2. Spezifikationen zur Datenübertragung

2.1. Netzwerkunterteilung

Netzwerke können nach geographischen Gesichtspunkten und der Art ihres Aufbaus (Topologien) unterteilt werden. Bei der geographischen Einteilung unterscheidet man Local Area Network (LAN), Metropolitan Area Network (MAN) und Wide Area Network (WAN). LAN und MAN werden hauptsächlich zur Vernetzung von Gebäuden und verschiedenen Unternehmensteilen innerhalb einer Stadt verwendet. Es werden häufig die gleichen Topologien verwendet. Die Übertragungsraten liegen heutzutage bei 100Mb/s. Das WAN benutzen hauptsächlich große und weltweit operierende Unternehmen für die Vernetzung ihrer Unternehmensteile. Die Aufwendungen dafür sind sehr groß und Kostenintensiv und werden hauptsächlich über Leitungen der nationalen Telekomunternehmen abgewickelt. Die Übertragungsmedien können in Form von Standleitungen, ISDN-Wählverbindungen und Satellitenverbindungen existieren.

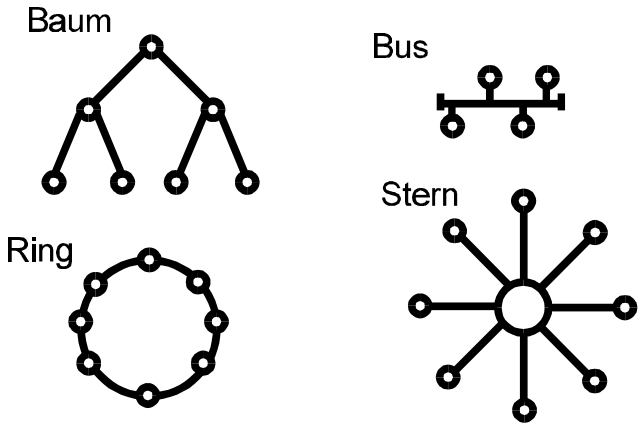

Abbildung 2.1-1 Netztopologien [nach 4, S.33]

Die physische Struktur eines Kommunikationssystems nennt man Netzwerktopologie, sie ist ein Abbild der räumlichen und geographischen Verteilung der einzelnen Komponenten, aus denen das Netzwerk besteht. Beim LAN findet man am häufigsten 4 Strukturen: Bus/Baum-Topologie, Ring-Topologie, Stern-Topologie und Punkt-zu-Punkt-Topologie. Im LAN können verschiedene Topologien miteinander verknüpft werden.

2.2. Unterteilung drahtloser Systeme

Die drahtlosen Übertragungssysteme (Wireless Systems) werden genauso wie die drahtgebundenen Übertragungssysteme verschieden charakterisiert. Die Systeme werden in Global-, Wide- und Local-Zonen eingeteilt.

Es wird grundsätzlich zwischen 2 verschiedenen Technologien unterschieden. Die analoge Technologie wird heutzutage nur noch in den bestehenden Systemen (NMT - Nordic Mobil-Telephone, AMPS-Advanced Mobile Phone Systems, TACS - Total Access Communication Systems, C-Tel - C-Netz der Telekom) angewandt und verbessert. Die Zukunft liegt nur noch in der digitalen Zell-Technologie. Einige Systeme sind GSM900, PCN (GSM1800) (Personal Communication Network, A-AMPS (Digital-AMPS) und PDC (Personal Digital Cellular, Japan).

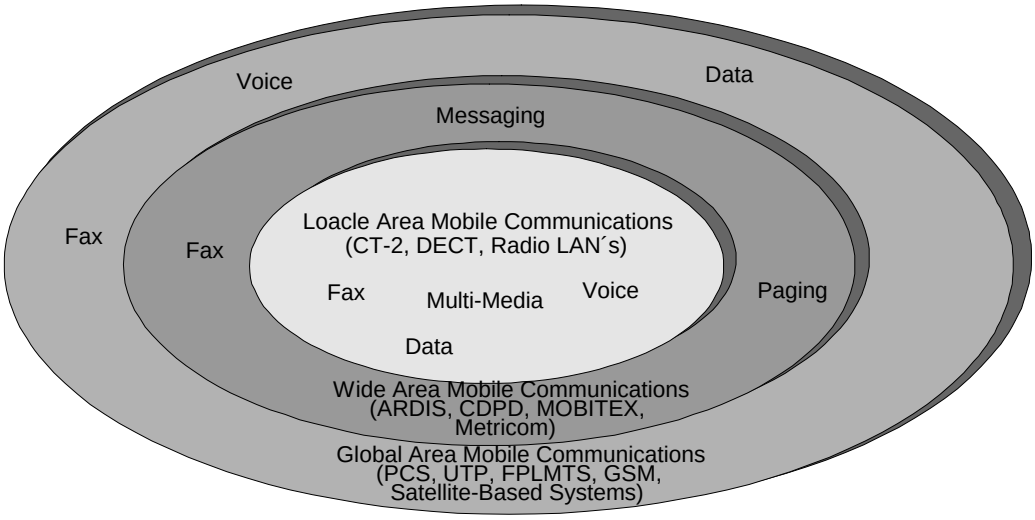

Abbildung 2.2-1 Wireless Systems, Services und Charakteristika [nach 12, S.2]

Die Abbildung 2.2-1 zeigt eine Einteilung der verschiedenen Dienste auf die Entfernungen, dabei wurden statistische Erhebungen herangezogen und Analysen, in welchem Umgebungsradius die verschiedenen Anwendungen sinnvoll sind.

2.3. ISO / OSI - Schichtenmodell

Das ISO / OSI - Schichtenmodell (Abbildung 2.3-1) wurde verabschiedet um einen einheitlichen Protokoll-Funktionsaufbau eines Netzwerkes realisieren zu können und die Kompatibilität zwischen den Topologien zu gewährleisten. Die 7 Schichten des Modells kann man in drei Teile unterteilen. Die Schichten 1 bis 3 beschreiben die netzorientierten Funktionen und die Schichten 5 bis 7 die Anwendungsprotokolle. In der Schicht 4 wird sichergestellt, daß die anwendungsorientierten Schichten vom physikalischen Transportnetz unabhängig sind, sie gewährleistet auch, daß verschiedene Transportnetze für die Verbindung zwischen Teilnehmern eingesetzt werden.
Durch die Standardisierung sind die Schnittstellen zwischen den Schichten eindeutig definiert und es können Produkte verschiedener Hersteller und Techniken kombiniert werden. Die Schichten sind bis auf ihre Schnittstellen völlig unabhängig voneinander und haben die ihnen nach Definition zugewiesenen Aufgaben zu erledigen.
Kurzbeschreibung der 7 Schichten:

Schicht 1: Bitübertragungsschicht (Physikalische Ebene, nicht Hardware)
In der Schicht 1 werden das Übertragungsmedium und die Regeln für die Übertragung von einzelnen Bits spezifiziert. Dazu gehören u.a.:
- Leitungscodes (NRZ-Code, Manchester-Code u.a.)
- Spezifikation von Kabeln und Steckern (V.24, X21 u.a.)
- Bitübertragungsverfahren

Schicht 2: Sicherungsschicht (Sicherungsebene)
Hier liegt die Verantwortlichkeit für die sichere Übertragung zwischen direkt benachbarten Stationen. Es erfolgt die Zusammenfassung der Bits in sogenannte Frames und das Erstellen einer Prüfsumme für die Fehlererkennung, die mit angehangen wird. Die Schicht 2 wird in einen gesicherten und ungesicherten Dienst unterteilt. Beim letzteren werden die fehlerhaften Frames eliminiert. Die wiederholte Datenanforderung wird durch eine der höheren Schichten ausgelöst. Im gesicherten Modus wird der verworfene Frame sofort neu angefordert.

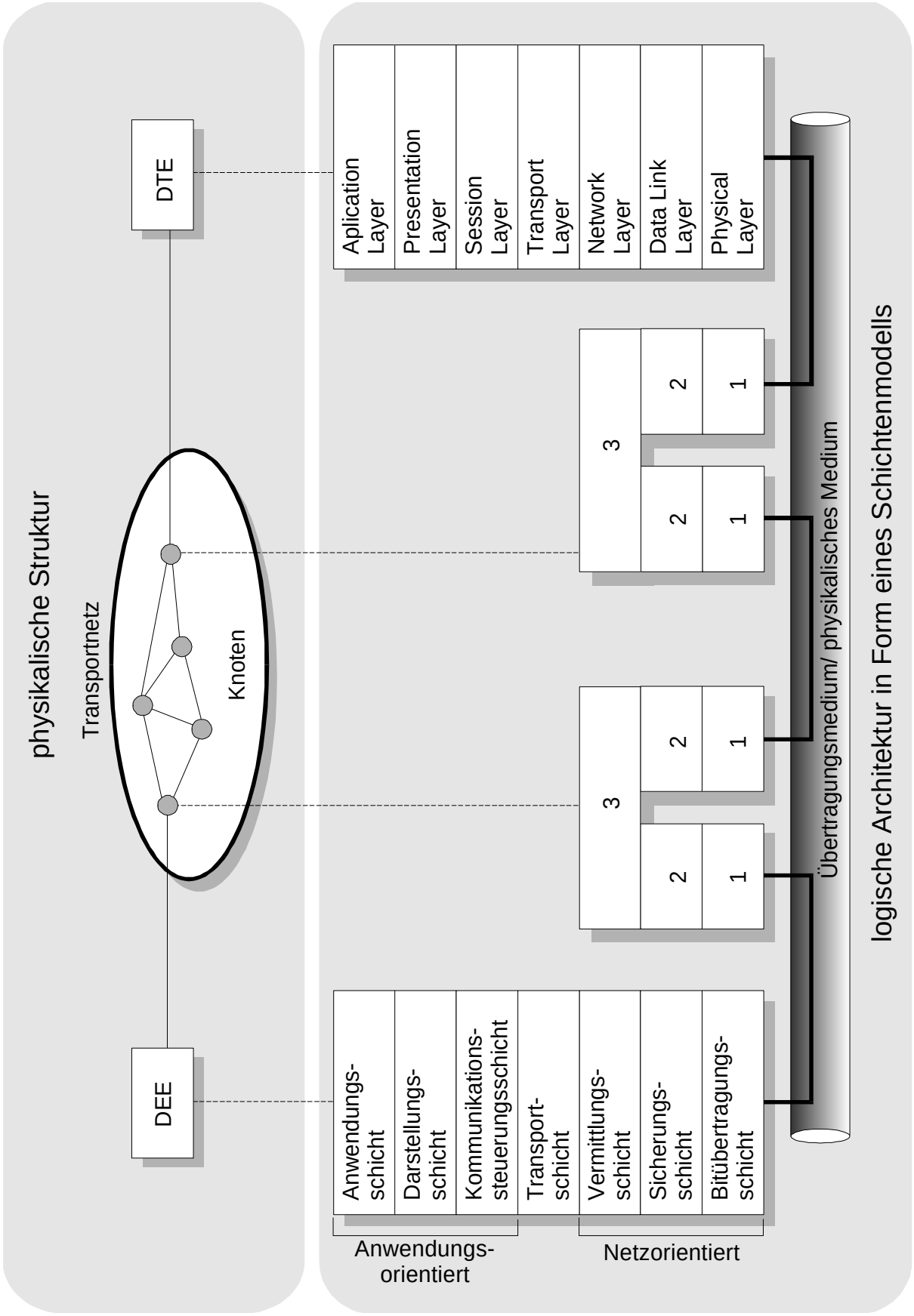

Abbildung 2.3-1 OSI-Referenzmodell

Schicht 3: Verbindungsschicht (Netzwerkebene)
Im Network Layer werden die Verbindungen von einem Teilnehmer zum anderen Teilnehmer aufgebaut. Es wird die Route durch das Netz für die einzelnen Datenblöcke festgelegt (Routing). Die Regeln sind im Routing-Protokoll hinterlegt. Die Schicht 3 kann als Paketvermittlungsschicht bezeichnet werden.

Schicht 4: Transportschicht
Es wird eine virtuelle Ende-zu-Ende-Verbindung für die in Paketen festgelegten Daten errichtet, gesteuert und beendet. Diese Schicht hat die Aufgabe die Übertragungsfehler zu korrigieren und ist sehr eng verbunden mit den Schichten 2 und 3. Es kann eine Anpassung an unterschiedliche Netzeigenschaften notwendig sein. Weitere Funktionen sind die Adressübersetzung und die Datensegmentierung.

Schicht 5: Sitzungsschicht (Kommunikationssteuerungsschicht)
Für die Synchronisation zwischen zwei Kommunikationsprozessen ist der Dialogablauf in Haupt- und Nebensynchronisationspunkt unterteilt, welche fortlaufende Nummern erhalten. Beim Verlust der Synchronität (Fehler) kann diese dadurch wieder hergestellt werden.

Schicht 6: Darstellungsschicht
In der Darstellungsschicht wird die Umsetzung der Information (Zeichensätze) in ein einheitliches Format auf der Sendeseite vorgenommen. Hier können auch Daten komprimiert, konvertiert und verschlüsselt werden.

Schicht 7: Anwendungsschicht
In der Schicht 7 sind die System- und Anwendungssteuerungen angesiedelt. Die Funktionen bestehen u.a. in der Identifikation der Kommunikationspartner und deren Berechtigungsprüfung und Zugang zur Kommunikation.

In den Rechnernetzen kann man zwei Arten von Kommunikation unterscheiden. Bei der verbindungslosen Kommunikation werden die Daten (Netzmanagement Kommandos, Parameterabfragen) an die Partnerin gesendet ohne eine Vereinbarung zum Kommunikationsablauf zu treffen. Diese Kommunikation kann mit oder ohne Bestätigung durchgeführt werden. Eine dauerhafte Kommunikation bezeichnet man als verbindungsorientiert. Das Senden von Daten von einem Teilnehmer zum anderen geschieht nur nach vorheriger Vereinbarung mit ihm, d.h. die Kommunikationsbeziehung ist beim Datensenden bereits aufgebaut. Diese beiden Kommunikationsarten werden in der Schicht 3 realisiert. Eine Bestätigung der Nachricht ist hierbei generell garantiert.
Beim Aufbau einer Verbindung zwischen zwei Partnersystemen entsteht von einer Schicht *n* des einen Systems zu dementsprechenden Schicht *n* des anderen Systems eine virtuelle Verbindung. Virtuell bedeutet, daß die Verbindung nicht direkt besteht sondern als gedacht angenommen werden kann. Diese Verbindung ist nicht meßbar, sondern ergibt sich aus den Zusammenhängen im Aufbau des Datensegmentes. Mehrere virtuelle Verbindungen können über ein und dieselbe physische Verbindung bestehen, oder in dieser zusammengeführt sein. Eine derartige Definition vereinfacht oft die Betrachtung von größeren Zusammenhängen und ermöglicht so die schnelle Verständlichkeit, ohne jedesmal auf die sich wiederholenden Einzelheiten einzugehen. Eine virtuelle Verbindung ist keine Verbindung im klassischen Sinne, sie stellt sich nach außen zwar so dar, muß aber nicht ständig bestehen. Die Steuerung wird von der Hardware und/oder Software übernommen und kann zeitweise, bruchstückhaft, parallel, mehrfach gleichzeitig oder springend von einer auf eine andere Leitung zwischen gleichem Sender und Empfänger

oder gleichem Sender und verschiedenen Empfängern und im Time Division Multiplex (TDM) mit anderen Verbindungen bestehen.
Eine virtuelle Verbindung kann auch aus mehreren physischen Verbindungen bestehen, z.B. ein Verbindung Filiale und Geschäftssitz, die nur durch ISDN-Wählverbindungen zusammen geschaltet werden. Im Internet bestehen meist nur virtuelle Verbindungen, die physisch für jedes Datenpaket einen anderen Weg nehmen können.
Für die Kommunikation zwischen zwei Schichten in Partnersystemen müssen diese sich in der Bereitschaft befinden eine gewünschte Verbindung aufzubauen und es müssen die Kommunikationsdienste der darunterliegenden Schichten verfügbar sein. Jede Dateneinheit setzt sich aus den Benutzerdaten und den Kontrollinformationen (Datenkopf) zusammen. Die Dateneinheit der Schicht *n* bildet zugleich die Benutzerdaten der Schicht *n-1*, der wieder ein Datenkopf angefügt wird. Die Dateneinheit der Schicht *n* wird in der Schicht *n-1* nicht interpretiert oder ausgewertet, dies geschieht erst in der dementsprechenden Schicht des Partnersystems.

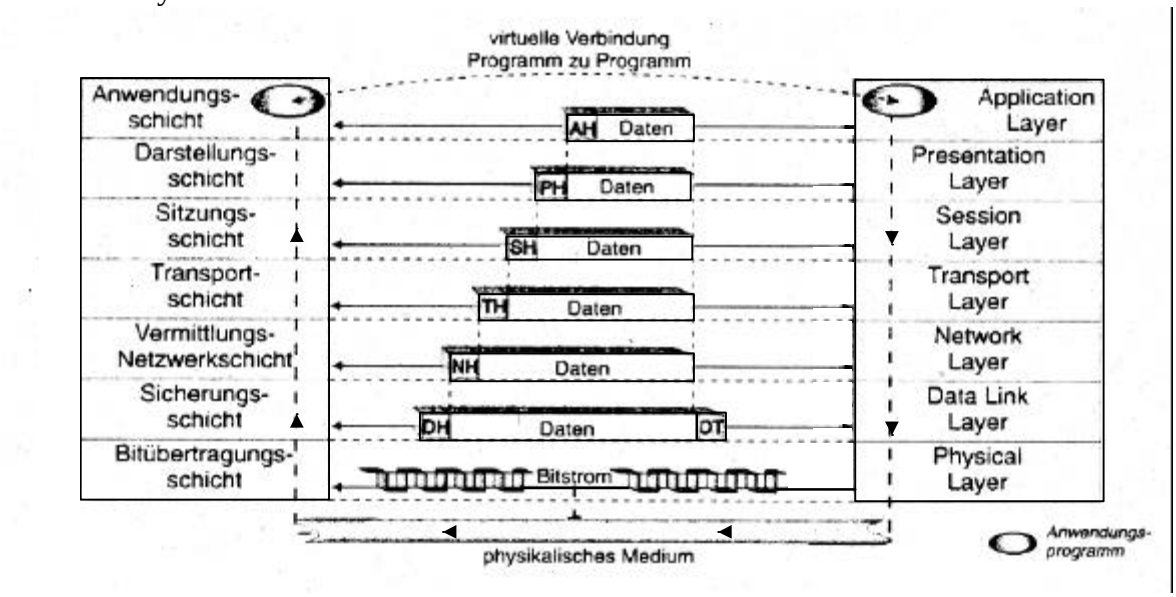

Abbildung 2.3-2 Zusammensetzung der Frames [nach 8, S.41]

AH Header der Anwendungsschicht
PH Header der Darstellungsschicht
SH Header der Sitzungsschicht
TH Header der Transportschicht
NH Header der Netzwerkschicht
DH Header der Sicherungsschicht
DT Trailer der Sicherungsschicht

Ein Rahmen (Frame) enthalten die Protokollstrukturen der jeweiligen Schicht, diese setzten sich aus dem Kopf und Daten zusammen. Als Daten bezeichnet man die eigentlichen Nutzdaten des Benutzers und die Protokollinformationen der darüberliegenden Schicht. Im Kopf befinden sich alle notwendigen Informationen, um die Verwaltungs-, Sicherungs- und Übertragungsarbeit zu leisten. Als Frame direkt wird allerdings nur die letzte Stufe in der Sicherungsschicht bezeichnet, vorher sind es im allgemeinen nur Datenpakete oder Datagramme. Für die Übertragung der Daten werden verschiedene Informationen benötigt, so enthält jedes Datagramm Angaben für die darüber liegende Schnittstelle, über aufgetretenen Übertragungs- oder Protokollfehler, die Quell-

und Zieladresse, sowie auch Portadressen für die Anwendungsverknüpfung. In welchem Umfang diese Angaben ausfallen hängt von der jeweiligen Schicht ab.
Die Frame-Architektur wurde notwendig, da es keine direkte Verbindung zur Gegenstelle gibt sondern es sich um virtuelle Verbindungen handelt, die nur aufgebaut werden, wenn es notwendig wird. In Bus-, Ring- und Punkt-zu-Mehrpunktverbindungen sind solche Frames notwendig, damit der Teilnehmer, für den die Daten bestimmt sind, eindeutig identifiziert werden kann. Bei einer Punkt-zu-Punkt-Verbindung ist dies so nicht notwendig, da der einmal aufgebaute Übertragungskanal für die ganze Zeit bestehen bleibt und nur durch den Benutzer selbst getrennt werden kann. Je komplexer die Netzstrukturen werden und je mehr Daten übertragen werden müssen, desto größer werden auch die Kopfinformationen in den Frames. Der Overhead, das Verhältnis von Übertragungs- zu Nutzdaten, wird immer größer. Um den Overhead möglichst klein zu halten, wurden Vereinbarungen und Normen geschaffen, die eine Identifizierung der einzelnen Informationen (Bits, Bytes) besser ermöglicht.
In manchen Netzen ist es notwendig, einen Übergang von einem zum anderen Verbindungssystem zu ermöglichen. Durch diese Verknüpfung können die vorhandenen Übertragungskapazitäten besser ausgenutzt und gesteuert werden. Beim einfachen Telefonat z.B. werden die Daten vom Teilnehmer A zur Vermittlungsstelle mittels einer Punkt-zu-Punkt-Verbindung übertragen. Zwischen den Vermittlungsstellen wird oft schon ein Paketvermittlungsverfahren eingesetzt, das die Daten in einzelne Datensegmente unterteilt. Durch diese Umsetzung in eine andere Art der Verbindung werden die vorhanden Kapazitäten besser ausgeschöpft. An der letzten Vermittlungsstelle werden die Daten wieder zusammengesetzt und mittels Punkt-zu-Punkt-Verbindung zum Teilnehmer B übertragen. Die reine Datenübertragung ist zeitlich nicht so eng gebunden, wie z.B. die Übertragung von Sprache und bewegten Bildern, dadurch können hier auf der ganzen Übertragungsstrecke Strukturen eingesetzt werden, die einer Vielzahl von Teilnehmern den scheinbar gleichzeitigen Zugriff auf alle Daten ermöglichen, aber nicht unbedingt immer die gleiche zeitliche Abfolge gewährleisten.

2.4. IEEE Projekt 802 - Lokal-Area-Network (LAN)

Für lokale Netzwerke wurde eine genauere Definition der Schichten notwendig, da das OSI-Schichtenmodell eher für die Bedürfnisse von WAN's ausgelegt ist.
Einen Überblick über die Normen der IEEE für lokale Netzwerke:

IEEE 802.1	Architektur
IEEE 802.2	Logical Link Control
IEEE 802.3	CSMA/CD (Ethernet)
IEEE 802.4	Token Bus
IEEE 802.5	Token Ring
IEEE 802.6	DQDB (MAN)
IEEE 802.7	Breitband LAN
IEEE 802.8	Fiberoptisches LAN
IEEE 802.9	Integriertes Sprach- und Daten LAN
IEEE 802.10	Übertragungssicherheit
IEEE 802.11	Wireless LAN (gegenwärtig in Arbeit)

Die Unterschiede zwischen den einzelnen Normen liegen hauptsächlich in der Verkabelung, dem Zugriffsverfahren und der Bitübertragung.

Die LAN-Netze können über verschiedene Kopplungselemente miteinander verbunden werden. Die eingesetzten Elemente unterscheiden sich hinsichtlich ihrer Funktionalität bezüglich der Schichten.

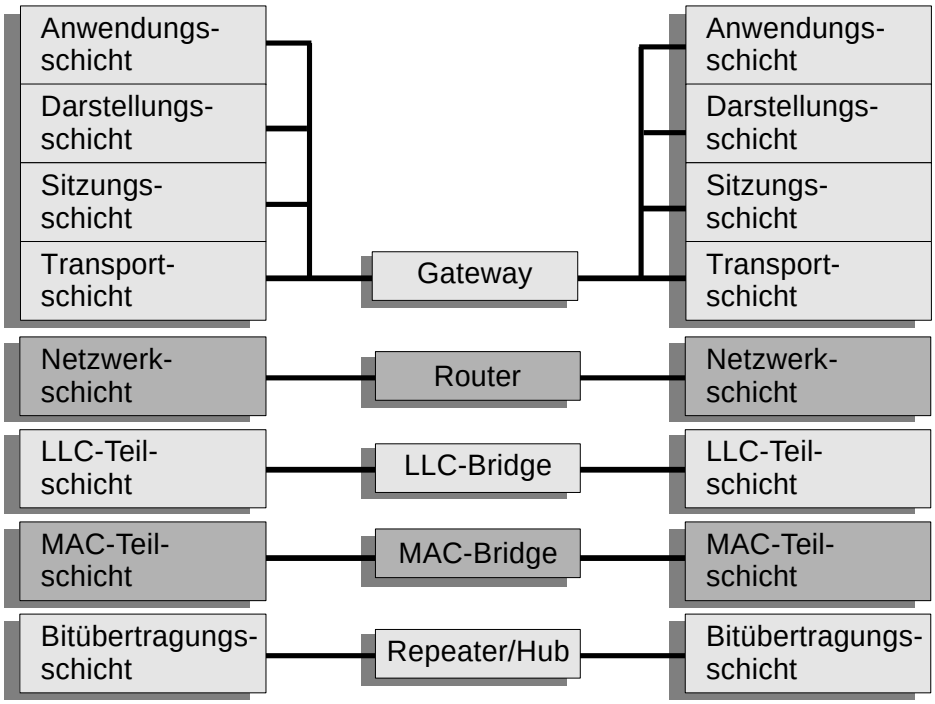

Abbildung 2.4-1 LAN-Kopplungselemnte [nach 8, S.52]

- Repeater/Hub: Ein Repeater stellt die einfachste Form der Netzwerkverknüpfung dar. Er hat die Aufgabe die ankommenden Signale vom Kabelsegment aufzunehmen, zu verstärken und weiterzuleiten. Es besteht die Möglichkeit, verschiedene Verkabelungsvarianten (Twisted Pair, Koax (10BASE5), Koax (RG58) (10BASE2)) miteinander zu koppeln. Ein Hub hat die Aufgabe die Ringstruktur aufzulösen und in eine Sternverkabelung zu überführen, was das Einbinden neuer Stationen erleichtert. Bei der Twisted-PairVerkabelung erfolgt die Anbindung der Stationen über Hubs, die das An- oder Abkoppeln von Stationen vom restlichen Netzwerk trennen, wodurch der Aufwand in größeren Bürolandschaften sehr viel kleiner wird.
- Bridge: haben auch die Aufgabe LAN-Netze zu verbinden, sie sind aber intelligenter als Repeater. Über Bridges lassen sich verschiedene LAN-Segment-Verknüpfungen herstellen. Ihnen obliegt die Fähigkeit Adressen zu lernen und im Stack abzulegen. Sie können LAN`s mit verschiedenen Übertragungstechniken koppeln, sowie den Einsatz von einfachen Filtern ermöglichen.
- Router: Mittels Router lassen sich LAN-WAN-Verbindungen herstellen. Sie entscheiden über den Weg einzelner Datenpakete durch das Netz und entkoppeln interne LAN`s vom externen Zugriff.
- Gateway: Es existieren für die Schichten 4-7 verschiedene Gateway-Typen, die je nach Unterschieden in den Protokollstrukturen in der ersten unterschiedlichen Struktur ansetzen müssen. Mit ihrer Hilfe ist es möglich verschiedene Netze (LAN, DATEX-P, ATM, GSM) zu verbinden. In Gateways erfolgt die Auswertung von Protokollstrukturen (Head-Informationen) und deren Anpassung an die verschiedenen Netz-Protokolle.

2.4.1. LAN - Referenzmodell

Die Schicht 2 des OSI-Modells wird im IEEE 802 - Referenzmodell durch zwei neue Schichten (2a und 2b) ersetzt. Die Schnittstelle zwischen der Sicherungs- und Vermittlungsschicht wurde nach OSI realisiert, dadurch besteht die Kompatibilität ab Schicht 3 zwischen OSI- und IEEE 802-Referenzmodel.

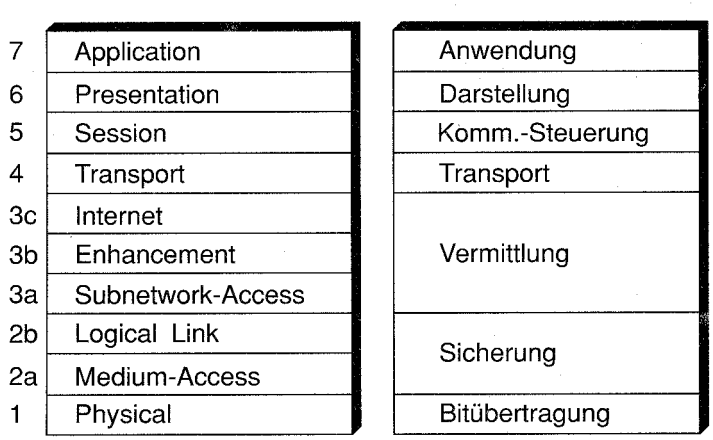

Abbildung 2.4-2 Schichtenmodell für LAN's [nach 6, S.24]

Schicht 1: Physikal Layer (PHY)
Die Funktionen entsprechen der Schicht 1 des OSI-Referenzmodels. In dieser Schicht werden die physikalischen Eigenschaften von Übertragungsmedien und die Prinzipien der Bitübertragung festgelegt.

Schicht 2a: Medium Access Control (MAC)
Die MAC-Schicht kontrolliert, wann die Bits auf das Übertragungsmedium gesendet werden dürfen und realisiert die Übertragung.

Schicht 2b: Logical Link Control (LLC)
Die Aufgabe der LLC-Schicht besteht in der fehlerfreien Übertragung der Frames zwischen Sende- und Empfangspuffer in zwei LAN-Stationen. Das LLC-Protokoll basiert auf dem bitorintierten HDLC-Protokoll. Die LLC-Schicht bildet sozusagen das Dach für die einzelnen Varianten, sie realisiert die Unabhängigkeit der Kommunikationsprotokolle vom LAN-Typ und ist ein sogenannter logischer Multiplexer zwischen den Kommunikationsprotokollen.

Wenn ein Netz aus einem Verbund von Teilnetzen besteht, muß die Schicht 3 weiter unterteilt werden, da die Wegewahl für das Senden der Daten komplexer wird. Die Schicht 3a übernimmt die Wegewahl in jedem Teilnetz, die Schicht 3c im Netzverbund (Internetworking). Die Verfahren der Wegewahl können sehr unterschiedlich sein, deshalb müssen unter Umständen in der Schicht 3b die Netzdienste angepaßt werden. Wenn der Teilnehmer im gleichen LAN vorhanden ist, dann entfallen die Schichten 3b und 3c.

Die Schichten 1 und 2a sind auf den LAN-Adapterkarten implementiert, sie stellen diese aber nicht dar. Die höheren Schichten werden vom Rechner in Form von einer oder mehr Softwarestufen gestellt. Auf der Schicht 2b werden sehr viele SAPs (Service Access Points) als Dienstzugangspunkte implementiert. Die SAPs sind weltweit eindeutig jedem Kommunikationsprotokoll zugeordnet und werden oft auch als Kommunikationspuffer bezeichnet. Durch diesen Puffer ist es möglich, daß die verschiedenen Protokolle über eine und dieselbe LAN-Adapterkarte ihre Daten versenden können.

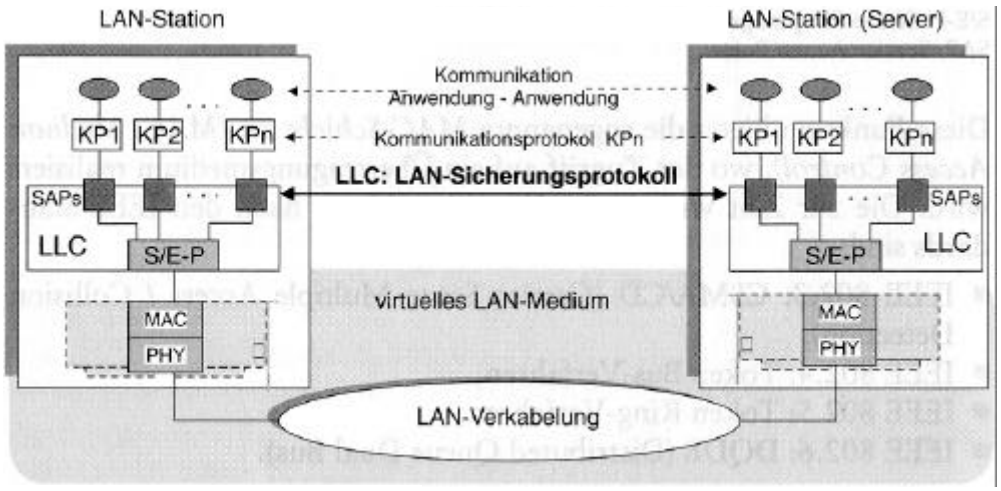

Abbildung 2.4-3 Bedeutung der LLC-Schicht [8, S.82]

S/E-P - Sende-/Empfangs-Puffer
SAPs - Service Access Point

In dieser Abbildung ist auch verdeutlicht, daß die LAN-Adapterkarten mit dem Übertragungsmedium ein virtuelles LAN-Medium bilden. Die Übertragungsfähigkeit ist dabei vom LAN-Typ abhängig. Die Übertragungsprotokolle (TCP/IP, SPX/IPX) können als Sprachen betrachtet werden, mit denen sich die Anwendungen auf den verschiedenen Rechnern verständigen. Bedingung ist, daß alle die gleiche Sprache sprechen. Die Protokolle entsprechen der Netzwerk- und Transportschicht im OSI-Referenzmodell.
Für die Übertragung der Daten im LAN ist es meistens notwendig eine Segmentierung vorzunehmen, da die Länge der übertragenen Frames begrenzt ist. Im dem Datensegment vorangestellten Kopf werden die für die Softwaremodule notwendigen Steuerungsangaben untergebracht, die das Kommunikationsprotokoll realisieren. Die meisten LAN-Protokolle setzen sich aus zwei Teilen zusammen, so daß der Kommunikationsprotokoll-Kopf (KP-Header) auch aus zwei Teilen besteht. Für die sichere Übertragung kommt ein LLC-Header dazu. Als letztes kommen noch die MAC-Steuerungsangaben dazu. Sie bestehen aus einem MAC-Header und einem MAC-Trailer. Das zu übertragene Paket wird als MAC-Frame bezeichnet.

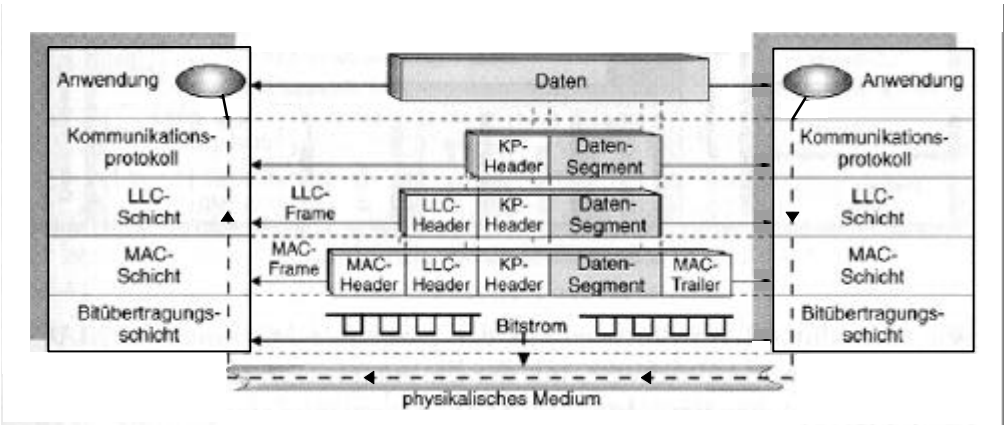

Abbildung 2.4-4 Aufbau eines Datensegmentes [nach 8, S.83]

2.4.2. Die MAC-Schicht

Durch die MAC-Schicht, in der auch die MAC-Adresse enthalten ist, wird jede Adapterkarte weltweit eindeutig identifiziert. Der Mac-Header setzt sich aus der Ziel- und der Quell-Adresse zusammen, die von der IEEE mit einer Länge von 6 Byte (48 Bit)

standardisiert wurden. Die ersten 3 Byte werden mit Ausnahme der ersten 2 Bit als Hersteller-ID (QUI-Code, Organizationally Unique Identifier - Code) bezeichnet. Diese muß jeder Hersteller bei der IEEE beantragen. Damit erhält er einen Block von 3 Byte (2^{24} Adressen), die er frei vergeben kann.

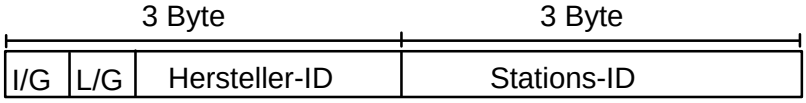

Abbildung 2.4-5 Aufbau der MAC-Adresse [nach 8, S.85]

I/G - Individualadresse (0) / Gruppenadresse (1)
L/G - Lokaladresse (0) / Globaladresse (1)

Mit dem I/G-Bit ist es möglich einen MAC-Frame nur eine Station oder eine ganze Gruppe von Stationen anzusprechen. Bei der Gruppenadressierung kann die Stations-ID eine Bitkombination enthalten, die eine ganze Gruppe kennzeichnet.
Das L/G-Bit kennzeichnet, ob eine Adresse von der IEEE vergeben wurde (Globaladresse) oder ob die Adresse vom unabhängig von der IEEE vergeben wurde (Lokaladresse). Diese Adressen sind dann weltweit nicht mehr eindeutig.
Beim Übergang von einem Zugriffsverfahren zum anderen kann es notwendig werden, die Reihenfolge der Bits zu verändern, da einige Verfahren zuerst das iederwertige Bit auslesen und andere zuerst das Höstwertige.

2.4.3. Die LLC-Schicht

Das LLC-Protokoll basiert auf dem im WAN eingesetzten HDLC (High Level Data Link Control), es muß aber noch zusätzliche Funktionen gewährleisten. Dazu gehören die Punkt-zu-Mehrpunkt-Verbindungen (Mulicast, Broadcast), verbindungslose und verbindungsorientierte Dienste, Multiplex-Funktion. Die Multiplex-Funktion wird benötigt, um die Daten aus dem Sende-/Empfangspuffer an den je nach Kommunikationsprotokoll erforderlichen SAP weiterzuleiten. In der LLC-Schicht werden verschiedene Diensttypen unterschieden:

- Typ 1: Verbindungsloser Dienst ohne Bestätigung,
- Typ 2: Verbindungsorientierter Dienst mit Bestätigung,
- Typ 3: Verbindungsloser Dienst mit Bestätigung.

Ein LLC-Frame ist in der Länge variabel und besteht aus einem Ziel-SAP-, einem Quell-SAP-, einem Control- und einem optionalen Info-Feld.

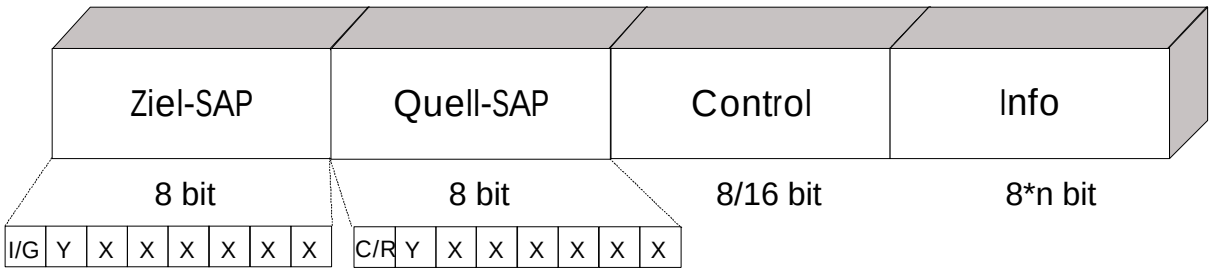

Abbildung 2.4-6 LLC-Frame [nach 8, S.88]

I/G - Individual-SAP (0) / Global-SAP (1)
C/R - Command (0) / Response (1)
Y - Lokaler-SAP-Wert (0) / Globaler-SAP-Wert (1)

Lokal - Benutzervergabe
Global - IEEE-Festgelegung
SAP - Service Access Point
XXXXXX - SAP-Angabe

Das Control-Feld kann 3 verschiedene Zustände annehmen:

- I-Frame - Information Frame,
- S-Frame - Supervisory Frame,
- U-Frame - Unnumbered Frame.

Mittels des I-Frames werden die Daten übertragen. Mit einer Sende- und Empfangsfolgenummer wird die Reihenfolge kontrolliert. Die Größe der Nummer beträgt max. 7 Bit. Die Empfangsbereitschaft oder Ablehnung sowie die Bestätigung des Empfangs eines I-Frames wird mit dem S-Frame realisiert, es werden folgende Frames unterschieden:

- Receive Ready (RR) (SS = 00),
- Receive Not Ready (RNR) (SS = 10),
- Reject (REJ) (SS = 01).

Die Funktion-Bits an Bit-Stelle 2 + 3 (SS) werden dementsprechend gesetzt.
Im U-Frame werden Managmentfunktionen übertragen, die keine Bestätigung benötigen. Es muß hier zwischen Antworten und Kommandos differenziert werden. Einige U-Format-Kommandos haben ein Info-Feld, andere nicht.

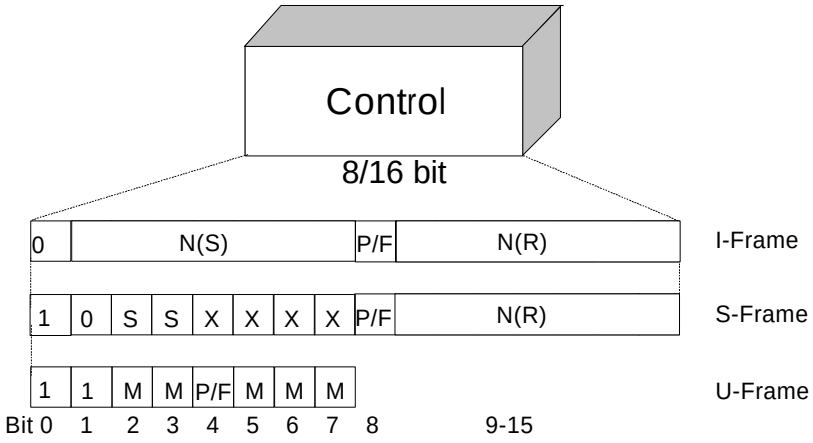

Abbildung 2.4-7 LLC-Frame Control-Feld [nach 8, S.89]

P/F-Bit: Poll / Final - Bit
Partner-Station verlangt Antwort P=1
Gegen-Station antwortet mit mehreren Frames, letzte Frame F=1

Die LLC-Schicht kann in die Software mit eingebettet werden oder als eigene Schnittstelle ausgelegt werden. Die letztere Variante wird heutzutage realisiert, da dies eine Implementierung in das Betriebssystem ermöglicht. Die LAN-Software hat dadurch die Möglichkeit auf die Sicherheitsmerkmale des Betriebssystems und der LLC-Schicht aufzusetzen und dessen Sicherheitsanforderungen mit zu integrieren.

2.4.4. LLC-MAC-Schnittstelle

Die LLC-MAC-Schnittstelle kann man auch als Schnittstelle zwischen dem virtuellen LAN-Medium (MAC-Schicht, Physische Schicht, Übertragungsmedium) und dem 1. Sicherheitsprotokoll bezeichnen. Die MAC-Schicht erbringt Dienste für die LLC-Schicht

und legt fest, wann der LLC-Frame gesendet werden darf. Dazu sind folgende Schnittstellendefinitionen (Primitive) notwendig:

- MA_UNITDATA.Request,
- MA_UNITDATA.Confirmation,
- MA_UNITDATA.Indication,
- MA_UNITDATA_STATUS.Indication.

Die Ziel-Adressen, Quell-Adressen und LLC-Frames sind in der Primitive MA_UNITDATA enthalten, die zum Transport eingesetzt wird. Die Primitive MA_UNITDATA_STATUS signalisiert der LLC-Schicht mögliche Übertragungsfehler, Framefehler, u.a. Es wird nach globaler und lokaler Signifikanz unterschieden. In der globalen Signifikanz, z.B. Token Ring, FDDI, bestätigt die MAC-Schicht die Übertragung des LLC-Frames. Beim Ethernet bestätigt die MAC-Schicht nur die Übernahme des LLC-Frames, dies nennt man lokale Signifikanz.

2.5. CSMA/CD / DIX V2.0 - Spezifikationen

Ethernet-LANs können in die bestehenden Netze ohne Probleme eingeordnet und mittels Gateways verknüpft werden. Die Verkabelungssysteme in den einzelnen Netzen und deren Anbindung ist dabei nicht entscheidend. Die einzelnen Netze sind in die verschiedenen Strukturen eingebettet und mittels Bus-, Ring-, Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-System verbunden. Innerhalb eines Netzes kann auch der Übergang von einem Verbindungssystem zu einem anderen notwendig werden.

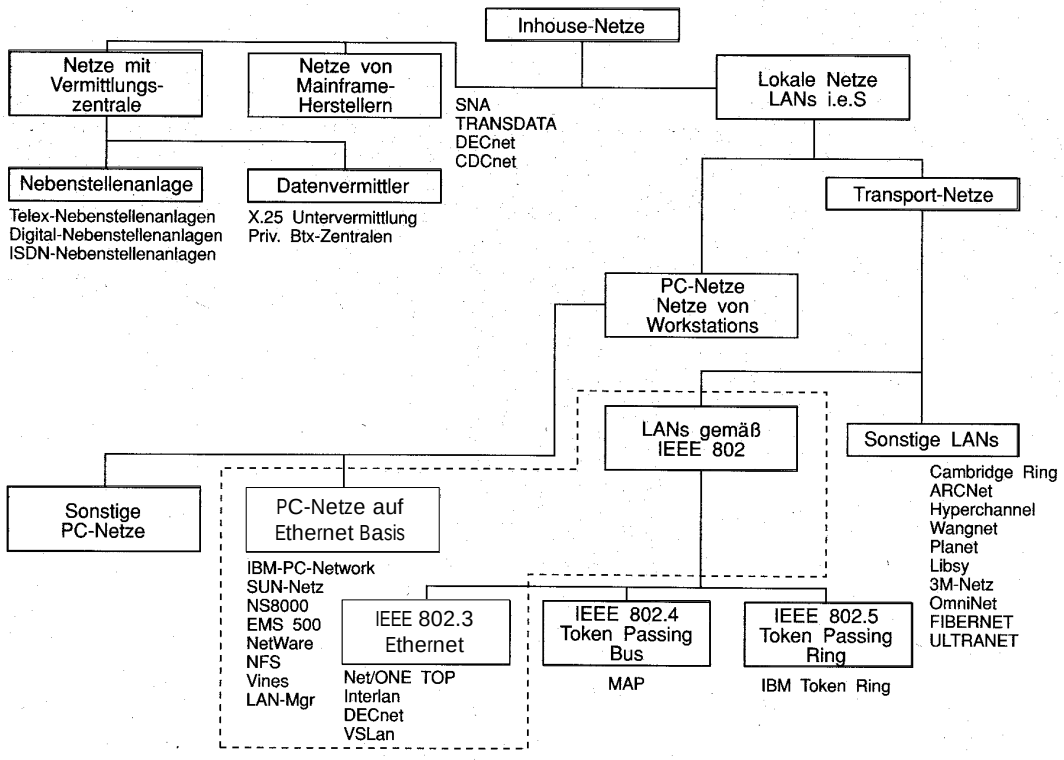

Abbildung 2.5-1 Einordnung von Ethernet Lan's [6, S.18]

Die offiziellen Standards sind IEEE 802.2 - LLC und IEEE 802.3 - CSMA/CD. In diesem Standard ist das Zugriffsverfahren und die Bitübertragungsschicht für ein Übertragungsmedium (Ethernet - Koaxialkabel, Übertragungsrate 10Mbit/s; 10BASE5) spezifiziert. Für die anderen Verkabelungsarten (10BASE2, 10BASE-T, 10BASE-F) gibt

es Ergänzungsstandards. Das CSMA/CD-Zugriffsverfahren (Carrier Sens Multiple Access with Collision Detection) ist ein kollisionsbehaftetes Verfahren, dem drei Teilaktivitäten zu Grunde liegen.

- sendewillige Station hört Kanal ab (Carrier Sens) und wartet bis dieser frei ist und sendet daraufhin
- mithören während des Sendens (Collision Detect) und Abbruch bei Erkennen eines Konfliktfalls
- wiederholen einer Kollisionssendung (Backoff Algorithm)

Die Güte für dieses Zugriffsverfahren bestimmt sich über die Größe *K*, bei der immer gelten muß *K<1*. Bei *K>1* könnte ein Sender seine ganze Nachricht auf dem Kanal übertragen, bevor eine Kollisionserkennung möglich wäre. In diesem Fall ist es dem Sender nicht mehr möglich durch ein wiederholtes Senden den Fehler zu beseitigen.

$$K = \frac{\text{max. Signallaufzeit}}{\text{Nachrichtenübertragunszeit}} = \frac{\dfrac{\text{Kanallänge}}{\text{Signalgeschwindigkeit}}}{\dfrac{\text{Nachrichtenlänge}}{\text{Kanalübertragungsrate}}}$$

Bei dieser Form der Datenübertragung sind festgelegte Rahmenbedingungen bezüglich der Distanz, der Bandbreite und der Nachrichtenlänge einzuhalten. Der Aufbau eines Ethernet wird mittels einer Busstruktur realisiert. Bei der Datenübertragung können keine Antwortzeiten garantiert werden, da der Datenverkehr selbstregelnd abläuft. Es müssen keine Teilnehmerlisten geführt werden oder Neukonfigurationen vorgenommen werden, so daß eine hohe Flexibilität gewährleistet werden kann und praktisch jeder mit seinem PC sich in das Netzwerk einklinken kann. Dies wird allerdings durch Sicherheitsprotokolle der höheren Schichten meistens unterbunden.
Die folgende Tabelle zeigt einen Vergleich der unterschiedlichen Übertragungsmedien zum Aufbau eines Ethernet-LANs.

Ethernet-Typ	**Medium**	**max. Länge**	**Bemerkungen**
10BASE5	Koaxialkabel	500 m	klassische Ethernet-Verkabelung; Anschluß über Transceiver und „Vampir“-Klemmen
10BASE2 (Cheapernet)	Koaxialkabel (RG 58)	185 m	dünnes Koaxialkabel mit geringer Schirmung; Anschluß über Transceiver und BNC-Stecker
10BASE-T	verdrilltes Kupferkabel STP-geschirmt, UTP-ungeschirmt	100 m	Ankopplung der Station sternförmig an sog. Sternkoppler (Hubs)
10BASE-FB	LWL	2 km	meist in Ethernet-Backbone-Netzen zwischen Sternkopplern
10BASE-FL	LWL	2 km	meist zwischen Regeneratoren

Die Standardisierung umfaßt Schicht 1 (Physical) und 2a (MAC), wobei sich Ethernet (DIX-DEC/INTEL/XEROX V2.0 - Spezifizierung) und IEEE 802.3 Spezifikation nur hinsichtlich des MAC-Frames unterscheiden.

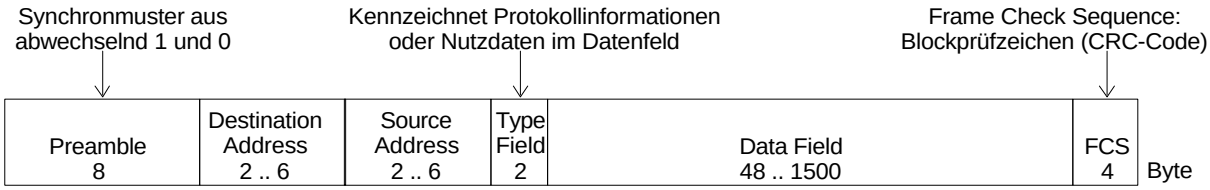

Abbildung 2.5-2 Ethernet Paketformat gemäß DIX V2.0

Bei der neueren IEEE 802.3 Norm ist die Kollisionserkennung besser und es besteht die Möglichkeit, variable Datenlängen zu übertragen. Die Größe des Datenfeldes kann zwischen 46 und 1500 Byte variieren. Die Gesamtpaketlänge variiert damit zwischen 64 und 1518 Byte.

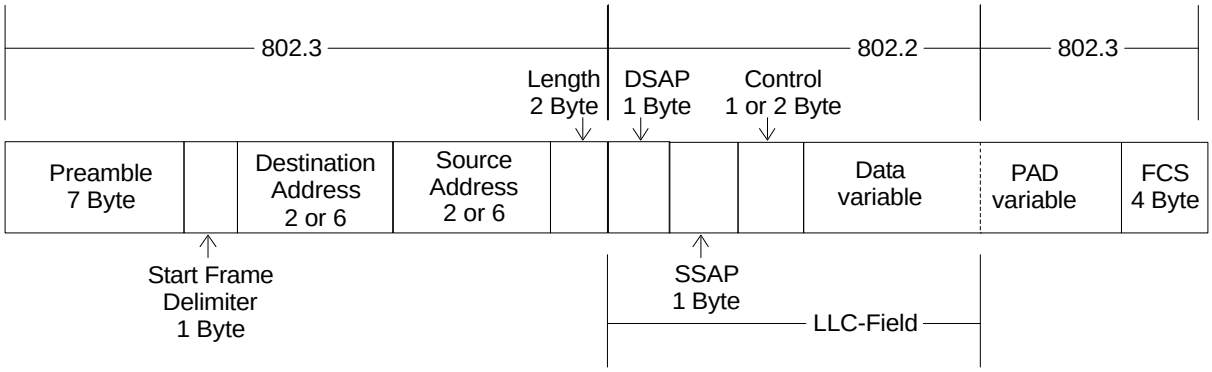

Abbildung 2.5-3 Ethernet Paket gemäß IEEE

- Präambel (PA): Folge von 0 und 1 über 7 Byte; dient zur Bitsynchronisation
- Start Frame Delimiter (SFD): Kennzeichnung des Frame Beginn (Format 10101011)
- Destination Address (DA), Source Address (SA) siehe Abschnitt 3.4.2
- Length (LEN): enthält Länge des Frames
- DSAP (Destination-SAP), SSAP (Source-SAP), Control (+Info): Daten, die innerhalb der LLC-Schicht erzeugt und an die MAC-Schicht übergeben werden. siehe Abschnitt 3.4.3
- Padding (PAD): Füllfeld; Wenn die Framelänge kleiner ist, als für das CSMA/CD-Verfahren notwendig, wird der Frame mit der entsprechenden Anzahl Bits aufgefüllt, um die Framemindestlänge (512 Bit = 64 Byte) zu erreichen.
- Frame Check Sequence (FCS): Frameprüfsequenz, die mittels eines zyklischen Kodierungsverfahren gebildet wird. Abgesichert werden die LLC-Daten, die Länge, die Adressen und die Füllzeichen.

Ein Frame wird als fehlerhaft erkannt, wenn die Framelänge nicht mit der Länge im Lenghtfeld übereinstimmt oder nicht ein vielfaches von 8 Bit ist. Eine weitere Möglichkeit der Fehlererkennung besteht auch wenn die FCS-Prüfung negativ ausfällt.
Da das Frame-Paket nach DIX 2.0 kein Längenfeld und vor allem kein LLC-Feld enthält wurde die Einführung des SNAP-Protokolls notwendig. Es übernimmt die Kopplung unterschiedlicher Netztechnologien.

2.5.1. Bitübertragungsschicht

Die Bitübertragungsschicht wird nochmals unterteilt, da dies eine bessere Beschreibung der unterschiedlichen Charakteristiken der Realisierungsvarianten ermöglicht.
Die PLS ist zuständig für die Verbindung zur MAC-Schicht und legt fünf Dienstprimitiven fest: PLS-DATA.request, PLS-DATA.confirm, PLS-DATA.indication, PLS-CARRIER.indication, PLS-SIGNAL.indication. Die PLS-DATA-Primitien dienen zur Kommunikationssteuerung zwischen zwei Teilnehmern, PLS-CARRIER zeigt den Status der Aktivitäten des Mediums an und PLS-Signal meldet die physische Signalqualität.
Mittels der AUI ist eine hardwaremäßige Trennung zwischen LAN-Karten und MAU erfolgt, durch die die Verwendung unterschiedlicher Übertragungsmedien (LWL, Koaxialkabel, Twisted-Pair) möglich ist.

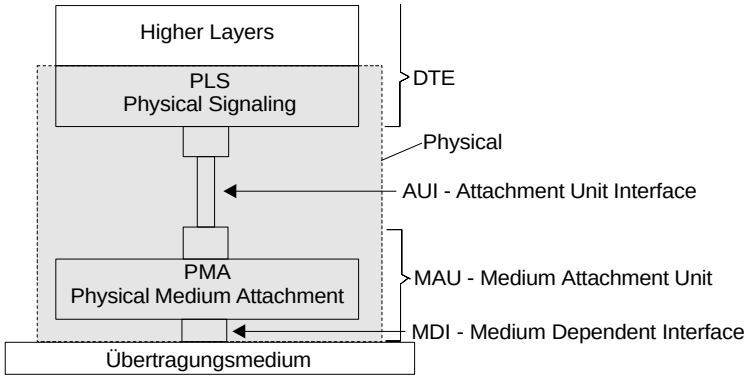

Abbildung 2.5-4 Bitübertragungsschicht

PMA und MDI bilden zusammen die MAU, welche die Funktionen zum Senden und Empfangen von codierten Signalen enthält. Die PMA stellt einen Transceiver dar und fungiert als Sende- und Empfangseinheit.
Die MDI ist die physikalische und mechanische Schnittstelle zwischen der MAU und dem Übertragungsmedium.
Die Bitübertragungsschicht hat nach IEEE 802.3 folgend Aufgaben:

- Bitstrom senden / empfangen,
- Signalcodierung / -decodierung,
- Taktgenerierung zur Synchronisation,
- Kollisionserkennung,
- Erzeugung der Präambel.

Die Kodierung erfolgt mittels des Manchester II-Verfahren. Die Bitübertragung erfolgt über 2 Takte, wobei im ersten Takt jeweils das Bit invertiert wird. Durch den ständigen Spannungswechsel ist die Synchronisierung relativ gut möglich und die Übertragungsrate nicht unnötig hochgesetzt.

2.6. Zugriffsverfahren

Übertragungskanäle im Fest- und im Funknetz sind sehr knapp. Um so vielen Benutzern wie möglich den Zugriff zu ermöglichen, müssen spezielle Verfahren eingesetzt werden. In diesen Multiple Access-Verfahren wird die zur Verfügung stehende Bandbreite jedem Benutzer nach seinen Anforderungen gerecht zugeteilt.

2.6.1. FDMA - Frequenz Division Multiple Access

Das Frequenzband wird in einzelne Kanäle unterteilt, dies ist für die drahtlose Übertragung ungeeignet, da die knappe Bandbreite nicht optimal ausgenutzt wird. Jedem Benutzer ist eine fixe Bandbreite zugeordnet, unabhängig davon ob er diese benötigt. Geräte im

FDMA-Verfahren sind auf Grund der Bauteile nicht als Kompaktgeräte herstellbar. Die Kosten für die Basisstationen werden durch den Aufwand für jeden Kanal (2 Codes, 2 Modems, Intermodulation bei Verstärkung) sehr hoch.

2.6.2. TDMA - Time Division Multiple Access

Alle Benutzer arbeiten mit dem gleichen Frequenzband, jedoch immer nur zu einer bestimmten Zeitpunkt mit einer festgelegten Zeitdauer. Dieser Zeitschlitz wird für eine kontinuierliche Übertragung periodisch wiederholt. Die Zeitschlitze werden in Zeitrahmen gruppiert und diese dann periodisch übertragen. Um eine Störung der Übertragung zu vermeiden, muß eine Schutzzeit (Guard Time) vorgesehen werden. Sie beträgt das zweifache der Signallaufzeit, z.B. bei 10km Entfernung der MS von der BS ist GT = 2 x $10x10^{10}$m / $3x10^{8}$m/s = 66µs. Lange Schutzzeiten führen zu einer Ineffizienz des TDMA-Systems. Im GSM-Netz veranlaßt die BS die MS entsprechent früher zu senden, dadurch wird die Schutzzeit auf ca. 30µs gesenkt. Das TDMA wird heutzutage im festen Telefonnetz und vielfach im Bündelfunk- und Funktelefonnetz (C- und D-Netz) eingesetzt. Beide Verfahren sind für den Einsatz in drahtlosen LANs schlecht geeignet, da die Frequenzkanäle und Zeitschlitze nur immer einem Teilnehmerpaar zugeordnet sind. In LANs teilen sich alle Teilnehmer ein und den selben Übertragungskanal.

2.6.3. CDMA - Code Division Multiple Access

Das CDMA-Verfahren hat erst in jüngerer Zeit eine große Verbreitung gefunden, da für die Übertragung sehr leistungsfähige digitale Signalprozessoren erforderlich sind. Bei diesem Verfahren belegen alle Teilnehmer dieselbe Frequenz, wobei jeder Station ein anderer Code zugeordnet wird. Durch diese Separierung können die Daten jedem Benutzer eindeutig zugeordnet werden und gleichzeitig die vorhandene Bandbreite effektiver genutzt und noch mehr Teilnehmern der Zugriff auf das Medium ermöglicht werden. (siehe auch Kapitel 3.2)

2.6.4. CSMA - Carrier Sens Multiple Access

Mittels des CSMA-Verfahrens können mehrere Benutzer auf das gleiche Übertragungsmedium zugreifen und jeder mit jedem kommunizieren. Die sendewillige Station hört den Kanal ab und fängt erst an zu senden, wenn sie den Kanal als frei erkennt.

1-persistent Verfahren

Im 1-persistent Verfahren beginnt jede Station mit der Wahrscheinlichkeit von 1 zu senden, d.h. sie sendet sofort, wenn sie den Kanal als frei erkennt. Beim Auftreten einer Kollision erkennen die beteiligten Stationen dies und warten eine zufällige Zeit ab, bis sie erneut senden. Durch die starke auf das ‘bei Frei sofort Senden’ treten sehr viele Kollisionen auf, die die Datendurchsatzrate deutlich senken, was in einem größeren Netzwerk schnell zum Zusammenbruch führen würde.

Nonpersistent Verfahren

Beim Nonpersistent Verfahren kontrolliert eine Station auch wieder ob der Kanal frei ist und beginnt dann zu Senden. Ist dieser aber besetzt, wartet sie erst eine zufällige Zeit ab und beginnt dann erneut mit der Kontrolle. Die Auslastung des Übertragungskanals steigt.

CSMA/CD Verfahren

Durch die Kollisionserkennung im CSMA/CD-Verfahren gibt es eine Möglichkeit gleich beim Senden ein Übertragungsfehler zu erkennen und die Sendung abzubrechen. Die Station, die einen Konflikt erkennt, bricht ihr Senden sofort ab und sendet ein 4-6 Byte

großes JAM-Signal aus, das beliebige Daten enthält, dies liegt deutlich unter der Mindestpaketlänge von 64 Byte. Beim Erkennen des Störsignals brechen die anderen Stationen ihre Sendung sofort ab. Die erneute Übertragung wird nach dem Zufallsprinzip fortgesetzt und beträgt Zufallszahl *i* mal Slot Time (Übertragungszeit für 64 Byte = 512 Bits = 51,2 µs; *i* - natürliche Zahl). Die Zahl i kann zwischen $0£i£2e^k$ und *n£k£10* (n - Anzahl der Wiederholungsversuche) liegen. Es sind maximal 16 Fehlversuche möglich, wobei nach 10 Versuchen das Backoff-Intervall nicht mehr erhöht wird. Ist nach dem letzten Versuch keine Übertragung zustande gekommen, wird eine Fehlermeldung erzeugt und die Übertragung bricht ab. Voraussetzung bei diesem Verfahren ist allerdings, daß sich alle Stationen hören können, was nur im leitungsgebundenen Netzwerk möglich ist. Im Ethernet nach IEEE 802.3 wird das 1-persistent CSMA/CD-Verfahren angewendet.

CSMA/CA Verfahren

Im CSMA/CA (Carrier Sens Multiple Access with Collision Avoidance) Verfahren wird wie beim CSMA/CD Verfahren das Medium vor dem Senden auf ein eventuelles Besetztzeichen geprüft. Im Gegensatz zum CSMA/CD Verfahren wird die Kollision der Daten durch das Benutzen von Request-to-Send (RTS), Clear-to-Send (CTS), Daten und Acknowledge (ACK) Übertragungsframes minimiert. Die sendewillige Station wartet nach ‘frei’ eine kurze Zeit ab und schickt dann eine RTS-Meldung zur Gegenstelle, diese enthält die Zieladresse und die Länge der Nachricht. Die Nachrichtenlänge steht im Network-Allocation-Vektor (NAV). Der NAV meldet allen anderen die Dauer der Übertragung. Die Gegenstation gibt eine CTS-Meldung ab, die die Senderadresse und den NAV zurückgibt. Wenn der CTS-Frame nicht aufgenommen wurde, dann lag eine Kollision vor und der RTS-Prozeß startet erneut. Nach der Datenübertragung wird vom Empfänger ein ACK-Frame gesendet, der eine Bestätigung der erfolgreichen Übertragung enthält. Kommt nach einer bestimmten Anzahl von Versuchen keine Verbindung zu stande, dann bricht der Sendeversuch ab und gibt eine Störmeldung an die höheren Schichten zurück. Ein Problem in drahtlosen LAN-Systemen sind versteckte Stationen (Hidden Nodes). Dadurch können über 40% der Kommunikationen unterbrechen werden. Das kann passieren, wenn eine Station nicht die Übertragung einer anderen Station detektieren kann und so das besetzte Medium nicht erkennt. Das Benutzen von RTS-, CTS-, Data und ACK-Meldungen beugt Unterbrechungen durch Hidden Stations vor.

2.7. Kommunikationsprotokolle

Für die Übertragung von Daten zwischen den Applikationen zweier Benutzer ist die Vereinbarung von Regeln notwendig, die ein Kommunizieren ermöglichen. Diese Regeln nennt man Kommunikationsprotokolle, kurz Protokoll. Es gibt viele verschiedene Protokolle, mit denen sich die Partner verständigen können, doch nur wenn beide das gleiche Protokoll verwenden, ist eine Verständigung möglich. Protokolle werden zwischen allen Schichten des OSI-Referenzmodells ausgetauscht, es können verschiedenn hierarchisch organisierte Protokolle ineinander eingebettet sein, so daß sie kurz vor der eigentlichen Übertragung ein gesamtes Protokoll bilden, das beim Empfänger in der entgegengesetzten Reihenfolge wieder auseinander genommen wird. Protokolle für die Übertragung sind z.B. TCP/IP und IPX/SPX, in diesen können Anwendungsprotokolle eingebunden sein, z.B. FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), TFTP (Trivial FTP), SNMP (Simple Network Management Protocol). Ein Protokoll ist immer nur eine Vereinbarung von bestimmten Algorithmen zur Verarbeitung der Daten.

Die Protokolle sind mit den menschlichen Sprachen vergleichbar. Gesprächspartner müssen sich vor einer Konversation einig sein, in welcher Sprache sie miteinander reden, nur so kann eine reibungslose Kommunikation erreicht werden. Die unterschiedlichen Kommunikationssprachen sind auf die verschiedenen Betriebssysteme (UNIX, Netware, Windows) und vielfach firmenspezifischen Netzarchitekturen (OSI/ISO, SNA/IBM, DANN/DEC) zurückzuführen. Wie im menschlichen Miteinander gibt es auch in der Computerwelt verschiedene Dialekte innerhalb der Protokolle, so daß die Protokolle meist eine Art Protokollfamilie bilden, die untereinander nicht immer kompatibel sein müssen.
Als erläuterndes Beispiel möchte ich einmal ein Telefongespräch der älteren Generation mit einem der neueren Generation sinnbildlich vergleichen.

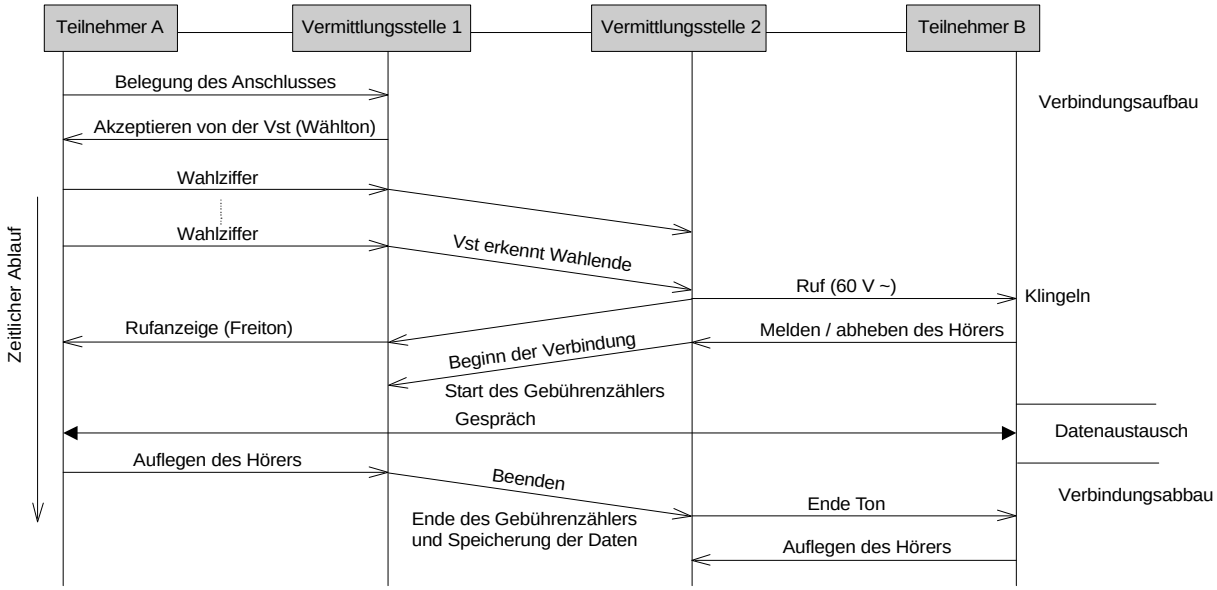

Abbildung 2.7-1 Telefongespräch über analoge Vermittlungsstelle

Protokolldarstellung anhand von Abbildung 2.7-1
Da ja bekanntlich ein Protokoll nur eine Menge von Vereinbarungen enthält, gibt es auch hier ein Protokoll für den Verbindungsaufbau und eines für der Verbindungsabbau. Das Aufbau-Protokoll beinhaltet das Erkennen der Leitungsbelegung durch Teilnehmer (Tln) A, daraufhin muß ein Ton gesendet werden (anlegen des Gleichstroms). Wenn die Kapazität der VSt nicht ausreicht, ertönt ein Besetztton, ansonsten erhält der Tln A das Freizeichen und beginnt zu wählen. Die Wahlziffern werden als Unterbrechung des Gleichstroms dargestellt. Sie werden, wenn nötig, an die nächste VSt weitergereicht und die dementsprechenden Leitungen belegt. Wenn die VSt das Wahlende erkannt hat und der gerufenen Anschluß frei ist, dann wird Tln B durch anlegen der Wechselspannung gerufen (Klingeln) und Tln A erhält das Freizeichen. Beim Abheben des Hörers durch Tln B wird auch hier die Gleichstromschleife geschlossen. Zwischen den Vermittlungsstellen wird das Beginnzeichen gesendet und an der VSt von Tln A der Gebührenzähler gestartet. Jetzt kann das Gespräch geführt werden. Das Protokoll für den Verbindungsabbau ist wesentlich kürzer. Wenn ein Tln A auflegt, wird der Gebührenzähler angehalten und die erfaßten Gebühren gespeichert. Die Leitungen zwischen den VSt`s werden wieder freigegeben und bei Tln B ertönt der Endeton, wenn er auflegt ist die gesamte Verbindung beendet.
Im folgenden möchte ich das Protokoll einer modernen Telefonverbindung erläutern, das schon etwas umfassender ist. Es enthält aber dennoch die gleichen Grundgedanken wie oben beschrieben und unterteilt sich auch in zwei Protokolle (Verbindungsaufbau,

Verbindungsabbau). Alle beteiligten Einheiten sind am Netz Telefonnetz angeschlossen, müssen sich aber nicht im selben Gebäude befinden.

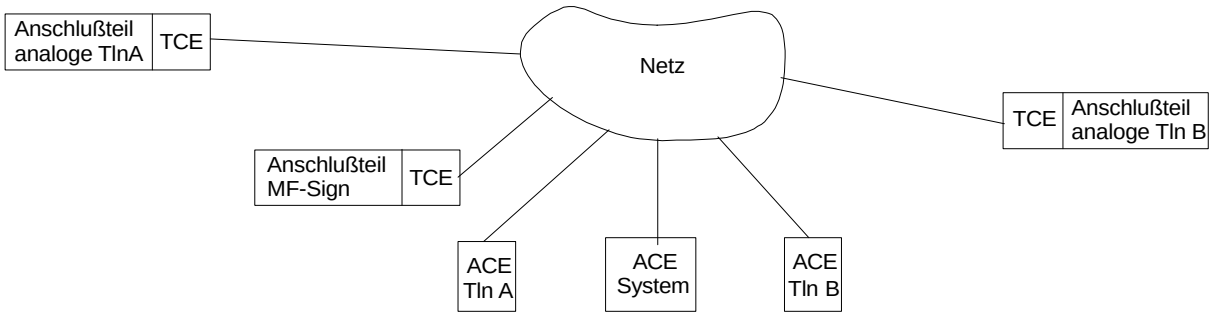

Abbildung 2.7-2 Telefongespräch über digitale Vermittlungsstelle

Verbindungsaufbau:
Tln A hebt seinen Hörer ab und meldet damit der ACE-Tln-A einen Belegungsversuch. Diese fordert die System-ACE an, die dann ein freies MF-Signalisierungsmodul auswählt. Zwischen MS-Sign und TCE-Tln-A wird ein Weg aufgebaut und der Freiton angelegt. Wenn die Wege stehen, erfolgt die Quittierung an ACE-Tln-A. Dies entspricht den ersten beiden Schritten in der analogen Technik. Nach dem Empfang der ersten Ziffer wird der Wählton abgeschaltet. Die Ziffern werden zur Analyse an die System-ACE übergegeben. Nach der letzten Ziffer wird das MF-Modul abgeschaltet und alle Wege zur MF-Sign getrennt und an den ACE-einheiten quittiert. Die ausgewertete Nummer wird an die TCE-Tln-A gemeldet, von hier der Weg zur TCE-Tln-B aufgebaut und die Nummer von Tln-A übertragen. ACE-Tln-B wird über die Belegung informiert und meldet dies an die ACE-Tln-A zurück. ACE-Tln-A weist die TCE-Tln-A an, den Sprechweg durchzuschalten und ACE-Tln-B bekommt den Auftrag die TCE-Tln-B zu rufen. Sie leitet die Rufanweisung inform der Rufanschaltung weiter an TCE-Tln-B. Diese leitet den Freiton an TCE-Tln-A weiter. Das entspricht den Schritten bis zur Rufanzeige in dem oben beschriebenen Protokoll. Tln-B hebt den Hörer ab und veranlaßt somit die Abschaltung des Rufstromes und Freitons, das wird an die TCE-Tln-A weitergemeldet. Die TCE-Tln-B übertägt das Beginnzeichen an ACE-Tln-B und diese leitet es an ACE-Tln-A weiter, wo die Gebührenerfassung gestartet wird. Das waren die letzten Schritte, die zum Verbindungsaufbau nötig waren, nun kann das Gespräch beginnen..
Wie man sieht, sind die Grundzüge der Verbindungsherstellung auch hier enthalten, aber es sind wesentlich mehr Schritte notwendig, um das gleiche zu erreichen. Durch die Weiterentwicklung der Technik ist dieser Ablauf dennoch schneller und effektiver, weil eine bessere Auslastung der Leitungen erreicht wird und der Platzbedarf der Geräte wesentlich geringer ist.

2.7.1. Begriffsklärung und Aufbau

Bei der Übertragung über kurze oder lange Entfernungen können die Daten infolge einer schlechten Übertragungsqualität des Mediums oder äußerer Einflüsse, z. B. elekromagnetische Felder, verfälscht werden oder ganz verloren gehen. Für die Gewährleistung einer sauberen und reibungsfreien Übertragung müssen die Protokolle folgende Funktionen enthalten die Fehlerkontrolle (Fault Control), die Flußkontrolle (Flow Control) und eine Überlastkontrolle (Congestion Control).

Die Fehlerkontrolle bildet das Hauptstandbein jeder Übertragung. Diese wird beim Empfänger mit standardisierten Quittungen und beim Sender mittels der Zeitüberwachung realisiert. Folgende Fehlersituationen können auftreten:

- Verlust oder Verfälschung der Daten,
- Verlust oder Verfälschung der Quittung,
- Verfälschung von Daten und Quittung.

Die Fehlerkontrolle

Für die Gewährleistung einer guten Übertragung müssen zwei Regeln unbedingt beachtet werden. Um eine Verfälschung der Daten auszuschließen, muß immer eine Kopie im Speicher des Senders verbleiben, falls eine wiederholte Übertragung notwendig wird. Es können Datenverluste auftreten, daraus folgt, das nur eine bestimmte Zeit auf eine Quittung gewartet werden darf. Es werden zwei Stufen der Fehlerkontrolle verwendet, da die Richtigkeit der einzelnen Datenblöcke (Pakete, Frames) nicht unbedingt bedeuten muß, daß die zusammengesetzte Datei auch richtig ist. Das kann dazu führen, daß einzelne Datenblöcke oder sogar eine komplette Datei neu übertragen werden muß. Bei einer wiederholten Datenübertragung kann es zu einer Verdopplung beim Empfänger kommen, das ist genauso schädlich wie ein fehlerhafter oder verlorengegangener Datenblock. Zur Vermeidung eines solchen Irrtums werden die Datenblöcke nummeriert (Sequenznummern). Die Nummerierung wird im Modulo-8-Verfahren, bei dem die Datenblöcke von 0 bis 7 gekennzeichnet werden, oder im Modulo-128-Verfahren, Nummern 0 bis 127, durchgeführt. Der Zähler wird nach der letzten Nummer immer wieder auf Null zurückgesetzt. Die Quittierung des Empfangs von Datenblöcken kann in der Zielstation zu einer Gruppenquittierung zusammengefaßt werden, was die Netzlast minimiert. Wie groß die Quittierungsgruppe sein darf, welches Nummerierungsverfahren (Fenster) verwendet wird und bei welcher Sequenznummer angefangen wird muß vorher zwischen Quell- und Zielstation vereinbart werden.

Erläuterung zu Abbildung 2.7-3

a) Einfache Datenübertragung ohne Fehler oder Datenverlust.

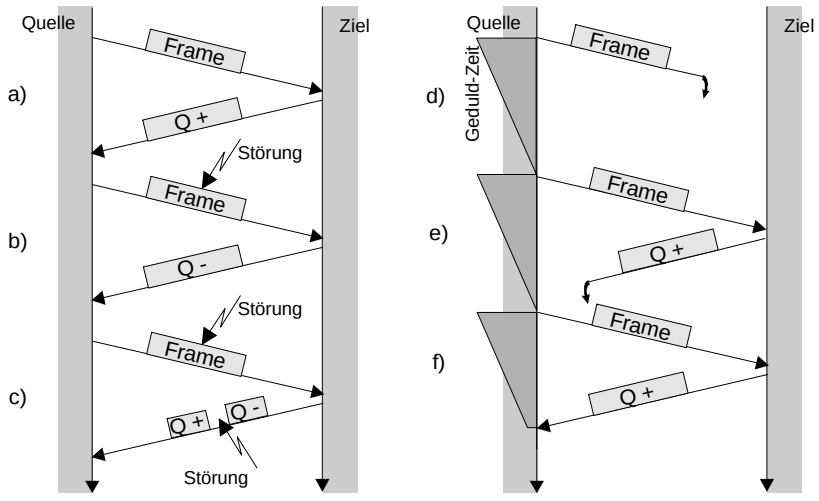

Abbildung 2.7-3 Fehlerkontrolle

a) Auftreten eines Framefehlers infolge einer Störung, der Empfänger sendet eine negative Quittung und bittet um nochmaliges Senden des Frames.

b) Hier tritt bei der Übertragung des Frames ein Fehler auf, der Empfänger gibt daraufhin eine negative Quittung zurück. Diese wird jedoch auch gestört und im schlimmsten Fall eine positive Quittung daraus, so daß der Sender den Übertragungsfehler nicht erkennt. Bei Realisierung einer Fehlererkennung in höheren Schichten ist es möglich, den Fehler dennoch zu erkennen.

c) Im vierten Fall geht ein ganzer Frame verloren, der Sender wartet eine gewisse Zeit ab (Geduld Zeit) und sendet dann erneut.
d) Jetzt wurde zwar der Frame ohne Verlust und Störung übertragen, aber die Quittung geht verloren, deshalb wird nach dem Abwarten der Geduld-Zeit nochmals mit der Übertragung begonnen.
e) In diesem Fall findet eine korrekte Übertragung statt und die Quittung kommt innerhalb der Geduld-Zeit an.

Die Flußkontrolle

Die Flußkontrolle übernimmt die Steuerung der Datenmengen, die zwischen Sender und Empfänger übertragen werden dürfen. Nicht jeder Empfänger, z.B. Drucker, ist in der Lage die Daten in der Geschwindigkeit zu verarbeiten, wie der Sender, z.B. Server, in der Lage ist sie anzubieten. Die Zielstation steuert somit den Datenfluß durch Kommandos wie Halt-Weitersenden, Krediten und einem Fenster-Mechanismus.
Die Flußkontrolle mittels Halt, Weitersenden ist sehr unsicher und störanfällig gegenüber Verfälschungen. Da bei dieser Art der Datenübertragung beide Teilnehmer miteinander kommunizieren handelt es sich um ein Duplex-Verfahren. Dieses Verfahren kann man in Duplex und Halbduplex unterteilen. Beim Duplex-Verfahren werden die Daten gleichzeitig in beide Richtungen gesendet, z.B. Twisted-Pair-Netze. Beim Halbduplex-Verfahren dagegen erfolgt das Senden und Empfangen von Daten nacheinander, z.B. Koaxialleitungsnetze. Beim älteren Simplex-Verfahren können Daten nur in eine Richtung übertragen werden, dies ist bei älteren unidirektionalen Druckern der Fall. Diese haben keine Möglichkeit eine Rückmeldung an den Computer zu geben, ob die Daten Fehlerfrei gedruckt wurden.
Bei der Kontrolle über Kredite kann der Sender eine bestimmte Anzahl von Datenblöcken senden ohne eine Quittung zu erwarten. Die maximale Länge der Datenblöcke wird vorher festgelegt. Der Empfänger gibt immer soviel Kredite an den Sender wie er in der Lage ist zu verarbeiten. Das Übertragen der Kredite muß besonders geschützt werden, da eine Fehlübermittlung auch hier einen Abbruch der Verbindung bedeuten könnte.
Der Fenster-Mechanismus stützt sich bei der Übertragung auf die Sequenznummern der Datenblöcke. Quell- und Zielstation handeln vorher die Größe des Fensters im Wertebereich der Sequenznummern aus. Die Fenstergröße W kennzeichnet die maximal zu sendenden Datenblöcke ohne Quittung vom Empfänger. W bezeichnet die Anzahl der Kredite beim Sender und die Größe des Empfangspuffers beim Empfänger. Der Sender darf nun nur soviel Datenblöcke übertragen, wie die Größe W vorgibt. Beim Erhalt einer Quittung wird W wieder heruntergezählt, je nach dem für wie viele Datenblöcke diese Quittung zählt. Danach beginnt der Sender wieder Datenblöcke an den Empfänger zu übertragen bis W den vereinbarten Wert erreicht hat. Die Quittung enthält die Anzahl der empfangenen Datenblöcke. Der Fenster-Mechanismus gilt als die sicherste Methode der Flußkontrolle und wird daher in den meisten Kommunikationsprotokollen eingesetzt, zugleich reduziert sich das Datentransfervolumen auf das unbedingt notwendige. Die Ermittlung der optimalen Größe des Fensters ist eine der wichtigsten Aufgaben der Kommunikationsprotokolle.

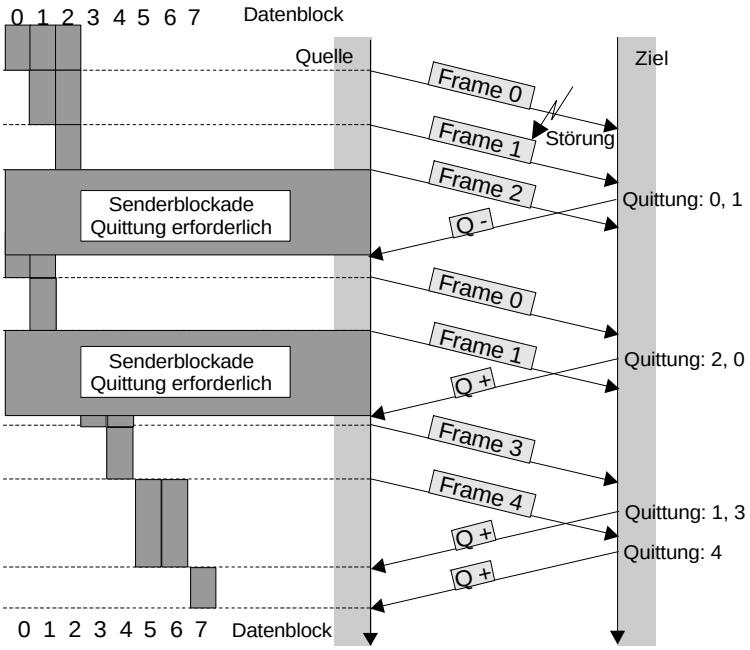

Abbildung 2.7-4 Flußkontrolle mit Störung

Bei dem Beispiel in Bild 3.7-4 wird das Modulo-8-Verfahren angewendet und die Fenstergröße ist *W=3*. Bei *W=3* darf die Quelle 3 Datenblöcke senden ohne eine Quittung zu erhalten. Die Nummer des Datenblocks ist die Sequenznummer, die verwendet werden darf. Die Quelle wartet nach dem Senden von Datenblock 2 auf die Quittung, es entsteht eine Senderblockade. Die Quittung erhält er auch, aber mit einer Fehlerangabe (negative Quittung), daraufhin werden die Blöcke 0 und 1 nochmals gesendet. Da jetzt wieder *W=3* erreicht wurde, blockiert der Sender bis die Quittung 2, 0 eintrifft. Jetzt kann Frame 3 und 4 übertragen werden, da *W* um zwei Stellen heruntergezählt wurde. Nachdem der 7. Datenblock übertragen wurde, beginnt der Zähler mit der Numerierung wieder bei 0.

Die Überlastkontrolle

Die Datennetze LAN, MAN, WAN haben nur eine begrenzte Durchsatzkapazität. Bei einer Überlastung kommt es dazu, daß die Zwischspeicherpuffer in den Knoten gefüllt sind und weiter Datenblöcke verworfen werden, zugleich erhöht sich die Verweilzeit, durch die Bildung von Warteschlangen, der Daten im Netz, was zu einem Abbruch der Übertragung und einem Zusammenbruch des Netzes führen kann. Um den Fall nicht eintreten zu lassen wurden bestimmt Vorkehrungen getroffen. Die beiden Kriterien für die Überlastkontrolle sind der Datendurchsatz und die Datenverweilzeit (Verzögerung). Der Datendurchsatz bezeichnet den Anteil des Datenaufkommens, der vom Netz akzeptiert wird. Je größer und umfangreicher das gesamte Netz wird und je mehr Netzübergänge bestehen, desto aufwendiger sind die Maßnahmen zur Vermeidung eines Netzzusammenbruchs. Dies kann in der Beschränkung von Datenmengen, die ins Netz gespeist werden dürfen, und in diesem Fall automatisch durchzuführender Ausweichroutings liegen. Diese sind allerdings sehr aufwendig und nur von Intelligenten Netzwerken (IN) zu erwarten. Die Maßnahmen gegen den Überlastfall hängen stark von der eingesetzten Flußkontolle ab. Für ATM-Netze ist die Überlastkontrolle von großer Bedeutung (siehe Kapitel 5.1).

2.7.2. IPX / SPX - Protokoll (Netware / Novel)

Das Netware-Protokoll IPX / SPX (Internet Packet Exchange / Sequential Packet Exchange) ist ein firmenspezifisches Betriebssystem, was für PC-Netze optimiert ist. Es wird das Prinzip des Zentralen Servers verfolgt. Er erhält die gesamte Kontrolle über das Netz und greift direkt auf die Hardware durch, wohingegen die Arbeitsplatzstationen nur über die residente Shell auf den Server zu greifen. Dies entspricht einer Client-Server-Beziehung.

Das IPX ist ein verbindungsloses Datagramm-Protokoll und verdeutlicht die Schicht 3. Die Realisierung im Rechner erfolgt über einen Treiber (IPX.com), der auf die LAN-Adapterkarte direkt zugreift. Jeder LAN-Karten-Hersteller liefert deshalb schon einen vorkonfigurierten IPX-Treiber mit.
Das in der Schicht 4 angesiedelte SPX garantiert die Zustellung und die richtige Reihenfolge der Datenpakete (Datagramme) am Ziel. Es ist ein verbindungsorientiertes Transportprotokoll.
Über das NCP (Netware Core Protocol) kommuniziert die residente Shell der Arbeitsstation mit dem Server. NCP ist das eigentliche Kommunikationsprotokoll und sendet über den direkten Zugriff auf IPX seine Daten ins Netz. Die NCP-Datenblöcke werden in IPX-Pakete eingebettet und beim Empfang auch wieder quittiert.
Das Service Advertising Protocol (SAP) dient zur Bekanntgabe aller im Netz verfügbaren Dienste (Gateway, Printserver). Durch ein Broadcast-Paket über das SAP wird allen Routern im Netz mitgeteilt, welche Dienste zur Zeit verfügbar sind. Jede Arbeitsstation ist in der Lage die Netzadressen bestimmter Dienste zu erfragen.
Mittels des Routing Information Protocol (RIP) wird in Netware die schnellste Route durch das Netz von einem Teilnehmer zum anderen ermittelt.
Den Netware-Protokollen liegt der Gedanke der absoluten Arbeitsteilung zwischen den einzelnen Protokollen zu Grunde. Daraus resultiert auch die Reihenfolge zum Aufbau einer Übertragung von einer Arbeitsstation (AS) zu einem Server. Zuerst erfolgt die Anfrage mittels SAP, um den nächstgelegensten Server zu finden. Wenn dies erfolgreich war, wird über das RIP der kürzeste Weg gefunden. Sind diese Informationen in der AS vorrätig, baut das NCP eine Verbindung zu Server auf und fordert einen bestimmten Dienst an. Nimmt der Server die Ausführung des Dienstes an, wird die zu sendende Datenpaketgröße ausgehandelt und mit dem Übertragen der Daten begonnen.

Das IPX-Protokoll

IPX stellt ein ungesichertes Datagramm-Protokoll dar, das hauptsächlich für die Kommunikation zwischen Arbeitsstation und Server gedacht ist. Es transportiert die Datenpakete von der Quell- zur Zielstation ohne auf deren Reihenfolge zu achten oder eine Empfangsbestätigung zu erwarten. Die Sicherung der Reihenfolge und das Erkennen der Fehler wird von den in den höheren Schichten angesiedelten Protokollen (SPX, SAP, RIP, NCP) vorgenommen. Im Datenbereich des IPX-Paketes befinden sich die Protokollinformationen der höheren Protokolle und die eigentlichen Nutzdaten, die eine typische Blockgröße von 512 Byte aufweisen. Der IPX-Header enthält Angaben zur Steuerung, die Ziel- und Quelladresse und ist je nach eingesetzter Technologie (Ethernet V2.0/IEEE 802.3, IEEE 802.3(4 Mbit/s) 1526 Byte bis 4096 Byte groß, mindestens aber 30 Byte.

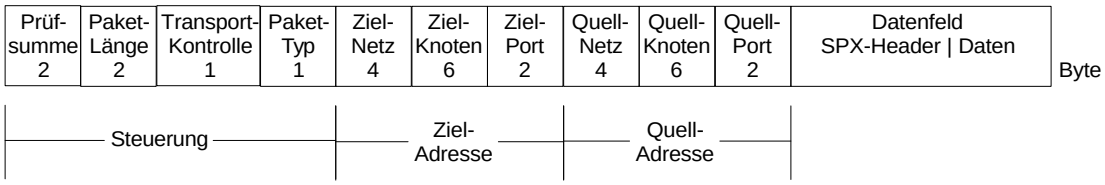

Abbildung 2.7-5 IPX-Paket

- Prüfsumme (Checksum): Prüfsumme des IPX-Headers; Ist innerhalb der LLC-Schicht eine Prüfsumme realisiert, dann wird dieser Allgorithmus auf Grund der Redundanz abgeschaltet und auf FFFF(hex) gesetzt.
- Paket-Länge (Lenght): Gesamtlänge des IPX-Pakets (Header + Datenfeld)
- Transport-Kontrolle (Transport Control): Dieses Feld wird nur von Netware-LAN-Systemen benutzt. Server mit Routingfunktionen oder IPX-Router tragen hier die Anzahl der Übertragungsabschnitte (Hops) zur Zielstation ein. Da nur die letzten vier Bits zur Verfügung stehen, können maximal 16 Sprünge eingetragen werden. Soll ein 17. Sprung eingetragen werden, wird das Paket verworfen. Es muß innerhalb von 16 Sprüngen von der Quell- zur Zielstation gelangt sein.
- Paket-Typ (Paket Type): Informationskennzeichnung für den Datenbereich
- Ziel-Netz (Destination Network): Adresse des Ziel-Netzes, die vom Administrator bei der Einrichtung des Servers vergeben wurde. Es sind nur hex-Werte zugelassen. Handelt es sich um das gleiche Netz wird das Feld auf 0 gesetzt.
- Ziel-Knoten (Destination Node): MAC-Adresse der Zielstation
- Ziel-Port (Destination Socket): Adressierung eines bestimmten Prozesses (Dienstes) in der Zielstation. Diese Information ist besonders für Server mit mehreren Aufgaben nötig, damit die Pakete nicht fehlgeleitet werden.
- Quell-Netz (Source Network): Adresse des Quell-Netzes; Ist der Wert 0, dann ist der Sendestation diese Adresse nicht bekannt.
- Quell-Knoten (Source Node): MAC-Adresse der Quellstation
- Quell-Port (Source Socket): siehe Ziel-Port

Die MAC-Adresse im IPX-Header stellt eine Redundanz im Paket dar, sie ist im MAC-Frame nocheinmal enthalten, dies vergrößert den Protokoll-Overhead unnötig.

Das SPX-Protokoll

Das in der Schicht 4 angesiedelte verbindungsorientierte SPX-Protokoll garantiert die Zustellung von Datansegmenten und ihre richtige Reihenfolge beim Empfänger. Jedes Datenpaket muß innerhalb der vorgegebenen Antwortzeit bestätigt werden und bei Fehlererkennung gegebenenfalls neu übertragen werden. Dieses Protokoll dient hauptsächlich zur Kommunikation zwischen Arbeitsstation und einem festgelegten Dienst oder in der Peer-to-Peer-Kommunikation. Für die Datenübertragung zwischen Arbeitsstation und Fileserver erfolgt grundsätzlich ein verbindungsloser Zugriff.
Die eindeutige Identifikation der Datenblöcke erfolgt über die Kombination von Verbindungs-ID und Sequenznummer.

Verbindungs-Kontrolle 1	Datenstrom-Typ 1	Verbindungs-ID (Quelle) 2	Verbindungs-ID (Ziel) 2	Sequenz-nummer 2	Quittungs-nummer 2	Allokations-Nummer 2	Datenfeld	Byte

Abbildung 2.7-6 SPX-Paket

- Verbindungs-Kontrolle (Connection Conrol): Kontrolle des Datenflusses über die ersten 4 Bit (Bit 7-4), Bit 3-0 haben keine Bedeutung;
  - Bit 7 System Packet: Unterscheidung von System- oder Nutzdaten
  - Bit 6 Aknowledge Required: erzwungene Quittungsabgabe bei gesetztem Bit
  - Bit 5 Attention: keine Bedeutung
  - Bit 4 End of Message: Markierung des letzten Dateipaketes

- Datenstrom Typ (Data Stream Type): Verweis auf entsprechenden Datentyp im Datenbereich
- Verbindungs-ID (Quelle) (Source Connection Identifier): Identifizierung der logischen Quell-Verbindung
- Verbindungs-ID (Ziel) (Destination Connection Identifier):Identifizierung der logischen Ziel-Verbindung
- Sequenznummer (Sequence Number): Identifizierung der Reihenfolge der Datenpakete
- Quittungsnummer (Acknowledgement Number): Sequenznummer des letzten korrekt empfangenen Datenpakets
- Allokations-Nummer (Allocation Number): Anzahl der Kredite für die Flußkontrolle; kennzeichnet, wieviel Datenblöcke gesendet werden können, bis die nächste Quittung eintrifft.

Weitere Informationen zu Netware

Das RIP wird benötigt, um den kürzesten Weg von der Quelle zum Ziel zu ermitteln. Durch die Begrenzung auf 16 Hops (Übertragungssprünge) ist dies in größeren Netzverbunden besonders wichtig. Ein Server sendet in bestimmten Zeitintervallen seine Routingtabelle als Broadcast über das Netz, zudem können zusätzliche Broadcasts bei einer Topologie Änderung (Router tot oder neu, Leitung tot oder neu) notwendig werden. Zur Einbindung neuer Print-, Fax- und File-Server oder Gateway-Dienste wurde das SAP entwickelt. Zur Aktualisierung der Informationen über angeschlossene Stationen wird ein Broadcast ins Netz geschickt, dies erkennen die Server sofort und antworten dementsprechend, so daß die Informationen in die Routingtabellen eingetragen werden können.Um die Server zu entlasten, sind grundsätzlich nr die Arbeitsstationen für die Fehlerbehebung zuständig.

Über das ODI-Konzept (Open Datalink Interface) wird eine Arbeitsstation befähigt mehrere Kommunikationsprotokolle zu benutzen, dadurch ist die gleichzeitige Verbindung zum Beispiel mit einem Netware-Server und einem TCP/IP basiertem UNIX-Server möglich.

2.7.3. TCP/IP - Protokollfamilie

Das TCP/IP-Protokoll hat weltweit eine große Verbreitung. Der erste Einsatz erfolgte im Vorgänger des heutigen Internets, dem ARPANET (Avanced Research Projekt Agency Network), in den USA. Es dient hauptsächlich zur Vernetzung von UNIX-Systemen. Durch den frei verfügbaren Quellcode des Protokolls wird es zunehmend aber auch in anderen Rechnernetzen eingesetzt. Die Weiterentwicklung und Pflege aller Protokolle bündelt das IAB (Internet Activities Board). Auch beim TCP/IP ist die verbindungsorientierte und verbindungslose Kommunikation möglich. Für verbindungsorientierte Anwendungen sind virtuelle Verbindungen notwendig, dazu wird TCP-Protokoll benötigt. Für die verbindungslosen Anwendungen benutzt man das UDP-Protokoll.

- IP (Internet Protocol): Es übernimmt die Aufgaben der 3. Schicht und besteht aus einer Sammlung von Programmroutinen, auf die die anderen Protokolle aufsetzen. Die Datenpakete der höheren Protokolle werden vom IP als Datagramme übertragen.
- TCP (Transmission Control Protocol): Beinhaltet Programmroutinen, auf die UNIX-Anwendungen zurückgreifen, die eine verbindungsorientierte Kommunikation benötigen.

- UDP (User Datagramm Protocol): verbindungslose Kommunikation ohne Garantie der korrekten Übertragung
- ARP (Address Resolution Protocol): Unterstützung der Adressierung und Zuordnung von logischen Internetadressen und MAC-Adressen
- RARP (Reverse ARP): Ermittlung von Internetadressen zu bestimmten MAC-Adressen
- ICMP (Internet Control Message Protocol): Übertragung von Fehler und Steuerinformationen

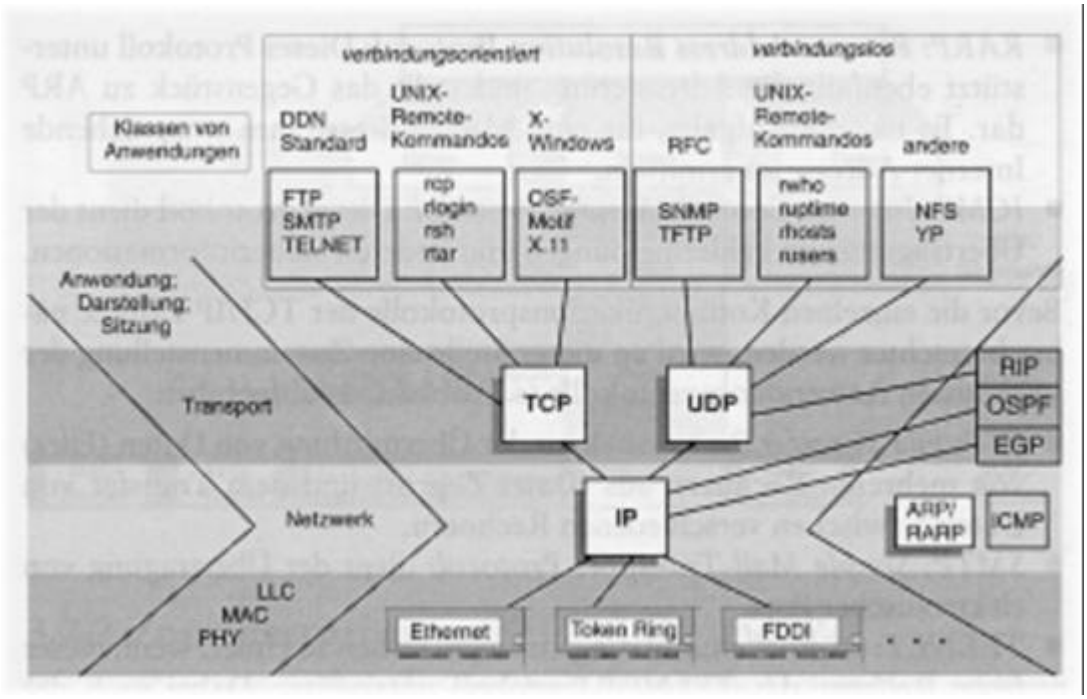

Abbildung 2.7-7 TCP/IP im Schichtenmodell, [8, S. 155]

In den Ebenen 5 bis 7 werden verschiedene Anwendungen realisiert. Zu diesen Anwendungen zählen u.a. das HTTP (Hyper Text Transfer Protocol) (bekannt als WWW - World Wide Web), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol) und NFS (Network File System).

IP-Protokoll

Die Datagramme werden vom IP-Protokoll verbindungslos zur Partnerstation gesandt, ohne zu wissen, ob der Empfänger bereit ist. Es findet keine Fehlerkontrolle statt und die Versendung der einzelnen Pakete erfolgt unabhängig voneinander, wodurch beim Empfänger nicht automatisch die Reihenfolge gewährleistet wird. Für die Bereitstellung der Funktionen sind die höheren Protokolle verantwortlich. Die wichtigste Aufgabe ist das Hinzufügen der Quell- und Ziel-IP-Adresse. Jedes Datenpaket ist eindeutig gekennzeichnet und kann seinen eigenen Weg durch das Netz nehmen. Die maximale Größe des IP-Pakets ist vom Übertragungsmedium abhängig und wird in der MTU (Maximum Transfer Unit) festgelegt. Die IP-Schicht ist in der Lage, die ankommenden Datenpakete zur Anpassung an die unterschiedlichen Netze (X.25 - 128 Byte, Ethernet - 1526 Byte) zu fragmentieren, dies bedeutet die Unterteilung des Paketes in kleinere Untereinheiten, so daß eine Übertragung zum nächsten Netzknoten oder zum Zielrechner möglich wird. Jedes Paketfragment erhält dabei den gesamten IP-Header und findet seinen eigenen Weg durchs Netz. Kommt das erste Fragment am Empfänger (Knoten oder Zielrechner) an, wird ein Zeitintervall gestartet (meist 30 Sekunden), in dem auf die weiteren Fragmente gewartet

wird. Fehlt am Ende ein Fragment, werden alle Teile verworfen. Durch diesen Mechanismus wird der Empfangspuffer nicht unnötig belegt. Die Größe eines IP-Pakets liegt zwischen 576 und 65536 Byte, die maximale Größe verringert sich um die Größe des IP-Headers, die mindestens 20 Byte beträgt.
Zur Überwachung des Datenflusses wird eine ICMP-Sendeunterdrückungsnachricht von der IP-Schicht ausgesandt.

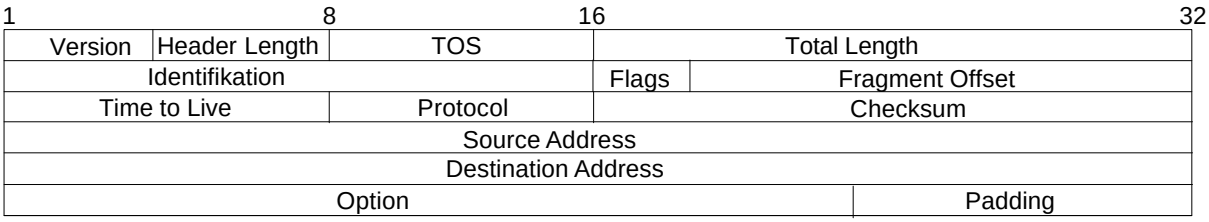

Abbildung 2.7-8 IP-Header (IPv4)

- Version: Versionsnummer des IP-Protokolls, aktuell Version 4
- Header Length (Länge des IP-Kopfes): Länge besteht aus 32 Bit-Worten, der kleinste IP-Header besteht aus den ersten fünf 32 Bit-Worten
- TOS (Type of Service, Sevice-Typ-Angaben): Angaben über die Kriterien eines IP-Paketes (Routing-Dienst, Paket mit Priorität)
- Total Length: Gesamtlänge des IP-Paketes in Byte
- Identification: Bei der Segmentierung wird eine eindeutige Identifikationsnummer vergeben, die es dem Zielrechner erlaubt, die IP-Pakete den entsprechenden Dateien zuzuordnen.
- Flags: Steuerung des IP-Protokolls, DF=1 (don't fragment) - Paket darf nicht fragmentiert werden; MF=1 (more fragments) - weitere IP-Pakete aus einer Datei folgen, mit MF=0 wird das letzte IP-Paket markiert
- Fragment Offset (Fragmentabstand): bei MF=1; gibt die relative Position des Dateifragmentes in Bezug auf den Dateianfang an und ermöglicht das richtige zusammensetzen der Datei
- Time to live (Lebenszeit): gibt Verweilzeit der Pakete im Netz vor, da diese zirkulieren können und wird vom Quellrechner gesetzt. In jedem Netzknoten verringert sie sich um 1 und gibt somit die maximale Anzahl der Netzknoten an, die das Paket durchlaufen darf. Bei TTL=0 wird vom Netzknoten eine ICMP-Nachricht an die Quelle gesandt.
- Protocol: enthält die Nummer des höheren Protokolls (ICMP - 1, TCP - 6, UDP - 17) an das das Paket weitergereicht werden muß.
- Checksum (Prüfsumme): Prüfsumme des IP-Headers zum Erkennen von Übertragungsfehlern; Prüfung der Nutzdaten im TCP-Protokoll
- Source IP-Address: IP-Adresse des Quellrechners
- Destination IP-Address: IP-Adresse des Zielrechners
- Option: Angaben für besondere Nutzung, meistens nicht benutzt
- Padding (Füllzeichen): auffüllen des Optionsfeldes auf 32 Bit

TCP-Protokoll

Im TCP-Protokoll werden virtuelle und duplexfähige End-to-End-Verbindungen aufgebaut. Die Übertragung erfolgt in festen Datenblöcken (TCP-Pakete). Aufgaben des TCP sind:

- Abstimmung der Länge von TCP-Paketen,
- Segmentierung der zu sendenden Dateien und Wiederherstellung im Zielrechner,
- einbinden einer Sequenznummer für die Reihenfolge der Segmente und
- Aufforderung des Quellrechners zur wiederholten Übertragung bei Fehlern.

Vor dem Beginn einer Übertragung muß zwischen den TCP-Schichten des Quell- und Zielrechners die maximale Länge des TCP-Paketes vereinbart werden. Nur eine Station kann die Verbindung zwischen zwei Stationen aufbauen. Ein mehrfacher Aufbau einer Verbindung nach Abbruch ist erst nach dem Timeout (Geduldzeit) möglich. Der Datenaustausch kann erst nach dem Aufbau der Verbindung erfolgen. Die Übertragung fehlerhafter Pakete kann nach dem Ablaufen des Timeouts erfolgen. Durch die Sequenznummer ist eine doppelte Übertragung leicht erkennbar. Durch die maximale Größe der Sequenznummer können bis zu 8 Gigabyte pro Verbindung übertragen werden.
Es wird die Flußkontrolle nach dem Fenster-Mechanismus angewandt, wodurch der Empfänger dem Sender die Größe des Empfangspuffers bekanntgeben kann. Tritt während der Übertragung beim Empfänger eine größere Belastung auf, kann dies über das Window-Feld reguliert werden. Jedes Paket unterliegt auch wieder einer Zeitüberwachung, nach der eine Quittierung erfolgen muß. Je nach Belastung des Netzes ist die Zeitdauer sehr unterschiedlich und wird für jedes Paket neu berechnet und eingestellt.

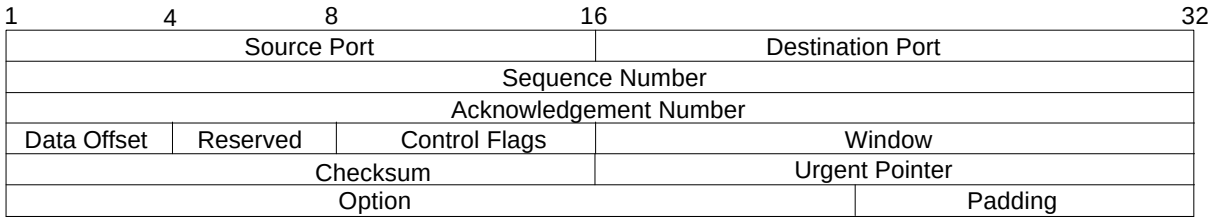

Abbildung 2.7-9 TCP-Header

- Source-Port (Quell-Port): Portnummer des Anwenderprozesses im Quellrechner
- Destination Port (Ziel-Port): Portnummer des Anwenderprozesses im Zielrechner
- Sequence Number: Die Sequenznummer dient zur Nummerierung der Datensegmente und gilt nur in Senderichtung. Die TCP-Schichten bilden Anfangssequenznummern, tauschen diese aus und bestätigen sie. Jede Nummer ist eindeutig und existiert während der Lebenszeit der Pakete nur einmal. Die Quelle erhöht die Nummer immer um die Anzahl der gesendeten Bytes.
- Acknowledgement Number (Quittungsnummer): gilt nur in Empfangsrichtung und kennzeichnet, wieviel Byte korrekt empfangen wurden.
- Data Offset (Datenabstand): Länge des TCP-Headers in 32 Bit-Worten; Die Stelle des Datenbeginns ist eindeutig gekennzeichnet.
- Control-Flags: Die Flags legen fest, welche Header-Felder gültig sind. Es sind 6 Bits, die bei Status 1 folgende Funktion haben:
  - URG: Urgent-Pointer ist gültig
  - ACK: Quittungsnummer ist gültig
  - PSH (Push-Funktion): sofortige Datenweitergabe an die nächst höhere Schicht
  - RST (Reset): Rücksetzen der Verbindung
  - SYN: Verbindungsaufbauwunsch, Quittierung erforderlich
  - FIN: einseitiger Verbindungsaufbau, Ende des Datenstroms aus der Richtung, Quittierung erforderlich

- Window (Fenstergröße): Steuerung des Datenstroms im Quellrechner durch den Zielrechner, empfängt der Sender ein TCP-Paket mit Window gleich 0, dann wird die Verbindung gestoppt.
- Checksum (Prüfsumme): prüft den TCP-Header, die Daten und die Quell- und Ziel-IP (aus IP-Header) auf Bitfehler
- Urgent Pointer (Urgent-Zeiger): Zeigt das Ende der Urgent-Daten an, diese befinden sich direkt hinter dem TCP-Header. Urgent-Daten signalisieren meist außergewöhnliche Zustände und bestehen aus wichtigen Kurznachrichten.
- Option: Angabe von Service-Optionen möglich
- Padding (Füllzeichen): Auffüllen des Optionsfeldes auf 32 Bit

UDP-Protokoll
Mittels UDP könne Anwendungen Datenpakete (eigenständige Datenblöcke) senden und empfangen. UDP wird meist für das NFS (Network File System), die Broadcast-Nachrichten oder im Netzmanagement eingesetzt. Der Header enthält nur jeweils ein Feld für den Quell-Port, den Ziel-Port, die Länge und die Prüfsumme.

Beispiel einer TCP/IP - Übertragung (Abbildung 2.7-10)
Die Datei wird im Quellrechner (Tln A) in einzelne Segmente unterteilt und jedem Segment wird ein IP-Header (Nr. 1-14) und ein TCP-Header (Nr. 15-26) vorangestellt. Jedes so entstandene Datenpaket kann auf verschiedenen Wegen durch das gesamte Netz gelangen. Die Entschlüsselung, zu welchem Rechner das Datenpaket geleitet werden soll, erfolgt über das Feld 12, in dem die Zieladresse steht. Jeder Knoten K wertet unter anderem dieses Feld aus und bestimmt danach den schnellsten Weg zum nächsten Knoten, jedes Datenpaket erhält somit seinen eigenen Weg zum Ziel. In den einzelnen Knoten kann

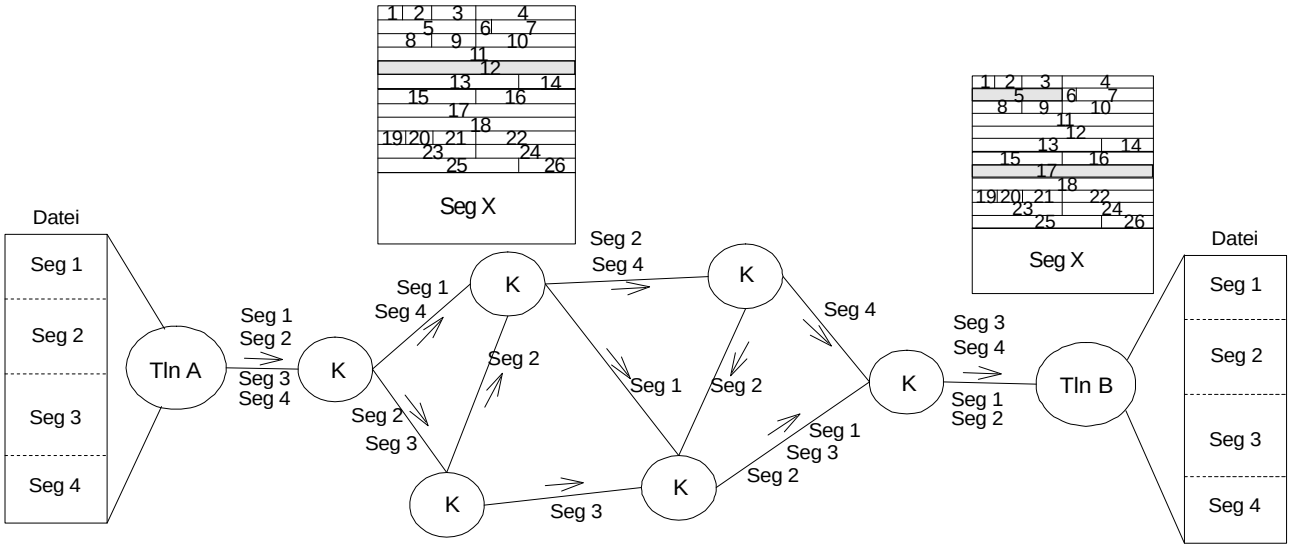

Abbildung 2.7-10 TCP/IP - Übertragung

es auf Grund erhöhter Verkehrslast zu Verzögerungen kommen. Erhöhte Verkehrslast bedeutet, das mehrere Daten zur gleichen Zeit im Vermittlungsknoten eintreffen, diese müssen nun der Reihenfolge nach verarbeitet und weitergeleitet werden. Ist der Empfangspuffer in einem Knoten voll, dann werden alle weiterhin ankommenden Pakete verworfen. Und müssen vom Quellrechner erneut gesendet werden. Die Datensegmente treffen nach dem Passieren aller Knoten im Zielrechner auf Grund der Knotenverzögerungen und der unterschiedlichen Laufzeiten im Zielrechner (Tln-B) ein. Die ankommenden Datenpakete werden über das Feld 5 (Identifikation) der richtigen Datei

zugeordnet. Nachdem alle Felder des IP-Headers ausgewertet wurden, wird im TCP-Header über das Feld 17 die richtige Reihenfolge der Datensegmente erkannt und diese dann nach Bereinigung von allen Kopfdaten wieder zusammengesetzt. Die Datei kann im Rechner von Tln-B weiter verarbeitet werden.

2.7.4. Aufbau von Internet-Adressen

Internetadressen sind zur weltweit eindeutigen Kennzeichnung von Rechnern gedacht oder Rechnersystemen geeignet und werden in der IP-Schicht dem Datenpaket hinzugefügt. Die IP-Adressen haben eine Länge von 32 Bit und werden zur besseren Beschreibung in 4 Byte unterteilt. Eine dezimale Darstellung erfolgt in der Form 127.12.15.1 und enthält die Struktur einer Netz- und Host-ID. IP-Adressen dürfen weltweit nur einmal vergeben werden und innerhalb eines Netzwerkes sich nur in dem Teil unterscheiden, der die Stationen kennzeichnet (Node-Teil). Soll die Adresse weltweit eindeutig sein, muß man bei der NIC (Network Information Center) in Kalifornien ein mehr oder weniger großen Adreß-Pool beantragen. Für die eindeutige Zuweisung innerhalb des eigenen Netzwerkes ist der Administrator verantwortlich. Wenn kein Adressbereich beantragt wird, muß beim Übergang vom internen Netz zum Internet eine eindeutige Trennung erfolgen und es darf keine dieser frei vergebenen Adressen nach außen sichtbar sein.
Es werden fünf Klassen von IP-Adressen unterschieden, dies wird durch die ersten 3 Bit der Netz-ID festgelegt. Es wurden Klassen A-E festgelegt, wobei die Bereiche der Adressen für A-C festgelegt sind und in der Klasse D die Aufteilung beliebig ist. Das Klasse E Netz wird noch nicht verwendet.

Klasse / Bits	**Adreß-Bereich**	**Bemerkung**
A / 0xx	1.0.0.0 -127.255.255.255	7 Bit für Netzadressierung (max. 126 Netze) 24 Bit für Adressierung von Unternetzen und Stationen (2^{24} Stationen)
B / 10x	128.0.0.0 -191.255.255.255	14 Bit für Netzadressierung (max. 4095 Netze) 16 Bit für Unternetze und Stationen (2^{16} Stationen)
C / 110	192.0.0.0 -223.255.255.255	21 Bit für Netzadressierung (max. 262143 Netze) 8 Bit für Unternetze und Stationen (255 Stationen)
D / 111	Multicast	Aufteilung der Bits beliebig
E / 1111	reserviert	für neue Adressierungsform freigehalten

Subnetze dienen der Unterteilung von größeren Unternehmensnetzen oder dem Uusammenfassen von Etagen oder großen Arbeitsgruppen. Subnetze sind eigenständige Netze, die die gleiche Netz-ID verwenden. Die Festlegung erfolgt über die Subnetmask. Verdeutlicht wird dies an folgendem Beispiel eines Klasse C Netzes:
11010110 . 00010101 . 11010010 . 00000000 (214.21.210.0)
Zur besseren Unterteilung benötigen wir 8 Subnetze, dazu muß folgende Subnetmask eingestellt werden:
11111111 . 11111111 . 11111111 . 11100000 (255.255.255.224)
Damit haben wir 3 Bit für die Adressierung von Subnetzen (2^3 - 8 Subnetze). Zur Stationsadressierung haben wir nur noch 5 Bit zur Verfügung, d.h. es können in jedem Subnetz 32 Stationen adressiert werden.
Da die IP-Adressen bald völlig ausgeschöpft sein werden, der Bedarf aber weiterhin gedeckt werden muß, wird momentan ein neuer Standard entwickelt. In der neuen Version

6 des IP-Protokolls (IPv6, IPng - Next Generation) werden die beiden Hauptprobleme von IPv4, Adressenknappheit und Routingsystem, beseitigt. Da die Standardisierung noch nicht vollkommen abgeschlossen ist können noch nicht alle Neuerungen aufgelistet werden. Wesentliche Verbesserungen sind:

- Verbesserte Routing-Funktionen,
- größerer Adressraum durch Erweiterung von 32 auf 128 Bit,
- hierarchische Adressierung als Grundlage zum Routing,
- automatische Konfiguration von IP-Adressen einzelner Netzwerkkomponenten,
- weltweite IP-Adressen auf Lebenszeit,
- Vereinfachung der IP-Header-Informationen,
- integrierte Funktionen für Authentisierung und Sicherheit, auch Verschlüsselung und Firewalls sowie
- definierte Güteklassen zur Leistungssteigerung bei Echtzeit Anwendungen (Sprache, Video).

Durch die Erweiterung der Adressen von 32 auf 128 Bit würden 2^{128} Knoten (Router, Hosts) möglich sein. Um ein reibungsloses Routing auch weiterhin zu ermöglichen, müssen jedoch genügend Reserven an Adressen gehalten werden. Erst dadurch wird ein einfaches Auffinden der Adressen möglich. Durch die rasante Ausbreitung des Internets und der enormen Datenmengen muß der Overhead verkleinert werden. Ein Ansatz dazu wäre ein hierarchisches Routing, dies läßt sich erst mit IPv6 verwirklichen.
In den neuen Routern wird eine automatische Adressvergabe eingebunden, so daß beim Verschieben von Rechnern oder dem Wechsel zu anderen Service-Providern keine lange andauernden Änderungsprozeduren an den PC`s und Servern erfolgen müssen. In den IPv6 fähigen Hosts können mehrere IPv6 Adressen für eine gewisse Zeit parallel gefahren werden. Ein wichtiger Faktor wird auch die Kompatibilität zu IPv4 sein. In einer Übergangszeit werden beide Protokollversionen nebeneinander existieren, wodurch in den Routern die Möglichkeit gegeben werden muß, beide Routings auszuführen. Die Softwareentwickler müssen ihre Programme anpassen oder gar ganz neu strukturieren. Das IPv6-Protokoll wird dabei in einem IPv4-Tunnel transportiert, dieser kann automatisch oder manuell konfiguriert sein. Neuere Überlegungen sehen auch ein eigenständiges IPv6-Netz vor, was über einen IPv4-Multicast-Netzwerk als lokaler Link zu erreichen sein wird. Um das neue Protokoll in der Praxis zu testen, wurde ein Testbackbone im Juni 1996 zunächst mit drei Teilnehmern errichtet. Die Beteiligung wächst rasant, so daß im Januar 1997 schon 90 Interessenten die Tests unterstützen. Die wichtigste Aufgabe für die nächste Zeit ist die Aufteilung der neuen Adressen,ob diese nun dynamisch oder statisch vergeben sind.

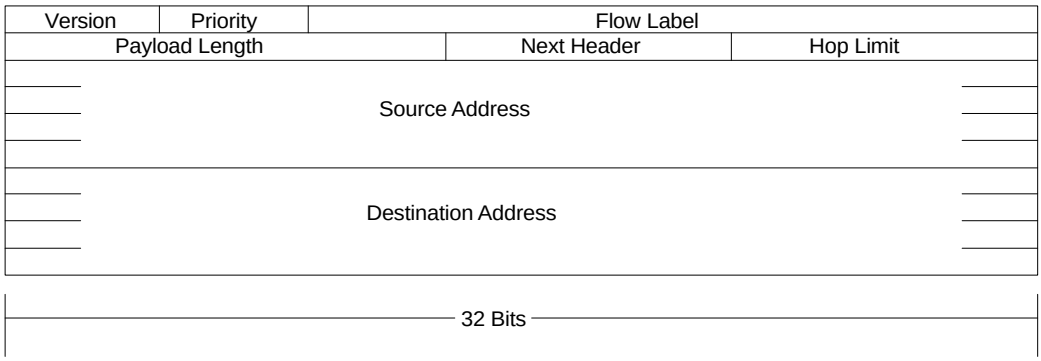

Abbildung 2.7-11 IPv6 Header

Das Aussehen der einzelnen Felder ist noch nicht näher bestimmt, dies wird erst in den nächsten RFC`s (Request for Comments) zu finden sein, die von der IETF (Internet Engineering Task Force) und deren Arbeitsgruppen festgelegt werden.