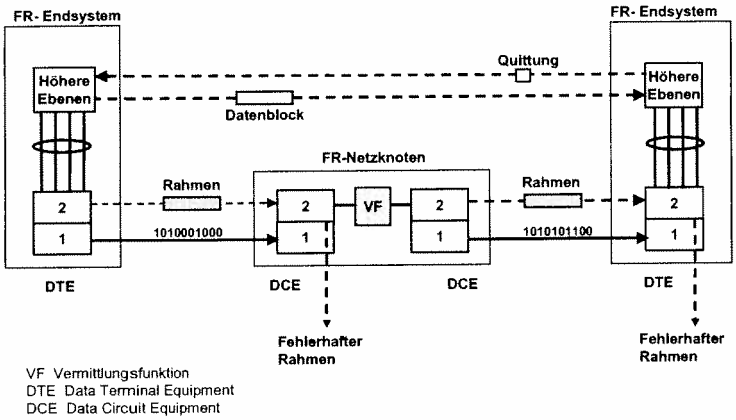


Bild: Paketvermittlung in Frame-Relay-Netzen

Das FR-Protokoll verwendet variabel lange, HDLC-artige Rahmen. Das Adressfeld ist 2 Byte lang (optional auch 3-4 Byte) und enthält neben einigen Bits mit Sonderfunktionen den 10-Bit-DLCI zur Identifikation der virtuellen Verbindung. Damit lassen sich 2^{10} = 1024 logische Kanäle adressieren. Mittels des DLCI wird die Funktion des statistischen Multiplexens auf Schicht 2 durchgeführt. Einige DLCI sind für Sonderaufgaben reserviert, weshalb noch 976 Stück zur Unterscheidung von Benutzerverbindungen bleiben.

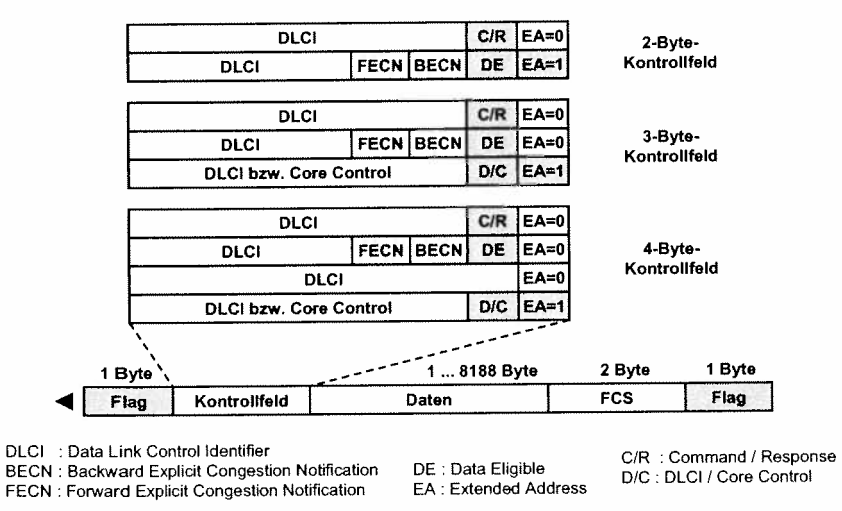


Bild: Aufbau des Frame-Relay-Rahmens

FECN: Das FECN-Bit (Forward Explicit Congestion Notification, nach vorn gerichtete Überlastanzeige) kann von einem überlasteten Netz auf 1 gesetzt werden, um dem empfangenden Endgerät anzuzeigen, dass die in seine Richtung übertragenen Rahmen durch überlastete Ressourcen der FR-Netzknoten gelaufen sind. FR-Netzknoten und Endgeräte dürfen das FECN-Bit setzen, kein FR-Netzknoten darf aber ein gesetztes FECN wieder auf 0 zurücksetzen.

BECN: Das BECN-Bit (Backward Explicit Congestion Notification, nach hinten gerichtete Überlastanzeige) kann von einem überlasteten Netz auf 1 gesetzt werden, um dem Endgerät anzuzeigen, dass die von ihm gesendeten Rahmen durch überlaste-

te Ressourcen gelaufen sind. Wie beim FECN auch, dürfen FR-Netzknoten und Endgeräte das BECN-Bit setzen, kein FR-Netzknoten darf aber ein gesetztes BECN wieder auf 0 zurücksetzen.

DE: Das DE-Bit (Discard Eligibility, Lösch-Priorität) ist im Überlast-Fall von Interesse.

Das DE-Bit wird für zwei verschiedene Zwecke eingesetzt:

- FR-Endgeräte können optional dieses Bit benutzen, um ihre Daten zu priorisieren. Sie zeigen damit den Transitknoten an, welche Daten (DE = 1) diese im Falle einer schweren Überlast bevorzugt verwerfen sollen. Damit wird es wahrscheinlicher, dass wichtigere Daten (DE =0) ihr Ziel erreichen.
- Einige FR-Netzknoten verwenden das DE-Bit, um vom Endgerät empfangene Daten zu markieren, die oberhalb der zwischen Anwender und Netzbetreiber vereinbarten Übertragungskapazität liegen. In diesem Fall setzt der FR-Netzknoten das Bit. Tritt dann irgendwo im Netz akute Überlast auf, so werden zunächst die Rahmen verworfen, die oberhalb der CIR liegen (also DE-markiert sind).

Endgeräte und Netz dürfen also dieses Bit setzen. Das Netz darf jedoch ein vom FR-Endgerät auf 1 gesetztes DE-Bit nicht mehr auf 0 zurücksetzen. Das Netz ist in Überlastsituationen außerdem nicht verpflichtet, nur Frames mit DE = 1 zu verwerfen. In der Praxis bieten die FR-Knoten die Auswertung des DE-Bits als optionale Methode zum selektiven Verwurf an. Ob das Merkmal aktiviert ist oder nicht, muss mit dem jeweiligen Netzbetreiber geklärt werden.

C/R: Das ebenfalls im Adressfeld stehende C/R-Bit (Command/Response) ist anwendungsspezifisch und wird vom FR-Netz transparent übertragen. Dieses Bit kann von der Applikation dazu verwendet werden, auf ein- und demselben logischen Kanal Steuer- von Benutzer-Informationen zu unterscheiden.

EA: Mittels der EA-Bits (Extended Address) wird die Form des Adressfelds bestimmt. Neben dem oben dargestellten 2-Byte-Format existieren noch eine 3- und eine 4-Byte-Version, in denen entsprechend mehr DLCI zur Verfügung stehen, die ansonsten aber die gleichen Funktions-Bits enthalten. Da die beim 2-Byte-Adressfeld möglichen 976 DLCI normalerweise nicht alle benötigt werden, sind die erweiterten Adressfelder von geringer praktischer Bedeutung.

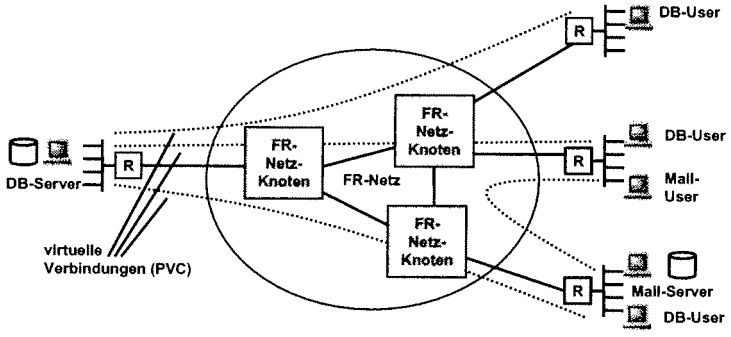


Bild: Endgeräte und FR-Netzknoten

Ein Frame-Relay Netz ermöglicht den dynamischen Auf- und Abbau von logischen Verbindungen

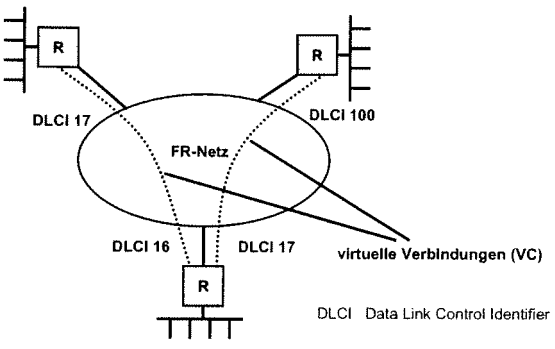
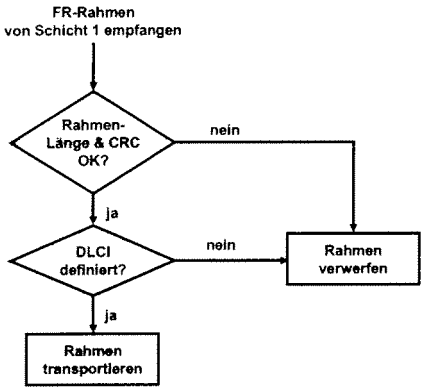


Bild: Bedeutung des DLCI
(Streckenweise Adressierung)

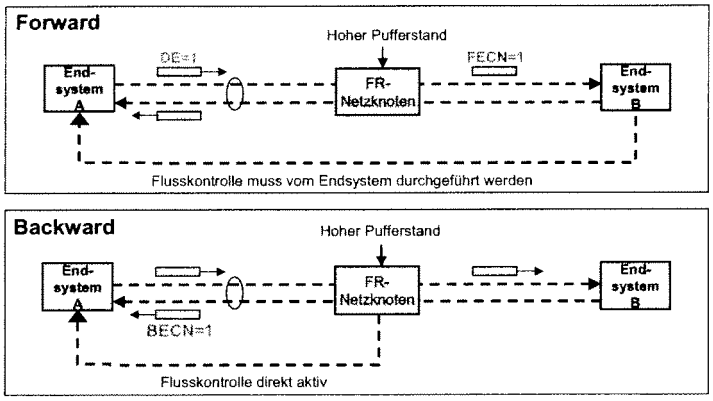
Logische Verbindungen in Frame Relay sind durch eine Reihe von DLCIs (Data Link Control Identifier) gegeben. Jede DLCI hat seine Gültigkeit über einen Streckenabschnitt. In jedem FR-Knoten ermöglichen Tabellen den Austausch der Identifier und die entsprechende Weiterleitung der Rahmen zu den richtigen Ausgangsports.



Die Einfachheit der Weiterleitung wird durch ein Flussdiagramm illustriert.

- Prüfung auf Korrektheit der empfangenen Rahmen.
- Verwerfung bei fehlerhaftem Rahmen.
- Prüfung von DLCI des Rahmens.
  Hat der DLCI einen erlaubten (dem Netz bekannten) Wert, so wird der Rahmen gemäß der Routing-Tabelle des Netzknotens weitergeleitet. Bevor der Rahmen dem Empfänger übergeben wird, ändert das FR-Netz noch den DLCI und berechnet den CRC neu.
- Prüfung auf Überlastung des Netzknotens.
  Bei Überlastung können Rahmen verworfen werden

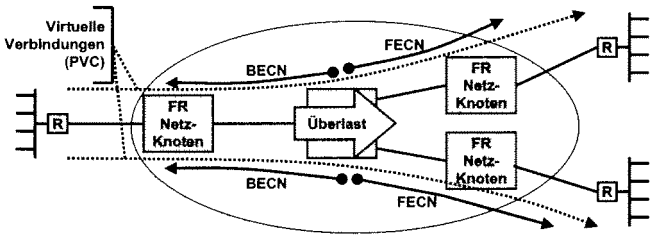
Bild: Flussdiagramm FR-Protokoll



BECN : Backward Explicit Congestion Notification
FECN : Forward Explicit Congestion Notification

Bild:Überlastabwehr: Explicit Congestion Notification

Stellt ein FR-Netzknoten die Überschreitung eines bestimmten Auslastungs-Schwellenwerts fest, so wird den betroffenen Endgeräten die möglicherweise bevorstehende Stau-Situation signalisiert. Damit soll diesen die Möglichkeit gegeben werden, den Stau durch die Reduzierung ihrer Datenrate zu verhindern. Es handelt sich nur um eine Überlast-Anzeige, keine Flusskontrolle. Diese Überlast-Anzeige geschieht in beide Richtungen der betroffenen Verbindung mittels zweier Bits des Adressfelds (FECN und BECN).



BECN : Backward Explicit Congestion Notification
FECN : Forward Explicit Congestion Notification

Bild: Überlastabwehr: FECN/BECN

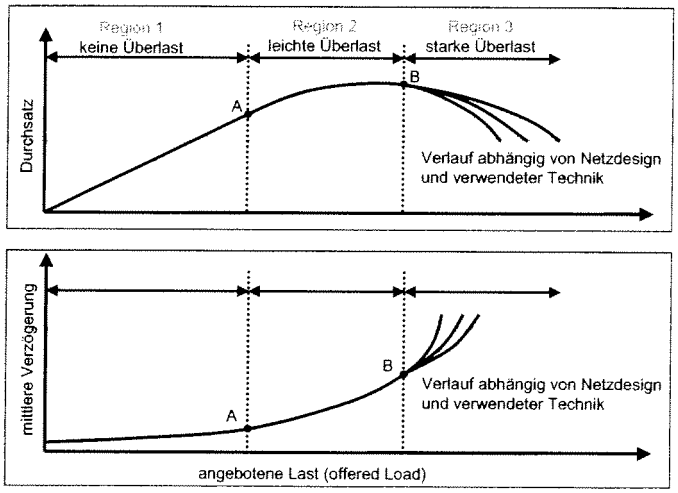


Bild: Durchsatz und Verzögerung bei Überlast

Die Summe des Verkehrs, den alle Endgeräte zu einer bestimmten Zeit ins Netz senden, wird offered Load (angebotene Last) genannt. Bezüglich der Verkehrssituation werden im FR-Netz drei Zustände unterschieden, die mit der angebotenen Last im Zusammenhang stehen.

Im Zustand nicht überlastet ergibt sich bei steigender angebotener Last keine Qualitätsminderung für die Endgeräte. Der Datendurchsatz des Gesamtnetzes erhöht sich linear mit der angebotenen Last.

Ab einem bestimmten Verkehrsaufkommen (Betriebspunkt A) steigt der Gesamtdurchsatz des Netzes jedoch nur noch degressiv. Die Verzögerung der Rahmen im Netz steigt dann überproportional zum Lastwachstum. Die Wahrscheinlichkeit für das Eintreten dieses Zustands kann durch entsprechende Dimensionierung der Übertragungskapazität bei der Netzplanung minimiert werden.

Er kann dennoch in dem seltenen Fall auftreten, dass zufällig viele User gleichzeitig Bursts produzieren. Dann versucht das FR-Netz durch Anwendung der unten beschriebenen Mechanismen zur Überlastbeseitigung (z.B. Setzen von FECN/BECN-Bits) wieder in den nicht überlasteten Bereich zurück zu gelangen.

Steigt die Datenmenge trotzdem weiter, so kann das Netz möglicherweise in den dritten Zustand (schwere Überlast, Betriebspunkt B) eintreten. Hier steigen die Delays der einzelnen Verbindungen weiter an, und der Durchsatz des Gesamtnetzes nimmt trotz steigender Datenmenge ab. Um in den nicht überlasteten Zustand zurückzukehren, müssen entsprechende Überlastabwehrmechanismen eingesetzt werden..

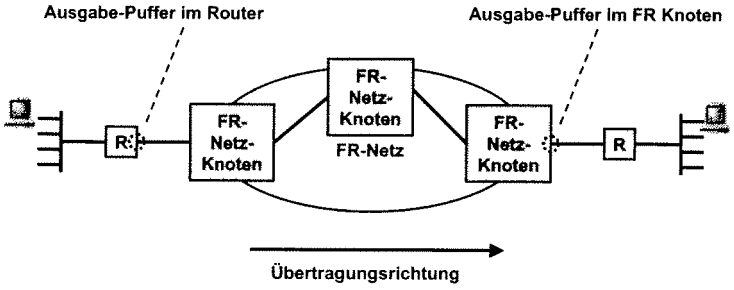


Bild: Staupunkte in Frame-Relay-Netzen

ATM (Asynchronous Transfer Mode)

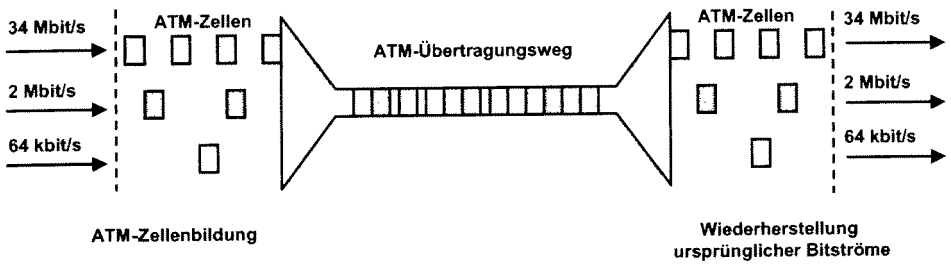
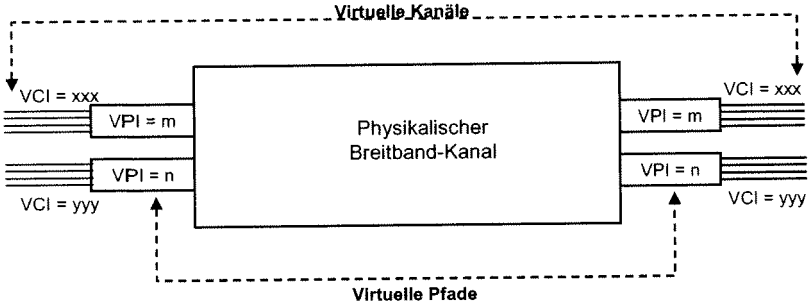


Bild: Asynchroner Transfer Modus

Der Asynchrone Transfer Modus (ATM) ist ein Übermittlungsverfahren, das auf einer verbindungsorientierten Paketvermittlung basiert. Die Nutzdaten werden in Form von Paketen mit festgelegter Länge übertragen. Diese Pakete werden als Zellen bezeichnet.

Jede Zelle ist 53 Byte lang und besteht aus einem Kopffeld (5 Byte) und einem Informationsfeld (48 Byte). In der Literatur verwendet man auch den Begriff Oktett für Byte. Es werden sowohl die Nutzdaten, als auch die Signalisierungsdaten und Daten zum Betrieb, zur Administration und zur Wartung des Netzes in Zellenform übermittelt.

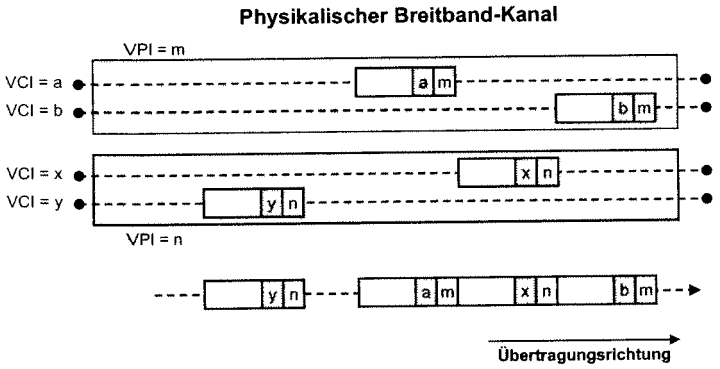
Der Transport der ATM Zellen zwischen den Datenendeinrichtungen erfolgt über Virtuelle Verbindungen. Diese Virtuellen Verbindungen werden durch das Konzept der Virtuellen Pfade und Virtuellen Kanäle definiert. Zur Unterscheidung der Virtuellen Pfade und Virtuellen Kanäle dienen Einträge im Zellenkopf. Die ATM Vermittlungsstellen werten diese Informationen zur Lenkung des Zellenflusses aus. Durch die Verwendung der Virtuellen Verbindungen bleibt die Zellenreihenfolge erhalten, da alle Zellen einer Virtuellen Verbindung denselben Virtuellen Pfaden und Virtuellen Kanälen zugeordnet werden und dadurch auf demselben Weg durch das Netz gelenkt werden.



VPI: Virtual Path Identifier
VCI: Virtual Channel Identifier

Bild: Konzept der virtuellen Pfade und Kanäle

Nach dem Verbindungsaufbau und der Anforderung von Betriebsmittel und Übermittlungseigenschaften folgt die Bereitstellung der Übertragungskapazitäten durch das Netz zur Datenübertragung. Nach dem Abbau der Verbindung werden die verwendeten Übertragungskapazitäten freigegeben.



VPI: Virtual Path Identifier
VCI: Virtual Channel Identifier

Bild: Realisierung der virtuellen Pfade und Kanäle

Den jeweiligen Virtuellen Verbindung werden keine festgelegten Zellenraten zugeordnet. Die dynamische Zuordnung der Zellenrate erfolgt entsprechend dem momentanen Bedarf und der verfügbaren Übertragungskapazität des Netzes. Die von einer Verbindung nicht benötigte Übertragungskapazität steht anderen Verbindungen zur Verfügung. Um einen kontinuierlichen Datenstrom zu gewährleisten, werden Leerzellen übertragen.

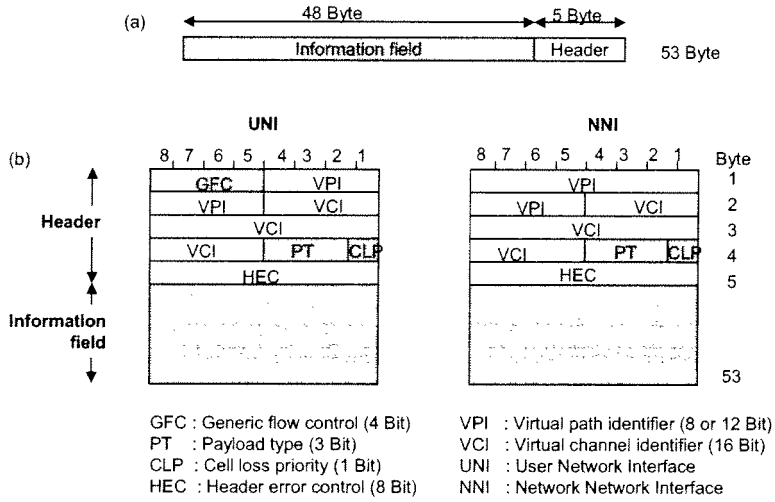


Bild: ATM Zellenstruktur

Eine ATM Zelle ist ein Paket mit einer fixen Länge von 53 Byte. Die Zelle wird in ein Kopffeld (5 Byte) und ein Informationsfeld (48 Byte) gegliedert.

Die Datenlänge von 53 Byte ist das Ergebnis eines Kompromisses zwischen möglichst großer Nutzdatenlänge und einer möglichst geringen Ende-zu-Ende Übertragungsverzögerung (end-to-end transmission delay). Die Forderung einer geringen Übertragungsverzögerung ergibt sich aus den Anforderungen von Echtzeitverkehr (Telefonie, Videotelefonie).

Die Gliederung des Kopffeldes einer ATM Zelle für eine Teilnehmer-Netz-Schnittstelle (User-Network-Interface, UNI) und eine Netz-Netz-Schnittstelle (Network-Network-Interface, NNI)

- Das **VPI (Virtual Path Identifier)** Feld wird zur Kennzeichnung der Virtuellen Pfade verwendet. Zellen, die dem gleichen Pfad zugeordnet sind, können durch spezielle Vermittlungsknoten sehr schnell vermittelt werden, da nur das VPI Adressierungsfeld verarbeitet wird.
- Das **VCI (Virtual Channel Identifier)** Feld dient zur Kennzeichnung der Virtuellen Kanäle. Zellen, die zur selben Virtuellen Verbindung gehören, werden durch die gleichen Werte sowohl im VPI Feld als auch im VCI Feld gekennzeichnet.
- Das **PTI (Payload Type Identifier)** Feld wird zur Unterscheidung verschiedener Zellentypen, wie z. B. Zellen mit Nutzdaten, Leerzellen, Signalisierungszellen oder Ressource-Managementzellen zur Verkehrskontrolle verwendet.
- Das **CLP (Cell Loss Priority)** Bit setzt die Priorität der Zellen fest.
- Das **HEC (Header Error Control)** Feld ermöglicht unter Verwendung eines festgelegten Generatorpolynoms die Identifizierung von Zellen mit fehlerhaftem Zellenkopffeld, wobei ein einzelner Bitfehler korrigiert werden kann. Zusätzlich wird das HEC Feld zur Synchronisierung der Zellen verwendet.

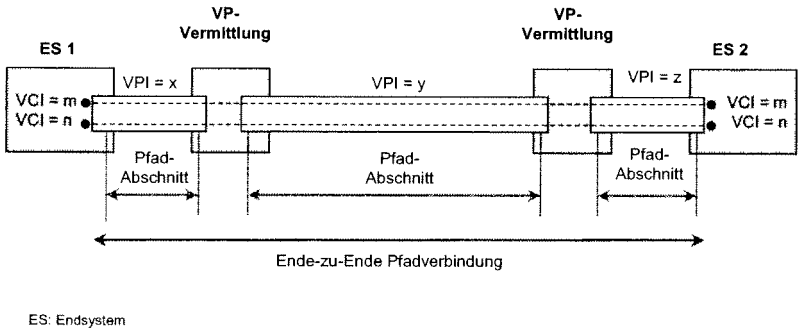


Bild: ATM virtuelle Pfade

Die Virtuellen Verbindungen zwischen den Netzelementen werden im Kopffeld durch die Werte im VPI Feld und im VCI Feld eindeutig festgelegt.

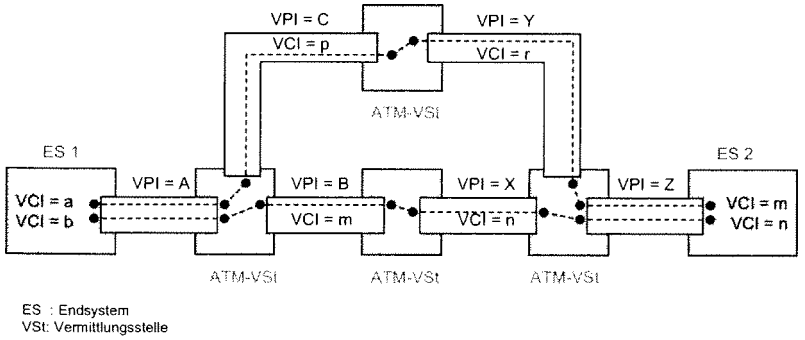
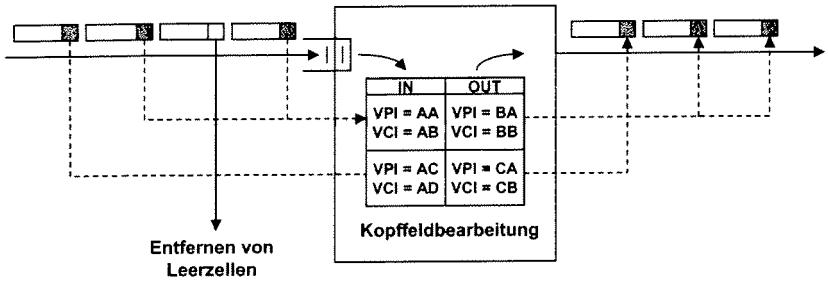


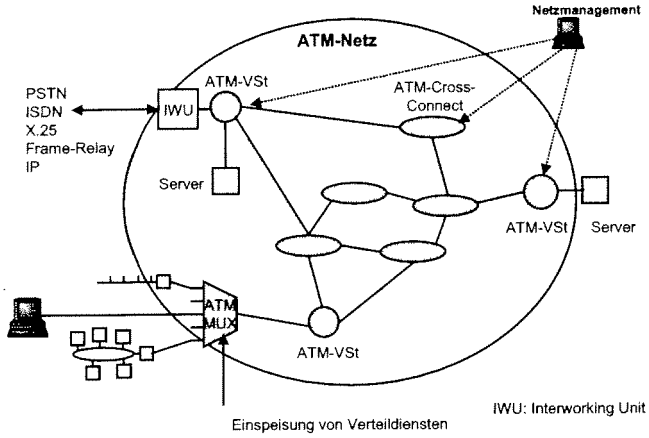
Bild: ATM virtuelle Kanäle und Pfade

Die Ursprungsadresse und die Zieladresse werden in der Verbindungsaufbauphase zur Festlegung einer Virtuellen Verbindung verwendet. Für jede Übertragungsrichtung muss eine eigene Virtuelle Verbindung festgelegt werden. Dadurch ist eine individuelle Ressourcenzuteilung möglich, die z.B. bei asymmetrischem Datenverkehr wichtig ist.



Für jeden Übertragungsabschnitt wird sowohl ein Virtueller Pfad als auch ein Virtueller Kanal durch VPI und VCI Werte festgelegt. Diese Werte werden in den Netzelementen in tabellarischer Form gespeichert und erst bei Verbindungsauflösung wieder gelöscht. Unter Verwendung dieser Tabellen erfolgt die Verkehrslenkung der Zellen.

Bild: Vermittlung der ATM-Zellen

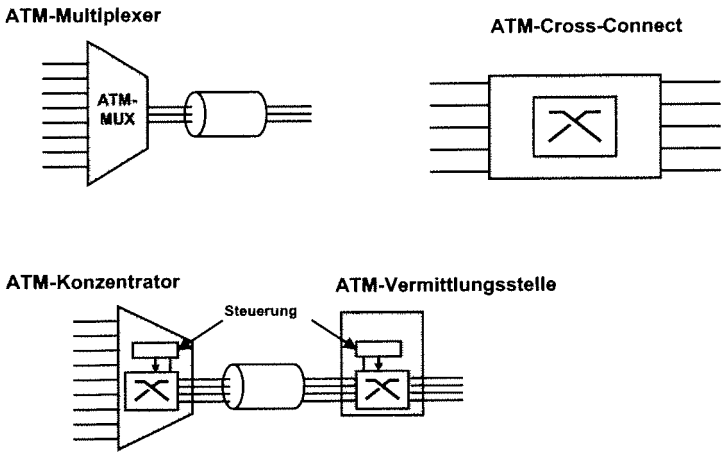


Im Bild sind die B-ISDN Netzelemente dargestellt:

- ATM Multiplexer
- ATM Cross-Connects
- ATM Vermittlungsstellen
- Netz der Synchronen Digitalen Hierarchie (SDH)
- Kontrolleinheit der Verkehrsmanagementnetzes (Traffic Management Network, TMN)

ATM Backbonenetze werden durch die ATM Cross-Connects und die ATM Vermittlungsstellen, sowie das Leitungsnetz gebildet.

Bild: ATM Netzelemente



Die physikalische Übertragung auf dem Leitungsnetz beruht auf dem Verfahren der Synchronen Digitalen Hierarchie (SDH). Im Gegensatz zu ATM Cross-Connects können SDH Cross-Connects die Köpfe der ATM Zellen nicht interpretieren, sondern nur die speziellen Transporteinheiten der SDH verarbeiten.
Im ATM Anschlussnetz werden die Endeinrichtungen und die privaten Netze (Local Area Network, LAN) über ATM Multiplexer mit der nächstliegenden ATM Vermittlungsstelle verbunden.

Bild: Netzelemente

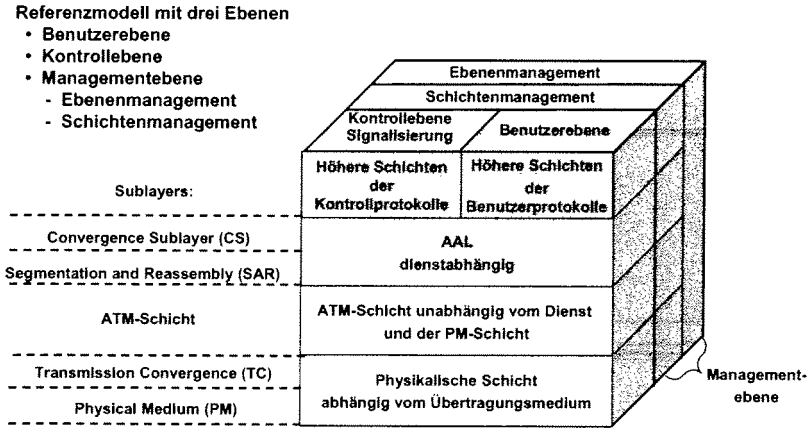


Bild: ATM-Referenzmodell

Die Dienstklassen werden durch die folgenden Eigenschaften beschrieben:
Zeitbezug zwischen Sender und Empfänger (Begrenzung der Verzögerung, Echtzeitverfahren),

- variable Bitrate: (Die Daten werden in veränderlichen Verkehrsmustern gesendet, Multimediaverkehr),
- konstante Bitrate: (Sprachverkehr, unkomprimierte Videoübertragung),
- Verbindungsart: verbindungsorientierter Dienst, verbindungsloser Dienst.

Dienstklasse	Klasse A	Klasse B	Klasse C	Klasse D
Synchronisation zwischen Endgeräten	erforderlich		nicht erforderlich	
Bitrate	konstant	Variabel		
Kommunikationsart	verbindungsorientiert			verbindungslos
Diensttyp	Typ 1	Typ 2	Typ 3/4	
			Typ 5	

Bild: ATM: Dienstklassen und Diensttypen

Es gibt die folgenden Dienstklassen:

- **Klasse A:** konstante Bitrate, Zeitbezug notwendig, verbindungsorientiert,
- **Klasse B:** variable Bitrate, Zeitbezug notwendig, verbindungsorientiert,
- **Klasse C:** variable Bitrate, Zeitbezug nicht nötig, verbindungsorientiert,
- **Klasse D:** variable Bitrate, Zeitbezug nicht nötig, verbindungslos.

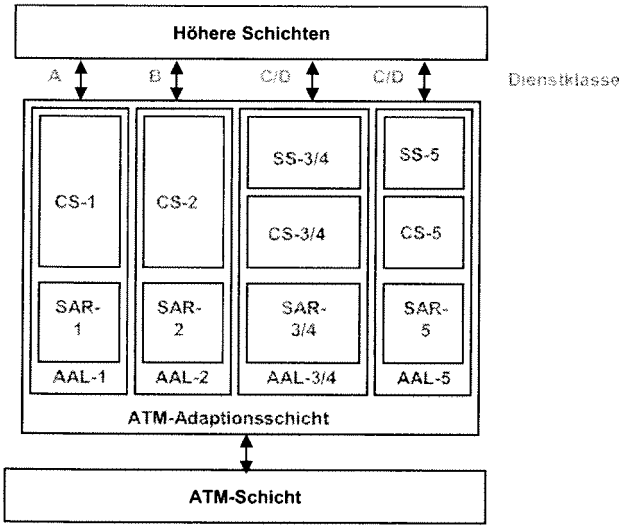


Bild: Aufbau der ATM-Adaptionsschicht

Die Aufgaben der ATM Anpassungsschicht (AAL, ATM Adaptation Layer) sind Protokolldateneinheiten der höheren Schicht auf einen ATM Zellenstrom und der Ausgleich der durch Verzögerungen folgenden unterschiedlichen Zellenlaufzeiten.
Die AAL Schicht gliedert sich in die Segmentierungsschicht und die Reassemblierungsschicht (Segmentation and Reassembly, SAR) sowie die darüber liegende Konvergenzschicht (Convergence Sublayer, CS). Die Konvergenzschicht wird weiters in eine allgemeine Konvergenzschicht (Common Part Convergence Sublayer, CPCS) und eine dienstspezifische Konvergenzschicht (Service Specific Convergence Sublayer, SSCS) gegliedert.
In der SAR Schicht werden die Protokolldateneinheiten auf den ATM Zellenstrom abgebildet und umgekehrt. Die CS Schicht bietet nach außen keine Zugangspunkte an und erfüllt dienstabhängige interne Aufgaben.
Die spezifischen Elemente der ATM Anpassungsschicht (AAL) befinden sich im Informationsfeld der ATM Zellen und sind dienstabhängig definiert

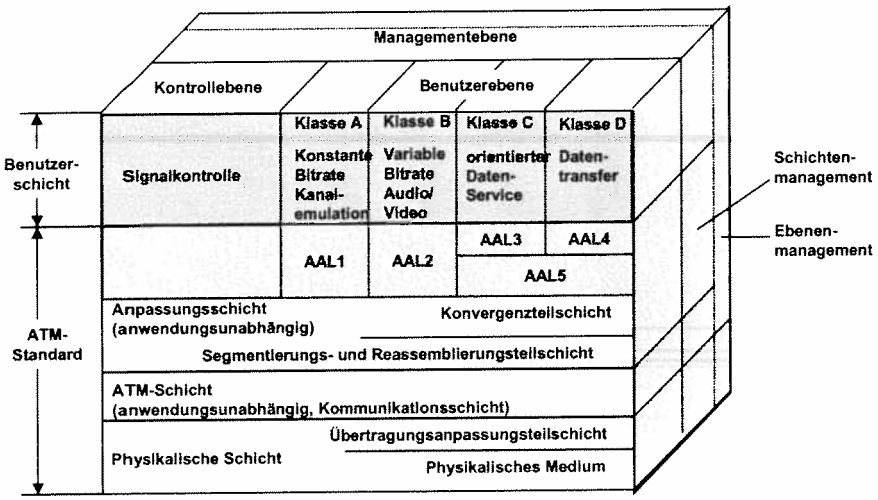


Bild: B-ISDN-Referenzmodell

Der **AAL-1 Dienstyp** unterstützt die Datenübertragung mit konstanter Bitrate. Die ATM Zellen werden nummeriert mit SN (4 Bits). SNP dient zur Prüfung von SN. Ferner werden eine Strukturinformation zur Unterstützung der Zusammenfassung von Bits zu Bitgruppen und eine Statusinformation hinzugefügt

Der **AAL-2 Diensttyp** dient zur Übertragung von zeitkontinuierlichen Nutzdaten mit variabler Bitrate. Die ATM Zellen werden ebenfalls nummeriert. CT gibt der verwendete Zellentyp an. Es gibt ferner ein Length Indicator und ein CRC.

Der **AAL-3/4 Diensttyp** unterstützt den Datendienst im traditionellen Sinn mit variabler Bitrate ohne Zeitbeziehung zwischen Sender und Empfänger. Der Segmenttyp gibt an, welche Position der Nachricht die ATM-Zelle überträgt: BOM (Beginn of Message), COM (Continuation of Message), EOM (End of Message) oder SSM (Single Segment Message). MID identifiziert die Nachricht.Es gibt ferner ein Length Indicator und ein CRC.

Der **AAL-5 Dienstyp** ist dem AAL-3/4 Typ sehr ähnlich. Der Aufbau einer PDU ist beim AAL-5 Typ jedoch vereinfacht.

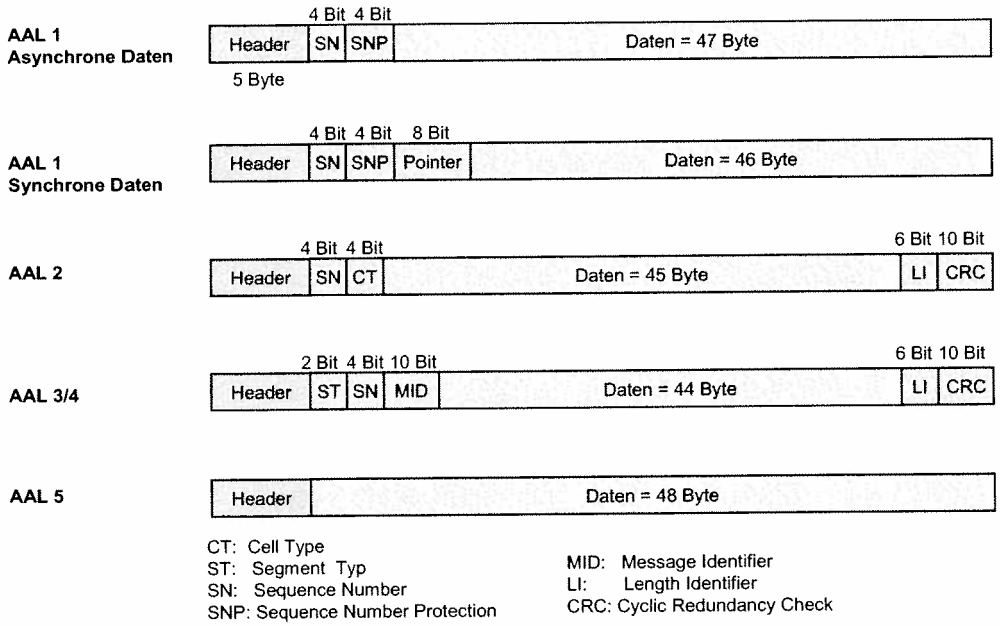


Bild: ATM Zellenstruktur

Signalisierungsverfahren

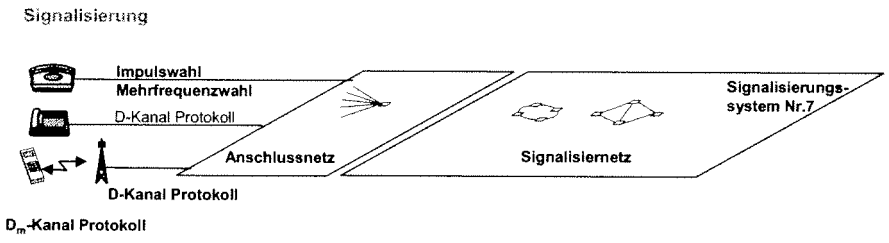
Signallisierung (Zeichengabe, signaling oder signalling) ist der Austausch alter Informationen, die zum Aufbau, zur Überwachung und zum Abbau von Verbindungen in einem Telekommunikationsnetz erforderlich sind.

Diese Aufgabe wird kurz als Call Control oder Connection Control (CC) bezeichnet. Die Signalisierung kann grundsätzlich auf zwei verschiedene Arten realisiert werden:

- **In-Band-Signalisierung** (In band signaling, auch CAS: Channel Associated Signaling): Die Signalisierungsinformation wird im gleichen logischen Kanal übertragen wie das Nutzsignal. In-Band-Signalisierung ist das ältere Verfahren.
- **Außer-Band-Signalisierung** (Out of Band Signaling, CCS: Common Channel Signaling, Zentralkanalzeichengabe): Die Signalisierungsinformation wird in einem anderen logischen Kanal (andere Frequenz, anderer Zeitschlitz/Zeitlage) übertragen als das Nutzsignal. Der Signalisierungskanal steht einer Vielzahl von Nutzkanälen zur Verfügung. Außer-Band-Signalisierung ist das modernere Verfahren, das den Vorteil einer höheren Flexibilität aufweist.

Signaling bezeichnet im Englischen auch die Leitungscodierung bzw. die Übertragung des Leitungssignals, also etwas anderes als Signalisierung im Sinn von Zeichengabe.

Die Signalisierung im Zugangsnetz **(Teilnehmersignalisierung)** und im Verbindungsnetz **(Netzsignalisierung)** sind klar zu unterscheiden. Für die **Ende-zu-Ende-Signalisierung** werden beide Signalisierungen benötigt.



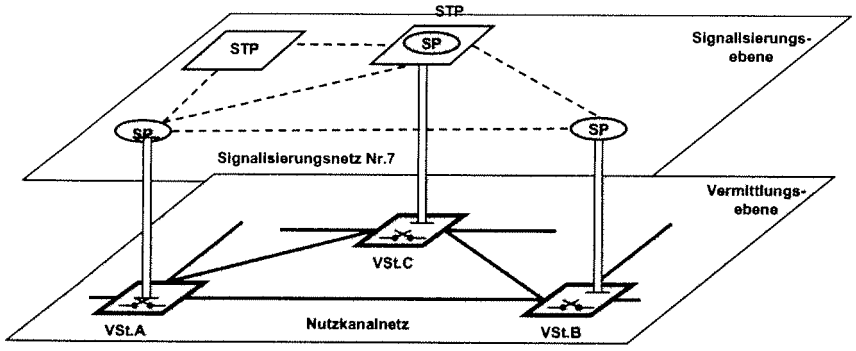
Teilnehmer Signalisierung
- Analoge Teilnehmer: Impulswahl, Mehrfrequenzwahl
- ISDN Teilnehmer: D-Kanal Protokoll
- GSM Teilnehmer: D_m-Kanal Protokoll

Netzsignalisierung
SS7 Signalling System Number 7
SIP Session Initiation Protocol

Bild: Netztechnolgien – Signalisierung

Einige verbreitete Signalisierungsverfahren sind

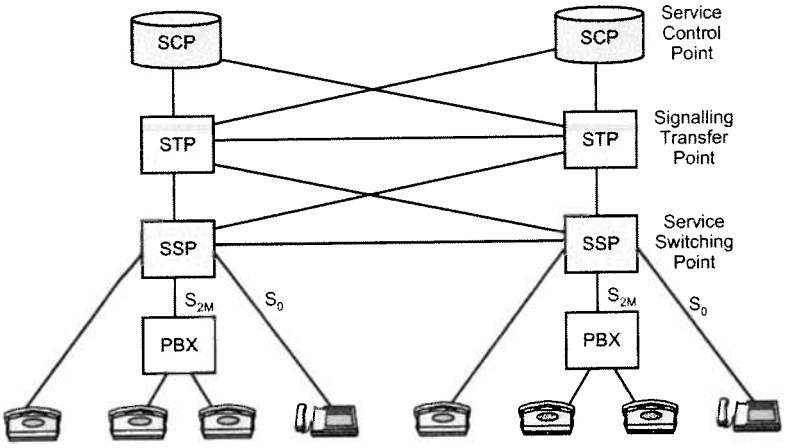
- **DTMF** (Dual Tone Multiple Frequency) bzw. MFV (Mehrfrequenz-Wahlverfahren) dienen zur Signalisierung an der Teilnehmerschnittstelle in Telefonnetzen. Dabei werden Ziffern (Hexadezimalziffern) als Summe zweier Sinusschwingungen bestimmter Frequenz dargestellt. DTMF ist eine In-Band-Signalisierung.
- **DSS1** (Digital Signalling System No. 1) wird bei ISDN für die Signalisierung im D-Kanal verwendet und kurz auch als Euro-ISDN bezeichnet.



VSt. Vermittlungsstelle
SP Signalling Point
STP Signalling Transfer Point

Bild: Signalisierungssytem Nr. 7

Signalisierungssystem Nr .7 (SS7)
Es bezeichnet ein modulares digitales Signalisierungssystem, das auf der Trennung der Übertragung von Nutzinformationen und Kontrollinformationen (Zeichengabe) aufbaut. Das so entstehende Netz nur für Signalisierungsinformationen ist prinzipiell ein Overlay-Netz. SS7 wird in allen neueren Telekommunikationssystemen eingesetzt (ISDN, GSM).



SP - Signalling Point
SCP - Signalling Control Point
STP - Signalling Transfer Point

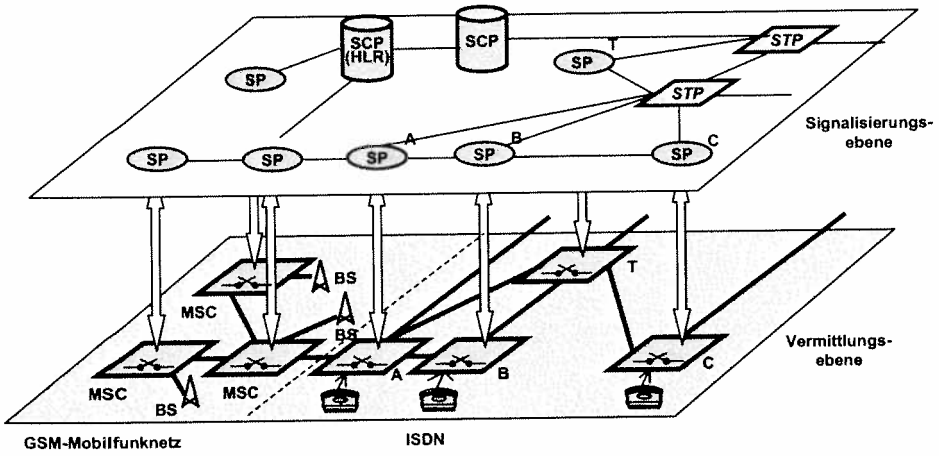
Bild: Signalisierungssystem 7 (SS7)

Ziel bei der Entwicklung von SS7 war ein universeller Einsatz in analogen Netzen, im ISDN, in Mobilfunknetzen sowie die Unterstützung des IN (Intelligenten Netzes) und von Netzmanagementaufgaben (TMN - Telecommunication Management Network). Ein solches Signalisierungsnetz wird betrachtet als eine Menge von Signalisierungspunkten (Signalling Points, SP) (Bild 8), die über Signalisierungsverbindungen (Signalling Links, SL) in Verbindung stehen. SPs sind dabei die digitalen Vermittlungsstellen in dem entsprechenden Netz. Sie sind durch eine eindeutige Identifizierungsnummer im SS7-Netz eines Betreibers gekennzeichnet. Über diese Nummer kann der SP eindeutig referenziert werden.

- **SSP**
  - Interface des Benutzers zum Transportnetz
  - Erzeugen und Übersetzen von SS7-Signalisierungsnachrichten
  - Wegewahl
  - Durchführen von Datenbankabfragen
- **STP**
  - Routing von Signalisierungsnachrichten, aber kein Erzeugen
  - Übersetzen von länderspezifischen Signalisierungsnachrichten
  - Statistiken für Operations and Management (OAM) und Billing
- **SCP**
  - Interface zur Datenbank
    - Business Services
    - Call Management Services
    - Line Information
    - Home/Visitor Location Register

Bild: SS7-Komponenten

Teilweise müssen Strecken von einem SP zu einem zweiten SP über einen dritten geführt werden. Dieser wird dann als Signalling Transfer Point (STP) bezeichnet und ist normalerweise im Fernnetz zu finden. SPs, an denen Verbindungen im SS7-Netz nur enden oder beginnen, werden mit Signalling Points (SP) bezeichnet.



GSM - Global System of Mobile Communication
MSC - Mobile Switching Center
BS - Base Station
ISDN - Integrated Services Digital Network

SP - Signalling Point
SCP - Signalling Control Point
STP - Signalling Transfer Point

Bild: Netzstruktur von GSM-Netzen

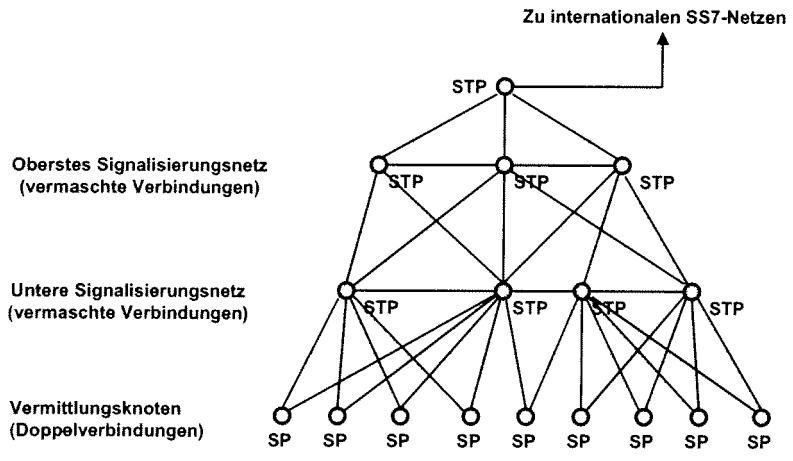
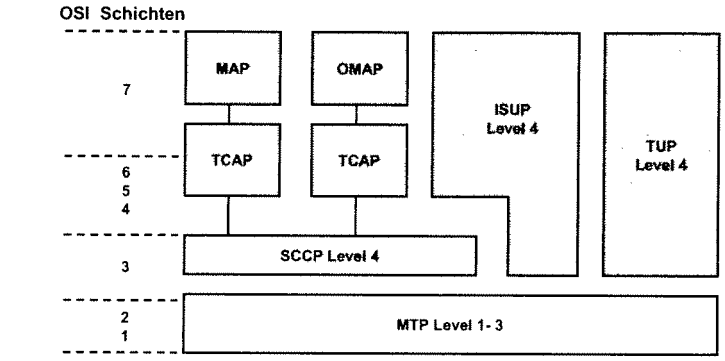


Bild: SS7 Netzstruktur



OMAP - Operation, Maintenance and Administration Part
MAP - Mobile Application Part
TCAP - Transaction Capabilities Application Part
SCCP - Signaling Connection Control Part
ISUP - ISDN User Part
TUP - Telephone User Part
MTP - Message Transfer Part
OSI - Open Systems Interconnection

Bild: Protokollarchitektur im SS7

In der Telefonie wird (wie auch z.B. in GSM) das Signalisierungs-System SS7 (Signalling System No. 7, auch SS#7) verwendet.

SS7 ist als Overlay-Netz aufgebaut, d. h., es ist physisch, nicht nur logisch, getrennt von den Nutzkanälen.

- **MTP-1, MTP-2, MTP-3** (Message Tranger Part): Diese Schichten sind für die Übertragung von SS7-Nachrichten zuständig und entsprechen in ihrer Funktion weitgehend den allgemeinen OSI-Schichten 1-3.
- **SCCP** (Signal Connection Control Part): entspricht dem oberen Teil der OSI-Schicht 3 und erlaubt den Austausch von Daten ohne Nutzkanalbezug und eine Ende-zu-Ende-Signalisierung.
- **TCAP (Transaction Capabilities Application Part) :** stellt Möglichkeiten zur Kontrolle von Transaktionen zwischen räumlich verteilten Anwendungen zur Verfügung
- **ISUP (ISDN User Part)** für die Nutzung im ISDN von Diensten und Dienstmerkmalen, die sich aus der Integration von Telefon- und Datendiensten ergeben. Mit ISUP werden Daten für Auf-, Abbau und Überwachung von leitungsvermittelten B-Kanalverbindungen zwischen den Knoten im ISDN übertragen.
- **TUP (Telephone UP)** für die Nutzung des Fernsprechdienstes.
- **MAP (Mobile AP)** für die Anwendung in Mobilfunknetzen, die ein SS7-konformes Netz haben (z.B. GSM).
- **OMAP (Operation and Maintenance AP)** für die Durchführung von Netzmanagementaufgaben. Es werden Daten zum Auf- und Abbau von Signalisierungsverbindungen übertragen, ebenso Daten für das Routing oder zur Messung des Verkehrs.

Grundlegendes Konzept ist die Teilung von SS7 Funktionen in für alle Anwendungen gleiche Message Transfer Parts (MTP, untere drei Schichten) und anwendungsspezifische User Parts (UP, obere Schicht), wobei der Term 'User' sich auf eine SS7 nutzende Instanz im Netz und nicht auf den Fernsprechteilnehmer bezieht (Instanz - das aktive Element einer Schicht. Kann in Software oder Hardware realisiert werden; engl. entity).
MTP stellt dabei ein allgemeines Transportsystem für die Daten der UPs zur Verfügung. UP-Daten dienen der Kontrolle von Nutzkanälen und den damit verbundenen, grundlegenden Funktionen der Dienstmerkmale. Die drei Schichten von MTP

entsprechen weitgehend den drei unteren Schichten des OSI-Referenzmodells (Schicht 3 nur teilweise).

Daten ohne Nutzkanalbezug können im SS7-Netz ausgetauscht werden, indem MTP um den Signalling Connection Control Part (SCCP) ergänzt wird. Mit dem SCCP können Adressen aus anderen Netzen ohne SS7-Signalisierung und entsprechendes Adressformat transportiert werden. SCCP entspricht dem oberen Teil von Schicht 3 im OSI Referenzmodell.

Alle APs greifen dabei zunächst auf einen **TCAP (Transaction Capabilities Application Part)** zurück. TCAP setzt auf SCCP auf und stellt Möglichkeiten zur Kontrolle von Transaktionen zwischen räumlich verteilten Anwendungen zur Verfügung.

SCCP (Signalling Connection Control Part) kontroliert Signalisierungsverbindungen und ist derart flexibel konfiguriert, um nahezu beliebige Daten verbindungslos oder -orientiert übertragen zu können. Hierzu gehört die Ende-zu-Ende-Signalisierung (z.B. Dienstewechsel während einer bestehenden Verbindung) oder der Austausch von Daten zwischen HLR und VLR im GSM.

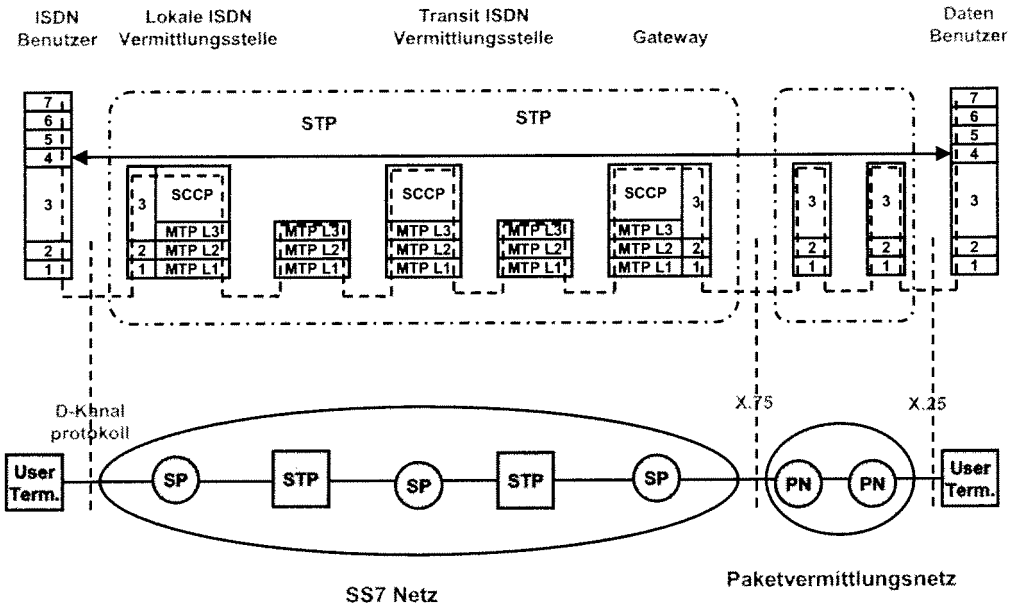
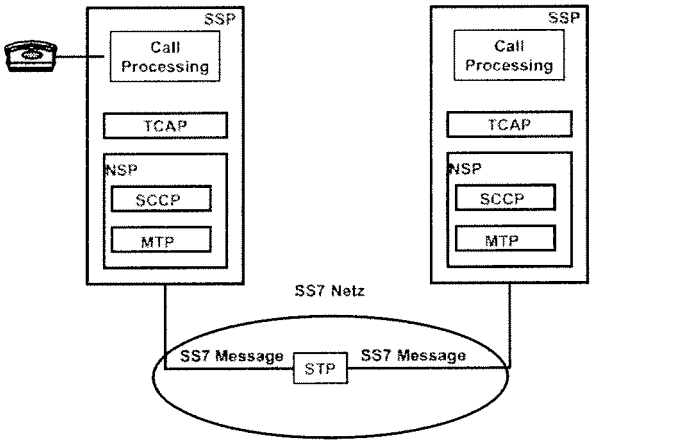


Bild: Beispiel einer Ende-zu-Ende Signalisierung



SSI: Service Script Interpreter
STP: Signal Transfer Point
SCP: Service Control Point
SSP: Service Switching Point

MTP: Message Transfer Part
NSP: Network Service Part
SCCP: Signaling Connection Control Part
TCAP: Transaction Capabilities Application Part

Bild: Meldungsaustausch

Abkürzung	Bezeichnung	Bedeutung
IAM	Initial Address Message	Anforderung einer Verbindung, enthält die Adressinformationen komplett oder zumindest teilweise
SAM	Subsequent Address Message	Enthält weitere Adressinformationen
ACM	Address Complete Message	Quittung in Rückrichtung über vollständige Adressinformation
CPG	Call in Progress	Ruf wird bearbeitet
ANM	Answer Message	Gerufener Teilnehmer hat sich gemeldet, Nutzverbindung ist aufgebaut
REL	Release	Anforderung eines Dienstewechsels
RLC	Release Complete	Quittierung der Verbindungsauslösung
SUS	Suspend Message	Dienstewechsel nach Timer-Auslauf
FIN	Facility Information	Information über mögliche Dienste und Dienstmerkmale
FACD	Facility Accepted	Positive Quittung über Dienstewechsel

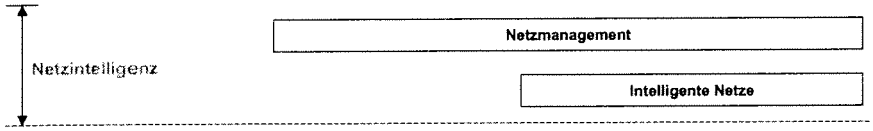
Tabelle: Wichtigste ISUP-Meldungen

Abkürzung	**Bedeutung**
Dialog Handling Primitive	
TC-BEGIN	**Beginn eines Dialogs**
TC-CONTINUE	**Fortsetzung eines Dialogs**
TC-ABORT	**Abbrechen eines Dialogs**
TC-END	**Ende eines Dialogs**
Component Handling Primitive	
TC-INVOKE	**Anforderung von Nutzinformation**
TC-RESULT-NL	**Übergabe von (Teil)-Ergebnissen als Antwort auf eine Anfrage, es folgen weitere Informationen (-NL: not last).**
TC-RESULT-L	**Übergabe von Ergebnissen als Antwort auf eine Anfrage, keine weiteren Informationen (-L: last)**

Tabelle: Wichtigste TCAP-Primitive

Abkürzung	Bezeichnung	**Bedeutung**
UDT	Unitdata	**Nutzdaten der Protokollklassen 0 od. 1**
CR	Connection Request	**Anforderung einer Ende-zu-Ende-Signalisierungsverbindung der Protokollklasse 2 oder 3**
CC	Connection Confirm	**Bestätigung der Signalisierungsverbindung**
DT1	Data Form 1	**Nutzdaten der Protokollklasse 2**
DT2	Data Form 2	**Nutzdaten der Protokollklasse 3**
AK	Data Acknowledgement	**Quittierung für Nutzdaten der Klasse 3**
RLSD	Released	**Auslösung der Signalisierungsverbindung**
RLC	Release Complete	**Quittierung der Auslösung**

Tabelle: Wichtigste SSCP-Meldungen



Netzmanagement
- SNMP Simple Network Management Protocol
- TMN Telecommunication Management Network
- TINA Telecommunications Information Networking Architecture

Netzintelligenz
IN Intelligent Network

Bild: Netzmanagement und Netzintelligenz

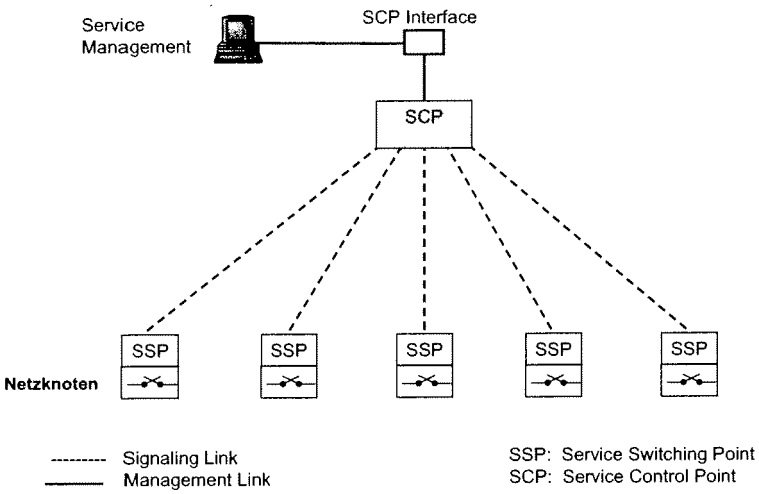


Bild: Intelligentes Netz (IN)

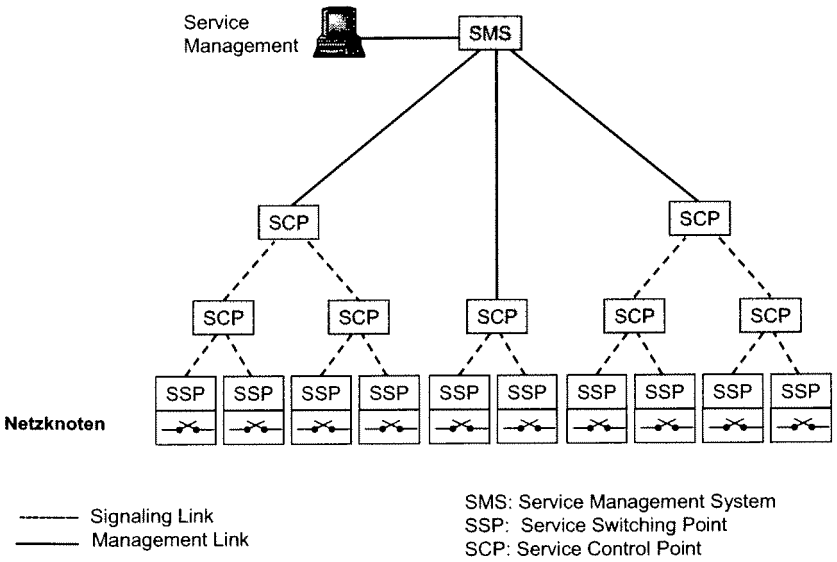


Bild: Hierarchisches intelligentes Netz

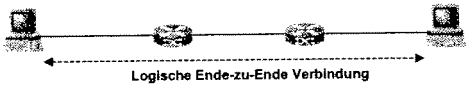
2.4 OSI-Referenzmodell: Schicht 4 - Transport

Version: Dez. 2003

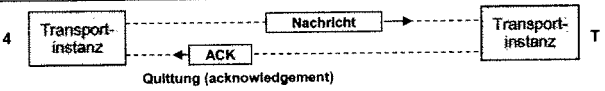
Inhalt

- Aufgaben, Funktionen und Dienste
- Dienstelemente
- Dienstqualität (Quality-of-Service)
- Transportprotokoll
- Verbindungsverwaltung
- Fehlererkennung und Fehlerkorrektur
- Ende-zu-Ende Flusskontrolle

Die **Transportschicht** stellt den miteinander kommunizierenden Endknoten eine Ende-zu-Ende-Verbindung zur Verfügung. Diese wird als transparent bezeichnet, da sie die Eigenschaften des dazwischen liegenden Netzes verbirgt. Sie stellt den zuverlässigen Transport von Nachrichten (Paketfolgen) zwischen zwei Endsystemen sicher.



Ziel:
Gesteuerte Übermittlung von Nachrichten zwischen Endsystemen



Aufgaben:

1) Auf- und Abbau der Schicht-4 Verbindung
2) Übertragung von Schicht-4 Datenblöcken
3) Reihenfolgeerhaltung
4) Flusskontrolle
5) Fehlersicherung

Schicht 4: Transportschicht
(T: Transport)

Die Transportschicht erweitert Endsystemverbindungen zu Verbindungen von Transportanwendungen. Unter einer Transportanwendung ist eine Zuordnung zwischen einer Anwendungsinstanz, einer Darstellungsinstanz und einer Sitzungsinstanz zu verstehen. Die Transportschichtverbindung ist, wie alle Schichtverbindungen darüber, eine logische Ende-zu-Ende Verbindung. Sie ermöglicht ähnliche Aufgaben wie sie auch die Schichten 2 und 3 abschnittsweise durchführen können, nämlich Reihenfolgeerhaltung, Flusskontrolle und Fehlersicherung

Bild: Schicht 4 : Transportschicht

Aufgaben der Transportschicht

Die Transportschicht bildet den Mittelpunkt eines Protokollstapels. Sie setzt auf der Vermittlungsschicht auf und ist die oberste Schicht des Transportsystems (zu dem die Schichten 1 bis 4 zählen). Die Transportschicht arbeitet nur mit Endsystemen und abstrahiert von den Details des darunter liegenden Netzes. Die Vermittlungsschicht steht unter der Kontrolle des Netzbetreibers, der Anwender hat keinen Einfluss auf sie. Die Transportschicht kümmert sich um Probleme, die von der Vermittlungsschicht nicht behandelt werden. Dazu gehören die Überbrückung von Ausfällen der Vermittlungsschicht und Nachlieferung von Paketen, die in der Vermittlungsschicht verloren gegangen sind. Die Transportschicht kann beliebig lange Nachrichten übertragen. Eine (lange) Nachricht wird in Segmente unterteilt, die als einzelne T-PDUs übertragen werden. Beim Empfänger werden die Segmente wieder zur ursprünglichen Nachricht zusammengesetzt.

(1) Auf- und Abbau von Transportverbindungen

Verbindungsaufbauphase:

- Aussuchen einer Netzverbindung
- Entscheidung über Notwendigkeit von Multiplexing oder Splitting
- Festlegung der optimalen Größe der Transport-Protokolldateneinheit
- Abbildung von Transportadressen auf Netzadressen
- Identifikationen der einzelnen Transportverbindungen

Verbindungsabbauphase

- Identifizierung der abgebauten Verbindung
- Information über Grund des Abbaus

Bild: Funktionen der Transportschicht

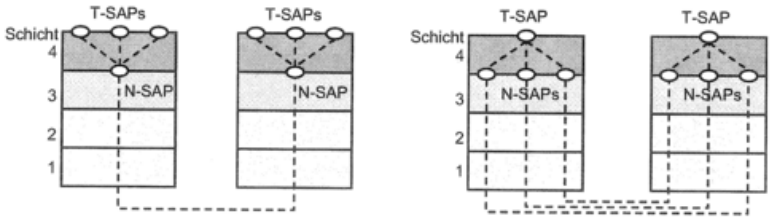
(2a) Abbildung von Transportadressen auf Netzadressen
- Eine eindeutige Identifizierung der entfernten Instanz der Sitzungsschicht mit der Transportverbindung muss durch ihre Transportadresse aufgebaut werden

(2b) Multiplexing von Transportverbindungen auf Netzverbindungen
- Optimierung der Auslastung der Netzverbindungen
- Abbildung Transportverbindung auf Netzverbindung muss nicht 1 :1 sein, sowohl Abbildungen n :1 (Multiplexing) als auch 1 : n (Splitten) ist erlaubt

Multiplexing: mehrere Transportverbindungen zwischen zwei Endsystemen können auf eine Netzverbindung abgebildet werden
Eine besseren Auslastung der Netzverbindung ist sinnvoll, weil in vielen Netzen Gebühr für Anzahl der aufgebauten Netzverbindungen bezahlt werden muss
Inverser Vorgang: **Demultiplexing**

Vertelen, Splitting: eine Transportverbindung nutzt mehrere Netzverbindungen damit auch bei Ausfall einer Netzverbindung die Kommunikation über die übrigen Verbindungen weitergeführt werden kann -> Verfügbarkeit der Transportverbindung wird erhöht
Inverser Vorgang: **Kombinieren, Recombining**

Bild: Funktionen der Transportschicht



Multiplexen/Demultiplexen

Multiplexen von T-Verbindungen über eine N-Verbindung

Verteilen/Kombinieren

Verteilen einer T-Verbindung über mehrere N-Verbindungen

Bild: Logische Transportverbindungen

(2c) Ende-zu-Ende Blocking, Segmentierung und Konkatenierung

- **Blockenformung, Blocking**
  - Zur Optimierung der Netzauslastung werden eine Anzahl von T-SDUs zu einer T-PDU zusammengefaßt. Inverser Vorgang: **Deblocking**
- **Segmentierung**
  - Aufteilen einer (langen) T-SDU in mehrere T-PDUs
  - Inverser Vorgang: **Zusammensetzen (Reassembly)**
  - Blocking und Segmentierung nur für Dateneinheiten derselben Transportverbindung
- **Konkatenierung**
  - Zusammenfassung der T-PDUs verschiedener Transportverbindungen zu einer Netz-Dienstdateneinheit (Network Service Data Unit, N-SDU)
    Inverser Vorgang: **Separation**

Unterschied zwischen Konkatenieren und Multiplexing:
keine dauerhafte Assoziation zwischen Transport- und Netzverbindung

Bei einem Datenaufkommen der Transportschicht aus kurzen Nachrichten mit langen Zwischenzeiten (z.B. Dialog-Anwendung) ist Konkatenierung dem Blocking überlegen, weil zu große Wartezeit beim Blockenformung von T-SDUs zu einer T-PDU entstehen.

Bild: Funktionen der Transportschicht

(2d) Datenübertragungsphase über die Transportverbindungen

(Funktionen abhängig von ausgehandelter Transportdienstklasse)

- Reihenfolgesicherung	- Flusskontrolle
- Blocking	- Fehlererkennung
- Segmentierung	- Fehlerbehebung
- Konkatenierung	- beschleunigte Datenübertragung,
- Multiplexing/Splitting	- Identifikation der Transportverbindung

Beschleunigte Übertragung von T-SDUs
Wird hauptsächlich zur Übertragung dringender Daten des Netzmanagement verwendet

Bild: Funktionen der Transportschicht

(3) Ende-zu-Ende Reihenfolgeerhaltung

- Transportschicht stellt Ende-zu-Ende Verbindung her
- Pakete können sich in Teilnetzen überholen bzw. verlorengehen
  ---> Reihenfolgeerhaltung muss sichergestellt werden
- Pakete bekommen vom Sender Sequenznummern zugeordnet
- Funktion kann in Transportschicht entfallen, wenn das unterliegendes Netz die reihenfolgetreue Auslieferung der Pakete garantiert

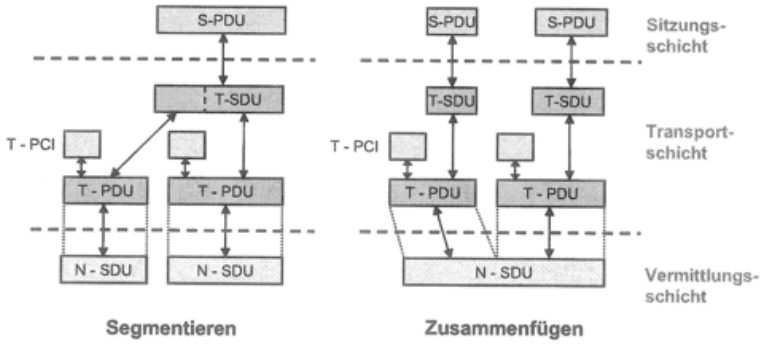
Bild: Funktionen der Transportschicht

(4) Ende-zu-Ende Flusskontrolle

- **Auswirkung von Multiplexing auf Datenfluss:** hohe Last einer Transportverbindung hat Auswirkungen auf alle anderen Transportverbindungen
- Problem durch lokale Flusskontrolle an Schnittstellen Sitzungsschicht/Transportschicht oder Transportschicht/Netzschicht nicht lösbar, da Rückwirkungen auf andere Verbindungen:
  - Instanz der Sitzungsschicht lehnt von Transportschicht übergebenes Paket wegen vollen Empfangspuffers ab
  - Paket muss von entfernter Transport-Instanz nochmals gesendet werden
  - Last steigt

daher: Flusskontrolle zwischen beiden Transport-Instanzen, z.B. durch explizite Empfangsbestätigungen.

Bild: Funktionen der Transportschicht



PDU Protocol Data Unit
SDU Service Data Unit
PCI Protocol Control Information

Bild: Zusammenfügen/Segmentieren

(5a) Ende-zu-Ende Fehlererkennung

- Sequenznummern zur Erkennung von fehlenden oder duplizierten Paketen
- zusätzlich: Sicherung gegen Übertragungsfehler, z.B. durch Bilden einer Prüfsumme **(Prüfsumme, Checksum, Cyclic Redundancy Check, CRC)**
- Überwachung und Sicherstellung der ausgehandelten Dienstgüte, z.B. durch Umschalten von einer stark gestörten Netzverbindung auf eine andere

(5b) Ende-zu-Ende Fehlerbehebung

- Versuch der Behebung von erkannten Fehlern, z.B. durch Verwendung fehlerkorrigierender Codes (Forward Error Correction, FEC)
  - wegen hoher Redundanz der Daten und Overheads weniger häufig
  - oder Anforderung wiederholter Sendung des gestörten oder verlorenen Paketes

Bild: Funktionen der Transportschicht

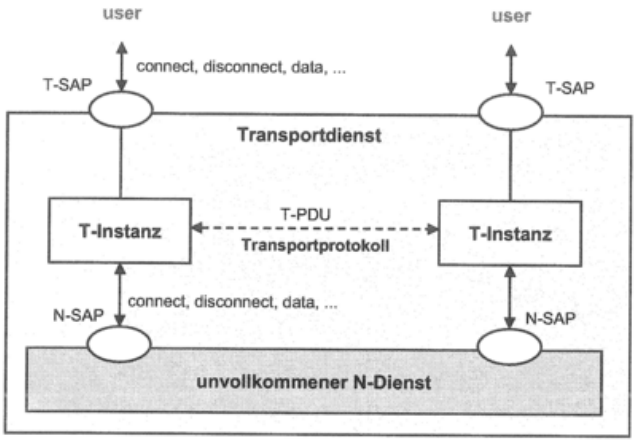


Bild: Der Transportdienst

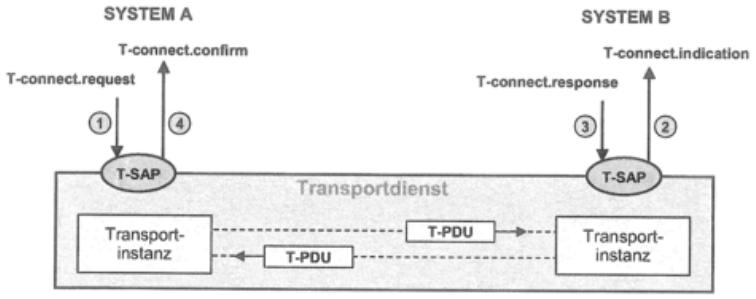


Bild: Der Transportdienst

(1) Aufbau einer Transportverbindung

- in Aufbauphase wird die Dienstgüte zwischen Instanzen der Sitzungsschicht und der Transportdienst ausgehandelt
- funktional unterschiedliche Klassen für Dienstgüte-Auswahl bestehen aus wählbaren und garantierten Parametern (z.B. maximaler Durchsatz, Übertragungsverzögerung)

(2) Abbau einer Transportverbindung

- beteiligte Instanz der Sitzungsschicht kann die Transportverbindung beenden, wobei die andere Instanz über die Beendigung benachrichtigt wird

Bild: Dienste der Transportschicht

(3) Datenübertragung

- Transportschicht muss Transport-Dienstdateneinheiten (Transport Service Data Units, T-SDUs) mit beliebiger Länge in Transport-Protokolldateneinheiten (Transport Protocol Data Units, T-PDUs) segmentieren können

Paketgrößen
In den diversen Datennetzen gibt es bestimmte Obergrenzen für maximal zulässige Paketgröße, z.B. durch begrenzte Größe der Puffer in Netzknoten

Effektivitätsgesichtspunkte
- bei Störung eines großen Pakets durch Übertragungsfehler gehen viele Daten auf einmal verloren
- bei Übertragung vieler kleiner Pakete steigt der Overhead durch Übertragung von Kontrollinformationen mit jedem Paket

Beschleunigte Übertragung
Die Transportschicht bietet auch beschleunigte Übertragung an

Bild: Dienste der Transportschicht

Verbindungsaufbaudauer: Dies ist die Zeitspanne von der Anforderung einer Transportverbindung bis zum Eintreffen der Bestätigung.
Der Parameter spezifiziert den maximal akzeptablen Wert dieser Zeitspanne.

Ausfallwahrscheinlichkeit beim Verbindungsaufbau: Anteil der fehlgeschlagenen Verbindungsaufbauversuche zur Summe aller Verbindungsaufbauwünsche.

Verzögerung beim Verbindungsabbau: Die Zeitspanne zwischen dem Auslösen eines Verbindungsabbaus durch den Transportdienstbenutzer und der tatsächlichen Trennung am entfernten Ende.

Durchsatz: Anzahl der Nutzbits, die pro Zeiteinheit erfolgreich übertragen werden. Der Durchsatz ist für jede Übertragungsrichtung getrennt zu ermitteln.

Übertragungsverzögerung: Zeitspanne von einem T-Data.request zu der entsprechenden T-Data.indication, also genau die Zeitspanne zwischen dem Absenden einer Nachricht durch den Transportdienstbenutzer auf dem Quellenknoten bis zum Eintreffen beim Transportdienstbenutzer auf dem Zielknoten. Auch hier sind zwei Werte für die beiden Übertragungsrichtungen zu unterscheiden.

Bild: Dienstgüte, Dienstqualität (quality of service)

Die **Dienstgüte** (Quality-of-Service) beschreibt die Qualitätsmerkmale, die ein Diensterbringer seinem Dienstnutzer zur Verfügung stellen kann.

Eine Aufgabe der Transportschicht besteht darin, die Dienstgüte der Vermittlungsschicht zu verbessern. Folglich führt eine gut funktionierende Vermittlungsschicht zu einer einfachen Transportschicht.

Restfehlerrate: Quotient der Summe aller fehlerhaften, verloren gegangenen oder duplizierten Pakete zur Summe aller übertragenen Pakete.

Fehlerquotient beim Transfer: Quotient aller fehlgeschlagenen Übertragungen zur Summe aller Übertragungsversuche in einem bestimmten Zeitraum.

Fehlerquotient beim Verbindungsabbau: Quotient der gescheiterten Verbindungsabbauwünsche zu der Summe aller Verbindungsabbauwünsche.

Schutz: Mechanismen zum Schutz der übertragenen Nachrichten gegen unerwünschte Manipulationen.

Priorität: Möglichkeit, vorrangige Verbindungen zuerst abzuwickeln und nachrangige entsprechend zu verzögern.

Robustheit (resilience): Mechanismen, dass die Transportschicht bei internen Problemen oder Überlastungen nicht spontan eine Verbindung auslöst, d. h. abbricht.

Bild: Dienstgüte, Dienstqualität (quality of service)

Bei einer fehleranfälligen Vermittlungsschicht muss die Transportschicht versuchen, dem Transportdienstbenutzer trotzdem eine akzeptable Dienstgüte anzubieten. Die Dienstgüte wird durch einzelne Dienstgütemerkmale beschrieben.

Die für diese Merkmale gewünschten Parameter können beim Verbindungsaufbau ausgehandelt werden. Falls die möglichen Werte der Parameter nicht akzeptabel sind, kann ein Verbindungsaufbau auch abgelehnt werden.

Elastische Anwendungen

- Hier sind keine Zeitgarantien für diese Auslieferung der Daten erforderlich.
- Die Verzögerungsabforderungen unterschiedlicher elastischer Anwendungen können stark variieren.
- Sie lassen sich dadurch charakterisieren, dass die Daten durch längere Verzögerungszeiten nicht unbrauchbar werden.

Die folgenden drei Kategorien werden unterschieden

- -Interaktiv
- - Interaktiv Bursts
- - Asynchron

Bild: Traditionelle Anwendungen

Verbindungsorientierte Dienstelemente der Transportschicht

T-Connect.request (callee, caller, exp-wanted, qos, user-data)
T-Connect.indication (callee, caller, exp-wanted, qos, user-data)
T-Connect.response (qos, responder, exp-wanted, user-data)
T-Connect.confirm (qos, responder, exp-wanted, user-data)
T-Disconnect.request (user-data)
T-Disconnect.indication (reason, user-data)
T-Data.request (user-data)
T-Data.indication (user-data)
T-Data-Acknowledge.request (user-data)
T-Data-Acknowledge.indication ( )
T-Expedited-Data.request (user-data)
T T-Expedited-Data.indication (user-data)

Verbindungslose Dienstelemente der Transportschicht

T-Unitdata.request (callee, caller, user-data)
T-Unitdata.indication (callee, caller, qos, user-data)

Bild: Dienstelemente der Transportschicht

Dienstelemente

Die Dienstelemente beinhalten Funktionen wie Verbindungsaufbau (CONNECT), Verbindungsabbau (DISCONNECT), Datentransfer (DATA) und beschleunigten Datentransfer (EXPEDITED-DATA) sowie Quittungen (DATA-ACKNOWLEDGE).

Diese Dienstelemente beziehen sich auf einen verbindungsorientierten Dienst. Ein verbindungsloser Dienst wird durch die Dienstelemente UNIDATA erbracht. Bei allen Dienstelementen kennzeichnet das vorangestellte T die Transportschicht mit den nachgestellten Angaben request, indication, response und confirm.

Der Aufwand für ein Transportprotokoll hängt wesentlich von der Qualität des darunter liegenden Vermittlungsdienstes ab. Zur Vereinfachung der Diskussion werden Vermittlungsdienste in drei **Qualitätsklassen (Netzklassen)** eingeteilt:

Auf Basis des OSI-Modells wird eine Familie von Transportprotokollen beschrieben, die aus fünf Klassen 0 bis 4 besteht. Die Klassen sind auf bestimmte Netztypen angepasst.

Protokoll-Klasse	Name	Netz-Typ
0	Einfachklasse	A
1	Basisklasse zur Wiederherstellung	B
2	Multiplexklasse	A
3	Klasse zum Wiederherstellen und Multiplexen	B
4	Klasse zur Fehlerbehandlung und Wiederherstellung	C

Netztyp A: vollständig ausreichende Qualität
B: verbesserungsbedürftig
C: nicht ausreichende Qualität

Bild: Transportprotokoll-Klassen

Typ A: hochwertiger, fast fehlerfreier Dienst ohne N-RESETs (N-RESETs können von der Netzschicht zur Problembehebung ausgelöst werden, dabei können Pakete verloren gehen). Einige LAN entsprechen dem Typ A. Transportprotokolle für Netze des Typs A sind einfach und leicht verständlich.

Typ B: perfekte Datenübertragung. aber mit N-RESETs. Die meisten X.25-Protokolle und WAN sind vom Typ B. Transportprotokolle für Netze des Typs B sind komplizierter als für Typ A.

Typ C: unzuverlässiger Dienst mit verlorenen und duplizierten Paketen und möglicherweise auch N-RESETs. WANs mit verbindungsloser Datagramm-Übertragung, Paket-Funknetze und viele Teilnetze des Internet sind vom Typ C. Die hierfür erforderlichen Transportprotokolle sind aufwändig und kompliziert.

Protokollklassen für OSI-Transportprotokolle

Protokollklasse	Netzklasse	Einsatzbereich
0	A	Einfaches Protokoll für Transportdienst über einem zuverlässigen, verbindungsorientierten Vermittlungsdienst (z. B, X.25). Bietet nur Verbindungsauf- und -abbau.
1	B	Wie Klasse 0, Transportverbindung bleibt bei kurzzeitiger Unterbrechung in der Vermittlungsschicht bestehen. Dazu sind Sequenznummern erforderlich. Keine Fehlerüberwachung oder Flusskontrolle.
2	A	Wie Klasse 0, jedoch mehrere Transportverbindungen über eine Verbindung der Vermittlungsschicht. Flusssteuerung möglich.
3	B	Kombination der Klassen 1 und 2: Behandlung von N-Resets und Mulliplexen. Flusskontrolle wird immer verwendet.
4	C	Aufwändiges Protokoll für Transportdienst über einem unzuverlässigen, verbindungslosen Vermittlungsdienst. Enthält alle Funktionen der Klasse 3, kümmert sich zusätzlich um verlorene, duplizierte und vertauschte Pakete.

Eine sinnvolle Kombination von Protokollen kann HDLC (Schicht 2), X.25 (Schicht 3) und ein Transportprotokoll der Klasse 1 sein. HDLC garantiert eine fast vollständige Fehlerkorrektur und Erhaltung der Rahmenreihenfolge. X.25 liefert eine fast fehlerfreie, virtuelle Verbindung mit korrekter Paketreihenfolge. Damit kann das Transportprotokoll sehr einfach sein und sich weitgehend auf den Verbindungsauf- und -abbau beschränken.

	Protokollklasse				
Funktionen	**0**	**1**	**2**	**3**	**4**
allgemeine Funktionen:					
T-PDU-Übertragung	x	x	x	x	x
Multiplexen/Demultiplexen			x	x	x
Fehlerbehandlung		(x)	(x)	(x)	x
Wiederherstellen		x		x	x
Funktionen in der Phase Verbindungsherstellung:					
Absprachen mit Vermittlungsdienst	x	x	x	x	x
Adresszuordnung zwischen T-SAP und N-SAP	x	x	x	x	x
Absprachen über Transportverbindung	x	x	x	x	x
Transport von T-SDUs	x	x	x	x	x
Funktionen während der Datentransferphase:					
Zusammenfügen/Trennen von T-PDUs		x	x	x	x
Segmentieren/Aneinanderreihen von T-SDUs	x	x	x	x	x
Splitten/Kombinieren von Netzverbindungen					x
Flusskontrolle			x	x	x
Identifikation der Transportverbindung	x	x	x	x	x
normaler Datentransfer von T-SDUs	x	x	x	x	x
vorrangiger Datentransfer		x	x	x	x
Funktionen zum Verbindungsabbau:					
Auslösen und Abbruch der Transportverbindung	x	x	x	x	x

Bild: Funktionen der T-Instanzen

Die Transportprotokolle sind in öffentlichen Netzen wichtig. Es sind zehn verschiedene **T-PDU-Typen** (Transport Protocol Data Unit) definiert.

Jeder Typ kann bis zu vier Felder enthalten. Der Längenindikator gibt die Länge des gesamten Headers (fester plus variabler Teil) an. Der Maximalwert ist 254 Byte.

Der feste Teil des Headers hängt vom Typ ab, im variablen Teil stehen Optionen, die nicht immer benötigt werden. Benutzerdaten können in verschiedenen T-PDU enthalten sein, nicht nur in Daten-T-PDU.

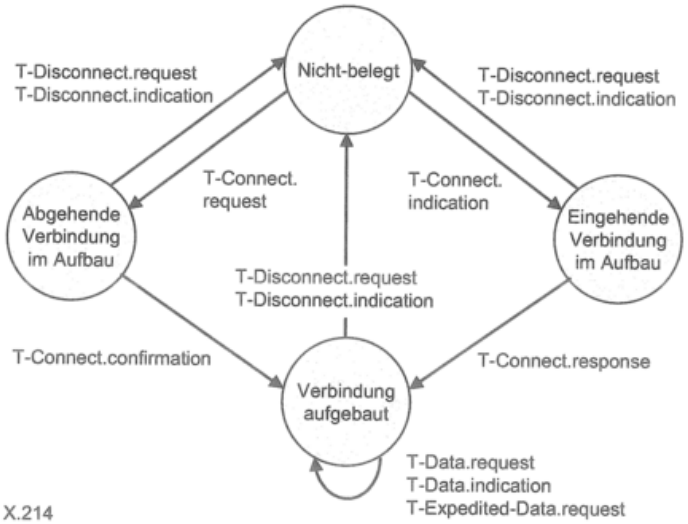


Bild: Zustandsdiagramm des Transportprotokolls

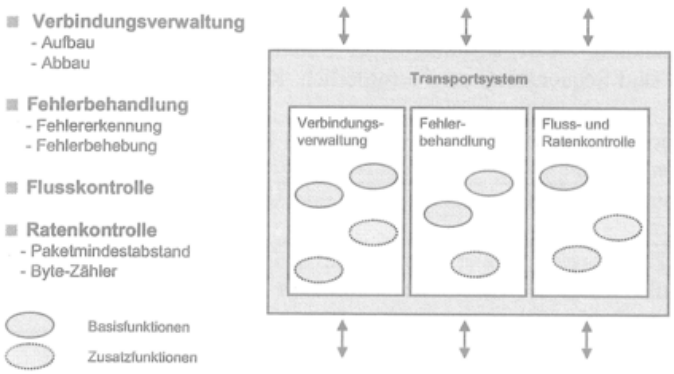
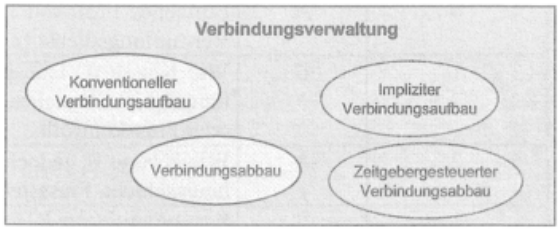


Bild: Mechanismen des Transportprotokolls



Zusätzliche Anforderungen an Verbindungsverwaltung:

- Geringe Verzögerung
- Schneller Verbindungsaufbau (z.B. Remote Procedure Call)
- Geringe Anzahl ausgetauschter Dateneinheiten
- Möglichkeiten zur Aushandlung der Dienstgüte

Bild: Verbindungsverwaltung

Verbindungslose Kommunikation

Informationen werden versendet, ohne vorherigen Aufbau einer Verbindung

Vorteil: schnelle Datenversendung möglich

Nachteil: keine Möglichkeit der Kontrolle, ob der Kommunikationspartner überhaupt empfängt bzw. empfangen kann

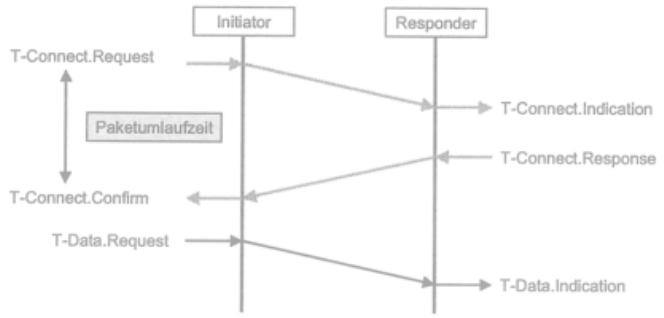
Verbindungsorientierte Kommunikation

Aufbau einer Verbindung bevor der Informationsaustausch stattfindet

Vorteil: Aushandlung von Kommunikationsparametern möglich:
Fenstergrößen, verwendeter Code, verwendete Fehlerkontrollmechanismen, Sequenznummern,...

Nachteile:
- eigentlicher Datenaustausch verzögert
- Overhead der Verbindungsetablierung und -verwaltung kann höher sein als der eigentliche Datenaustausch (kurze Daten)

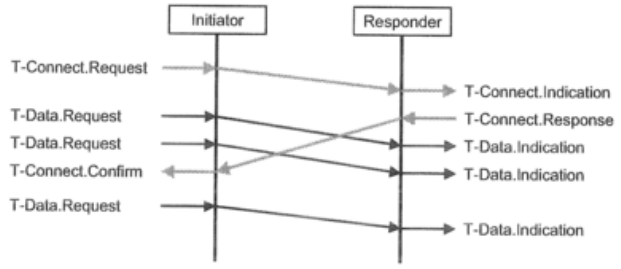
Bild: Verbindungslos vs. Verbindungsorientiert



- 2-fach oder 3-fach Handshake
- Datenaustausch erst nach T-Connect.Confirm möglich

Nachteil:
Verzögerung des Datenaustausches um mindestens eine Paketumlaufzeit

Bild: Konventioneller Verbindungsaufbau

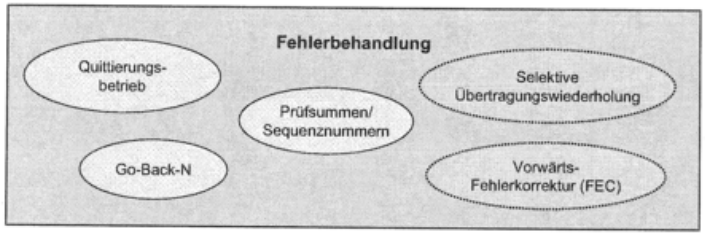


- Sofortiger Datenaustausch nach T-Connect.Request möglich
- Evtl. können bereits im Verbindungsaufbau-Paket Nutzdaten enthalten sein

Vorteil: Keine Verbindungsaufbauverzögerung

Nachteil: Erster Datenaustausch vor Aushandlung der Dienstgüte

Bild: Impliziter Verbindungsaufbau



- Zu berücksichtigende Charakteristiken moderner Netze:
  - Hohe Pfadkapazität
  - Hohe Bandbreite
- Zusätzliche Anforderungen an Fehlerbehandlung:
  - Geringe Übertragungsverzögerung

Bild: Fehlerbehandlung

Go-Back-N basiert auf dem Prinzip der Übertragungswiederholung

- Empfänger zeigt dem Sender erkannte Fehler an
- Sender überträgt alle Pakete ab dem fehlerhaft übertragenen Paket erneut
- Unter Umständen werden auch korrekt übertragene Pakete wiederholt gesendet

Vorteil:
- Einfacher Algorithmus
- Einfach zu implementieren

Nachteil:
- Hohe Kosten für Übertragungswiederholungen

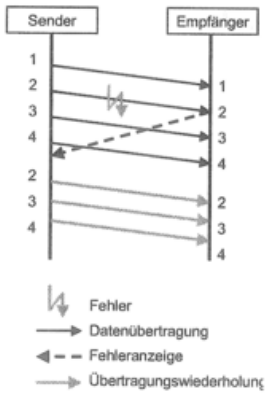


Bild: Fehlerbehandlung mittels Go-Back-N

- Fehleranzeige trifft frühestens nach einer Paketumlaufzeit beim Sender ein.
- alle Pakete nach dem fehlerhaften Paket müssen wiederholt werden.

Nachteil:
- Übertragungskapazitätsverlust in Höhe der doppelten Pfadkapazität

⇒ Hoher Verlust der Übertragungskapazität in Hochgeschwindigkeitsnetzen

Vorteil:
- Die Datenmenge einer Pfadkapazität muss beim Empfänger nicht gepuffert werden

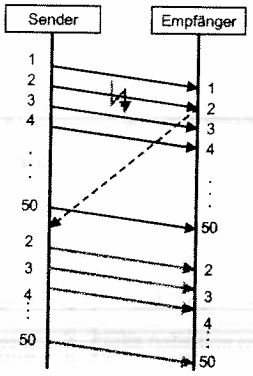


Bild: Go-Back-N in schnellen Netzen

- Vermeidung des Kapazitätsverlusts durch selektive Übertragungswiederholung
- Es werden nur tatsächlich fehlerhaft übertragene Pakete erneut gesendet

Vorteil:
- Geringer Bandbreitenverlust

Nachteil:
- Bei reihenfolgetreuer Auslieferung an den Benutzer sind große Pufferspeicher notwendig
- Hoher Verwaltungsaufwand in den Endsystemen

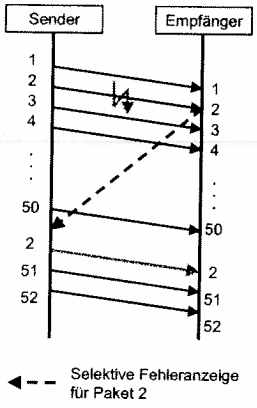


Bild: Selektive Übertragungswiederholung

Zu berücksichtigende Charakteristiken moderner Netze
- Hohe Pfadkapazität

Zusätzliche Anforderungen an Fluss- und Ratenkontrolle:
- Gleichmäßiger Datenfluss (z.B. Video- oder Audioübertragung)
- Vermeiden von burstartigem Senden der Daten

Bild: Fluss- und Ratenkontrolle

- **Flusskontrolle steuert die Datenmenge, die zwischen den Endsystemen ausgetauscht wird**
  - **Ziel:** Vermeiden von Pufferüberläufen beim Empfänger
- **Ratenkontrolle kontrolliert den Fluss im Kommunikationsnetz**
  - **Ziel:** Steuern der Senderate

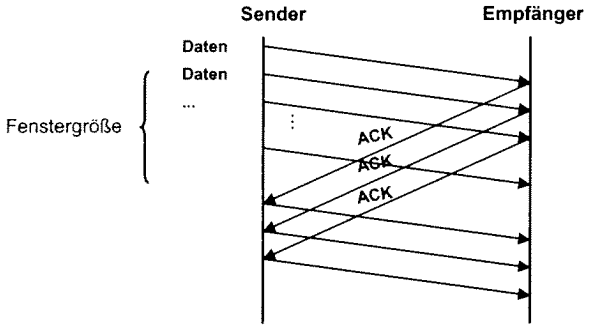
Bild: Unterschied zwischen Fluss- und Ratenkontrolle

Fensterbasierende Flusskontrolle:
- begrenzt als Reaktion auf Rückmeldungen die Anzahl der von der Quelle ausgesendeten Dateneinheiten durch eine veränderliche Fenstergröße.

Ratenbasierende Flusskontrolle:
- passt die Quellenübertragungsrate unter Verwendung eines Feedbackalgorithmus an.

Kreditbasierende Flusskontrolle:
- bietet der Quelle eine Gutschrift für die Anzahl der zu sendenden Dateneinheiten.
- Ist das Guthaben aufgebraucht, muss auf eine neuerliche Zuteilung von Krediten gewartet werden.

Bild: Methoden der Flusskontrolle



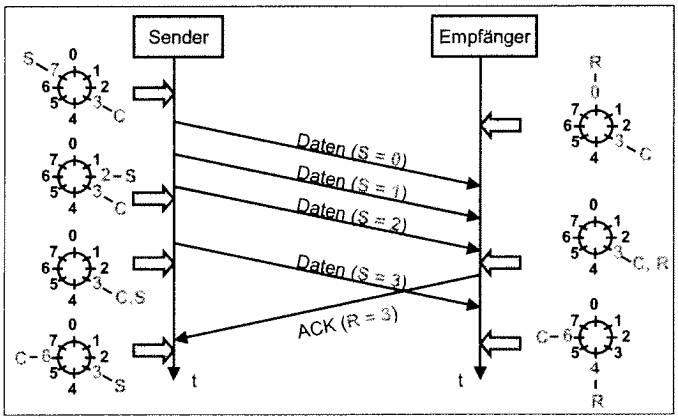
Prinzip

Sender kann bis zu einer maximalen Anzahl Dateneinheiten senden, ohne eine Quittung zu empfangen.

- Maximale Anzahl der Dateneinheiten repräsentiert die Pufferkapazität des Empfängers und wird als Sendekredit bezeichnet.
- Oftmals als fortlaufendes Fenster bezeichnet (Sliding Window)
- Fenster wird dann mit jeder empfangenen positiven Quittung weitergeschaltet.
- Empfänger kann meist zusätzlich den Kredit explizit bestimmen.

Bild: Kreditbasierte Flusskontrolle

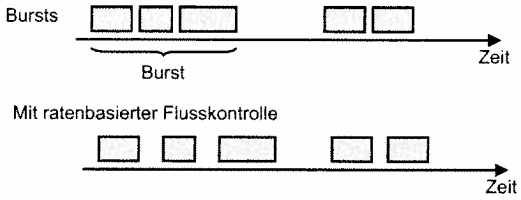
Fenstermechanismus (Kredit 4)



Nachteil: Kopplung von Fluss- und Fehlerkontrolle.

S: Sende-Sequenznummer (der zuletzt gesendeten Dateneinheit)
R: Nächste erwartete Sende-Sequenznummer = Quittierung bis Empfangs-Sequenznummer R-1
C: Oberer Fensterrand (maximal erlaubte Sequenznummer)

Bild: Kreditbasierte Flusskontrolle



Prinzip
Sender kann Daten mit einer nach oben begrenzten Rate senden, d.h. es existiert ein minimales Zeitintervall zwischen aufeinanderfolgenden Dateneinheiten, das nicht unterschritten werden darf.

Folgende Parameter sind relevant
- Zeitintervall zwischen zwei aufeinanderfolgenden Dateneinheiten
- Maximale Größe der Dateneinheiten

Vorteil
Vermeidet Bursts (Deutsch: Büschel)

Bild: Ratenbasierte Flusskontrolle

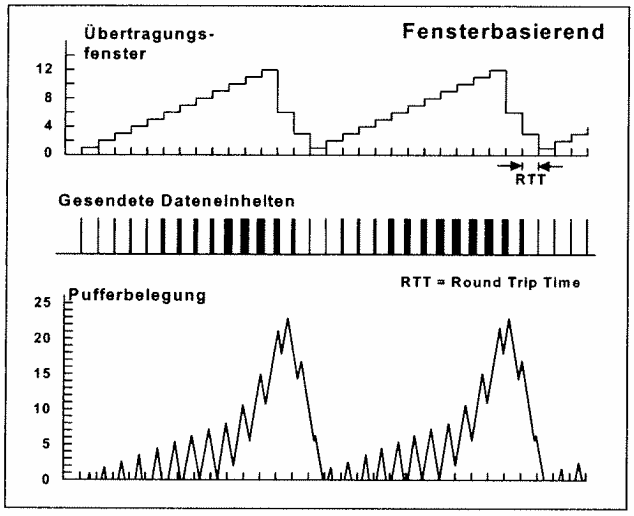


Bild: Fensterbasierte Flusskontrolle

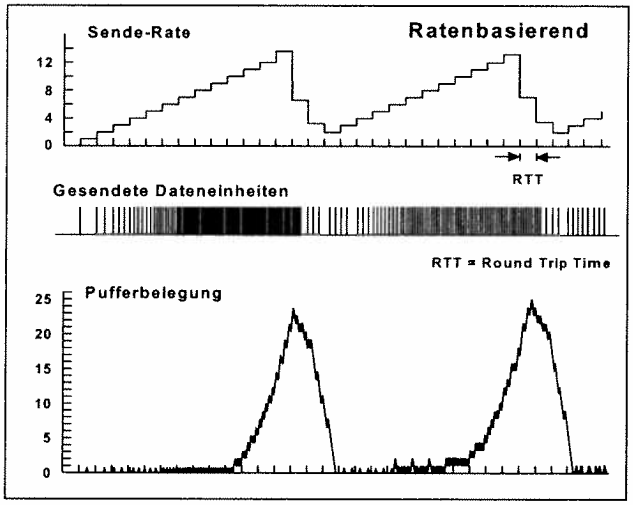


Bild: Ratenbasierte Flusskontrolle

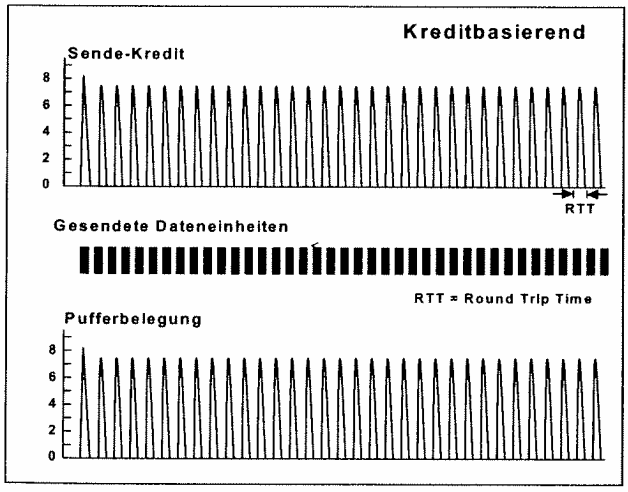


Bild: Kreditbasierte Flusskontrolle

Beispiel (Anfangskredit =3):

ACK = i
Quittierung der Pakete
bis zur Paketfolgenummer i

CREDIT= j
Sender darf bis zur
Paketfolgenummer i+j senden

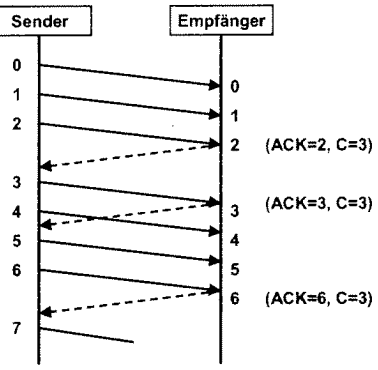
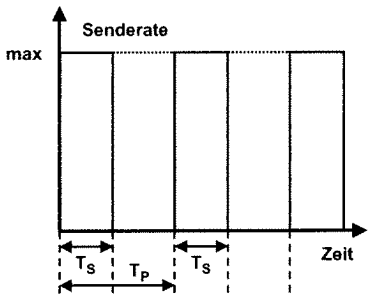
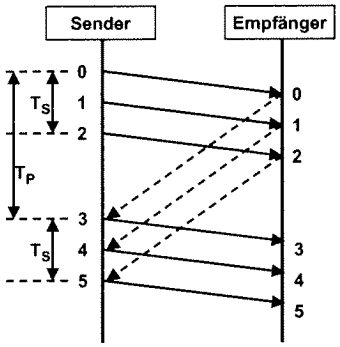


Bild: Flusskontrolle





Probleme:

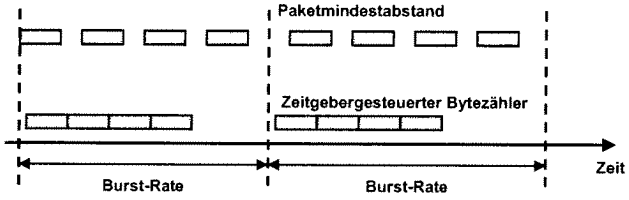
Zu welchem Zeitpunkt soll dem Sender ein neuer Kredit gewährt werden (Protokolloverhead vs. gleichmäßigem Sendeverhalten)?

- Große Paketumlaufzeit führt bei hoher Übertragungskapazität und kleinem Sendekredit zu burstartigem Sendeverhalten

Bild: Flusskontrolle

- **Festgelegte Parameter:**
  - Rate = Übertragungsrate in Byte/s
  - Burst = Anzahl von Bytes, die innerhalb eines Bursts mit beliebiger Rate gesendet werden dürfen
- **Definierte Hilfsgrößen:**
  - RTimer = Zeitgeber, der mit dem Wert Burst/Rate initialisiert wird und bei Ablauf sofort wieder neu gestartet wird
  - Counter = Anzahl von Bytes, die im aktuellen Burst noch gesendet werden dürfen
- **Ablauf der Ratenkontrolle auf Senderseite:**
  - Bei Ablauf von RTimer wird Counter auf den Wert von Burst gesetzt
  - Beim Senden von Daten wird der Zähler Counter um die Anzahl gesendeter Bytes erniedrigt
  - Daten dürfen nur gesendet werden, solange Counter > 0

Bild: Ratenkontrolle mittels Zeitgeber-Bytezähler



- Ratenkontrolle mittels Paketmindestabstand als Spezialfall der Ratenkontrolle mit zeitgebergesteuertem Bytezähler
- Unterschied der Ratenkontrolle mittels zeitgebergesteuertem Bytezähler zur Flusskontrolle liegt in der Unabhängigkeit von der Paketumlaufzeit

Bild: Ratenkontrolle

- **Begrenzung der maximalen Senderate durch Einführung eines zeitlichen Paketmindestabstands**

Prinzip:
- **Beim Senden eines Pakets wird ein Zeitgeber gestartet**
- **Nachfolgendes Paket darf erst nach Ablauf des Zeitgebers gesendet werden**

Bewertung:
- **gleichmäßiger Paketfluss**
- **hochauflösende Zeitgeber erforderlich**

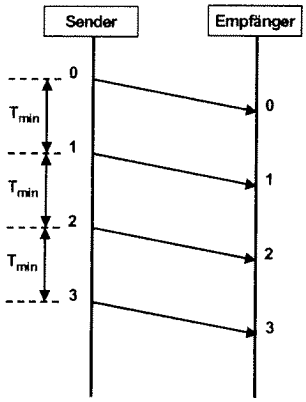
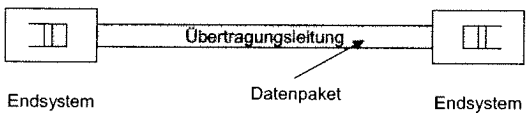
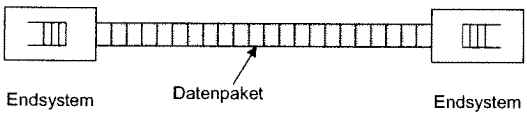


Bild: Ratenkontrolle mittels Paketmindestabstand

Langsames Netz mit 10 kbit/s ⇒ Pfadkapazität = 250 bit

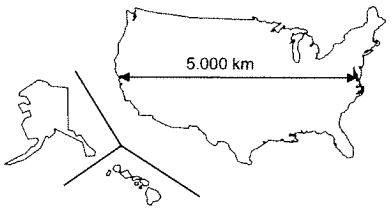


Schnelles Netz mit 1 Gbit/s ⇒ Pfadkapazität = 25 Mbit



Netzausdehnung 5.000 km
Signalausbreitungsgeschwindigkeit ca. 200.000 km/s = 5 µs/km

Bild: Pfadkapazität einer Übertragungsstrecke



Beispielszenario:
- Übertragung einer Datei zwischen Ost- und Westküste der USA
- Dateigröße: 1 Mbyte
- Übertragungsstrecke: ca. 5.000 km
- Signallaufzeit: 25 ms

- **Bitrate von 64 kbit/s:** Das erste Bit den erreicht den Empfänger nach Übertragung von etwa 1.600 Bits
- **Bitrate von 2 Mbit/s:** Es befinden sich bereits 50.000 Bits in der Übertragung, bevor das erste Bit den Empfänger erreicht.
- **Bitrate von 1 Gbit/s:** Übertragung bereits nach 8 ms beendet. (gesamte Datei im Netz gespeichert)

Bild: Pfadkapazität einer 5000 km Übertragungsstrecke

2.5 OSI-Referenzmodell: Schicht 5 - Sitzung

Version: Mai 2003

- Aufgaben und Funktionen
- Dienstelemente
- Synchronisation von Datenflüssen

Die Sitzungsschicht (Kommunikationssteuerungsschicht) regelt den Ablauf der Kommunikation zwischen den Anwendungsprozessen auf den beteiligten Endsystemen.

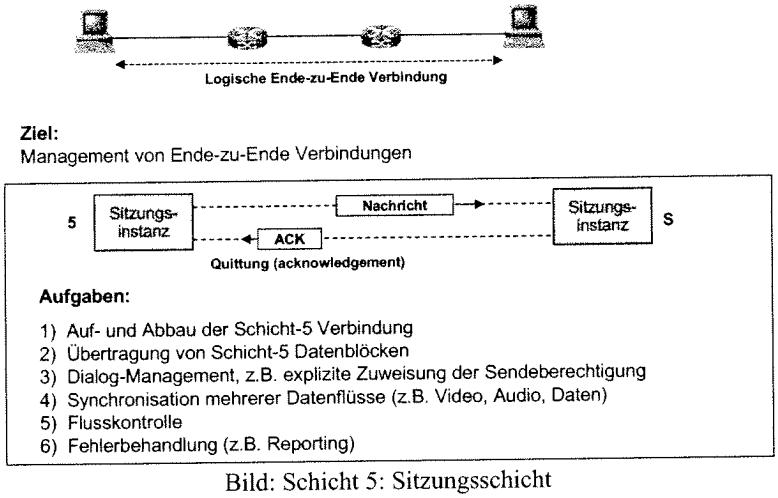


Bild: Schicht 5: Sitzungsschicht

Die Kommunikationssteuerungsschicht oder Sitzungssicht stellt Protokollelemente zur Verfügung, die zur Eröffnung einer Kommunikationsbeziehung (Sitzung), ihrer geordneten Durchführung und Beendigung notwendig sind. Diese Protokollelemente dienen zur Dialogmanagement, zur Synchronisation mehrerer Datenflüsse und zur Feststellung von Übereinstimmungen zwischen den beiden Sitzungsinstanzen. Die Sitzungsschicht ist auf dieser Weise in der Lage, z. B. beim Wegfall der Transportverbindung einer Datenaustausch in der Mobilfunk, die Anwendung darüber zu informieren und die Transportverbindung wieder kontrolliert aufzusetzen.

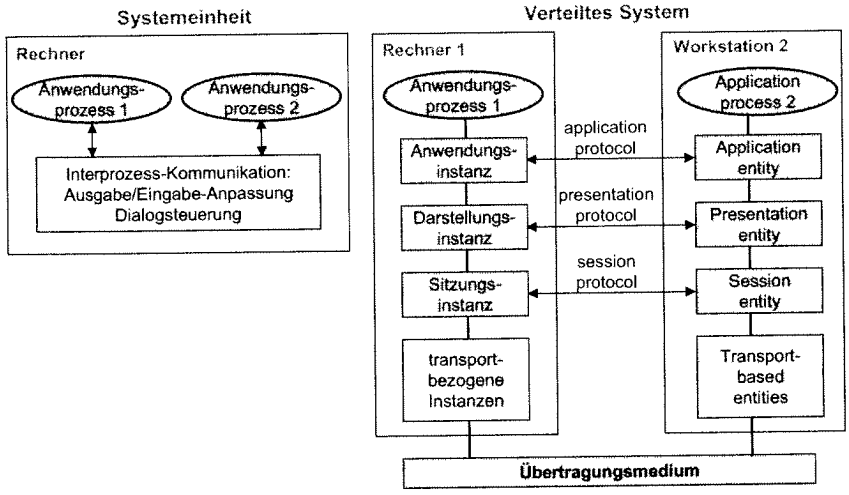


Bild: Zentrale und verteilte Kommunikation

Die **Sitzungsschicht** (Schicht 5, auch als Kommunikationssteuerungsschicht, session layer bezeichnet) bietet ihrem Benutzer (der Darstellungsschicht oder dem Benutzerprozess) die Möglichkeit, eine Verbindung aufzubauen, über die geordnet Daten übertragen werden können. Dafür stehen **Dienstelemente zur Dialogsteuerung** und zur **Synchronisation** des Datentransfers zur Verfügung. Die wesentlichen Konzepte der Sitzungsschicht sind **Tokens** für die Berechtigungssteuerung und Haupt- und Nebensynchronisationspunkte zur Gliederung der Datenströme in Dialogeinheiten.

Die Sitzungsschicht erfüllt die folgenden Aufgaben für die Darstellungsschicht:

- Einrichten und Auflösen einer Sitzungsverbindung
- Normaler und beschleunigter Datentransfer
- Dialogsteuerung
- Synchronisierung der Sitzungsverbindung
- Benachrichtigung über irreparable Fehler.

Zur Ausführung ihrer Aufgaben verfügt die Sitzungsschicht über die folgenden Funktionen:
- Zuordnung der Sitzungsverbindung zur Transportverbindung
- Flusssteuerung der Sitzungsverbindung
- Beschleunigter Datenaustausch
- Sitzungsverbindung wiederherstellen
- Sitzungsschicht-Verwaltung.

Die Abbildung einer Sitzung auf eine Transportverbindung kann auf drei verschiedene Arten geschehen.
- Im einfachsten Fall wird genau für die Dauer einer Sitzung eine Transportverbindung eingerichtet.
- Falls mehrere Sitzungen direkt aufeinander folgen, können diese dieselbe Transportverbindung benutzen.
- Wenn eine Transportverbindung hin und wieder ausfällt, kann die Sitzungsschicht dies gegenüber der Anwendungsschicht überbrücken, indem sie eine neue Transportverbindung aufbaut.

Auf einer Transportverbindung kann jedoch höchstens eine Sitzung gleichzeitig ablaufen.

Token
Dies sind Berechtigungsmarken für bestimmte Dienste. Der Besitzer des Tokens hat ein exklusives Recht auf den zugehörigen Dienst. Das Token kann die Ausführung des Dienstes zulassen oder verzögern.

Die Vergabe von Token wird beim Sitzungsaufbau ausgehandelt, dabei hat der rufende Teilnehmer zu Beginn Priorität. Es gibt Token verschiedener Typen:
- Data Token: Es repräsentiert im Halbduplex-Betrieb die Sendeberechtigung. Ein Teilnehmer darf nur senden, wenn er das Data Token besitzt.
- Synchronized Minor Token: zum Setzen eines Nebensynchronisationspunktes.
- Major/Activity Token: zum Initiieren von Aktivitäten bzw. Setzen von Hauptsynchronisationspunkten.

Für den Umgang mit den Token gibt es mehrere **Dienstelemente:**
- **S-Token-Give:** Damit können Token unbestätigt übergeben werden. Durch S-Token-Give.Request wird die Abgabe eines Tokens eingeleitet, durch S-Token-Give.Indication wird die Annahme durch die andere Sitzungsinstanz abgeschlossen. Der Typ des Tokens wird durch einen Parameter angegeben.
- **S-Token-Please:** zur unbestätigten Anforderung eines Tokens durch S-Token-Please.Request und S-Token-Please. Indication. Die Instanz, die zur Abgabe des Tokens aufgefordert wird, ist jedoch nicht verpflichtet, dieser Aufforderung nachzukommen.
- **S-Control-Give:** zur Übergabe aller Token.

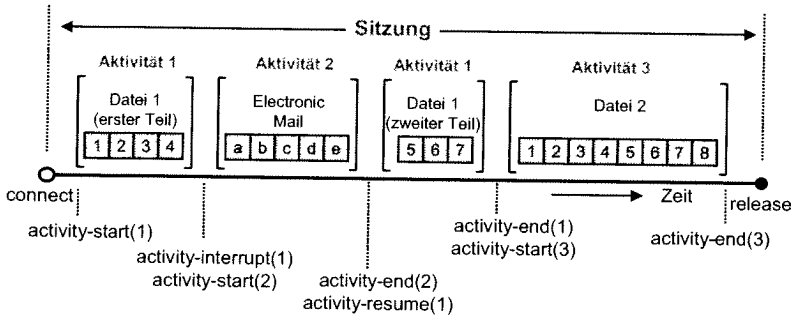


Bild: Aktivitäten-management

Synchronisation

Der zeitliche Ablauf von Sitzungen wird durch Begriffe wie Aktivität, (activity), Dialogeinheit (dialog unit), Haupt- und Nebensynchronisationspunkt (major-sync-point, minor-sync-point) beschrieben.

Eine **Aktivität** fasst zusammengehörige Datenaustauschoperationen zwischen den Dienstelementen S-Activity-Start und S-Activity-End zusammen. Eine Aktivität kann durch S-Activity-Interrupt bzw. S-Activity-Resume unterbrochen bzw. wieder aufgenommen werden.

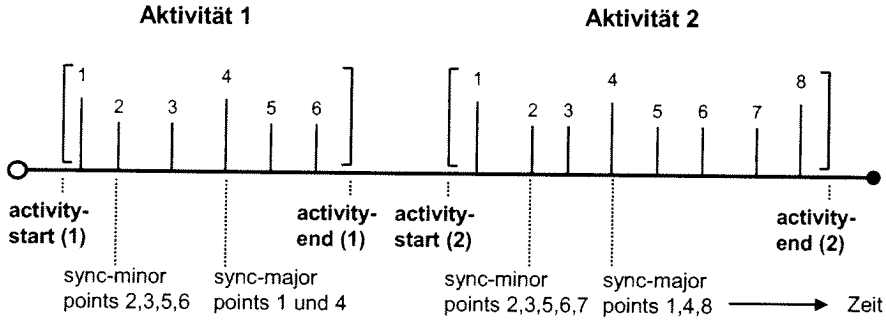


Bild: Synchronisation von Aktivitäten der Sitzungsschicht

Dies bedeutet das Ende der bestehenden Sitzung und den späteren Aufbau einer neuen Sitzung. Nach Auftreten eines Fehlers in einer Kommunikationsinstanz können die Sitzungsinstanzen durch eine Synchronisation wieder in einen bekannten Zustand versetzt werden. Dazu dienen Haupt- und Nebensynchronisationspunkte.

Zwischen zwei aufeinander folgenden **Hauptsynchronisationspunkten** befindet sich genau eine **Dialogeinheit.**

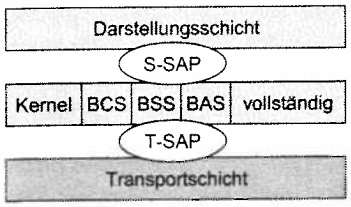
Bei einer Neusynchronisierung erfolgt eine Rückkehr zum letzten Hauptsynchronisationspunkt. Durch **Nebensynchronisationspunkte** werden die Dialogeinheiten weiter unterteilt. Bei einer Neusynchronisierung kann zu jedem Nebensynchronisationspunkt zurückgekehrt werden, der seit dem letzten Hauptsynchronisationspunkt gesetzt wurde

Die **Dienstelemente** für den Umgang mit Aktivitäten sind:

- **S-Activity-Start:** Begin einer Aktivität.
- **S-Activity-End:** Ende einer Aktivität.
- **S-Activity-Discard:** Abbruch einer Aktivität.
- **S-Activity-Interrupt:** Unterbrechung einer Aktivität.
- **S-Activity-Resume:** Eine unterbrochene Aktivität wird wieder aufgenommen.

Funktionseinheit	Dienstelemente	Funktion
Kernel	S-connect S-data S-release S-user-abort S-provider-abort	Sitzung aufbauen Daten übertragen Sitzung normal abbauen Abbruch durch Benutzer Abbruch durch Dienstbringer
Half Duplex	S-token-please S-token-give	Token-Anforderung Token-Übergabe
Duplex	keine zusätzlichen	--
Negotiated Release	S-release S-token-please S-token-give	Sitzung normal abbauen Token-Anforderung Token-Übergabe
Expedited Data	S-expedited-data	Beschleunigter Datentransfer
Minor Synchronization	S-sync-minor S-token-please S-token-give	Nebensynchronisationspunkt Token-Anforderung Token-Übergabe
Major Synchronization	S-sync-major S-token-please S-token-give	Hauptsynchronisationspunkt Token-Anforderung Token-Übergabe
Resynchronization	S-resynchronize	Resynchronisation
Activity Management	S-activity-start S-activity-resume S-activity-interrupt S-activity-discard S-activity-end S-token-please S-token-give	Beginn einer Aktivität Wiederaufnahme einer A. Unterbrechung einer A. Aufgabe einer Aktivität Beenden einer Aktivität Token-Anforderung Token-Übergabe

Bild: Funktionseinheiten und Dienstelemente der Sitzungsschicht



BCS Basic Combined Subset
BAS Basic Activity Set
BSS Basic Synchronized Set

SAP Service Access Point

Bild: Struktur der Sitzungsschicht.

Die Dienstelemente der Funktionseinheit Kernel werden in jeder Sitzung benutzt. Zusätzlich ist mindestens die Funktionseinheit Half Duplex erforderlich, weitere Funktionseinheiten sind optional. Funktionseinheiten lassen sich zu Gruppen kombinieren, die als **Profile** bezeichnet werden. Beispiele hierfür sind:

- **BCS (Basic Combined Subset):** Es umfasst den Kernel und die Funktionseinheit Halbduplex.
- **BAS (Basic Activity Set):** enthält die Funktionseinheiten für das Aktivitätsmanagement und für Fehlermeldungen.
- **BSS (Basic Synchronized Subset):** enthält die Funktionseinheiten für die Synchronisation.

Dienstelemente der Funktionseinheit Kernel:

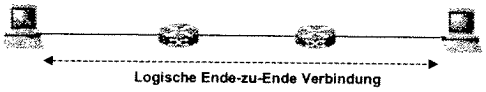
- **S-Connect:** Sitzungsaufbau
- **S-Data:** Normaler Datentransfer
- **S-Release:** Ordnungsgemäßes Sitzungsende.
- **S-User-Abort:** Abrupter Abbruch, durch den Benutzer ausgelöst.
- **S-Provider-Abort:** Abrupter Abbruch, durch den Diensterbringer ausgelöst.

2.6 OSI-Referenzmodell: Schicht 6 - Darstellung

Version: Mai 2003

Inhalt

- Aufgaben und Funktionen
- Dienstelemente
- ASN.1 (Abstract Syntax Notation One)



Ziel:
Darstellungsanpassungen von Ende-zu-Ende Verbindungen

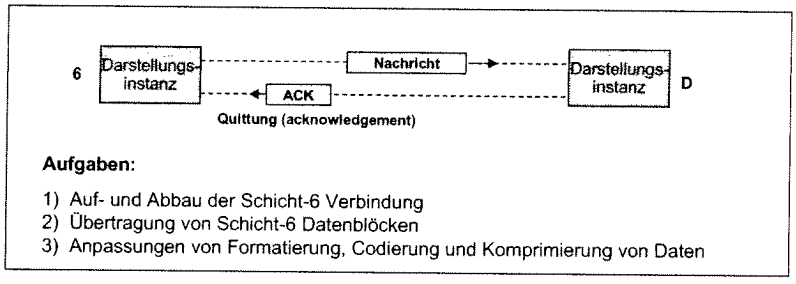


Bild: Schicht 6: Darstellungsschicht

Die Darstellungsschicht stellt Protokollelemente zur Verfügung, die es die Darstellungsinstanzen ermöglichen, die Formatierungsanpassung sowie Codierung und Komprimierung eindeutig zu bestimmen, und legt im Darstellungsprotokoll die Regeln fest, wie die in der gemeinsamen Sprache die Darstellung der Information auszutauschen ist. Die Darstellungsschicht sorgt für die korrekte Interpretation der übertragenen Informationen. Dazu wird die lokale Syntax (Codierung) der Information in Endsystemen in eine einheitliche Transfersyntax übersetzt. Datenkompression und Verschlüsselung gehören ebenfalls zu ihren Aufgaben.

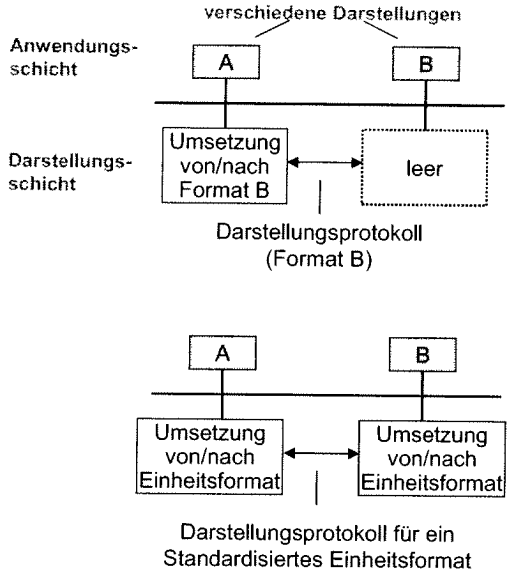


Bild: Formatkonvertierung in der Darstellungsschicht

Dienstelemente

Die Darstellungsschicht (Präsentationsschicht) enthält echte Dienste (die eine Funktion beinhalten) und Durchreichedienste, die nur die Verbindung zwischen Anwendungs- und Sitzungsschicht herstellen.

Der Verbindungsaufbau wird durch die **P-Connect-Dienstelemente** veranlasst, der geordnete Verbindungsabbau durch **P-Release** und der abrupte Verbindungsabbau durch **P-Abort.** Die Dienstelemente des Context Management können einen Presentation Context aushandeln. Dazu besitzt jede Instanz eine Liste der ihr bekannten abstrakten Syntaxen und der zugehörigen Transfersyntaxen.

Die Anwendungsschicht teilt der Darstellungsschicht beim Verbindungsaufbau die gewünschte abstrakte Syntax mit. Die Darstellungsschicht ergänzt die verfügbaren Transfersyntaxen und sendet die Liste an die Partnerinstanz.

Diese wählt einen ihr bekannten Presentation Context aus der Liste aus. Er wird für die Übertragung verwendet. Falls keine Einigung auf einen Presentation Context möglich ist, kann die Verbindung nicht hergestellt werden.

(1) Syntax-Auswahl
Auswahl einer geeigneten Syntax für eine Übertragung und gegebenenfalls Änderung dieser Wahl

(2) Syntax-Transformation
Konvertierungen von Code oder Zeichensatz (z.B. ASCII -> EBCDIC), Modifikation im Datenlayout (z.B. auf Bildschirm, mobiles Gerät)

Bild: Dienste der Darstellungsschicht

Eine **abstrakte Syntax** wird benötigt, um Datenstrukturen und Inhalte logisch zu beschreiben. Die abstrakte, logische Beschreibung der Datenstrukturen ist nach OSI in allen beteiligten Systemen dieselbe.

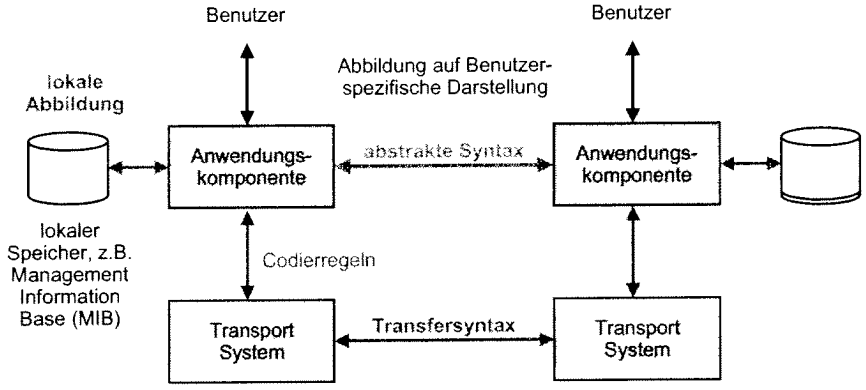


Bild: Abstrakte Syntax und Transfersyntax

Nach einem erfolgreichen Verbindungsaufbau übergibt die Anwendungsschicht ihre Datenpakete an die Darstellungsschicht unter Angabe der abstrakten Syntax und des enthaltenen syntaktischen Typs. Die Darstellungsschicht kann nun den Darstellungskontext auswählen und die Datenpakete in die Transfersyntax übersetzen. Diese Übersetzung wird beim Empfänger rückgängig gemacht.

Die systeminterne Darstellung wird als konkrete, lokale Syntax bezeichnet. sie kann in Abhängigkeit vorn Prozessor und vom Betriebssystem unterschiedlich sein. Für die Übertragung wird die lokale Syntax mit Hilfe der abstrakten Syntax in die (konkrete) Transfersyntax übersetzt.

Aufgaben der Darstellungsschicht

Hauptaufgabe der **Darstellungsschicht (auch Präsentationsschicht,** presentation layer) ist es, Dateneinheiten der Anwendungsschicht unter Wahrung ihres Informationsgehaltes zu übertragen.

(1) Anforderung des Aufbaus einer Sitzungsverbindung

(2) Datenübertragung

(3) Aushandeln der zu wählenden Transfersyntax

Transformationen der lokalen Syntax auf ausgehandelte Transfersyntax

(4) Syntax-Transformationen

- drei unterschiedliche Syntaxen für Daten möglich: Sender- und Empfängerseite, Transfersyntax
- Transformationen zwischen Syntaxen innerhalb der Darstellungsschicht:
  -> senderseitige Syntax
  -> Transfersyntax bzw. Transfersyntax
  -> empfängerseitige Syntax
- geeignete Formatierung (zur Darstellung auf dem Ausgabegerät), Codierung und Kompression von Daten

(5) Anforderung des Abbaus einer Sitzungsverbindung

Bild: Funktionen der Darstellungsschicht

Da in den Endsystemen unterschiedliche Codierungen (als **lokale Syntax** bezeichnet) vorliegen können, wird eine einheitliche, genormte Codierung (als **Transfersyntax** bezeichnet) für die Übertragung verwendet. Paare aus einer abstrakten Syntax und einer Transfersyntax werden als Darstellungskontext bezeichnet.

Der Darstellungskontext bestimmt die **Übersetzungsregeln** für die Codierung und Decodierung.

Die Darstellungsschicht hat insgesamt die folgenden Aufgaben zu erfüllen:

- Verbindungsauf- und –abbau,
- Kontext-Management,
- Datentransfer mit Datentransformation.

Dienstelemente der Darstellungsschicht

Dienst	Dienstelemente	Parameter
Verbindungsaufbau	P-Connect.Request P-Connect.Indication P-Connect.Response P-Connect.Confirm	Presentation-Context- Definition-List, Quality-of-Service, Initial-Assignment-of-Tokens, Result-List, Quality-of-Service, Initial-Assignment-of-Tokens
Verbindungsabbau	P-Release.Request P-Release.Indication P-Release.Response P-Release.Confirm P-U-Abort.Request P-U-Abort.Indication P-P-Abort.Indication	User-Data, Reason
Kontext-Management	P-Define-Context.Request P-Define-Context.Indication P-Define-Context.Response P-Define-Context.Confirm P-Delete-Context.Request P-Delete-Context.Indication P-Delete-Context.Response P-Delete-Context.Confirm	Presentation-Context-1d Definition-List Result-List Presentation-Context-1d- List Result-List
Datentransfer	P-Data.Request P-Data.Indication P-Expedited-Data.Request P-Expedited-Data.Indication	User-Data: Presentation- Context-1d, Tag, Value

Die Durchreichedienste der Darstellungsschicht stellen dem Anwender die Funktionen der Sitzungsschicht für die Dialogsteuerung zur Verfügung.

Durchreichedienste der Darstellungsschicht (Req = Request, Ind = Indication, Resp = Response, Conf = Confirm)

P-Token-Give.Req, .Ind	P-Activity-Start.Req, .Ind
P-Token-Please.Req, .Ind	P-Activity-Interupt.Req, .Ind, .Resp, .Conf
P-Sync-Minor.Req, .Ind, .Resp, .Conf	P-Activity-Resume.Req, .Ind
P-Sync-Major-.Req, .Ind., .Resp, .Conf	P-Activity-End.Req, .Ind, .Resp, .Conf
P-Resinchronize.Req, .Ind, .Resp, .Conf	P-Activity-Discard.Req, .Ind, .Resp, .Conf

Anwendung	Elemente des Darstellungsprotokolls
einfacher Text	Zeichenalphabet, Steuerzeichen für Beginn, Ende, Zeilenende (LF), Seitenende (FF) usw.
Textverarbeitung	Zeichenalphabet, Steuerzeichen für Beginn, Ende, Zeilenende (LF), Seitenende (FF) usw., Schriftarten, Schriftgrößen, Absätze, Einzüge, Kopf- und Fußzeilen usw.
Zeichenprogramme (objektorientiert)	Codierung von Positionen, Größe und Objektarten wie Striche, Rechtecke, Kreise usw.
Schwarz/Weiß oder Graustufen-Festbilder (z.B. Telefax)	Codierung von Bildbeginn und Ende, Graustufen-Codierung der Bildelemente, Redundanzreduzierende Codierung
Sprache	Quantisierung und Codierung der Abtastwerte, Redundanzreduzierende Codierung

Einige Basiselemente in Darstellungsprotokolle.

Bild: Anwendung und Darstellung von Objekten

Anwendung	Darstellungsformat
Text	ASCII, EBCDIC
Bildübertragung	GIF, JPEG
Video	MPEG
Audio	PCM, H.261
WWW	HTML
E-Mail	MIME
SNMP	ASN.1/ BER
RPC	eXternal Data Representation (XDR)

Einige Beispiele für Darstellungsformate.

SNMP Simple Network Management Protocol
RPC Remote Procedure Call
PCM Pulse Coded Modulation
ASN Abstract Syntax Notation Number One
BER Basic Encoding Rules

GIF Graphical Interchange Format
JPEG Joint Photographic Expert Group
MPEG Motion Picture Expert Group
HTML Hypertext Markup Language
MIME Multipurpose Internet Mall Extension

ASCII American National Standard Code for Information Interchange
EBCDIC Extended Binary-Coded-Decimal Interchange Code

Bild: Anwendungen und ihre Darstellungsformate

- Verschiedene Maschinen verwenden unterschiedliche Reihungen von Bytes
- Beispiel: Zahl 34677374:

- Big Endian (z.B. Motorola)

00000010	00010001	00100010	01111110

- Little Endian (z.B. Intel)

01111110	00100010	00010001	00000010

hohe Adresse
(MSB: Most Significant Byte)

niedrige Adresse
(LSB: Least Significant Byte)

Bild: Darstellung von Integer-Zahlen

Bei der Übermittlung von Nachrichten zwischen zwei Endsystemen mit Betriebssystemen, die auf verschiedenen CPUs laufen, kann der Reihenfolge der Byte-Abspeicherung verschieden sein. In diesem Fall muss die Byte-Reihung der ankommenden Nachrichten abgeändert werden.

Abstrakte Syntax

- Menge von Typdefinitionen für Datenobjekte, z.B.
  - ASN.1
  - XDR language (eXternal Data Representation)
- beschreibt generische Datenstruktur unabhängig von der Art der Codierung

Transfersyntax

- konkrete Repräsentation der beschriebenen Daten bei der Übertragung
- definiert durch eine Menge von Codierregeln, z.B.
  - Basic Encoding Rules (BER) für ASN.1
  - XDR Regeln

Bild: Abstrakte Syntax und Transfersyntax

ASN.1 und BER

ASN.1 (Abstract Syntax Notation One) ist eine Sprache zur Spezifikation abstrakter Syntaxen. Mittels ASN.1 können Datentypen und ihre Werte beschrieben werden. BER (Basic Encoding Rules) beschreibt eine Transfersyntax, erlaubt also die eindeutige Beschreibung der Daten (Typ und Wert) auf der Bitebene.

- Beschreibungssprache für Datentypen
  - Untermenge wird für SNMP Objekte verwendet (abstrakte Syntax)
- Basic Encoding Rules (BER)
  - beschreiben die Abbildung der Datentypen auf die übertragenen Bits (Transfersyntax)

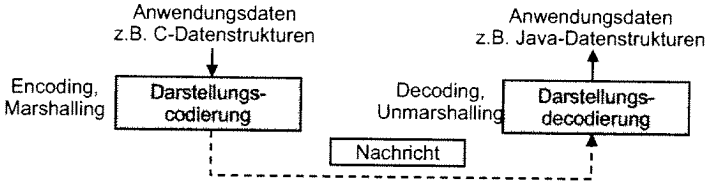


Bild: Abstrakte Syntax Notation One ASN.1

ASN.1 und BER sind von ITU-T und ISO standardisiert.

ASN.1 wird für mehrere Zwecke eingesetzt:

- zur Definition abstrakter Syntaxen für Anwendungsdaten,
- zur Beschreibung von Anwendungs- und Darstellungs-PDUs,
- zur Beschreibung der MIB (Management Information Base) beim Systemmanagement sowohl nach OSI als auch nach SNMP.

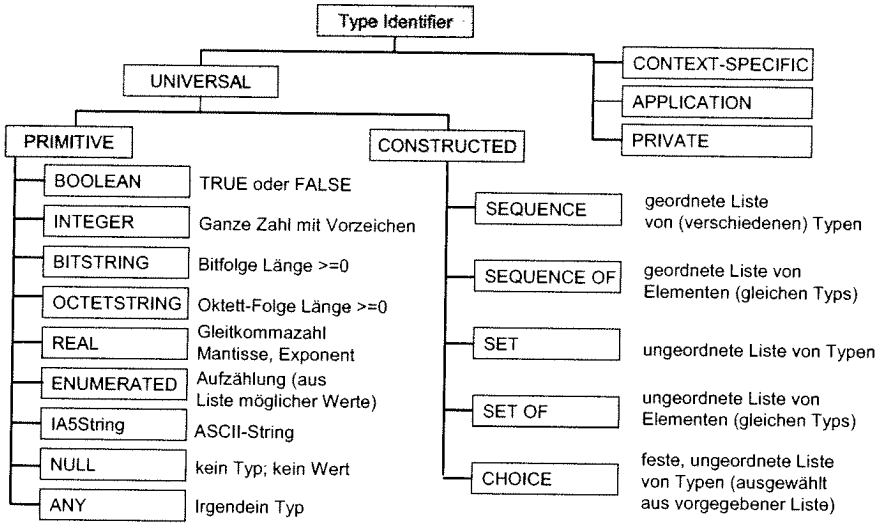


Bild: Datentypen in ASN.1

Ein **Datentyp** (kurz: Typ) kann als Menge (collection) von Werten aufgefasst werden. Ein Typ kann eine unendlich große Anzahl von Wert annehmen. Dies ist beim Typ INTEGER der Fall.

Typen können **einfach** (primitive) sein (diese sind atomar, bestehen also nicht aus Komponenten).

Zusammengesetzte Typen (structured oder constructed) bestehen aus Komponenten, denen jeweils wieder ein Typ zugeordnet ist. ASN.1 unterscheidet vier Klassen von Datentypen bzw. Tags.

BER-Codierung eines Datenwertes umfasst

- **Typ** (Ein oder mehrere Oktett, welche codierung für Datentyp-Klasse und -Nummer enthalten)
- **Länge**
- **Wert** (Value, Codierung des eigentlichen Inhalts)

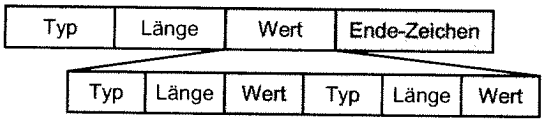


Bild: Basic Encoding Rules (BER)

Die **Transfersyntax** wird erhalten, indem die Basic Encoding Rules (BER) auf die abstrakte Syntax angewendet werden.

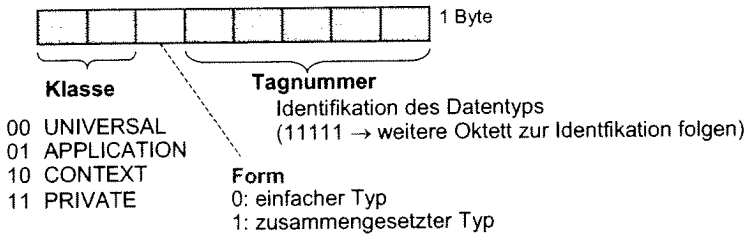
Dazu wird jeder (Wert eines Typs durch ein Datenelement dargestellt, das aus **drei Felder** besteht, die je ein oder mehreren Bytes enthalten können:

- Das **Identifier-Feld** kennzeichnet den vorliegenden Typ gemäß ASN.1
- Das **Länge-Feld** enthält die Anzahl der Bytes im Feld Inhalt.
- Das **Feld Inhalt** enthält den eigentlichen Wert, bei strukturierten Typen können dies weitere Datenelemente sein.

Tags in ASN.1

Klasse des Datentyps	Aufbau des Typs	Definition	Gültigkeit
UNIVERSAL	elementar, zusammengesetzt	vordefiniert	Internationaler Standard
APPLICATION	zusammengesetzt	selbst definiert	Eine Anwendung, mehrere Organisationen
PRIVATE	zusammengesetzt	selbst definiert	Eine Organisation
CONTEXT- SPECIFIC	zusammengesetzt	selbstdefiniert	Ein strukturierter Typ innerhalb einer Anwendung

Jeder Datentyp (mit Ausnahme von ANY und CHOICE) wird durch ein Tag gekennzeichnet, das aus dem Klassennamen und einer Nummer besteht, z. B. UNIVERSAL 5 oder PRIVATE 22.



Bekanntes Längenfeld (Länge des Inhalts in Oktett)

- kurze Form: 1 Byte
  - erstes Bit 0, weitere 7 Bits codieren Länge als binäre Ganzzahl
- lange Form: n Bytes, n > 1
  - erstes Byte: erstes Bit 1, weitere Bits codieren Anzahl der folgenden Längenoktett
  - folgende Längenoktett codieren Länge als binäre Ganzzahl

Unbekanntes Längenfeld

- 00000000_{16} als spezielles Ende-Zeichen
- Kennung: 1 Byte
  - erstes Bit 1, alle anderen Bits 0

Datenelemente dieser Form werden als TLV (Type Length Value) bezeichnet.

Das Typfeld muss den Typ eindeutig spezifizieren. Das Identifier-Feld besteht aus einem Byte oder - falls die Tagnummer größer als 30 ist - aus mehreren Bytes.

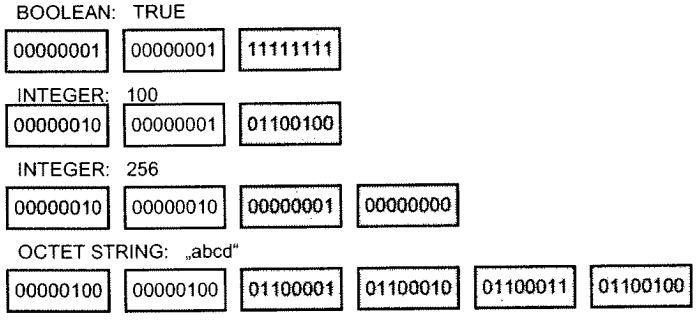
Das Längenfeld besteht aus einem Byte (falls Länge < 128) oder aus mehreren Bytes. Für bestimmte Typen muss das Längenfeld nicht im Voraus bekannt sein. Dann wird das Längenfeld als ein Byte mit dem Wert 8016 und das Ende des Datenelements durch zwei Bytes mit dem Wert 000016 dargestellt.

Bild: Typ- und Längenfeld

Tag: 0 ... 30 für Klasse UNIVERSAL

1 = Boole'scher Typ
2 = Ganzzahltyp
3 = Bitstring-Typ
4 = Bytestring-Typ
5 = Null-Typ
9 = Real-Typ
10 = Aufzählungstyp
16 = Sequence/Sequence-of-Typ
17 = Set/Set-of-Typ
18-22 = Stringtypen mit alternativen Zeichensätzen
23-24 = Zeittypen
25-27 = Stringtypen mit alternativen Zeichensätzen
> 30 = alle 5 Bit auf Eins, weiter im nächsten Byte

Einfache Typen	Zusammengesetzte Typen	Andere Typen
- BOOLEAN	- SET	- NumericString
- INTEGER	- SET OF	- PrintableString
- ENUMERATED	- SEQUENCE	- TeletexString
- REAL	- SEQUENCE OF	- VideotexString
- BIT STRING	- CHOICE	- VisibleString
- OCTET STRING	- SELECTION	- IA5String
- NULL	- TAGGED	- CharacterString
	- ANY	- GraphicString
		- GeneralString
		- UTCTime
		- ObjectDescriptor
		- ObjectIdentifier



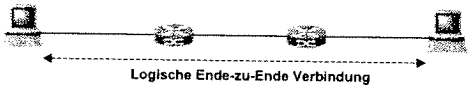
Einige Beispiele einer BER-Codierung sind im Bild gegeben.

Bild: Beispiele für BER-Codierung

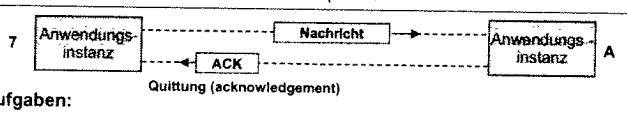
2.7 OSI-Referenzmodell: Schicht 7 – Anwendung

Version: Mai 2003

- Aufgaben und Funktionen
- Dienstelemente



Ziel:
Einigungsprozess zwischen Kommunikationspartnern



Aufgaben:

1) Auf- und Abbau der Schicht-7 Verbindung
2) Übertragung von Schicht-7 Datenblöcken
3) Identifizierung der gewünschten Kommunikationspartner
4) Authentisierung der Kommunikationspartner
5) Feststellung der momentanen Verfügbarkeit der Partner
6) Festlegung der Verantwortlichkeit bei Fehlerbehebung
7) Feststellung von eventuellen Einschränkungen bezüglich der Syntax
8) Einigung auf ein Verfahren zur Ressourcenaufteilung
9) Aushandlung der akzeptablen Dienstqualität
10) Synchronisation kooperierender Anwendungen

Bild: Schicht 7: Anwendungsschicht

In der Anwendungs- oder Verarbeitungsschicht als der höchsten Schicht des Referenzmodells manifestiert sich die Funktion der Informationsverarbeitung in einer Kommunikation. Die kommunizierenden Anwendungsinstanzen bilden die verteilten Anwendungen. Die Anwendungsprotokolle, die ihre Zusammenarbeit regeln, sind deshalb anwendungsspezifisch. Die Aufgaben sind grob wie folgt einzuteilen: 1) Identifizierung und Authentisierung der Partner, 2) Verfügbarkeitsüberprüfung, 3) Feststellung der Verantwortlichkeit für die Fehlerbehebung sowie die Feststellung einer Syntaxeinschränkung, 4) Aushandlung der Ressourcen und Dienstqualität, und 5) Synchronisation der Anwendungen.

(1) Identifizierung der gewünschten Kommunikationspartner
- Diese Identifizierung kann durch einen expliziten Namen geschehen, durch eine Adresse, durch eine spezifische Beschreibung (für einen bestimmten Partner) oder durch eine allgemeine Beschreibung (für einen Partner aus einer Gruppe von funktional gleichartigen Partnern).

(2) Feststellung der momentanen Verfügbarkeit der Partner
- z.B. durch eine entsprechende Anfrage

(3) Authentisierung der Kommunikationspartner
- z.B. durch Austausch von Codeworten oder über eine dritte, vertrauenswürdige Instanz

(4) Einigung auf ein Verfahren zur Kostenaufteilung
- Kommunikationskosten: verbrauchte CPU-Zeit, belegter Speicherplatz, Benutzung eines öffentlichen Kommunikationsnetzes entstehen (Telefongebühren)

(5) Feststellung über Eignung der beiderseits verfügbaren Ressourcen
- z.B. hinreichend große freie Plattenkapazität beim Empfänger bei Übertragung großer Dateien

(6) Aushandlung der akzeptablen Dienstgüte (Quality of Service, QoS)
- z.B. maximal zulässigen Antwortzeiten, tolerierbare Fehlerraten

(7) Synchronisation kooperierender Anwendungen
- Synchronisation der einzelnen Kommunikationsaktivitäten, um eventuellen Konflikten vorzubeugen, z.B. Sperren des Zugriffs auf eine Datenbank

(8) Festlegung der Verantwortlichkeit bei Fehlerbehebung
- bei Auftreten von Kommunikationsfehlern, die sich trotz Fehlerbehebungsmechanismen der unteren Schichten bis in die Anwendungsschicht auswirken, versucht ein Kommunikationspartner, diesen Fehler zu beheben

(9) Feststellen von eventuellen Einschränkungen bezüglich der Syntax
- verwendete Zeichensätze und/oder verwendete Datenstrukturen
- gemeinsame Transfersyntax wird von Darstellungsschicht unter Berücksichtigung dieser Einschränkungen ausgehandelt

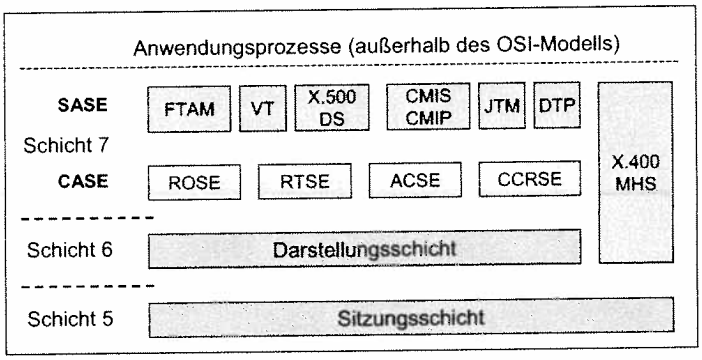
Bild: Dienste der Anwendungsschicht

Die Anwendungsschicht führt die folgenden Dienste durch:

Die Anwendungsschicht (application layer) bietet den Anwendungsprogrammen/-prozessen Kommunikationsdienste an. Sie stellt damit bestimmte Dienstleistungen, die von den Details der Kommunikation hinreichend abstrahieren, zur Verfügung. Die Anwendungsschicht enthält eine Anzahl von Anwendungsdienstelementen (ASE, Application Service Element), die Dienste für die Anwendungsprozesse erbringen. Die Anwendungen selbst befinden sich außerhalb des OSI-Modells.

Die ASEs werden in zwei Gruppen eingeteilt:

- ASEs mit allgemeinen Aufgaben **(CASE,** Common Application Service Element),
- ASEs mit spezifischen Aufgaben **(SASE,** Specific Application Service Element).



CASE Common Application Service Element
SASE Specific Application Service Element
ROSE Remote Operations Service Element
RTSE Reliable Transfer Service Element
ACSE Association Control Service Element
CCRSE Commitment, Concurrency and Recovery Service Element

FTAM File Transfer, Access and Management
VT Virtual Terminal)
MHS Message Handling Service (X.400)
DS Directory Service (X. 500)
CMIP Common Management Information Protocol
CMIS Common Management Information Service
JTM Job Transfer and Manipulation
DTP Distributed Transaction Processing

Zur Gruppe CASE gehören:

- ACSE, ROSE, RTSE und CCRSE.

Zur Gruppe CASE gehören:

- FTAM, VT,
- X.500 Directory Service (DS),
- CMIS, CMIP,
- JTM, DTP,
- X.400 Message Handling System (MHS).

Bild: Protokolle der Anwendungsschicht

CASE (Common ASE)

ACSE (Association Control Service Element)	Auf- und Abbaut von elementaren Verbindungen zwischen Anwendungsinstanzen (Application Association).
RTSE (Reliable Transfer Service Element)	Zuverlässiger Datentransfer mit einem vollständigen Transfer, der nur einmal stattfinden muss.
ROSE (Remote Operations Service Element)	Entfernter Operationsaufruf für asymmetrische Zusammenarbeit zwischen Client und Server
CCRSE (Concurrency and Recovery Service Element)	Verteilte Transaktionsverarbeitung mit Synchronisation und Fehlerbehebung zur Gewährleistung der Datenkonsistenz

SASE (Specific ASE)

FTAM (File Transfer, Access and Management	Entfernter Dateizugriff bzw. Dateiverwaltung
VT (Virtual Terminal)	Zugriff eines lokalen Terminals auf eine entfernte Anwendung ohne gegenseitige Kenntnis der Realisierung selbst.
DS (Directory Service)	Verzeichnisdienst zur Abbildung von Namen auf Adressen. Empfehlungen: ITU-T X.500 und weitere
CMIP (Common Management Information Protocol)	CMIS dient dem Zugriff auf entfernte Managementobjekte
CMIS (Common Management Information Service)	CMIP transportiert Managementinformation
JTM (Job Transfer and Manipulation)	Kontrolliert die Verarbeitung auf einem entfernten Rechner.
DTP (Dstributed Transaction Processing)	Ermöglicht verschachtelte Transaktionen mit vielen Beteiligten und unterschiedlichen Koordinatoren
MHS (Message Handling Service)	Austausch von Meldungen zwischen Anwendungsprozessen bzw. Personen, Empfehlungen: ITU-T X.400 und weitere

Ähnliche Dienste existieren im Internet:

- VT entspricht Telnet,
- FTAM entspricht FTP (File Transfer Protocol),
- CMIP entspricht SNMP (Simple Network Management Protocol).

ACSE (Association Control Service Element)

stellt Assoziationen (Verbindungen) zwischen Anwendungsprozessen her. Eine Assoziation begründet einen Anwendungskontext, der durch einen eindeutigen Namen benannt wird.

ACSE Dienstelemente

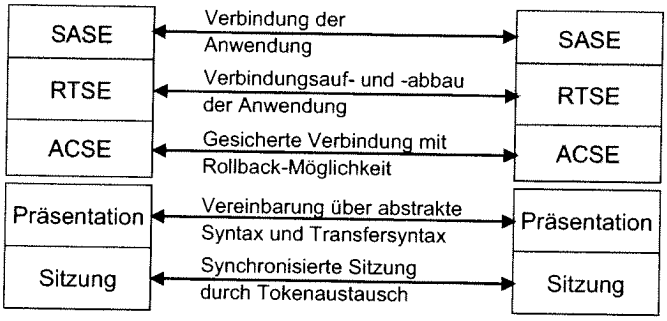
ACSE-Dienstelement	Beschreibung	Request/ Indication	Response/ Confirm
A-Associate	baut eine Assoziation auf	x/x	x/x
A-Release	baut eine Assoziation ab	x/x	x/x
A-Abort	Abbruch durch Benutzer	x/x	-/-
A-P-Abort	Abbruch durch Diensterbringer	-/x	-/-

x: vorhanden; - nicht vorhanden

RTSE (Reliable Transfer Service Element)

überträgt eine Benutzernachricht vollständig und genau einmal. Ist dies wegen nicht behebbarer Fehler in einer bestimmten Zeitspanne nicht möglich, erhält der Sender eine negative Quittung.

RTSE setzt auf ACSE auf. Es leistet einen Datenaustausch, dessen Zuverlässigkeit höher ist als diejenige der Darstellungsschicht. Dazu wiederholt RTSE im Fehlerfall den Datentransfer, bis er vollständig abgeschlossen ist. Die Zuverlässigkeit wird durch Quittungen dokumentiert, die RTSE dem Sender ausstellt, ohne dass der Empfänger sich darum kümmern muss. Über RTSE sind nur einfache Assoziationen möglich. Für verkettete Assoziationen ist CCRSE erforderlich.



SASE Specific Application Service Element
RTSE Reliable Transfer Service Element
ACSE Association Control Service Element

Bild: Protokollstruktur des Relable Transfer Service Element (RTSE)

RTSE greift direkt auf die folgenden Dienste der Darstellungs- bzw. Sitzungsschicht zu:

- Aktivitätsverwaltung,
- Synchronisation (nur Nebensynchronisationspunkte),
- normale Datenübertragung (P-Data),
- Exception Report (P-Control-Give),
- Tokenverwaltung (P-Token-Please).

RTSE kann zusammen mit ROSE einfache, verteilte Anwendungen unterstützen.

RTSE-Dienstelemente

RTSE-Dienstelement	Beschreibung	Request/Indication	Response/Confirm
RT-Open	baut eine RT-Beziehung auf	x/x	x/x
RT-Close	baut eine RT-Beziehung ab	x/x	x/x
RT-Transfer	gesicherte Übertragung eines Datenblocks	x/x	-/x
RT-Turn-Please	Tokenanforderung	x/x	-/-
RT-Turn-Give	Tokenübergabe	x/x	-/-
RT-U-Abort	Abbruch durch den Benutzer	x/x	-/-
RT-P-Abort	Abbruch durch Darstellungsschicht	-/x	-/-

x: vorhanden; - nicht vorhanden

ROSE (Remote Operations Service Element)

nutzt die Dienstprimitive von RTSE, wenn diese im Applikationskontext definiert sind. Sonst setzt es direkt auf ACSE auf. Der **Initiator** (invoker) löst eine Operation aus, der **Ausführende** (performer) führt sie aus. Eine Operation kann Folgeoperationen nach sich ziehen.

Es sind die folgenden **Operationsklassen** definiert:

- Klasse 1: synchron, mit Bestätigung für Erfolg oder Misserfolg,
- Klasse 2: asynchron, mit Bestätigung für Erfolg oder Misserfolg,
- Klasse 3: asynchron, negative Bestätigung nur bei Misserfolg,
- Klasse 4: asynchron, Bestätigung nur bei Erfolg,
- Klasse 5: asynchron, ohne Bestätigung.

Synchron bedeutet, dass eine Operation abgeschlossen sein muss. bevor eine weitere gestartet werden kann. Dies ist für Dialoge angebracht. Für Dateitransfers können **asynchrone Operationen,** die sich zeitlich überlappen können, vorteilhaft sein. Der Standard empfiehlt die Verwendung der Klassen 1 und 2, da bei den anderen Klassen Probleme wie mehrfache oder gar keine Ausführung auftreten können.

ROSE-Dienstelemente

Dienstelement	Parameter
RO-Invoke.req, .ind	InvokeID, OpCode, Eingabe-Argumentliste
RO-Return-Result.req, .ind	InvokeID, Ausgabe-Argumentliste
RO-Return-Error.req, .ind	InvokeID, Fehlercode
RO-Reject.ind	InvokeID, Problemcode

(req = request, ind = indication)

ROSE wirkt mit anderen Dienstelementen zusammen

CCRSE (Commitment, Concurrency and Recovery Service Element)

wird zusammen mit DTP für die Transaktionsverarbeitung eingesetzt. CCRSE ist dabei für das Commitment (Abschließen) und das Rollback (Zurücksetzen) der einzelnen Schritte einer Transaktion zuständig, während DTP die Koordination der gesamten Transaktion steuert. Zur Vergleich: **RTSE** ist nur für einfache Übertragungen gedacht.

Eine **Transaktion** ist eine Folge von Aktionen, die entweder vollständig oder gar nicht (alle vor Beginn der Transaktion bestehen Zustände bleiben unverändert) ausgeführt wird.

Die Eigenschaften einer Transaktion werden in der Abkürzung ACID (Atomicity, Consistency, Isolation, Durability) zusammengefasst.

- **Atomizität** (Atomicity) bedeutet, dass eine Transaktion entweder vollständig oder gar nicht ausgeführt wird. In verteilten Systemen mit potenziell unzuverlässigen Verbindungen sind dafür geeignete Verfahren notwendig.
- **Konsistenz** (Consistency) bedeutet, dass Daten von einem konsistenten Zustand in einen anderen konsistenten Zustand überführt werden. Widersprüchliche Daten (Inkonsistenzen) werden also verhindert.
- **Isoliertheit** (Isolation) stellt sicher, dass Teilergebnisse einer Transaktion, die während ihrer Ausführung entstehen, von außerhalb nicht sichtbar werden.
- **Dauerhaftigkeit** (Durability) ist gewährleistet, wenn die Ergebnisse einer erfolgreich abgeschlossenen Transaktion unter allen Umständen (Leitungsunterbrechung, Systemabsturz etc.) dauerhaft gespeichert bleiben.

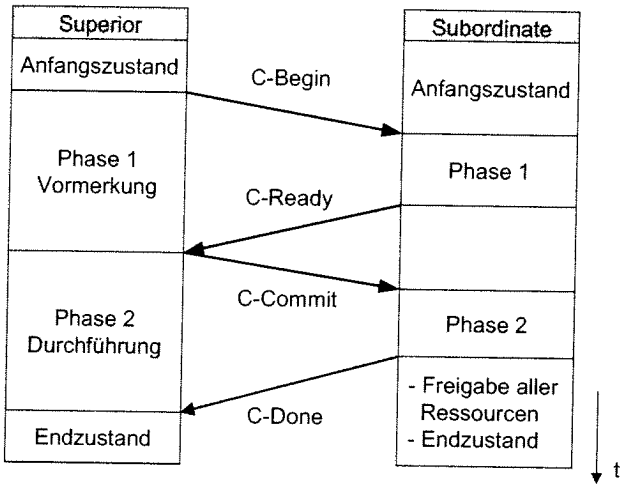


Bild: Ablauf beim Two-Phase Commit

Die Bezeichnung CCR (Commitment, Concurrency, and Recovery) weist auf diese Aspekte hin:

- Erfolgreicher Abschluss der Transaktion (commitment),
- Umgang mit parallel ablaufenden Transaktionen unter Ausschluss gegenseitiger Beeinflussung (concurrency, Konkurrenzsteuerung),
- Zurücksetzen (recovery), falls die Transaktion nicht erfolgreich abgeschlossen werden kann.

Zentrale Konzepte für die Transaktionsverarbeitung sind der **atomare Aktionsbaum** (atomic tree) und das **zweistufige Festschreiben** der Ergebnisse (two-phase commit) am Ende der Transaktion. Eine Transaktion wird von einem Master gesteuert. Die beauftragten, untergeordneten Instanzen (Subordinates) melden die Ergebnisse an den Master zurück. Nur wenn alle Subordinates ihre Aufgaben erfolgreich erfüllt haben, kann die Transaktion abgeschlossen werden. Andernfalls muss zurückgesetzt werden. Die Bezeichnung Baum weist darauf hin, dass ein Subordinate selbst wieder Master gegenüber weiteren Subordinates sein kann.

Die erste Phase einer Transaktion wird mit Hilfe des Dienstelements C-Begin eingeleitet und mit C-Prepare abgeschlossen. Falls mindestens einer der Subordinates mit C-Refuse antwortet, muss die Transaktion mit C-Rollback zurückgesetzt werden. Wenn alle Subordinates mit C-Ready antworten (also erfolgreich waren), leitet der Master mit C-Commit die Phase zwei ein. Die Transaktion ist abgeschlossen, wenn alle Subordinates mit C-Done geantwortet haben.

CCRSE-Dienstelemente

Phase	Dienstelement	Beschreibung
1	C-Begin.req,.ind	Aufforderung an den Subordinate zum Beginn einer Transaktion
1	C-Prepare.req,.ind	Aufforderung an den Subordinate, C-Ready bzw. C-Refuse zu senden
1	C-Ready.req,.ind	Der Subordinate bestätigt seine Bereitschaft zum C-Commit
1	C-Refuse.req,.ind	Der Subordinate weist die Aufforderung zum C-Commit zurück
2	C-Commit.req,.ind	Der Superior fordert den Subordinate auf, die Transaktion dauerhaft zu machen
2	C-Done.req,.ind	Der Subordinate bestätigt, dass er die Transaktion korrekt abgeschlossen hat
2	C-Rolback.req,.ind	Der Superior fordert den Subordinate auf, alle in der Transaktion bisher durchgeführten Änderungen rückgängig zu machen
2	C-Rollback.resp,.conf	Der Subordinate bestätigt das Zurücksetzen aller Änderungen
1,2	C-Restart.req,.ind	Der jeweilige Partner wird aufgefordert, auf einen früheren Zustand zurückzusetzen
1,2	C-Restart.resp,.conf	Der Partner bestätigt die Ausführung des Zurücksetzens

OSI-Anwendungsdienste

Von genannten Diensten der SASE-Gruppe existieren mehrere (VT, FTAM, CMIP, CMIS) in ähnlicher Form im Internet und werden dort beschrieben. Deshalb werden nur die Dienste JTM und DTP kurz beschrieben.

JTM (Job Transfer and Manipulation)

leistet den Austausch von Dokumente (sog. Job Specifications), die sich auf Verarbeitungsaufträge für ein bestimmtes System beziehen. Daran beteiligt sind der JTM-Dienst und eine Reihe von Agencies, denen bestimmte Teilaufgaben zufallen. Der Anwendungsprozess, der einen Verarbeitungsauftrag auslöst, wird als Initiating Agency bezeichnet, der ausführende Prozess als Execution Agency. Die Source Agency (z. B. ein lokaler Massenspeicher) liefert Informationen/Daten, die für die Auftragsausführung benötigt werden. Ein weiterer Anwendungsprozess kann als Job Monitor beteiligt sein. Dieser erhält vom JTM-Dienst Informationen über den Zustand der Auftragsausführung. Nach Abschluss des Auftrages werden Ergebnisse an die Sink Agency übermittelt. Die Agencies müssen sich nicht auf verschiedenen Systemen befinden.

JTM-Dienstelemente

Dienst	Funktion
J-Initiate-Work	Initiating Agency beauftragt ihre lokale JTME
J-Give	Ein JTME verlangt ein Dokument von einer Source oder Execution Agency
J-Dispose	JTNIE übergibt ein Dokument an eine Execution oder Sink Agency
J-Taskend	Die Execution Agency meldet das Ende einer Aktivität an ihre lokale JTME
J-Status	Eine JTME verlangt Information über den Fortgang einer Aktivität
J-Kill	Eine JTNIE beendet alle Aktivitäten eines Auftrags abrupt
J-Stop	Eine JTME hält alle Aktivitäten eines Auftrags vorübergehend an

JTM bietet umfangreiche Dienste, weshalb hier nur die Basie Class betrachtet sei. Diese unterstützt nur einen Job, der keine Sub-Jobs erzeugen kann. Die Initiating Agency wird im Folgenden als JTM Service Requester bezeichnet. JTM Service Responder sind diejenigen Agencies, die Anforderungen vom JTM Service Provider erhalten.

DTP (Distributed Transaction Processing)
ermöglicht die Transaktionsverarbeitung unter Beteiligung mehrerer Systeme. Anwendungsprozesse auf Clients und Servern nutzen das ASE (Application Service Element) DTP, das seinerseits auf CCRSE und ACSE aufsetzt). Clients können Transaktionen auslösen, die mehrere Server mit einbeziehen.