2. Grundlegende Betrachtungen

2.1. Das OSI-Referenzmodell

Kompatibilität kann nur durch Standards (Protokoll- und Schnittstellendefinitionen) gewährleistet werden. Den wichtigsten Standard für Netze stellt das OSI-Referenzmodell dar. Es dient zur Beschreibung der Netzstruktur, den Protokollcharakteristika und Aufgaben.

Die Schichtenstruktur ist in folgender Abbildung dargestellt.

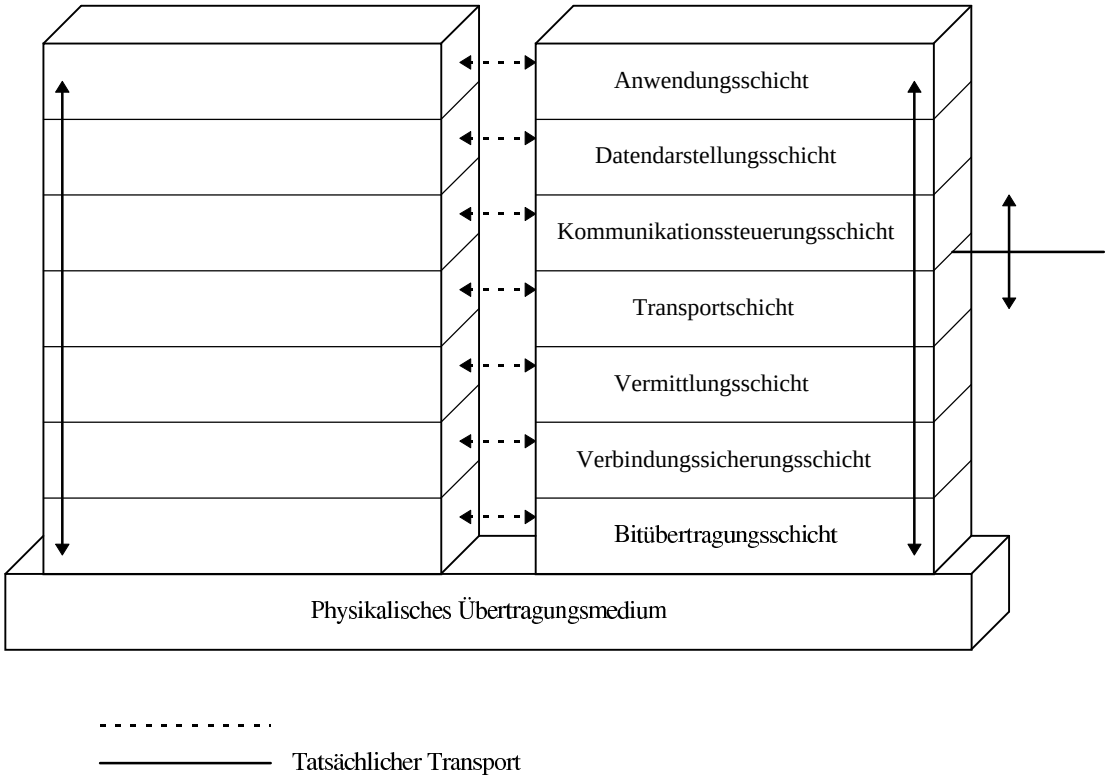


Abb. 2.1: OSI-Referenzmodell [Kau 96]

Konzept: Eine Schicht nimmt Dienste der unter ihr liegenden Schicht in Anspruch und stellt durch die eigene Funktionalität erweiterte Dienste der über ihr liegenden Schicht zur Verfügung.

(Die Funktionen der einzelnen Schichten sind in Tabelle 2.1. aufgeführt.)

Bemerkung: Die aus dem OSI-Modell resultierenden Produkte für PC-Netze und andere Anwendungen sind heute meist zu umfangreich. Funktionen (jenseits der Übertragungstechnik werden mit z.T. „leichteren“ Protokollen realisiert (Untermengen der OSI-Funktionen). [z.B.: TCP/IP]

OSI-Schicht	Funktionen

Anwendungsschicht	■ anwendungsunterstützende Dienste (Protokolle, die Programme zur Erbringung bestimmter Leistungen benötigen (z.B.: Dateiaustausch) ■ Netzmanagement (generelle Verwaltungsaufgaben) ■ Namensumsetzung (log. > verwertbare physische Namen/ Adressen)
Darstellungsschicht	■ Umsetzung von lokalen Formaten und Datendarstellungen in für das Netz allgemeingültige Standardformate ■ Interpretation dieser gemeinsamen Formate
Kommunikationssteuerungsschicht	■ Interprozeßkommunikations-Mechanismen (Prozeß-zu-Prozeß-Verbindung, Prozeßsynchronisation) ■ Steuerung der logischen Verbindung
Transportschicht	■ logische Ende-zu-Ende-Verbindungen in Abstraktion der technischen Übertragungssysteme ■ Transport von Nachrichten zwischen Kommunikationsendpunkten (Transport von Datenpaketen flexibler Länge mit Zielangabe oder Aufbau einer log. Verbindung zwischen 2 Elementen des Adreßraumes) ■ ggf. Datenflußkontrolle und Überprüfung der Unverfälschtheit
Vermittlungsschicht	■ Wegebestimmung/-steuerung in verzweigten Netzen, Routing ■ Ersatzwegeschaltung ■ Datenflußkontrolle
Sicherungsschicht	■ gesicherte Übertragung von Informationseinheiten zwischen zwei Punkten (Codierung/Decodierung, Fehlersicherungsmechanismen ■ Adressierung angeschlossener Stationen
Bitübertragungsschicht	■ nachrichtentechnische Hilfsmittel für die Übertragung ■ Regelung des Austausches einzelner Informationsbits über ein Übertragungsmedium mit den entsprechenden Funktionen (Bitcodierung, Übertragungsgeschwindigkeit, Anschlußart,...)

Tab. 2.1.: OSI-Schichtenfunktionen

[Kau 96], [Zeh 94], [c´t 10/96], [Hea 94]

2.2. Local Area Networks

2.2.1. Grundlegende Aspekte

„LAN´s sind Systeme für den Hochleistungs-Informationstransfer, die es einer Anzahl gleichberechtigter Benutzer ermöglichen, auf einem räumlich begrenzten Gebiet unter Anwendung eines schnellen Übertragungsmediums, partnerschaftlich orientierten Datenaustausch hoher Güte durchzuführen.“ [Kau 96]

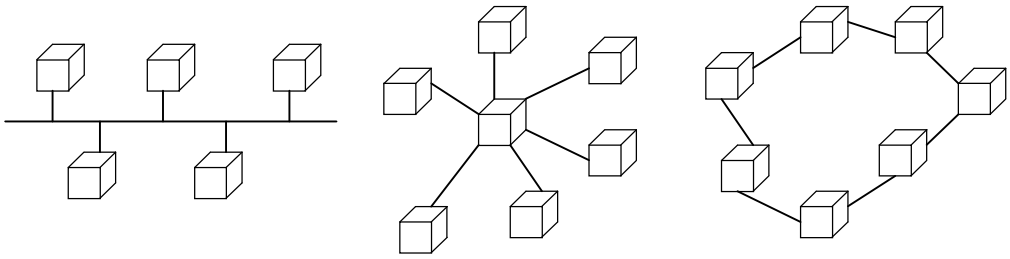
Einzelne LAN´s haben eine maximale Ausdehnung von ca. 10 km. Größere Netze sind durch die Zusammenschaltung mehrerer LAN´s entweder direkt durch Brücken/Router oder indirekt durch ein Backbone-Netz realisierbar.

Als Übertragungsmedien finden:

- verdrillte Kabel (UTP, S-UTP, STP) {bis 100 Mbit/s}
- Koaxialkabel {lange Zeit Standardmedium}
- Lichtwellenleiter {hauptsächlich im Backbone-Bereich Verbindung großer Hubs}

weitverbreitete Anwendung.

Im LAN-Bereich haben sich im wesentlichen 3 Topologien etabliert.



Bus-Topologie Stern-Topologie Ring-Topologie

Abb. 2.2.: LAN-Topologien [Kau 96]

Bussysteme	Sternsysteme	Ringsysteme
- ein Medium, welches in gewissen Abständen angezapft wird	- zentraler Umsetzer, Hub, Switch - zu jeder Station eigene Leitung	- Stationen in „Reihe“ geschaltet und erste mit letzter verbunden

Diffusionsnetze (schleifenfreie Topologien)

Bestehende LAN´s mit typischen Übertragungsgeschwindigkeiten von 4-16 Mbit/s sind meist als BUS-Diffusionsnetz oder serielles Ringnetz ausgeführt.

Im Zuge der Implementierung moderner LAN-Systeme in Verbindung mit der strukturierten Verkabelung werden h eute hauptsächlich sternförmige Topologien eingesetzt. Jede Station wird an einen Hub oder Switch angeschlossen (d.h. der „Bus“ wird auf kleinem Raum realisiert). Sternsysteme bieten zudem den Vorteil der schnelleren Fehlerisolation.

[Kau 96]

2.2.2. LAN´s im OSI-Referenzmodell

LAN´s sind Transport-Subsysteme im Rahmen einer Netzwerkarchitektur. Unterschiede bestehen lediglich in der Struktur der unteren Schichten.
Ab Oberkante Schicht 2 ist ein einheitliches LAN-Transportsystem existent (d.h. gemeinsame Oberfläche auf Schicht 2 (LLC)).

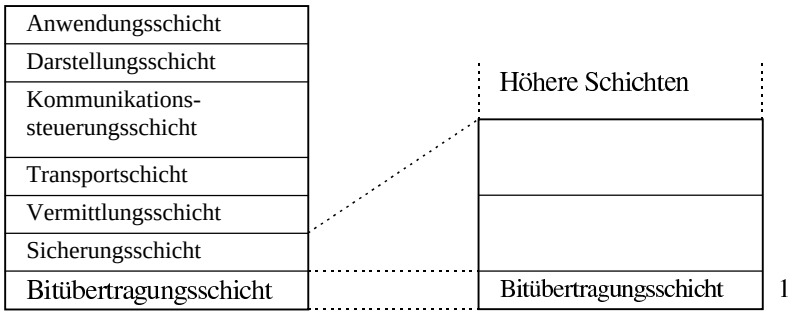


Abb. 2.3.: LAN´s im OSI-Referenzmodell

Teilschicht	Funktion
Logical Link Control (LLC)	■ Formung der Ressourcen der Zugriffskontroll- und Übertragungs-einrichtungen zu einer abstrakten Paketübertragungsressource, auf die sich höhere Schichten beziehen können ■ LLC1 - nichtbestätigter verbindungsloser Service ■ LLC2 - verbindungsorientierter Service ■ LLC3 - bestätigter verbindungsloser Service
Media Access Control (MAC)	■ Zugriffssteuerung

Tab. 2.2.: LAN-Layer-Funktionen

[Kau 96]

2.2.3. Grundlegende LAN-Standards

Vor ca. 10 Jahren hat sich eine Reihe unterschiedlicher LAN-Systeme entwickelt. Mittlerweile sind durch Normierungsgremien Standards verabschiedet.

z.B.:	IEEE Standard 802 bzw. ISO 8802	Ethernet, Token Ring
	ANSI	FDDI

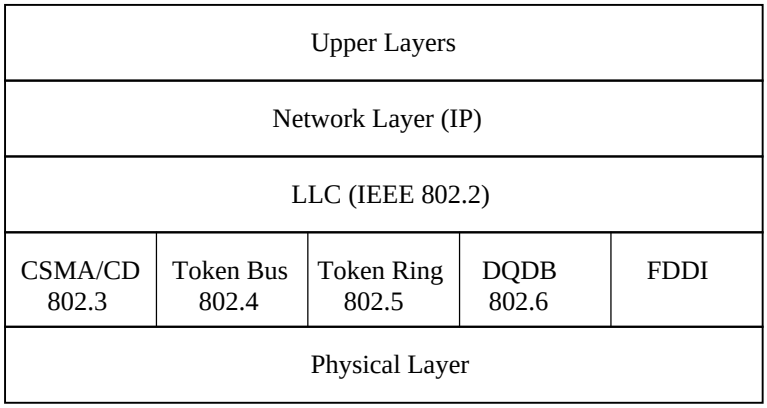


Abb. 2.4.: LAN-Standards (Einordnung) [in Anlehnung an IEEE 4/96]

2.2.4. LAN-Steuerungsverfahren

Zentrales Problem: Regelung des wechselseitigen Ausschlusses auf dem prinzipiell jederzeit allgemein benutzbaren Übertragungsmedium

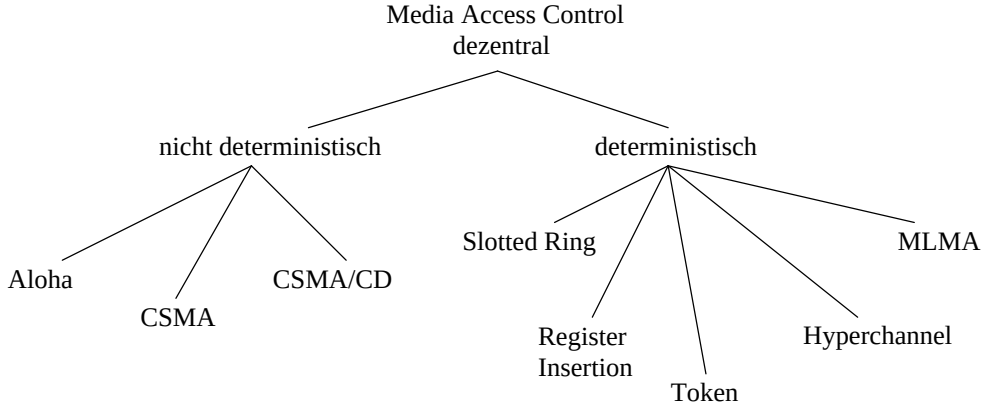


Abb. 2.5.: LAN-Zugriffsverfahren [Kau 96]

Bei Bus- und Ringstrukturen, in welchen zu einer Zeit jeweils nur eine Station sendeberechtigt ist, muß der Medienzugriff durch Steuerungsalgorithmen, welche im MAC-Sublayer der Sicherungsschicht definiert sind, geregelt werden.

Folgende zwei Zugriffsverfahren bilden die Basis für die drei meistverwendeten LAN-Typen.

Steuerungsverfahren	**CSMA/CD** (Carrier Sense Multiple Access/Collision Detection)	**Token Passing**
angewendet in...	Ethernet	Token Ring, FDDI
Prinzip	Wettbewerb mit Kollisionskontrolle - sendewillige Station muß Verkehr mithören und warten bis Medium verfügbar - Kollisionen werden durch Überlagerung mehrerer Datenpakete erkannt - nach 16 erfolglosen Versuchen > Abbruch	Weitergabe einer Sendeberechtigung - umlaufende Senderechtsvergabe - definierte Sendezeitdauer (durch logische Kontrollstruktur mittels Speicherverweisen auch auf Bus-LAN implementierbar)
Eigenschaften	nicht deterministisch	deterministisch konfliktfrei

Tab. 2.3.: CSMA/CD und Token Passing

Unter den Gesichtspunkten Sicherheit und Fairneß ist deterministischen Verfahren der Vorrang zu geben (insbesondere bei vielen sendenden Stationen). Mit CSMA/CD ist unter Hochlastbedingungen kein sinnvoller Durchsatz erreichbar. Bei unregelmäßiger Verteilung der Sendeintensität einzelner Stationen kann CSMA/CD unter Umständen eine bessere Effizienz erzielen.

[Kau 96], [Kya 96]

2.2.5. Kurzcharakteristik etablierter LAN-Typen und deren Leistungsgrenzen

2.2.5.1. Ethernet (10 Mbit/s)

Übertragungsmethode: - halb-duplex Verfahren (d.h. Senden und Empfangen nicht gleichzeitig möglich),

- aufbauend auf Busstruktur,
- Senderechtzuteilung basierend auf non-deterministischem CSMA/CD-Verfahren

Wenn eine Station sendet, befinden sich alle anderen im Empfangsmodus. Senden zwei Stationen parallel, kommt es zur Kollision (und Zerstörung) der Datenpakete. Die Kollision wird von beiden Stationen detektiert, welche ihren Sendewunsch daraufhin nach einer bestimmten Zeit (Zufallsgenerator) wiederholen.

Leistungsgrenzen: Die Leistungsgrenzen von Ethernet werden durch 3 Parameter bestimmt.

1) Wie aus vorangegangenem Szenario abzuleiten, steigt die Wahrscheinlichkeit von Kollisionen mit zunehmender Teilnehmerzahl. Damit besteht der erste Parameter in der **Anzahl der aktiven Teilnehmer**.

2) Eine weitere wichtige Rolle spielt die **Länge des Netzwerksegments**. Mit steigender Segmentlänge erhöht sich der zentrale CSMA/CD-Parameter:
   - die **Slotzeit** (2x Signallaufzeit zwischen am weitesten entfernten Stationen), welche im worst case der Erkennungszeit für Kollisionen entspricht.

3) Die **Paketlänge** stellt den dritten wesentlichen Parameter für CSMA/CD-basierte Netze dar. Je kürzer die Pakete desto geringer ist die Leistungsfähigkeit bzw. die Bandbreitenausnutzung (Effizienz).

Charakteristische Ethernet-Betriebscharakteristik:

- nondeterministische, stark variierende Übertragungsverzögerungen
- geringste Effizienz bei kleinen Paketgrößen (siehe Abbildung 2.6)
- CSMA/CD funktioniert nur in wenig belasteten Netzwerken gut
  (ab 40-50% Netzlast bei mehr als 10 Teilnehmern sinkt die Effizienz drastisch ab; bei

mehr als 4 Stationen verringert sich die Bandbreiteneffizienz auf <50%)

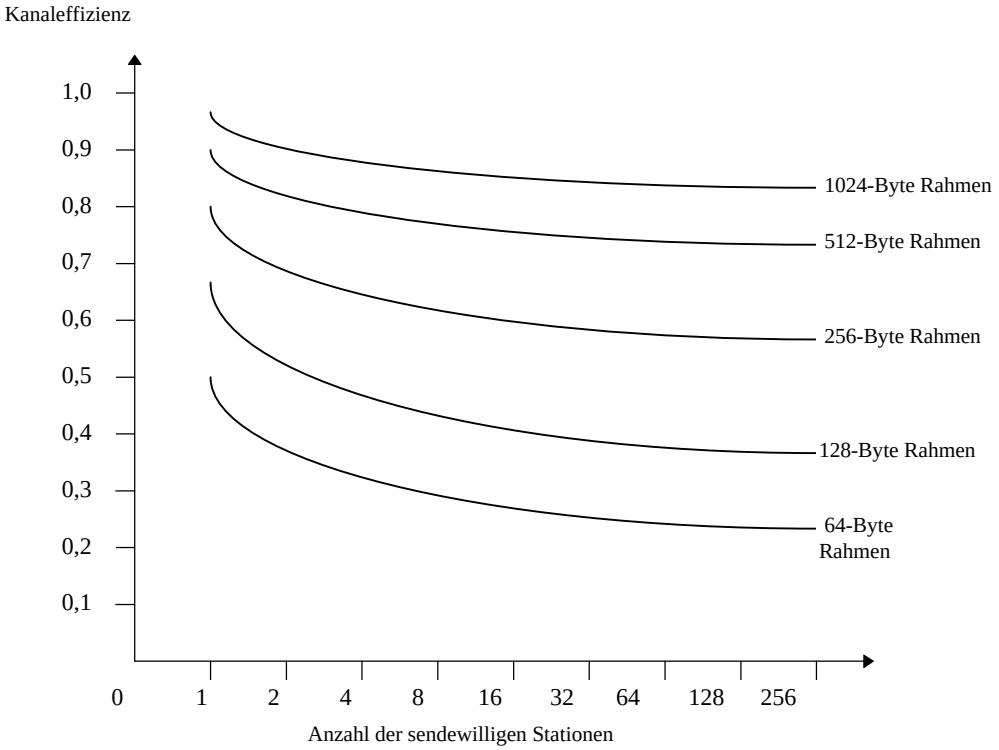


Abb. 2.6.: Effizienz von Ethernet (Sendewahrscheinlichkeit 1/k bei k Stationen)

[Kya 96]

Schlußfolgerungen:

- Ethernet ist von den 3 traditionellen LAN-Technologien für die multimediale Revolution am schlechtesten geeignet.
- Jedoch ist die Leistungsfähigkeit dieser LAN-Technologie nicht zu unterschätzen. Für einen großen Teil der Netzwerkanwendungen ist Ethernet noch einige Zeit ausreichend.

[Kya 96]

2.2.5.2. Token Ring (4/16 Mbit/s) und FDDI (100 Mbit/s)

Übertragungsmethode: - halb-duplex Verfahren (Token Ring),
- aufbauend auf Ringstruktur,

- basierend auf deterministischem Token Passing Verfahren

Jeder Station (im Ring) wird per Definition Gelegenheit gegeben, in regelmäßigen Abständen Daten zu übertragen. Die Senderechtsteuerung erfolgt durch den verwendeten Token (spezielle Bitsequenz). Nach einer definierten Maximalzeit (Token Holding Time) muß der Token in Umlaufrichtung weitergegeben werden.
Bei Sendewunsch wartet die betreffende Station auf den Erhalt des Token und beginnt unmittelbar nach Zuteilung mit der Datenübertragung. Die Empfangsstation erkennt anhand der Zieladresse die für sie bestimmten Pakete und kopiert diese.
Im Token Ring setzt die Empfangsstation die Bits „Adresse erkannt“ und „Paket kopiert“. Die Sendestation kontrolliert diese und nimmt das Paket vom Ring.
Das FDDI-Protokoll, welches speziell für hohe Bandbreiten und die Verwendung in Glasfasersystemen entworfen wurde, implementiert einen großzügigen Token, an das jede Station die Datenpakete anhängen kann. Die Voraussetzung für eine einwandfreie Funktion besteht darin, daß jede Station das ausgesendete Paket nach einem Umlauf vom Ring herunternimmt. Die entstandene Lücke kann von nächster in Ringrichtung liegender Station geschlossen werden.

Betriebscharakteristik und Leistungsgrenzen:

- Da jeweils nur eine Station im Besitz des Senderechts ist, sind keine Kollisionen möglich.
- Das Ziel der optimalen Bandbreitenausnutzung wird besser erreicht als bei Ethernet, jedoch liegt die Schwachstelle im Übertragungsverfahren. Die ausschlaggebende Größe ist in diesem Falle die begrenzte **Token-Holding-Time** (und daraus resultierende **Wartezeiten**).

  z.B.: Token-Holding-Time für Token Ring: i.a. 10 ms
  FDDI: i.a. 4 ms

- Erst bei einer Netzlast von 80 % ist eine Verdopplung der Wartezeit und ein Absinken der Netzleistung zu verzeichnen.

Schlußfolgerungen:

Netzwerktopologie	Maximale Übertragungsverzögerung (30 Stationen)
Ethernet	nicht vorhersagbar
Token Ring	300 ms
FDDI	120 ms

Tab. 2.4.: Echtzeitfähigkeit von Ethernet, Token Ring und FDDI [Kya 96]
(als Vergleichswert: für Multimedia-Anwendungen max. zulässig 10 ms !)

- Selbst FDDI ist im Regelbetrieb nicht in der Lage Multimedia-Anwendungen zu übertragen.
- Ausnahme: FDDI in synchroner Betriebsart (bestimmten Stationen wird eine feste synchrone Bandbreite zugewiesen) > eingeschränkter Betrieb von Echtzeitanwendungen möglich

[Kau 96], [Kya 96]

2.3. Die TCP/IP-Protokollfamilie

Die TCP/IP-Protokollfamilie wurde vor über 20 Jahren vom US Department of Defense entwickelt. (daher auch: DoD-Protokollfamilie)
TCP/IP wurde nicht für ein spezielles Nachrichtentransportsystem konzipiert, sondern ist auf verschiedenen Übertragungsmedien, -systemen und -netzen und Rechnern einsetzbar. Die relativ einfache Implementierbarkeit von IP (existiert auf zahlreichen Betriebs-systemplattformen, z.B.: Apple MacOS, VMS, UNIX, IBM SNA, MS Windows,...) führte zu einer weiten Verbreitung. IP, mit dem darauf aufsetzenden Protokollstack, ist das weitverbreiteste Protokoll im Internet, dem derzeit größten Computernetzwerk der Welt.
Aufgrund der breiten Anwendung war/ist eine Anpassung des IP-Stacks an ATM unumgänglich.

2.3.1. TCP/IP im OSI-Referenzmodell

Die Internet Protocol Suite, eine der wichtigsten Kommunikationsarchitekturen, entstand aus der TCP/IP-Entwicklung der Advanced Research Project Agency (ARPA) der amerikanischen Regierung, aus der sich die IETF (Internet Engineering Task Force) herausbildete.
Die Internet Protokolle sind nicht direkt in den OSI-Stack einordbar, da der TCP/IP-Stack wesentlich älter ist und auf einem 4-Schichten-Ansatz basiert.
Eine gängige Einordnung ist in folgender Abbildung dargestellt.

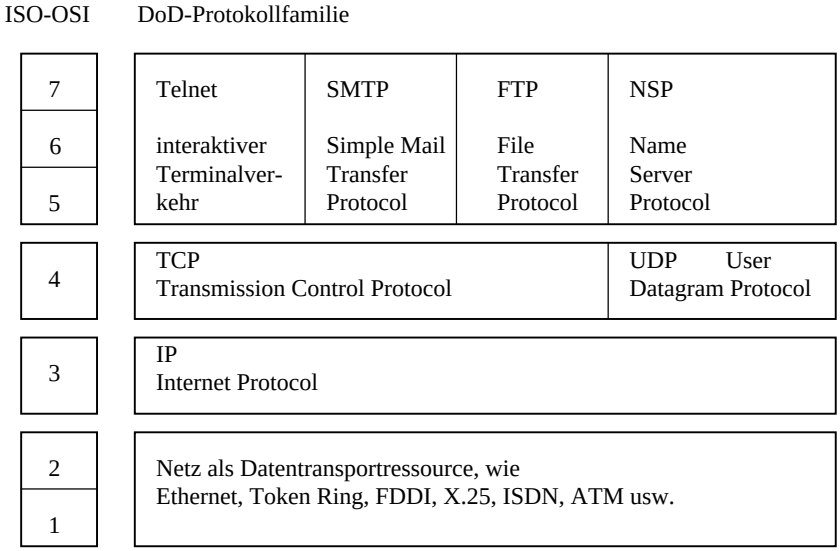


Abb. 2.7.: Internet Protocol Suite [Kau 96]

Demnach werden IP auf Layer 3 und TCP (UDP) auf Layer 4 angesiedelt. Exakt betrachtet übernimmt IP auch Fragmentierungsaufgaben der Schicht 2.

[Bad 95], [Kau 96], [c´t 10/96]

2.3.2. IP (Internet Protocol)

Das IP, als Basisprotokoll des Internet, definiert die Internet-Datagramme als eine Einheit von Informationen, die das Internet durchlaufen, und stellt die Basis für einen verbindungslosen best-effort Übertragungsdienst dar.
Die Hauptaufgabe von IP besteht in der Weiterleitung von Paketen zwischen Netzwerken und der Fragmentierung von Paketen (bei Bedarf) zur Anpassung an tieferliegende Protokollschichten.
IP bietet der Transportschicht nur einen ungesicherten verbindungslosen Datagrammdienst, ohne Flußkontrolle und Fehlerbehandlung (keine Garantie für Übermittlung des Paketes, keine Ende-zu-Ende-Fehlersicherung implementiert). Diese Funktionen werden für Anwendungen (FTP, Telnet) in verbindungsorientierten Transportprotokollen, wie TCP, implementiert. Andere Anwendungen, die diese Mechanismen nicht benötigen (SNMP), nutzen als Transportprotokoll UDP.
IP unterstützt (durch Definition von speziellen Adressen und Adreßräumen) virtuelle Verbindungen zwischen 2 (Punkt-zu-Punkt-Kommunikation) oder mehreren (Punkt-zu-Mehrpunkt-Kommunikation) Rechnersystemen.

2.3.2.1. IP-Datenpakete und Fragmentierung

Das IP-Datenpaket besteht aus einem Header- und einem Nutzdatenfeld, welches maximal 65535 Byte Payload-Daten aufnehmen kann. Für die Nutzdaten ist keine Fehlererkennung/-korrektur vorgesehen (lediglich Kopfprüfsumme).
Bestimmte Netzwerkkarten unterstützen lediglich festgelegte Paketgrößen (MTU - Message Transfer Units). IP muß in der Lage sein, seine Datagramme dem jeweiligen Netztyp anzupassen, um Daten über verschiedene Netzwerke verschicken zu können. IP übernimmt die Fragmentierung und Wiederherstellung von TCP-Segmenten, die erforderlich für den Transport der Daten durch mehrere Netze und deren Gateways sind.

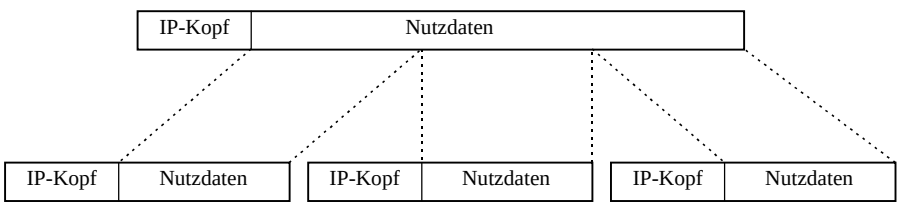
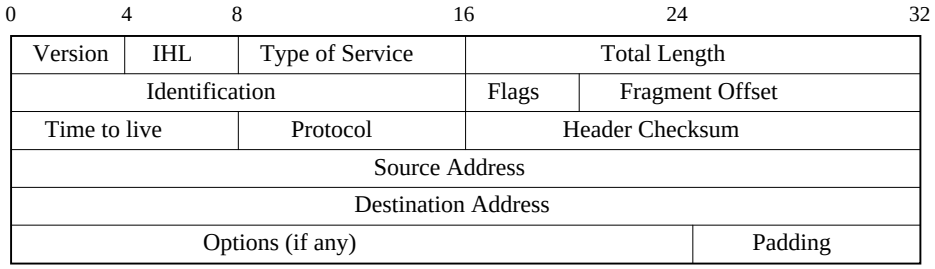


Abb. 2.8.: IP-Fragmentierung [Zeh 94]

Alle Teile einer fragmentierten Nachricht enthalten einen vollständigen IP-Protokollkopf, in dessen Identifikationsfeld der Wert der Ausgangsnachricht enthalten ist. Die Lage des Fragments innerhalb der Gesamtnachricht wird mittels des Fragmentabstandsfeldes ermittelt.
Der komplette IP-Header mit den entsprechenden Kopffeldfunktionen ist im folgenden für die derzeit dominierende IPv4 (Version 4) dargestellt.



IHL - IP-Header Length

Abb. 2.9.: IPv4-Header [PCN 10/96]

IP-Header-Feld	Funktion
Version	Internet-Protokoll-Versionsnummer (z.B.: 4)
Länge	Länge des IP-Kopfes in 16-Bit-Worten (mind. 5)
Servicetypen	Klassifikation des Paketes bezüglich Priorität, Delay, Throughput und Reliability (Zuverlässigkeit)
Paketlänge	Länge des IP-Paketes inklusive Protokoll-Kopf in Oktett (max. 2^{16})
Identifikation	zur Festlegung von zusammengehörenden, fragmentierten Paketen (i.d.R. einfacher Zähler)
Flags (DF, DM)	k.A.
Fragmentabstand	bei fragmentierten Paketen - Abstand zum Gesamtanfang dient der Reassemblierung von Paketen
Lebenszeit	max. Netzknotenanzahl, die das Paket durchlaufen muß, bevor es verworfen wird
Transport-Protokoll	Verweis auf verwendetes Transportprotokoll (z.B.: TCP) (entscheidend für Demultiplexvorgang)
Kopfprüfsumme	Header-Fehlererkennung/-korrektur
Sender-/Empfänger-adresse	32-Bit Internet-Adressen
Option	Angabe besonderer Protokolleigenschaften
Füllzeichen	Auffüllen der Protokoll-Kopflänge auf Vielfache von 16 Bit

Tab. 2.5.: Funktionen der IP-Headerfelder [Zeh 94]

2.3.2.2. IP-Adressen und Adreßauflösung

Zur Adressierung eines Anwendungsprogramms wird eine MAC-Adresse (z.B.: Ethernet), eine Internet-Adresse, eine Transportschicht-Identifikation (z.B.: TCP/UDP; im IP-Header enthalten) und eine Transportendpunkt-Identifikation (Portnummer) zum Finden der Anwendung benötigt.
Ein TCP/IP-Netz ist abhängig von einer sauberen Adressierung für einzelne Geräte, Subnetze, Broadcasts usw.. Dies erweist sich in der Praxis oft als problematisch. Jeder Rechner muß über eine Internet-Adresse verfügen, welche eine Abstraktion der physikalischen Adresse darstellt und die Grundlage für Kommunikation und Routing bildet.
IP-Adressen haben eine feste Adreßlänge (z.B.: 32 Bit für IPv4) und sind strukturiert aufgebaut.

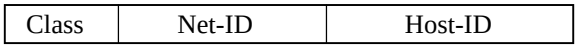


Abb. 2.10.: IP-Adresse (Grundstruktur)

Mittels der IP-Adreßklasse kann zwischen unterschiedlichen Aufteilungen von Net-ID und Host-ID unterschieden werden, entsprechend der Verteilung von Rechner- und Netzwerkanzahl. Im wesentlichen sind 3 Formate zu unterscheiden.

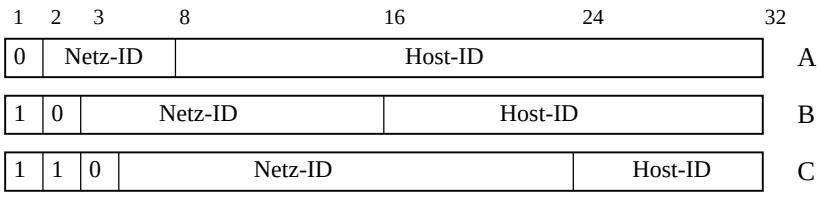


Abb. 2.11.: IP-Adreßklassen [Zeh 94]

Klasse	Bemerkung
A	wenige Netzwerke, viele Rechner
B	mittlere Verteilung von Netzen und Rechnern
C	viele Netzwerke, wenige Rechner
D	Multicastadressen
E	undefiniert

Tab. 2.6.: IP-Adreßklassen [Kau 96]

Adreßauflösung:

Die unter IP liegende Protokollschicht verwendet eine durch den Netzwerkstandard (FDDI, Ethernet) definierte Adressierung. Zur notwendigen Adreßumsetzung wird ein ARP (Address Resolution Protocol) angewendet.

Für die Adreßumsetzung bieten sich verschiedene Möglichkeiten an.

1) statische Umsetzung/Umrechnung mittels fester Tabellen
2) dynamische Umsetzung
   (Jeder Rechner enthält eine Liste, welche regelmäßig aktualisiert wird, mit allen ihm bekannten Netzwerkadressen. Zur Adressierung eines unbekannten Rechners wird ein Broadcast gestartet. Jedoch erscheint die Verwendung von Broadcasts nur innerhalb eines LAN´s als sinnvoll. Bei subnetzübergreifender Suche wird das Paket an den Router geschickt.)

- ARP-Algorithmus: 1) IP übergibt Datagramm, adressiert an Rechner B, an die Netzwerk-Schnittstelle von Rechner A, welcher daraufhin in seiner internen Tabelle nach der Hardwareadresse von Rechner B sucht. Nach erfolgreicher Suche kann der Datentransfer erfolgen.

  Sonst: 2) Erzeugung und Aussendung eines ARP-Broadcast-Pakets (mit Adresse von Rechner B) > ARP-REQUEST

  3) Alle Rechner im Netz vergleichen die im Request enthaltene Softwareadresse mit ihrer eigenen. Der gesuchte Rechner B sendet seine MAC-Adresse an Rechner A (entsprechend der übertragenen Adresse von A) > ARP RESPONSE

4) Rechner A registriert Adresse von B in seiner Tabelle und kann Datentransfer vollziehen.

[Bad 95], [Kau 96], [Zeh 94], [c´t 10/96], [PCP 9/95]

2.3.3. TCP (Transmission Control Protocol) und UDP (User Datagram Protocol)

TCP: stellt das bekannteste übergeordnete Protokoll dar, welches sowohl für WAN´s als auch LAN´s geeignet ist. Sein Vorteil liegt darin, daß es unabhängig vom Netztyp ist und auf diese Weise auch Ende-zu-Ende-Verbindungen über im Rahmen des Internetworking zusammengeschaltete Netze unterstützt.
Es erstellt voll-duplexfähige virtuelle Verbindungen und spiegelt dem Benutzer eine kontinuierliche Datenübertragung vor.
Als zuverlässiges Inter-Prozeß-Kommunikationsprotokoll zwischen Computern, die an paketvermittelte Netze angeschlossen sind, sichert TCP die Datenübertragung durch Sequenznummern, Prüfsummen, Quittungen mit Zeitüberwachung und automatischer Segmentwiederholung im Fehlerfall.
TCP benötigt einen einfachen zuverlässigen Datagramm-Service von der unterliegenden Schicht (normalerweise IP, jedoch Spezifikation offen, so daß prinzipiell auch anderes Protokoll verwendet werden kann, wenn dessen Schnittstelle an TCP angepaßt wird). Auf Vermittlungsschicht wird lediglich ein Internet-Protocol erwartet, das den Nachrichtenaustausch auf der Basis von Informationssegmenten variabler Länge, eingeschlossen in Internet-Datagram „envelopes“, ermöglicht.
TCP als verbindungsorientiertes Protokoll arbeitet in 3 Phasen (Verbindungsaufbau, -durchführung, -abbau).

Funktionsweise:

- TCP kommuniziert mit höheren Schichten als auch mit der IP-Schicht
- Prozesse rufen TCP auf und übergeben Daten als Argumente
- TCP segmentiert Daten und ruft IP zur Übertragung zum Ziel-TCP auf

- IP-Modul packt TCP-Segmente in Internet-Datagramme und sendet diese zum Ziel-TCP
- (im LAN: IP-Datagramme wiederum in Protokolle des LAN verpackt)
- empfangsseitig entfernt IP-Modul die Datagram-Hülle des Segments und übergibt diese an Ziel TCP
- Ziel-TCP stellt wiedergewonnene Daten in den Puffer des Ziel-Prozesses und informiert diesen

TCP überträgt Daten in einem kontinuierlichen bidirektionalen Datenstrom, wobei die Daten in Segmente verpackt werden. Die Segmentgröße wird zwischen den TCP-Endpunkten festgelegt.
Ein Multiplexmechanismus unterstützt mehrere Adressen oder Ports im Host, so daß eine gleichzeitige Kommunikation mehrerer Anwendungen möglich ist.

Abschließende Bemerkungen:
Der Gesamtaufwand für TCP/IP ist wesentlich geringer als für OSI-Netzwerk- und Transportprotokolle, u. a. dadurch, daß viele Funktionen durch IP-Adressierung bereits gut vorbereitet werden.
Die hervorragenden Sicherungsmechanismen und der aufwendige Routing-Mechanismus können auch Nachteile mit sich bringen (z.B.: in LAN`s sinkt der Durchsatz der reinen Benutzerdaten im Vergleich zu LAN-optimierten Protokollen (Novell IPX/SPX)).

Als Alternative wurde **UDP** entworfen.

UDP zeichnet sich durch ähnliche Funktionen wie TCP aus. Es verzichtet jedoch auf wesentliche Fehlerkontroll- und Sicherungsmechanismen (z.B.: Transportquittungen) und baut keine Verbindung zwischen Sender und Empfänger auf, sondern verschickt Datagramme als voneinander unabhängige Einheiten (wie das darunterliegende IP). UDP wird daher auch oftmals als „TCP light“ bezeichnet. Aufgrund des geringeren Overheadanteils arbeitet UDP schneller und effektiver und eignet sich beispielsweise zum Einsatz bei Hochgeschwindigkeitsübertragungen.

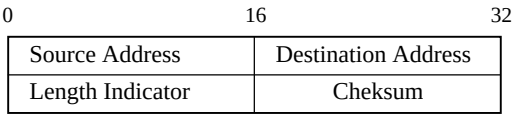


Abb. 2.12.: UDP-Header

[PCP 9/95], [Kau 96]

2.3.4. Ausblick auf IPv6

Das massive Wachstum des Internets (drastische Erhöhung der insgesamt weltweit verfügbaren Adressen, zukünftig werden Milliarden von IP-Adressen benötigt) und drohende Probleme im Zusammenhang mit der Explosion der IPv4-Routingtabellen trieben die Entwicklung eines neuen Standards voran (IPv6). RFC 1752 spezifiziert unter dem Titel „Recommendation for the IP Next Generation“ den Generationswechsel zu IPv6 als einheitliche Plattform.

Der an seine Grenzen gelangende Adreßraum von IPv4 (32 Bit Adressen) und der Wunsch nach verbesserten Sicherheitsfunktionen, sowie Multimedia- und Echtzeitanwendungen, die bisher mit IPv4 nicht praxistauglich waren, treiben den Wechsel zu IPv6 voran. IPv6 wird breite Unterstützung bei den Anwendern und Verantwortlichen finden. Mit einem ersten großen Schub wird in der 2. Hälfte 1997 gerechnet. Eine breite Marktdurchsetzung wird erst ab 1998 vorausgesagt.

Microsoft wird IPv6 noch 1997 (spätestens 1998) in seine Betriebssysteme und Browser implementieren. Cisco und andere Routerhersteller werden IPv6 als Software-Upgrade in ihre Router implementieren.

Wesentliche Vorteile von IPv6:

- mehr IP-Adressen
- leichteres Routing, vereinfachte Headerstruktur
- verbesserte Subnetzstruktur
- automatische Konfiguration
- verbesserte Sicherheitsfunktionen
- Unterstützung von Multimedia- und Echtzeit-Applikationen

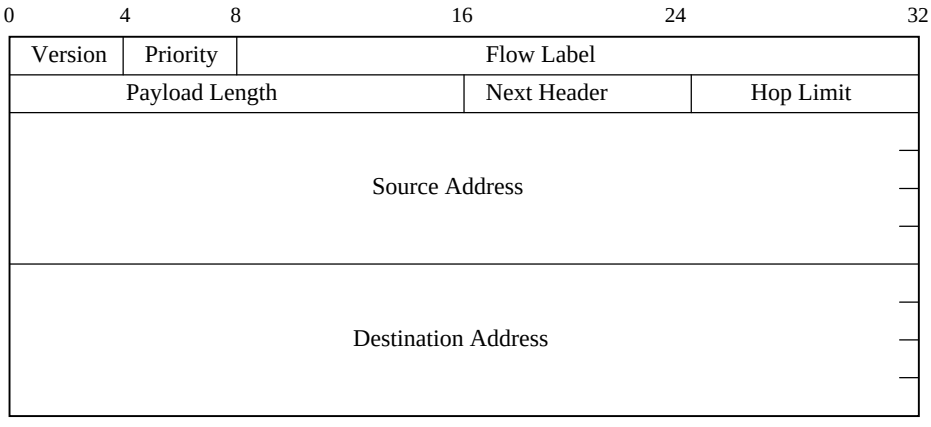


Abb. 2.13.: IPv6-Header [PCN 10/96]

Die Header-Format-Vereinfachung ermöglicht die Geringhaltung der für die IP-Datenübermittlung notwendigen Bandbreite. Die minimale Feldanzahl resultiert in einer Verbesserung der Routinggeschwindigkeit und Effizienz, sowie einer Verringerung des Paket-Overheads. Die Adressierung kann bei Bedarf mit optionalen Feldern ergänzt werden, die neueste TCP/IP-Technologien wie RSVP, Gruppenadressierung (Multicast), RTP, ... unterstützen.

Erhebliche Verbesserungen in Fragen der Netzsicherheit werden durch einen zusätzlichen Optional/Extension Header erreicht.

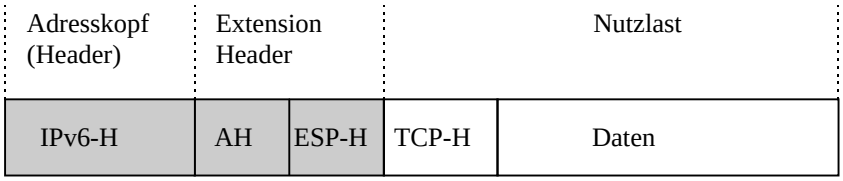


Abb. 2.14.: IPv6-Header und Extension-Header [FS 2/97]

- Authentication Header (AH):
  - ermöglicht dem Empfänger die Echtheit des Absenders und die Unverfälschtheit der Datenpakete zu prüfen
  - basierend auf Prüfsummenbildung und Vergleich

- Encrypted Security Header (ESP-H):
  - teilt der empfangenden Station mit, daß die nachfolgende Nutzlast verschlüsselt ist
  - IPv6 gibt hierzu nur den Rahmen an, aufgrund mangelnder Spezifizierung bleibt Verschlüsselung vorerst nur eine Option

Vergleich von IPv4 und IPv6:

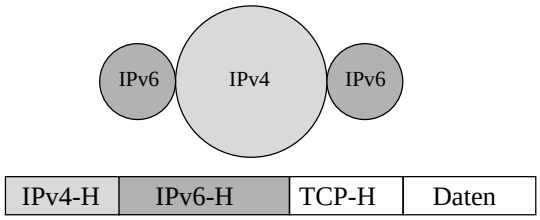
IP-Version	IPv4	IPv6
Header		
■ Struktur	■ 10 Felder ■ 2 Adressen ■ zusätzliches Optionsfeld, welches immer zur nächsten 32 Bit Grenze aufgefüllt wird	■ 6 Felder ■ 2 Adressen ■ keine Optionen
■ Headerlänge	■ 160 Bit oder 20 Byte (ohne Option)	■ 320 Bit oder 40 Byte ■ trotz 4 mal längerer Adressen > nur doppelt so groß wie IPv4-Header
Adressen		
■ Adreßlänge ■ Adreßraum	■ 2 jeweils 32-Bit-Adressen ■ 2^{32} mögliche Adressen	■ 2 jeweils 128-Bit-Adressen ■ $2^{128} = 3{,}4 \times 10^{38}$ mögliche Adressen ■ anschaulich: je Quadratmeter Erdoberfläche sind $6{,}6 \times 10^{23}$ Adressen verfügbar
minimale Paketlänge	384 Bit (48 Byte)	4608 Bit (576 Byte)
Multimedia und Echtzeit-Anwendungen	■ theoretisch unterstützt	■ deutliche Performance-Steigerung ■ Informationen für Bandbreiten-reservierung und Steuerung der Multimediadaten sind im Haupt-Header untergebracht und somit für Router leicht zugänglich (2 Felder) • Flow Label (24 Bit): ■ identifiziert Sequenz von Datenpaketen zwischen 2 spezifischen Adressen und unter Einbeziehung von RSVP kann diesen die benötigte Bandbreite zugeteilt werden ■ Filterfunktion, Prioritätszuordnung für einzelne Datenpakete • Drop Priorities (4 Bit): ■ identifizieren Paket-Prioritäten innerhalb eines Datenflusses ■ ermöglichen Bearbeitung nach Wichtigkeit (Abstufungen 0-15) ■ 0-7 für lastgesteuerten Verkehr

		■ 8-15 für Echtzeit- oder nicht lastgesteuerten Verkehr)
Sicherheitsaspekte	theoretisch vorhanden, jedoch praktisch nicht angewendet (zu aufwendig)	■ integriert Sicherheitsbedürfnisse auf der Kernel-Ebene, d.h. Authentifikation und Verschlüsselung finden durch das bei allen Übertragungen verwandte Kommunikations-protokoll statt ■ IP-Security auf Feldern des Optional-Header/Extension Header [Authentification-Header (stellt die Identität des Kommunikations-partners sicher) und Encryption-Security-Payload (Verschlüsselung)]
automatische Adreß-Zuweisung		■ Plug-and-Play-Funktionen, die Konfigurationen von IP-Adressen im Netzwerk automatisch ausführen (selbständige Adreß-vergabe) ■ löst Installationsprobleme

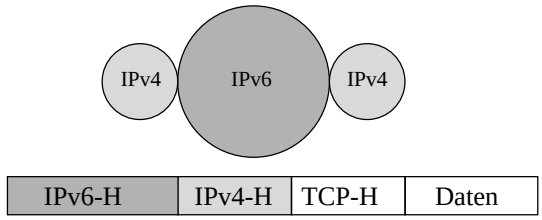
Tab. 2.7.: Vergleich IPv4 und IPv6

Wechselszenario von IPv4 auf IPv6:

Ein Stichtag für den Wechsel von IPv4 zu IPv6 ist nicht vorgesehen, wäre auch aus ökonomischen Gründen kaum vertretbar. Vielmehr wird eine sanfte Migration angestrebt, wie sie in RFC 1933 beschrieben wird. Danach werden (in der Übergangsphase) beide Protokollsätze auf den Rechnern installiert und koexistieren mit separaten IP-Adressen (Dual-Stack-Strategie). [Investitionsschutz für Anwender]
Zwei Netzinseln oder Domains (IPv6 basiert) können so über bestehende IPv4-Netze übertragen werden, indem den IPv6-Datenpaketen ein IPv4-Header vorangestellt wird. Die Nutzlast stellen in diesem Fall die eigentlichen Nutzinformationen und der IPv6-Header dar. An der Schnittstelle zum Zielnetz wird der IPv4-Header wieder entfernt.
Derselbe Mechanismus kommt zum Tragen, wenn IPv4-Pakete durch IPv6-Netze geroutet werden.



In der Einführungsphase erhalten IPv6 Pakete einen IPv4 Header vorangestellt, anhand derer sie durch die IPv4-Welt geroutet werden.



In einigen Jahren dürfte sich das Bild umkehren: Datenpakete aus den verbliebenen „IPv4-Wiederstandsinseln“ müssen durch die IPv6-Welt geroutet werden.

Abb. 2.15.: IP-Migration durch Tunneln [FS 2/97]

[Data 10/96], [PCN 10/96], [FS 2/97]